I'm not robot	reCAPTCHA
	reCAPTCHA

Continue

```
The obvious drawback to the buddy system is that rounding up to the next highest power of 2 is very likely to cause fragmentation within allocated segments. implementation are separate, allowing the machine's administrator to decide which type of swapping to use. Economy. 15.5 An experimental addition to UNIX allows a user to connect a
watchdog program to a file. However, if none of these flags are set when clone() is invoked, no 146 Chapter 4 Threads sharing takes place, resulting in functionality similar to that provided By the forkO system call. Every time a fault occurs, we show which pages are in our three frames. However, the problem is not entirely solved. Thus, the Pentium
allows four levels of protection. Consider the following sequence of events: A low-priority process faults. (0, 0) neither recently used nor modified—best page to replace 2. Some operating systems pass resources to child processes. The send(A, message)—Send a message to mailbox A. Mauro
and McDougall [2001] discussed virtual memory in Solaris. Several capability-based protection; it is described in Appendix B. • Type. This separation, allows an extremely large virtual memory to be
provided for programmers when only a smaller physical memory is available (Figure 9.1). executes with role 1 privileges Figure 14.8 Rote-based access control in Solaris 10. Asymmetrical algorithms based on elliptical curves are gaining ground, however, because the key length of such an algorithm can be shorter for the same amount of
cryptographic strength. It consists of a class loader and a Java interpreter that executes the architecture-neutral bytecodes, as diagrammed in Figure 2.17. The distance (in pages) between the hands of the clock is determined by a system parameter, lumdspread. When this program begins, a single thread of control begins in 4.3 Thread Libraries
#include #include 133 •> int sum; /* the thread */ int main(int argc, char *argv[]) { pthread t tid; /* the thread identifier */ pthread attributes */ if (argc != 2) { fprintf(stderr, "usage: a.out "); return -1; } if (atoi(argv[1]) < 0) { fprintf(stderr, "wd must be >=
0",atoi(argv[1])); return -1; /* get the default attributes */ pthread.attr.init (&attr); /* create the thread */ pthread.attr.init (&attr); /* create the thread */ pthread.attr.init (&attr); /* wait for the thread will begin control in this function */ void *runner(void *param) { int i, upper = atoi(param); sum = 0; for
(i = 1; i = 0."); else { // create the object to be shared Sum sumObject = new Sum(); int upper = Integer.parseint(args [0]); Thread thrd = new Thread(new Summation(upper, sumObject.getSum()) } catch (InterruptedException ie) { } else
System.err.println("Usage: Summation") Figure 4.8 Java program for the summation of a non-negative integer. FIFO page replacement is easy to program but suffers from Belady's anomaly. A web browser might have one thread display images or text while another thread retrieves data from the network, for example. In other situations, we may use
just one of the APIs to demonstrate a concept. Buff eredReader extends the Java, io .Reader class, which is used for reading character streams. However, interrupts must be handled quickly. Although Windows XP and Win
Data files may be numeric, alphabetic, alp
not share memory. Processes are created in the Win32 API using the CreateProcessO function, which is similar to f ork () in that a parent creates a new child process. The operating system then starts executing the first process, such as "init," and waits for some event to occur. These facilities constitute a significant development in protection
technology.; i;:-••-. In one solution, the microcode computes and attempts to access both ends of both blocks. The transaction acquires locks as needed. The cover illustrator was Susan Cyr, and the cover designer was Madelyn Lesure. If the association between processes and domains is fixed, and we want to adhere to the need-to-know principle.
then a mechanism must be available to change the content of a domain. Because threads share resources of the process to which they belong, it is more economical to create and context-switch threads. 4.2 Multithreading Models Our discussion so far has treated threads in a generic sense. 3.3 Consider the RPC mechanism. Thus, for a set of n
transactions, there exist n\ different valid serial schedules. If access(/,/) includes the control right, then a process executing in domain D. When a client connection is requested, the file is specified via an index into this table,
so no searching is required. The server will break out of the loop only when it has determined that the client has closed the connection. If a process is at its working-set maximum and it incurs a page fault, it must select a page for replacement using a local page-replacement policy. Generally, these programs are the first to be attacked by people
trying to break into a system; unfortunately, the attackers are frequently successful. Even other operating systems may be loaded on top of this virtual machine. Division C, the next level of security, provides discretionary protection and accountability of users and their actions through the use of audit capabilities. Using a sparse address space is
beneficial because the holes can be filled as the stack or heap segments grow or if we wish to dynamically link libraries (or possibly other shared objects) during program execution. Capability-based protection relies on the fact that the capabilities are never allowed to migrate into any address space directly accessible by a user process (where they
could be modified). ....|... Recall that the fork() system call creates a child process as a duplicate of its parent. A problem arises, however, when a page is used heavily during the initial phase of a process but then is never used again. The first Catalan numbers for n = 1. [1997]). We say that O, and Oj conflict if they access the same data item and at
least one of them is a w r i t e operation. If only two rings exist, this scheme is equivalent to the monitor—user mode corresponds to D\. In addition, we have no universally accepted definition of what is part of the operating system. These systems vary in their complexity and in the
types of policies that can be implemented on them. Careful selection of data structures and programming structures can increase locality and hence lower the page-fault rate and the number of pages in the working set. In this case, the set of objects that can be accessed depends on the identity of the user. Computer manufacturers often round off
these numbers and say that a megabyte is 1 million bytes and a gigabyte is 1 million bytes.) A more common definition is that the operating system is the one programs and application programs. E-mail delivered via the industry standard SMTP
protocol is stored and forwarded, frequently multiple times, before it is delivered. Thus, if a user has "." in her search path, has set her current directory to a friend's directory instead. At one extreme, a system administrator can use it to
modify a copy of the source code of the operating system. 564 Chapter 15 Security The emulator stored away the password, printed out a login error message, and exited; the user was then provided with a genuine login prompt. Since every file must be opened to be used, and opening a file requires searching the directory structure, the directories
will be accessed frequently. The Spafford article appears with three others in a special section on the Morris Internet worm in Communications of the ACM (Volume 32, Number 6, June 1989). Even with a very good true-alarm rate of P(A\1) = 0.0001 yields P(I\A) % 0.14. When the Linux kernel
creates a new task, it requests the necessary memory for the structtask, it requests the necessary memory for the struct task. We should note that in our discussion of security, we vise the terms intruder and cracker for those attempting to breach security. If the directory entry were on the middle cylinder, the head would have to move, at most, one-half the width. Pthreads Mutex Locks The
following code sample illustrates how mutex locks available in the Pthread API can be used to protect a critical section: Exercises #include pthread_mutex_init (&mutex, NULL); /* acquire the mutex lock */ pthreadjmtex_lock(&mutex); / * * * c r i t i c a l section * * * / /* release the mutex lock
*/ pthreadjmutex_unlock(&mutex); Pthreads uses the pthreadjnutex^t data type for mutex locks. If all resources must be requested at the beginning of the process, then the process must initially request the DVD drive, disk file, and printer. It is easier to protect against accidental loss of data consistency than to protect against malicious access to the
data. Overflow of the clock must be considered. One solution is to have the server run as a single process that accepts requests. Classes running in the same JVM may be from different sources and may not be equally trusted. Threads also play a vital role in remote procedure call (RPC) systems. Exercises 4.1 Provide two programming examples in
which multithreading does not provide better performance than a single-threaded solution. 14.4 What hardware features are needed in a computer system for efficient capability manipulation? If a client needs to send a larger message, it passes the message through a section object, which sets up a region of shared memory. The number of bits in
each part of the linear address varies according to architecture. 1.1.2 System View From the computer's point of view, the operating system is the program most intimately involved with the hardware. Once in place, the main worm undertook systematic attempts to discover user passwords. Windows XP uses two types of message-passing techniques
over a port that the client specifies when it establishes the channel. A modem at the destination site converts the analog signal back to digital form, and the back hand's investigating its value depends on the scanrate and the handspread. In addition,
remember that, when a page fault occurs before an executing instruction is complete, the instruction must be restarted. Both the machines must be secured. When both sendQ and r e c e i v e () are blocking, we have a rendezvous between the sender and the receiver. Photo
Courtesy: Maskot/Getty Images You can even search for books that are from each continent. Other processes that wish to communicate using this shared-memory segment must attach it to their address space. If a customer enters the barbershop and all chairs are occupied, then the customer leaves the shop. Distributing capabilities safely and
efficiently among customer processes: In particular, mechanisms ensure that a user process will use the managed resource, 2. swap map 1 0 3 0 F 1 Figure 12.10 The data structures for swapping on Linux systems. Further, when page replacement is required, we must select the frames that are to be
replaced. The remainder of the log can thus be ignored. The most serious consequence of an insecure protected procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which that procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the subsystem for which the procedure is a protection breakdown of the 
exercises at the end of this chapter. When a connection request is received, accept () returns a socket that the server can use to communicate with the client. 252 Chapter? A disk that has a boot partition is recorded in a new entry in
a file table associated with, the process. Second-chance replacement degenerates to FIFO replacement if all bits are set. the corresponding wait-for graph. From a user's perspective, a tile is the smallest allotment of logical secondary storage; that is, data cannot be written to secondary storage unless they are within a file. These processes are spooled
to a mass-storage device (typically a disk), where they are kept for later execution. New hardware features are allowing systems to be made more secure, as we shall discuss. And, since ROM is read only, it cannot be infected by a computer virus. We can think of this strategy as the optimal page-replacement algorithm looking backward in time, rather
than forward. Project—Matrix Multiplication Given two matrices A and B, where A is a matrix with M rows and K columns, the matrix B contains K rows and N columns. Beginning with Solaris 9, Java threads were mapped using the one-to-one model. The digital
signature of a message is derived by computing S(ks)(m) — H(m)k< mod N. 16.5 Communication Structure Now that we have discussed the physical aspects of networking, we turn to the internal workings. In general, however, we cannot prevent deadlocks by denying the mutual-exclusion condition, because some resources are intrinsically
nonsharable, 7.4.2 Hold and Wait To ensure that the hold-and-wait condition never occurs in the system, we must guarantee that, whenever a process requests a resource, it does not hold any other resources. This is by no means the only architectural problem resulting from adding paging to an existing architecture to allow demand paging, but it
illustrates some of the difficulties involved. Some may require a membership signup, but for most of them, you can go straight to the link and start reading. Wilbooks offers free digital books for kids ages pre-K through third grade and reading. Wilbooks offers free digital books for kids ages pre-K through third grade and reading. Wilbooks offers free digital books for kids ages pre-K through third grade and reading levels A through third grade and reading.
working-set maximum. We can include dynamic protection in the access-matrix model by considering domains and the access matrix itself as objects. (It would be nice to know about improperly formed commands that are handed off to execvpO that appear to look valid and are not, and not include them in the history as well, but that is beyond the
capabilities of this simple shell program.) You should also modify setup () so it returns an int signifying if has successfully created a valid args list or not, and the main () should be updated accordingly. Otherwise, a capability is created a valid args list or not, and the main () should be updated accordingly.
problems. The page-table entry for a page that is brovight into memory is set as usual, but the page-table entry for a page that is not currently in memory is either simply marked, invalid or contains the address of the page on disk. Because the parent thread cannot begin outputting Exercises 149 the Fibonacci sequence until the child thread finishes,
this will fequire having the parent thread wait for the child thread to finish, using the techniques described in Section 4.3. 4.12 Exercise 3.9 in Chapter 3 specifies designing an echo server using the Java threading API. Using a semaphore, fix the race condition. It also has informative videos on topics like getting along with siblings or dealing with
bullies. Meanwhile, a user at B may access a file that resides at A. Privileges and programs can also be assigned to roles. 6.15 Discuss the tradeoff between fairness and throughput of operations in the readers-writers problem. Passing a value of FALSE indicates that the thread creating the mutex is not the initial owner; we shall soon see how mutex
locks are acquired. The receiver retrieves either a valid message or a null. Denial-of-service, or DOS, attacks are sometimes accidental. 536 Chapter 14 Protection Other methods are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in which user IDs are used for domains in operating systems in the operation of the ope
one process has to wait, another process can take over use of the CPU. Although effective for a wide class of attacks, Tripwire does have limitations. The equivalent code using Java threads is shown in Figure 4.13. In fact, even most nonprogram security events have as their goal causing a program threat. When the server receives a request, it creates
a separate process to service that request. In a message-authentication code (MAC), a cryptographic checksum is generated from the message using a secret key. Virtual memory allowrs us to run extremely large processes and to raise the degree of multiprogramming, increasing CPU utilization. One mailbox name is the mailbox to which the message
is being sent. Some of the transformations are black-box transformations, in that their algorithms are hidden. First, the user will be able to list these commands when he/she presses, which is the SIGINT signal. On some systems, the long-term scheduler may be absent or minimal. However, delivering signals is more complicated in multithreaded
programs, where a process may have several threads. Finally, we discuss ways to handle file protection, necessary when we have multiple users and we want to control who may access files and how files may be accessed. Include the header files lirmx/linkage. This option is a good one in certain circumstances, and we consider it further in Section
9.6. Here, we discuss the most common solution: page replacement. Some of these programs are effective against only particular known viruses. The TCB also contains a mechanism to monitor events that may indicate a violation of 602 Chapter 15 Security security policy. Monitors provide the synchronization mechanism for sharing abstract data
types. 3.6 Communication in Client-Server Systems In Section 3.4, we described how processes can communicate using shared memory and message passing. The pageout process is similar to the second-chance algorithm, described in Section 9.4.5.2, except that it uses two hands while scanning pages, rather than one as described in Section 364
Chapter 9 Virtual Memory 8192 fastscan 100 siowscan minfree desfree amount of free memory lotsfree Figure 9.30 Solaris page scanner. 3.6 Communication in Client-Server Systems 111 a connection with the server at IP address 127.0.0.1 on port 6013. These data can be useful for protection, security, and usage monitoring. Auxiliary rights can be
described in a capability for an instance of the type. It uses symmetric encryption and uses the IKE protocol for key exchange. The free-frame buffer provides protection against the relatively poor, but simple, FIFO replacement algorithm. Read in the page. When the application is terminated, the license count is incremented. This problem can be
solved in two different ways. The array of buffer_item objects will be manipulated as a circular queue. 9.8 Allocating Kernel Memory 355 An advantage of the buddy system is how quickly adjacent buddies dan be combined to form larger segments using a technique known as coalescing. We would expect p to be close to zero—that is, we would expect
to have only a few page faults. The strategy is to bring into memory at one time all the pages that will be needed. It provides an environment for execution of programs written in any of the languages targeted at the .NET Framework. Using clone () in this fashion is equivalent to creating a thread as described in this chapter, since the parent task
shares most of its resources with its child task. combining threads with RPC. All these strategies have the same goal: to keep many processes in memory simultaneously to allow multiprogramming. Therefore, canceling a thread asynchronously may not free a necessary system-wide resource. The parent waits until some or all of its children have
terminated. Therefore, the only alternative is somehow to eliminate the need to trust the network. The segment base contains the starting physical address where the segment. How, then, is an operating system to decide whether to grant a request when it cannot trust
the named source of the request? In an isolated computer, the operating system can reliably determine the sender and recipient of all interprocess communication, since it controls all communication, since it controls all communication, since it controls all communication (MVC) on the IBM 360/370 when
the source and destination regions are overlapping. This phenomenon, referred to as cascading termination, is normally initiated by the operating system. Lets look more closely at how this process works. The callback mechanism allows them to perform asynchronous message handling. If a transaction T, has obtained an exclusive-mode lock (denoted
by X) on data item Q, then 7} can both read and write Q. A simple base register or a base-limit register pair is sufficient for the single- and multiple-partition schemes, whereas paging and segmentation need mapping tables to define the address map. This extension allows all objects to be tagged with their types by the hardware. Most systems use a
combination of access lists and capabilities. Once the method is completed, the skeleton marshals JVM JVM Figure 3.22 Remote method invocation. 7.4.4 Circular Wait The fourth and final condition for deadlocks is the circular-wait condition. Then, sector slipping remaps all the sectors from 17 to 202, moving them all down one spot. In fact, a
network firewall can separate a network into multiple domains. Operating systems as different as Windows and UNIX dispatch interrupts in this manner. Thus, we have shown that schedule 2 is equivalent to a serial schedule. An integer b3 such that b3 > bl. Much research focuses on garbage collection algorithms for increasing the performance of
To define a file properly, we need to consider the operations that can be performed on files. Cancellation of a target thread may occur in two different scenarios: 1 f i | 1 •. Networklayer security generally has been standardized on IPSec, which defines IP packet formats that allow the insertion of authenticators and the encryption of packet contents.
Discussions concerning the working-set model were presented by Denning [1980]. Because of the longer interval between executions, the long-term scheduler can afford to take more time to decide which process should be selected for executions, the long-term scheduler can afford to take more time to decide which process should be selected for executions. In this instance, duplicating only the calling thread is appropriate. h. Capturing secret data from a
system or a data stream, such as credit-card information or identity information for identity in
memory as necessary while providing as much inexpensive, nonvolatile memory as possible. Project—Adding a System call interface provided by the Linux Kernel In this project, you will study the system call interface provided by the Linux Kernel In this project, you will study the system call interface. It can be a useful
augmentation to any pagereplacement algorithm, to reduce the penalty incurred if the wrong victim page is selected. The slab allocator provides two main benefits: 1. Switching the domain corresponds to changing the user identification, it is run by the Java interpreter. If the frame is locked, it cannot be
provides storage for both programs and data. The author clearly had the expertise to include such commands; in fact, data structures were present in the bootstrap code that could have been used to transfer Trojan-horse or virus programs. 1.2 Computer-System Organization Before we can explore the details of how computer systems operate, we
need a general knowledge of the structure of a computer system. The short-term scheduler must select a new process for the CPU frequently, 9.13 A page-replacement algorithm should minimize the number of page faults. Noncontainer objects inherit no other permissions. If set, the mode flag allows the shared-memory region to be attached in read-
only mode; if set to 0, the flag allows both reads and writes to the shared region. Processes execute in domain, to access and manipulate objects. The problem of guaranteeing that no information initially held in an object can migrate outside of its execution environment is called the confinement
problem. Alternatively, we can use the virtual memory techniques discussed so far to treat file I/O as routine memory accesses. A reference to segment 3) + 852 = 4052. Knuth [1966] presented the first algorithm with a bound; his bound was 2" turns. The goal is to maximize the work (or play) that
the user is performing. Division C has two levels: Cl and C2. The message itself is never actually copied. Then, when an access is attempted, the capability is found to point to an illegal table entry. Cooperating processes require an interprocess communication mechanism to communicate with each other. -I; ::: 1:!; i;: i: I: r i: !MI1I 1^|If|Ill|I| If|
fill!': ::: ::: tieacl*:::: N ii; write: i;:: :; imi ii. It may also get the name of the output device. 342 Chapter 9 Virtual Memory Of course, we must adjust each «,- to be an integer that is greater rha^i the minimum number of frames required by the instruction set, with a sum not exceeding m. Again, the directory is searched for the associated entry, and the
system needs to keep a read pointer to the location in the file where the next read is to take place. 9.4.3 Optimal Page Replacement One result of the discovery of Belady's anomaly was the search for an optimal page-replacement algorithm. ..' ' '.':.: ... buffer Figure 9.29 The reason why frames used for I/O must be in memory. These six basic
operations comprise the minimal set of required file operations. A protection system is ineffective if user authentication is compromised or a program is run by an unauthorized user. In 2001, NIST adopted a new encryption algorithm, called the advanced encryption standard (AES), to replace DES. Each message is addressed to an RPC daemon
listening to a port on the remote system, and each contains an identifier of the function to execute and the parameters to pass to that function. If blocks go bad during normal operation, a special program (such as chkdsk) must be run manually to search for the bad blocks and to lock them away as before. Thus, this echo server must use an object that
extends Java. The buddy system allocates memory to kernel processes in units sized according to a power of 2, which often results in fragmentation. 2.11 Summary Operating systems provide a number of services. The matter of what constitutes an operating system has become increasingly important. A communication link in this scheme has the
following properties: • A link is established automatically between every pair of processes that want to communicate. This is a common kind of tradeoff seen throughout operating system design. Thus, the outline of a worker thread appears as follows: public class WorkerThread implements Runnable { private private private private int row,in
col; int [] [] A; int [] [] B; int [] [] B; int [] [] B; int [] [] C; public WorkerThread(int row, int col, int [] [] B, int [] [] B, int [] [] B, int [] [] B, int [] [] B; int [] [] C; public workerThread(int row, int col, int [] [] B, int [] [] B, int [] [] B; int [] [] C; public workerThread(int row, int col, int [] [] B, int [] 
workers [NUM]THREADS], for (int i = 0; i < NUM THREADS; i++) pthread join {workers [i], NULL}; Figure 4.12 Phtread code for joining ten threads. To improve the efficiency of physical memory use, Intel Pentium page tables can be swapped to disk. More specifically, we must ensure that a process executing in domain D, can access only those
objects specified in row \, and then only as allowed by the access-matrix entries. A file has a certain defined structure, which depends on its type. It is possible, however, that each of these processes, for a particular data set, may suddenly try to use all ten of its pages, resulting in a need for sixty frames when only forty are available. Such a capability
gives a process a means of indirect access (through the operation P) to the representation of A, but only for specific purposes. 544 Chapter 14 Protection 14.5.4 A Lock-Key Mechanism The lock-key scheme is a compromise between access lists and capability lists. Two steps are necessary to create a file. To make remote methods transparent to both
the client and the server, RMI implements the remote object using stubs and skeletons. For instance, the current file pointer for each file is found here. frame valid-invalid bit swap out victim page /-TNj change i V f y t o invalid 0 f V — . remote service, 650-651 and consistency, 649-650 remote file systems, 398 remote file transfer, 614-615 remote
login, 614 remote method invocation (RMI), 114—115 remote operations, 443-444 remote procedure calls (RPCs), 825 remote-service mechanism, 446 remote procedure calls (RPCs), 825 remote-service mechanism, 443-443 application interface with, 481-482 disks, 478-480 and file naming, 482-483 and hierarchical storage mental, 483 magnetic disks, 451-453 magnetic tapes, 453-453 magnetic disks, 451-453 magnetic tapes, 453-453 magnetic disks, 451-453 magnetic disks, 451-453 magnetic tapes, 453-453 magnetic disks, 451-453 magnetic disks, 451-453 magnetic tapes, 453-453 magnetic disks, 451-453 magnetic disks, 4
454, 480? A simpler solution to the two-process mutual-exclusion problem has since been modified must be sent back to site B. ;;K.::: ;c>pjeGt:;!;;;;;::;:;:*. At a transfer rate of 2 MB per second, it takes only 0.2 milliseconds
to transfer 512 bytes. Among other fields, the TEB contains the thread identifier, a user-mode stack, and an array for threadspecific data (which Windows XP terms thread-local storage). The benefits of multithreading include increased responsiveness to the user, resource sharing within the process, economy, and the ability to take advantage of
from that call, which is executed by the DFS daemon on behalf of the client. They can wreak havoc in a system by modifying or destroying files and causing system to the Win32 API. For example, a retinal (or eye) scanner might be used
to verify that the user is who she says she is. Because of the short time between executions, the short-term scheduler must be fast. This is shown in Figure 9.30 (with fastscan set to the maximum). Of course, if there are more active processes than there are register sets, the system resorts to copying register data to and from memory, as before. io.
detection rate. Mach guarantees that multiple messages from the same sender are queued in first-in, first-out (FIFO) order but does not guarantee an absolute ordering. 3.4.1 Shared-Memory Systems Interprocess communication using shared memory systems in the shared memory systems in the shared memory systems in the shared memory systems in 
Data Threads belonging to a process share the data of the process. When f ork() is invoked, a new task is created, along with a copy of all the associated data structures of the parent process. When f ork() is invoked, a new task is created, along with a copy of all the associated data structures of the parent process. When f ork() is invoked, a new task is created, along with a copy of all the associated data structures of the parent process. When f ork() is invoked, a new task is created, along with a copy of all the associated data structures of the parent process.
computationally infeasible to derive D(/Q, N) from E{kc, A/), and so E (kc, IV) need not be kept secret and can be widely disseminated; thus, E (ke, N) (or just kt.) is the public key and D{kLi, N) (or just kt.) is the private key. 16.3.1 Local-Area Networks Local-area networks emerged in the early 1970s as a substitute for large mainframe computer
systems. One reason is that sockets allow only an unstructured stream of bytes to be exchanged between the communicating threads. Page sizes are invariably powers of 2, generally ranging from 4,096 (212) to 4,194,304 (222) bytes. If the keys match, the operation is allowed to continue; otherwise, an exception condition is raised. 1 ':'-: -I-.
Accesses are often performed indirectly, through system libraries or other classes. Those interested in socket programming in C or C++ should consult the bibliographical notes at the end of the chapter. This violation involves preventing legitimate use of the system. Both S and S(k) for any k should be efficiently computable functions. An encryption
algorithm must provide this essential property: Given a ciphertext c e C, a computer can compute m such that E(k)(m) = c only if it possesses D(k). A domain is a set of access rights. The consumer process must also create a view of the mapped file, just as the producer process did in the program in Figure 9.25. Tanenbaum [2001] discusses Intel
80386 paging. If either block (source or destination) straddles a page boundary, a page fault might occur after the move is partially done. To decide whether the resources currently allocated to each process, and the future requests
and releases of each process. The consumer process will communicate using this shared-memory segment by creating a mapping to the same named object. For example, a web server accepts client requests for web pages, images, sound, and so forth. Once the region of shared memory is attached to a process's address space, the process can access
the shared memory as a routine memory as a routine memory access using the pointer returned from shmat (). The trade-off is between the convenience of allocation and management in the file system and the performance of swapping in raw partitions. 4.3 Thread Libraries 131 - user thread Figure 4.4 Many-to-many model. They will not be provided. 9.9
The VAX/VMS system uses a FIFO replacement algorithm for resident pages and a free-frame pool of recently used pages. See also directories device queues, 86-87 device reservation, 514-515 DFS, see distributed file system digital certificates, 583-584 digital signatures,
419—420 recovery of, 435-437 single-level, 387 tree-structured, 389-391 two-level, 388-389 directory objects (Windows XP), 794 direct virtual memory access (DVMA), 504 dirty bits (modify bits), 329 disinfection, program, 596-597 disk(s), 451^153. 14.5.3 Capability Lists for Domains Rather than associating the columns of the access matrix with the
objects as access lists, we can associate each row with its domain. rendezvous, 102 repair, mean time to, 469 replay attacks, 560 replication, 475 resident monitor, 841 resolution: name, 623 and page size, 358 resolving links, 392 resource allocation
restart area, 817 restore: data, 436-437 state, 89 retrofitted protection mechanisms, 407 revocation of access rights, 546-547 rich text format (RTF), 598 rights amplification (Hydra), 548 ring algorithm, 685-686 ring structure, 668 risk assessment, 592-593 RMI, see remote method invocation roaming profiles, 827 robotic jukebox, 483 robustness.
631-633 roles, 545 role-based access control (RBAC), 545 rolled-back transactions, 223 roll out, roll in, 282 ROM, see read-only memory Index root partitions, 417 root uid (Linux), 778 rotational latency (disks), 457 round-robin (RR) scheduling algorithm, 164-166 routing: and network communication, 625-626 in partially connected networks,
structure, 180, 752 RW (read-write) format, 24 safe computing, 598 safe sequence, 256 safety algorithm, 260 safety-critical systems, 696 sandbox (Tripwire file system), 598 SANs, see storage-area networks SATA buses, 453 save, state, 89 scalability, 634 SCAN (elevator) scheduling algorithm, 459-460, 724 schedules, 226 scheduler(s), 87-89 long-scheduler(s), 87-89 long-s
term, 88 medium-term, 89 short-term, 89 short-term, 88 scheduler activation, 142-143 scheduling: cooperative, 156 CPU, see CPU scheduling 913 disk scheduling 913 disk
synchronization, 753-755 process, 751-753 symmetric multiprocessing, 755-756 nonpreemptive, 156 priority-based, 700-701 proportional share, 708 Pthread, 708-707 thread, 172-173 in Windows XP, 789-790, 831-833 scheduling rules, 832 SCOPE operating system, 853 script kiddies, 568 SCS (system)
contention scope), 172 SCSI (small computer-systems interface), 10 SCSI buses, 453 SCSI initiator, 455 SCSI targets, 455 search path, 389 secondary memory, 322 secondary memory, 322 secondary storage, 9, 411. This method is less flexible than that used in UNIX, however. Sometimes, a waiting process is never again able to change state, because the resources it has
requested are held by other waiting processes. pure paging 8.9 Consider a paging system with the page table stored in memory. We are interested only in the sequence of memory addresses generated by the running program. The second method allows the process to request initially only the DVD drive and disk file. A transaction may obtain locks but
may not release any lock. Install a faster hard disk or multiple controllers with rnilltiple hard disks. A transaction may release locks but may not obtain any new locks. 15.4.1.4 Key Distribution Certainly, a good part of the battle between cryptographers (those inventing ciphers) and cryptanalysts (those trying to break them) involves keys.
Segmentation on Linux systems is presented in Bovet and Cesati [2002] V " vCHAPTER In Chapter 8, we discussed various memory-management strategies used in computer systems. Assuming there is one cache per object type, explain why this doesn't scale well with multiple CPUs. What could be done to address this scalability issue? They may
include small microprocessors, workstations, minicomputers, and large general-purpose computer systems. During a context switch, the value of the CR3 register is saved and restored in the TSS segments of the tasks involved in the context switch, the value of the CR3 register is saved and restored in the TSS segments of the tasks involved in the context switch.
e i v e 0 statements. We thus use pager, rather than swapper, in connection with demand paging. This variation, sometimes referred to as the tivo-level model (Figure 4.5), is supported by operating systems such as IRIX, HP-UX, and Tru64 UNIX. Another defense is to avoid opening any e-mail attachments from unknown users. We can reduce this
overhead by using a modify bit (or dirty bit). 15.3 System and Network Threats 571 • Tunneling. A new process is created by the fork O system call. It began by trying simple cases of no password constructed of account-user-name combinations, then used comparisons with an internal dictionary of 432 favorite password choices, and
allows read permission by the owner of the shared-memory segment. This information is stored on the per-process table so the operating system can allow or deny subsequent I/O requests. Even if a virus does infect such a program, its powers usually are limited because other aspects of the system are protected. • Chapter 21, The Linux System, is
throughout the section. In this case, we must write that page to the disk. This strategy is used in the M.ULTICS system and in the CAL system. The first step in understanding these algorithms is to explore hash functions. At a slightly less tailored level, the system description can cause the creation of tables and the selection of modules from a
precompiled library. The LRU algorithm produces 12 faults. 556 Chapter 14 Protection The access matrix is a general model of protection that provides a mechanism for protection without imposing a particular protection that provides a mechanism for protection without imposing a particular protection that provides a mechanism for protection without imposing a particular protection that provides a mechanism for protection without imposing a particular protection without imposing a particular protection that provides a mechanism for protection without imposing a particular protection without imposing a parti
authorized host by meeting some authorization criterion. If it is not, we trap to the operating system (logical addressing attempt beyond, end of segment). Thus, the user-protection requirement can be circumvented. Each ring corresponds to a single domain (Figure 14.2). The other approach is to transfer to site A only those portions of the file that
can be designed to be either volatile or nonvolatile. Thus, in Figure 14.4, a process executing in domain D3 or to domain D3 or to domain D4 can switch to domain D4 can switc
only nonprivileged instructions. Since Windows XP operates with a client-server model, two classes of subjects are used to control access: simple subjects are used to control access: simple subjects are used to control access: simple subjects and server subjects. - . Page p will be in memory after the first reference, so the immediately following references with a client-server model, two classes of subjects are used to control access: simple subjects are used to control access.
again treat the rows in the matrices Allocation and Request as vectors; we refer to them as Allocation of the index into the file table. exe. In Figure 3.9, we see two children of in t — in each and Request as vectors; we refer to them as Allocation and Request as vectors; we refer to them as Allocation and Request. Bibliographical Notes 313 Address translation in software is covered in Jacob and Mudge [199F]. All operations on the file are made by specification of the index into the file are made by specification of the index into the file are made by specification of the index into the file are made by specification and Request.
t d and dtlogin. In addition, the content of the text corresponds to the suggestions from Computing Society and the Association for Computing Machinery (ACM). 15.2 A password may become known to other users in a variety of \vays. We leave it
as an exercise for you to provide a solution where BUFFER-SIZE items can be in the buffer at the same time. Connection-oriented (TCP) sockets are implemented with the Socket class. For instance, a user may be editing, printing, and compiling in parallel. 94 Chapter 3 Processes #include i int main(VOID) { STARTUPINFO signature.
PROCESS INFORMATION pi; // allocate memory ZeroMemory(&si, sizeof (si)); si.cb = sizeof (si); // command line "C:\\WINDOWS\\system32\\mspaint.exe", // command line "ULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle FALSE, // disable NULL, // don't inherit thread handle NULL, // don't inherit th
handle inheritance 0, // n o creation flags NULL, // use parent's environment block NULL, // use parent's existing directory &si, fprintf("Child Complete"); // close handles CloseHandle(pi.hProcess);
CloseHandle(pi.hThread); Figure 3.12 Creating a separate process using the Win32 API. Privileges can be assigned to processes, limiting them to exactly the access they need to perform their work. Amplification of rights can be stated explicitly in the declaration of an abstract type to the Hydra operating system. In the extreme case, we can start
executing a process with no pages in memory. Most computer users sit in front of a PC, consisting of a monitor, keyboard, mouse, and system unit. (The keyword . Chapters 15 through 17, updated with coverage of new material. Similarly, each domain has a list of unique bit patterns, called keys. Many operating
instance, web servers use HTTP to communicate with web browsers. Virtual memory is a technique that allows the execution of processes that are not completely in memory. One solution is to use a proportional allocation scheme wherein the ratio of frames depends not on the relative sizes of processes but rather on the priorities of processes or on
combination of size and priority. For example, Solaris creates a set 4.2 Multithreading Models 129 of threads in the kernel specifically for interrupt handling; Linux uses a kernel thread for managing the amount of free memory in the system. By time h, the working set has changed to {3, 4}. If a user at one site (say, "cs.uvm.edu") wants to access a
file located on another computer (say, "cs.yale.edu"), then the file must be copied explicitly from the computer at Yale to the computer (say, "cs.yale.edu"), then the file must be copied explicitly from the computer at Yale to the computer (say, "cs.yale.edu"), then the file must be copied explicitly from the computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer at Yale to the Computer (say, "cs.yale.edu"), then the file must be computer (say, "cs.yale.edu"), then the file must be computer (say, "cs.yale.edu"), then the file must be computer (say, "cs.yale.edu"), th
an illegal memory access) may be handled by terminating the program. For example, the move instruction for the PDP-11 includes more than one word for some addressing modes, and thus the instruction for the PDP-11 includes more than one word for some addressing modes, and thus the instruction for the PDP-11 includes more than one word for some addressing modes, and thus the instruction itself may straddle two pages. We discuss both types in the following sections. The incorporation of protection concepts into programming
languages, as a practical tool for system design, is in its infancy. An operating system is software that manages the computer hardware. Every process token. The kernel code can then perform the requested services such as interacting with I/O devices, perform process
management and other such activities that cannot be performed in user mode. The linear address in Linux. This example buffer-overflow attack reveals that considerable knowledge and programming skill are needed to
 recognize exploitable code and then to exploit it. What modifications to the virtual memory system provide this functionality? When the reference to page 4 occurs, however, LRU replacement sees that, of the three frames in memory, page 2 was used least recently. Since each mailbox has a unique owner, there can be no confusion about who should
receive a message sent to this mailbox. Paging systems may simply store pages that have been pushed out of main memory. The use of a TCB merely ensures that the system can enforce aspects of a security policy; the TCB does not specify what the policy should be. This change is accomplished through the file system as follows. As long as the page-
fault rate is reasonably low, performance is acceptable. On the one hand, the page replaced may be an initialization module that was used a long time ago and is no longer needed. Basically, such queues can be implemented in three ways: • Zero capacity. When the user no longer needed access to the *file, a copy of the file (if it has been modified) is
sent back to site B. A survey of memory-allocation strategies can be found in Wilson et al. The user's view is mapped onto physical memory. A4atrices A and B can be initialized statically, as shown below: #define M 3 #define K 2 #define N 3 int A [M] [K] = { {1,4}, {2,5}, {3,6} }; int B [K][N] = { {8,7,6} }; int C [M] [N]; Alternatively,
they can be populated by reading in values from a file. A reference to byte 1222 of segment 0 would result in a trap to the operating system, as this segment is only 1,000 bytes long. Another form of electronic disk is flash memory, which is popular in cameras and personal digital assistants (PDAs), in robots, and increasingly as removable storage on
general-purpose computers. A process can select a replacement from among its own frames or the frames of any lower-priority process. For example, if we trace a particular process, we might record the following address sequence: 0100, 0432, 0101,0612, 0103, 0104, 0101, 0611, 0102, 0103, 0104,0101,0610, 0102, 0103, 0104,0101,0610, 0102, 0103, 0104,0101,0610, 0104,0101,0610, 0104,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0101,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0610,0
immediately allocated to it (that is, the process must wait), then all resources currently being held are preempted. A segment for kernel code 2. When run initially, Tripwire takes as input the tw.config file and computes a signature for each file or directory consisting of its monitored attributes (inode attributes and hash values). A new section on
allocating memory within the kernel discusses the buddy algorithm and the slab allocator. One event that triggers an upcall occurs when an application thread is about to block. Whereas local procedure calls fail only under extreme circumstances, RPCs can fail, or be duplicated and executed more than once, as a result of common network errors.
Access-control information determines who can do reading, writing, executing, and so on. Let the number of processors in the system. The variable in points to the first full position in the buffer. Therefore, the secrecy of E(k) must be
protected to the same extent as that of D{k}. 14.9 What is the need-to-know principle? The consumer process will then read and output the sequence from shared memory. Such architectures provide the further benefit of having a smaller pool—thereby consuming less memory—when the load on the system is low. The disadvantage in both of these
schemes (symmetric and asymmetric) is the limited modularity of the resulting process definitions. This information is the basis for many page-replacement algorithms that approximate LRU replacement. In this situation, whenever the server receives a request, it creates a separate thread to service the request. It can use key lengths of 128, 192, and
256 bits and works on 128-bit blocks. Once the correct information has been received, the user must connect to the subdirectory where the file Server. Thus, several copies of the same file may exist, resulting in a waste of space. These programs require certain common operations, such as those controlling the I/O devices. This data structure, instead
of storing data for the task, contains pointers to other data structures where these data are stored—for example, data structures that represent the list of open files, signal-handling information, and virtual memory. It is up to application developers to write programs that follow the ordering. 9.4.7 Page-Buffering Algorithms Other procedures are often
used in addition to a specific page-replacement algorithm,. Once it detects thrashing, what can the system do to eliminate this problem? The number of threads in the pool can be set heuristically based on factors such as the number of threads in the pool can be set heuristically based on factors such as the number of threads in the pool can be set heuristically based on factors such as the number of threads in the system, the amount of physical memory, and the expected number of concurrent client requests. Often,
the short-term scheduler executes at least once every 100 milliseconds. These operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions and the bytecode operations are then cached so that subsequent invocations of a method are performed using the native machine instructions are then cached so that subsequent invocations are the native machine instructions are then cached so that subsequent invocations are then cached so that subsequent invocations are then cached so that subsequent invocations are the native machine instructions are the native machine in 
e c e i v e () operations: • Direct or indirect communication • Automatic or explicit buffering We look at issues related to each of these features next. Correct the page table and other tables to show that the desired page is now in memory. Because a process is usually either reading from or writing to a
file, the current operation location can be kept as a per-process currentfile-position pointer. Write the victim frame to the disk; change the page and frame to the disk; cha
UltraSPARC — was described by Jacob and Mudge [1998a]. The process that creates a new mailbox is that mailbox's owner by default. Consider that a successful advertising campaign that greatly increases traffic to a site could be considered a DDOS. To solve this problem, we can use proportional allocation, in which we allocate available memory to
each process according to its size. Caches can be installed to improve performance where a large access-time or transfer-rate disparity exists between two components. One major advantage of this scheme is that programs can be larger than physical memory. Figure 3.9 illustrates a typical process tree for the Solaris operating system, showing the
name of each process and its pid. In the simplest case, we associate with each page-table entry a time-of-use field and add to the CPU a logical clock or counter. Type safety ensures that classes cannot treat integers as pointers, write past the end of an array, or otherwise access memory in arbitrary ways. The responsibility for providing
communication may rest with the operating system itself. These resources include information stored in the system (both data and code), as well as the CPU, memory, disks, tapes and networking that are the computer. 14.9.1 Compiler-Based Enforcement At this point, programming languages enter the picture. If we run six processes, each of which
is ten pages in size but actually uses only five pages, we have higher CPU utilization and throughput, with ten frames to spare. receiver 562 Chapter 15 Security To protect a system, we must take security measures at four levels: "1. Any remote system could obtain the needed information (that is, the list of current users) by sending an RPC message
to port 3027 on the server; the data would be received in a reply message. We also need a mechanism to allow addition of new rights and removal of some rights. The stacks used, by each thread 5. A pair of processes communicating over a network employ a pair of sockets—one for each process. Within the debate is the issue of whether or not there
even exists a monoculture today (consisting of Microsoft products). Protection from viruses thus is an important security concern. Thus, D, Figure 14.1 System with three protection domains. In this scheme, the send (P, message)—Send a message to process P. 16.2 Types of Distributed Operating
Systems In this section, we describe the two general categories of network-oriented operating systems: network operating systems and distributed operating systems. A common represents a queue. A shell interface provides
the user a prompt after which the next command is entered. A connection between a pair of sockets, one at each end of the communication channel. Green threads—a thread library available for Solaris—uses this model, as does GNU Portable Threads. 6.19 A file is to be shared among different processes, each of which
has a unique number. ft H a fH cfl et!: fis shared by D? It is easier to protect against malicious misuse. While it has only limited functionality, it illustrates the system will stop functioning and will need to
be restarted manually. Once anonymous login is accomplished, care must be taken by the system to ensure that this partially authorized user does not access inappropriate files. To illustrate the concept of conflicting operations, we consider the nonserial Tn: T, read(A) write(B) read(B) write(B) read(B) write(B) Figure 6.22 Schedule
1: A serial schedule in which To is followed by 7"i. However, a page-sized portion of the file is read from the file system into a physical page (some systems may opt 9.7 Memory-Mapped Files 349 to read in more than a page-sized chunk of memory at a time). The second parameter indicates whether the creator of the mutex is the initial owner of the
mutex lock. This tricky virus attempts to avoid detection by modifying parts of the system can be organized in a hierarchy (Figure 1.4) according to speed and cost. Similarly, if the user copies a file from one directory to a new directory, the file will inherit the
permissions of the destination directory. Since there are many processes in the system, the disk may be busy with the I/O request of some other process. At each memory reference appears at one end and the oldest reference drops off the other end. There are also two possibilities in terms of the address space of the new process: 1.
Typically, a given computing environment develops a security policy for certification and has the plan accredited by a security agency, such as the National Computer Security agency 
1. For example, suppose there is a known vulnerability (or bug) in sendmail. Increase the degree of multiprogramming. rsh attack finger attack grappling; hook y — " * — • ;;WQrrti: ;;; sendmail attack finger attack grappling; hook y — " * — • . The operation of the computer system. Whereas a system
normally has one network address, it can have many ports within that address to differentiate the many network services it supports. In this section, we look at several parts of this structure to round out our background knowledge. Often, the operating system will reclaim system resources from a canceled thread but will not reclaim all resources.
Write a simple set of code for the next space in the stack that includes the commands that the attacker wishes to execute—for instance, spawn a shell. Commonly, the virus will also e-mail itself to others in the user's contact list. In addition, the TCB is expected to
mediate. Once a program is compiled, the server cannot change the port number of the requested service. However, for a monthly fee or annual subscription, you can receive physical books in the mail and access educational printables. The application programs—such as word processors, spreadsheets, compilers, and web browsers—define the ways
in which these resources are used to solve users' computing problems. • A link is associated with exactly two processes. The resources are partitioned into several types, each consisting of some number of identical instances. Typically, operating systems have a device driver for each device controller. In Solaris, for example, creating a process is
about thirty times slower than is creating a thread, and context switching is about five times slower. For instance, a message might contain a request to transfer a whole file to a client or be limited to a simple block request. When the process terminated, the 93 frames would once again be placed on the free-frame list. Concepts are presented using
intuitive descriptions. The leftover three frames can be used as a free-frame buffer pool. Password authentication with insecure communications is considered by Lamport [1981]. This program will be structured using POSIX shared memory as described in Section 3.5.1. The program first requires creating the data structure for the shared-memory
segment. Antivirus programs may have catalogs of thousands of viruses for which they search. Historically, Linux suggests setting swap space to double the amount of physical memory, although most Linux systems now use considerably less swap space to double the amount of physical memory, although most Linux systems now use considerably less swap space.
of recipient addresses, and deliver the spam message to those users from the Windows machine. Adding more swap space requires repartitioning them and restoring them from backup) or adding another swap space elsewhere. This scheme gives better performance on
modern computers, which have more physical memory than older systems and tend to page less. 15.7 Firewalling to Protect Systems and Networks 15.6.5 Auditing, Accounting, and Logging 599 ., Auditing, accounting, and logging can decrease system performance, but they are useful in several areas, including security. However, a program may
impose arbitrary restrictions on how a resource can be used during execution of a particular code segment. Notice that such a speedup can be achieved only if the computer has multiple processing elements (such as CPUs or I/O channels). I/O takes place only between system memory and the I/O device. The first and third tasks can be reduced, with
careful coding, to several hundred instructions. On a single-user system, the overuse of locking would hurt only the user doing the locking would hurt only the user doing the locking. In fact, some systems now use the terms swapping and paging interchangeably, reflecting the merging of these two concepts. Process execution begins with a CPU burst. Demand paging interchangeably, reflecting the merging of these two concepts.
directly from the file system. Raw I/O bypasses all the filesystem services, such as file I/O demand paging, file locking, prefetching, space allocation, file names, and directories. With each transaction T, in the system, we associate a unique fixed timestamp, denoted by TS(T/). A skeleton outlining these functions appears as: Exercises #include 237 "/*
the buffer */ buffer.item buffer [BUFFERS IZE]; int insert item (buffer item item) { /* remove an object from buffer placing it in item return 0 if successful, otherwise return -1 indicating an error condition */ } The
insert-.item() and remove item() functions will synchronize the producer and consumer using the fork () system call may initially bypass the need for demand paging by using a technique similar to page sharing (covered in Section 8.4.4). Please refer to that chapter for
specific instructions. The LPC in Windows XP communicates between two processes on the same machine. The ordinary kind is called a data capability. If O, and O, an
potentially a source of considerable overhead, either we must give it hardware support to reduce the cost of each validation or we must accept that the system designer may compromise the goals of protection. key exchange can take place directly between the two parties or via a trusted third party (that is, a certificate authority), as discussed in
```

Section 15.4.1.4. An encryption algorithm consists of the following components: • A set K of keys. • Breach of integrity. Some systems may choose to update the physical file when the operating system periodically checks whether the page in memory has been modified. • \* • ... Should this situation occur (because of a bug in the operating system, for example), the locked frame becomes unusable. Methods of preventing or detecting security incidents include intrusiondetection systems, antivirus software changes, system-call monitoring, and firewalls,. Later, the back hand of the clock examines the reference bit for the pages in

```
memory, appending those pages whose bit is still set to 0 to the free list and writing to disk their contents if modified. Thus, the LRU algorithm replaces page 2, not knowing that page 2 is about to be used. Notice that sys close is stored at entry numbered 6 in the table to be consistent with the system call number defined in unistd. For example, all of
the routers on the way to the destination will receive the packet, too. Remote procedure calls (RPCs) are executed via msg rpc (), which sends a message and waits for exactly one return message from the sender. We do not give a complete description of the memory-management structure of the Pentium in this text. Alternatively, the JVM may be
implemented in hardware on a chip specifically designed to run Java programs. The date server is shown in Figure 3.19. It waits there tmtil it is selected for execution, or is dispatched. Human. Recall from Chapter 3 that two or more processes can communicate through the use of shared memory. Memory is better utilized with smaller pages,
however. However, since all its pages are in active use, it must replace a page that will be needed again right away. In general, there is no definitive answer. In addition, the coverage of segmentation has seen significant modification, including an enhanced discussion of segmentation in Pentium systems and a discussion of how Linux is designed for
such segmented systems. 466 Chapter 12 Mass-Storage Structure 12,6 Swap-Space Management Swapping was first presented in Section 8.2, where wre discussed moving entire processes between disk and main memory. If the mutex lock is unavailable when pthread in Section 8.2, where wre discussed moving entire processes between disk and main memory.
pthreadjnutex unlock(). For this project, standard counting semaphores will be used for empty and f u l l, and, rather than a binary semaphore, a mutex lock will be used to represent mutex. Here, the first time a Java method is invoked, the bytecodes for the method are turned into native machine language for the host system. However, the situation
 with asynchronous signals is not as clear. It also provides significantly updated coverage of virtual machines. The information in a file is defined by its creator. Also consider the key-management challenge. The list of processes waiting for a particular I/O device is called a device queue. For instance, one partition can hold a copy of the operating
system's executable code, while another holds user files. [1983], and Herlihy and Moss [1993]. 16.1.2 Computation Speedup If a particular computations that can run concurrently, then a distribute distribute the subcomputations among the various sites; the subcomputations that can run concurrently, then a distribute the subcomputation speedup If a particular computation speedup If a parti
can be run concurrently and thus provide computation speedup. Main memory is the only large storage area (millions to billions of bytes) that the processor can access directly. Typical speeds are a few milliseconds. When an access to a protected resource is subsequently requested, either by this method or a method it calls, a call to
checkPermissionsO is used to invoke stack inspection to determine if the request should be allowed. We can generate reference strings artificially (by using a random-number generator, for example), or we can trace a given system and record the address of each memory reference. The goal of spyware is to download ads to display on the user's
system, create pop-up browser windows when certain sites are visited, or capture information from the user's system and return it to a central site. 14.5.1 Global Table The simplest implementation of the access matrix is a global table consisting of a set of ordered triples. Thus, a computer holding S(k) can generate authenticators on messages so
that any other computer possessing V(k) can verify them. An alternative is to recognize that various processes will need differing amounts of memory. In Solaris 1 (SunOS), the designers changed standard UNIX methods to improve efficiency and reflect technological changes. When a user passes an object as an argument to a procedure, we may need
to ensure that the procedure cannot modify the abject. detail in Figure 8.23. Adding a System Call to the Kernel Now that you are familiar with the various background tasks corresponding to building and booting Linux kernels, yeai can begin the process of adding a new system call to the Linux kernel. 242 Chapter 6 Process Synchronization
Bibliographical Notes * The mutual-exclusion problem was first discussed in a classic paper by Dijkstra [1965a]. • Transaction T, needs to be redone if the log contains both the < T, s t a r t s > and the < 7/ commits> records. Some operating systems can handle only a sector size of 512 bytes. That is followed by an I/O burst, which is followed by
another CPU burst, then another I/O burst, then another I/O burst, and so on. For the information to be available, an external page table (one per process) 360 Chapter 9 Virtual Memory must be kept. The enhanced clock algorithm was discussed by Carr and Hennessy [1981], The working-set model was developed by Denning [1968]. Tf the value of a counter is 0, the
corresponding page slot is available. At the close of the workday on November 2,1988, Robert Tappan Morris, Jr., a first-year Cornell graduate student, unleashed a worm program on one or more hosts connected to the Internet. Whereas creating a separate thread is certainly superior to creating a separate process, a multithreaded server
nonetheless has potential problems. When the FIFO replacement algorithm mistakenly replaces a page that is still in active use, that page is quickly retrieved from the free-frame pool, and no I/O is necessary. : - - : . For this project, we use unnamed semaphores. We implement revocation by searching the global table for the desired entry and deleting
it. Let the size of the virtual memory for process pt be s-, and define Then, if the total number of available frames is m, we allocate a, frames to process and a domain may be either static, if the set of resources available to the process is fixed throughout the process's
lifetime, or dynamic. Therefore, writing a program that creates a breach of security, or causing a normal process to change its behavior and create a breach, is a common goal of crackers. 11. For example, the selection mask might specify that a file's permissions be monitored but its access time be ignored. WANs are generally slower than LANs; their
transmission rates range from 1,200 bits per second to over 1 megabit per second. As with the working-set strategy, we may have to suspend a process. Mattson et al.: 32rKB: J32 K8 Figure 9.27 Buddy system allocation. This high paging activity is called thrashing. System services can be classified into several categories: program control, status
requests, and I/O requests. pure paging 8.5 Compare the main memory organization schemes of contiguousmemory allocation, pure segmentation, and pure paging with respect to the following issues: a. Thus, if a user manages to read this list, password protection is no longer provided. When the child process completes (by either implicitly or
explicitly invoking e x i t ()) the parent process resumes from the call to wait (), where it completes using the e x i t () system call. Most of the transactions that, according to our algorithm, need to be redone have already actually updated the data that the log says they need to modify. One problem with a global replacement algorithm is that a process
cannot control its own page-fault rate. x (where the suffix corresponds to the kernel version number). Message digests are useful for detecting changed messages but are not useful as authenticators. The operating system keeps a small table, called the open-file table, containing information about all open files. Each close 0 decreases this open count
and when the open count reaches zero, the file is no longer in use, and the file's entry is removed from the open-file table. By allowing a Java program to invoke methods on remote objects, RMI makes it possible for users to develop Java applications that are distributed across a network. Like a government, it performs no useful function by itself.
Create a new file called helloworld. 2.18 In Section 2.3, we described a program that copies the contents of one file to a destination file. We have avoided a discussion of how things are done internally in these chapters. A Java program cannot directly access memory. With an access-list scheme, revocation is easy. We conclude our discussion with an
overview of Linux address translation on Pentium systems. However, if the data item Q is currently locked by some other transaction, then 7) may have to wait. Most multithreaded versions of UNIX allow a thread to specify which signals it will accept and which it will block. It completes the separation between logical memory and physical memory-
With this mechanism, an enormous virtual memory can be provided for programmers on a smaller physical memory. 9.5.1 Minimum Number of Frames Our strategies for the allocation of frames are constrained in various ways. The replacement of a bad block generally is not totally automatic because the data in the bad block are usually lost. The old
Chapter 21 (Windows 2000) has been turned into Appendix C. 6.8 Servers can be designed to limit the number of open connections. This function is passed three parameters: 1. When the object is released, it returns to signaled. Finally, many operating system kernels are now multithreaded; several threads operate in the kernel, and each thread
performs a specific task, such as managing devices or interrupt handling. As the memory-management algorithm becomes more complex, the time required to map a logical address to a physical address to a physical address increases. At this point, it must replace some page. Balanced against that cost, of course, is the frequency (or infrequency) of such changes
Continuing with this procedure of swapping nonconflicting operations, we get: • Swap the read(B) operation of TQ with the read(B) op
x 6 2 ~ 5 7. When a client process initiates a request for a connection, it is assigned a port by the host computer. Solomon and Russinovich [2000] described how Windows 2000 implements virtual memory. Preface xiii • Chapter 19, Real-Time Systems, is a new chapter focusing on realtime and embedded computing systems, which have requirements
problems, some operating systems give special programs the ability to use a disk partition as a large sequential array of logical blocks, without any file-system data structures. The timestamps of the transactions determine the serializability order. In certain situations, a single application may be required to perform several similar tasks. Thus, a
smaller page size should result in less I/O and less total allocated memory. 16.1.4 Communication When several sites are connected to one another by a communication network, the users at different sites have the opportunity to exchange information. Capabilities are usually distinguished from other data in one of two ways: 9 Each object has a tag to
denote its type either as a capability or as accessible data. => If TS(T,) < W-timestamp(Q), then T, is attempting to write an obsolete value of Q. One way to solve that problem involves the use of digital certificates. Also of general interest is the text by Lobel [1986]. 14.6 Access Control 545 Since access is checked when the file is opened, protection is
ensured^ This strategy is used in the UNIX system. On computer networks, worms are particularly potent, since they may reproduce themselves among systems and thus shut down an entire networks, worms are particularly potent, since they may reproduce themselves among systems and thus shut down an entire networks, worms are particularly potent, since they may reproduce themselves among systems and thus shut down an entire networks, worms are particularly potent, since they may reproduce themselves among systems and thus shut down an entire networks, worms are particularly potent, since they may reproduce themselves among systems and thus shut down an entire networks.
capacity is finite, however. This example illustrates a general principle for IDSs and IDPs: For usability, they must offer an extremely low false-alarm rate. In addition, it can interpret protection system. The fifth version of the "Sobig" worm
more properly known as 'iW32. Sobig. F@mm/" was released by persons at this time unknown. In fact, these attacks are more effective and harder to counter when multiple systems are involved. Because entries must be removed from the middle of the stack, it is best to implement this approach by using a doubly linked list with a head and tail pointer
If processes P and Q want to communicate, they must send messages from each other; a communication link must exist between them. 16.5.1 Naming and Name Resolution The first component of network communication is the naming of the systems in the network. When a computer refers to IP address 127.0.0.1, it is
referring to itself. The simplest, which is used for small messages, uses the port's message queue as intermediate storage and copies the binding of instructions and data to memory addresses? Debugging code in the utility permits testers to verify and display the state of
the mail system. */ Figure 3.25 Outline of simple shell. With multiprogramming, we try to use this time productively. This example illustrates a deadlock involving the same resource type. The number of objects in the cache depends on the size of the associated slab. Allowing controlled change in the contents of the access-matrix entries requires three
 additional operations: copy, owner, and control. Thus, a bad replacement choice increases the page-fault rate and slows process execution. To use a disk to hold files, the operating system still needs to record its own data structures on the disk. Protection will likely become a matter of greater concern to the designers of new systems with distributed
architectures and increasingly stringent requirements on data security. • Obtain the kernel source code for the Linux distribution. For example, a TEMPEST-certified system has terminals that are shielded to prevent electromagnetic fields from escaping.
page with the smallest count was probably just brought in and has yet to be used. This cat-and-mouse game is likely to continue, with more security violations (or misuse) of the system can be categorized as intentional (malicious) or accidental. Wait for the device seek
and /or latency time. The main disadvantage of these user-coded solutions is that they all require busy waiting. The operating system could instead swap out a process, freeing all its frames and reducing the level of multiprogramming. This chapter introduces many concepts associated with multithreaded computer systems, including a discussion of
the APIs for the Pthreads, Win32, and Java thread libraries. A slightly different view of an operating system emphasizes the mede, which indicates how the shared-memory segment is to be used—that is, for reading, writing, or both. A capability list
for a domain is a list of objects together with the operations allowed on those objects. This arrangement usually is not possible for the following two reasons: 1.2 Computer-System Organization 9 1. jii wrjte:L;:L: (b) Figure 14.6 Access matrix with owner rights. Tf a process has multiple threads of control, it can perform more than one task at a time.
Usually, special I/O instructions allow data transfers between these registers and system memory. This mechanism can be thought of as an automated FTP system. Consider a single-user system with 128 KB of memory composed of pages 1 KB in size. kernel objects caches slabs 3-KB objects physically contiguous pages 7-KB objects Figure 9.28 Slab
allocation. To illustrate the problems that are possible with a FIFO page-replacement algorithm., wTe consider the following reference string: 1,2,3,4,1,2,5,1,2,3,4,5 Figure 9.13 shows the curve of page faults for this reference string was allocation.
and I/O buffering. A segment for user code 4. The segment register points to the appropriate entry in the LDT or GDT. When the file is no longer being actively used, it is closed by the process, and the operating system removes its entry from the open-file table, c r e a t e and d e l e t e are system calls that work with closed rather than open files. In
general, any such hard-coding techniques, where identifiers must be explicitly stated, are less desirable than techniques involving indirection, as described next. Similarly, the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fault rate for the LRU algorithm on S is the same as the page-fa
string is shown in Figure 9.15. In general, user-level threads, as no intervention from the kernel is required. The identifier in turn locates the other file attributes. The problem has no best answer. Once it has created the producer and consumer threads, the main form the kernel is required. The identifier in turn locates the other file attributes.
of time and, upon awakening, will terminate the application. This cache lets the Pentium avoid having to read the descriptor from memory for every memory reference. In this section, we examine features that Windows XP uses to perform security functions. Separating code and data and generating reentrant code means that code pages can he read-
only and hence will never he modified. These documents can contain macros (or Visual Basic programs) that programs in the Office suite (Word, PowerPoint, and Excel) will execute automatically. In addition, virus droppers and other full files that are part of a virus infestation are frequently hidden via file attributes or unviewable file names. We
would expect that giving more memory to a process would improve its performance. To improve performance, recall that the TLB is searched first, before the hash table is consulted. • Limit. process P, is shown in Figure 6.26. This observation is important when we deal with the deadlock problem. The most common method
for doing so is to use a timestamp ordering scheme. Each device has its own device queue (Figure 3.6). • A function D: K -> (C -> M). 6. (The CR3 register points to an inner page directory for the current process.) The page directory entry points to an inner page table that is indexed by the contents of the innermost ten bits in the linear address. Consider
what could happen if the operating system allocated a disk page to a file and the application wrote data into that page before the operating system had a chance to flush the modified inode and free-space list back to disk. If the request mode is allowed, the file is opened for the process. compete for shared resources. Install more main memory. 15.2.2
Trap Door The designer of a program or system might leave a hole in the software that only she is capable of using. Obviously, as the number of frames allocated to each process decreases, the page-fault rate increases, slowing process to each process decreases, the page-fault rate increases, slowing process decreases, the page-fault rate increases, slowing process decreases, the page-fault rate increases, slowing process decreases, slowing process d
the system than the user is authorized to have. ;li;i the ;faya :?yn,::afcq:u(Hng):adeck requires for the three pages in memory. That is, fewer than one in every seven alarms indicates a real intrusion! In systems
where a security administrator investigates each alarm, a high rate of false alarms—called a "Christmas tree effect"—is exceedingly wasteful and will quickly teach the administrator to ignore alarms. Two people at geographically distant sites can collaborate on a project, for example. As mentioned in Section 15.7, auditing is a useful security
technique. CHAPTER OBJECTIVES • To discuss security threats and attacks. The processor (such as matrix inversion on an array processor, rather than on a microprocessor). 12.5.1 Disk Formatting A new magnetic disk is a blank slate: It is just a platter of
a magnetic recording material. Rather than incurring this overhead, Windows XP uses a variation on the FIFO algorithm discussed in Section 9.4.2. 9.10.2 Solaris, when a thread incurring this overhead, Windows XP uses a variation on the FIFO algorithm discussed in Section 9.4.2. 9.10.2 Solaris, when a thread incurring this overhead, Windows XP uses a variation on the FIFO algorithm discussed in Section 9.4.2. 9.10.2 Solaris In Solaris, when a thread incurring this overhead, Windows XP uses a variation on the FIFO algorithm discussed in Section 9.4.2. 9.10.2 Solaris In Solaris I
can be linked together to form a ready queue. The TCB also denotes the sensitivity level at the top and bottom of each page of any human-readable output. When the server waits until one becomes free. For instance, seven or more devices
can be attached to the small computer-systems interface (SCSI) controller. sh> cat prog. One technique for implementing a shell interface is to have the parent process first read what the user enters on the command line (i.e. cat prog. In general, of course, a user may trust that a procedure performs its task correctly. However, other types of events
may result in deadlocks (for example, the 1PC facilities discussed in Chapter 3). For a process at site A to exchange information with a process at site B, each must be able to specify the other. Distinguish between software and hardware operations. 8.6.2 Hardware Although the user can now refer to objects in the program by a two-dimensional
address, the actual physical memory is still, of course, a one-dimensional sequence of bytes. The sched process also creates the in t process, which serves as the root parent process for all user processes. Both belong to a class of page-replacement algorithms, that can never exhibit Belady's anomaly. During execution, the
system maintains the write-ahead log. Exercises 147 4.3 Under what circumstances does a multithreaded solution on a single-processor system? A common implementation has the Internet as the untrusted domain; a semitrusted and semi-secure network, called
the demilitarized zone (DMZ), as another domain; and a company's computers as a third domain (Figure 15.10). There are two common solutions to this problem. The basic approaches can be combined, however, allowing us to select an optimal approach for each class of resources in a system. 16.2.1.1 Remote Login An important function of a
network operating system is to allow users to log in remotely. • Exclusive. The counter is incremented after a new timestamp is assigned. Before returning from the signal-handling function, it should reissue the command prompt. With any scheduling algorithm, however, performance depends heavily on the number and types of requests. However, performance depends heavily on the number and types of requests.
the historical trend is toward larger page sizes. A process receiving a signal may handle it by one of the following techniques: • Ignoring the signal handler, or • providing a separate signal handler, or • providing a separate signal handler, or • providing a separate signal handler, or • providing the signal handler, or • providing a separate signal handler, or 
always shorter than the message and its ciphertext. If the operating system sends a batch of requests to the controller, the controller can queue them and the rotational latency. After the last access, the capability is destroyed. The stub unmarshals the return value and passes it to the client.
Common message-digest functions include MD5, which produces a 128-bit hash, and SHA-l, which outputs a 160-bit hash. The page fault is restarted. That is, for each k e K, V(k) is a function for verifying authenticators on messages. This command lists the status of
various POSIX interprocess communication mechanisms, including shared-memory segments. The TCB also protects itself from modification of its code or data structures. This improves space use and transmission time efficiency. Thus, the total paging time is about 8 milliseconds, including hardware and software time. 9.5.2 Allocation Algorithms The
easiest way to split in frames among n processes is to give everyone an equal share, m/n frames. The Mach kernel supports the creation and destruction of multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks, which are similar to processes but have multiple tasks and the similar tasks are similar to processes but have multiple tasks are similar to processes but have multiple
data[i] [j] = 0; zeros all the words on one page before starting the next page, reducing the number of page faults to 128. Here, a legitimate-looking e-mail or web page misleads a user into entering confidential information. Network operating systems are simpler to implement but generally more difficult for users to access and utilize than are
distributed operating systems, which provide more features. Chapters 19 and 20 deal with systems used for specific purposes, including real-time systems and multimedia systems. Let's consider as an example the boot process in Windows 2000. Related to the hit ratio is a similar metric: the TLB reach. It is important that the long-term schedule:
select a good process mix of I/O-bound and CPU-bound 3.2 Process Scheduling to the gueueing diagram. The inspection examines stack frames on the calling thread's stack, starting from the most recently added frame and working
toward the oldest. One part is accessible to the program and contains the program and contains the program and instructions. This technique is known as demand paging and is commonly used in virtual memory systems. Finally, both processes remove the view of the mapped file with a call to UnmapViewOfFileO. If a page fault is going to occur, it will happen at
this step, before anything is modified. An alternative protocol allows a process to request resources only when it has none. 3.4 2 Interprocess Communications models, (a) Message passing, (b) Shared memory. 6.24 In log-based systems that provide support for transactions, updates to data items cannot be
performed before the corresponding entries are logged. At a later stage, the compiler and loader can have a significant effect on paging. Here, we present only a single variation of it, and even then in a very simplified and abstract form, so as to maintain focus on its use of cryptographic primitives. Chapter 23 briefly describes a few other influential
operating systems. A code segment that misuses its environment is called a Trojan horse. 14.8.2 An Example: Cambridge CAP System A different approach to capability-based protection has been taken in the design of the Cambridge CAP system.
implements the Win32 API. Each entry in the LDT and GDT consists of an 8-byte segment descriptor with detailed information about a particular segment, including the base location and limit of that segment. 16.2.2 Distributed Operating Systems In a distributed operating system, the users access remote resources in the same way they access local
resources. The system-call level must provide the basic functions, such as process control and file and device manipulation. -:-;:: ---:: thread-local storage ... Send by copy and send by reference d. Interaction is achieved through a sequence of load or s t o r e instructions to specific memory addresses. Thus, the children still have a
parent to collect their status and execution statistics. **/ A pointer to PoolFunctionQ is passed to one of the functions in the thread pool API, and a thread from the pool executes this function. For example, the security descriptor of the file foo.bar might have owner avi and this discretionary access-control list: • avi—all access • group cs—read-write
access • user cliff—no access In addition, it might have a system access-control list of audit writes by everyone. space. Exercises • Define a new system call number for _JJR_tielloworlstate = new..state; Suppose the process makes an I/O request to a shared device, such as a disk. This ensures that all connections consist of a unique pair of sockets. For
more information and background on Windows XP, see Chapter 22. We expect S to be equivalent to S', as all operations appear in the same order in both schedules, except for O, and Oj, whose order does not matter. This is most easily accomplished using a struct. This method will not work for transactions that occur on separate systems or for
processors that do not share a clock. On the one hand, more protocols benefit from protections placed lower in the stack. The virus first decrypts and then executes. It is normally implemented either as access lists associated with each object or as capability lists associated with each domain. • The parent is exiting, and the operating system does not
 allow a child to continue if its parent terminates. A hash function creates a small, fixedsized block of data, known as a message digest or hash value, from a message. Other common operations include appending new information to the end of an existing file and renaming an existing file. A similar stub on the server side receives this message and
implementation of swap space is to provide the best throughput for the virtual memory system. The worst case occurs when the MVC instruction is the operand of an EXECUTE instruction that straddles a page boundary; in this case, we need eight frames. Virtual memory uses disk space as an extension of main memory. The following code
demonstrates how the mutex lock created above can be acquired: WaitForSingleObj ect(Mutex, INFINITE); The parameter value INFINITE indicates that we will wait an infinite amount of time for the lock to become available. For sites requiring faster Internet access, Tls are collected into multiple-Tl units that work in parallel to provide more
empty directory. 12.6.1 Swap-Space Use Swap space is used in various ways by different operating systems, depending on the memory-management algorithms in use. By performing this step, you have the option of either booting a new kernel or booting the unmodified kernel if the newly built kernel does not function properly. Unlimited threads
could exhaust system resources, such as CPU time or memory. Here, MFU would actually be more efficient than LRU. 15.9 An Example: Windows XP is a general-purpose operating system designed to support a variety of security features and methods. The top four levels of memory in Figure 1.4 may be constructed using
semiconductor memory. Even in those cases where the entire program is needed, it may not all be needed at the same time. Therefore, fully connected networks are impractical in any large system. If we associate a list of keys with each object, then selective revocation can be implemented. In this case, 7] must wait until the lock on Q is released. For
modern disks, the rotational latency can be nearly as large as the average seek time. Consequently, we must have enough frames to hold all the different pages that any single instruction can reference. It provides more concurrency than the many-to-one model by allowing another thread to run when a thread makes a blocking system call; it also
allows multiple threads to run in parallel on multiprocessors. Once established on the computer system under attack, the grappling hook connected to the main worm onto the hooked system (Figure 15.6). Most denial-of-service attacks involve systems that the attacker has 576 Chapter 15.
Security not penetrated. As with most penetration attacks, viruses are very specific to architectures, operating systems, and applications. In this scheme, a communication link has the following properties: 3.4 Interprocess Communication 101 • A link is established between a pair of processes only if both members of the pair have a shared mailbox
Chapters 3 through 7 describe the process concept and concurrency as the heart of modern operating systems. A more effective defense method is to avoid opening any e-mail attachment that contains executable code. 346 Chapter 14 Protection Notice that this facility is similar to the access matrix described in Section 14.4. This relationship will be
further explored in the exercises at the end of the chapter. In this section we discuss the details of crypography and its use in computer security. With deferred cancellation, in contrast, one thread indicates that a target thread is to be canceled, but cancellation occurs only after the target thread has checked a flag to determine if it should be canceled
or not. This situation effectively doubles the page-fault service time and increases the effective access time accordingly. Multithreading on a multi-CPU machine increases concurrency. We would prefer to separate the mechanism from the protection policy, allowing the same system to have complex or simple protection depending on the needs of its
users. As an example, consider the situation shown in Figure 8.20. See also file access; program threats; protection; user authentication of, 592-599 and accounting, 599 and accounting, 599 and accounting, 599 and accounting, 599 and intrusion detection, 594-596 and logging, 599 and security policy,
592 and virus protection, 596-598 and vulnerability assessment, 592-594 levels of, 562 in Linux, 777-779 access control, 775-779 authentication, 775 as operating system service, 41 as problem, 559-563 protection vs., 559 and system/network threats, 571-576 denial of service, 575-576 port scanning, 575 worms, 572-575 use of cryptography for, 576
587 and encryption, 577-584 implementation, 584-585 SSL example, 585-587 via user authentication, 587-592 biometrics, 591-592 passwords, 588-591 Windows XP), 602-603 security descriptor (Windows XP), 603 security domains, 599
security policy, 592 security reference monitor (SRM), 808-809 security-through-obscurity approach, 594 seek, file, 375 seek time (disks), 452, 457 segment limit, 304 segment tables, 304 semantics:
consistency, 401-402 copy, 513 immutable-shared-files, 402 session, 402 session, 402 session, 402 session, 402 session, 402 session, 402 semaphore(s), 204 defined, 200 implementation of monitors using, 214-215 and starvation, 204 defined, 200 implementation, 202-204 implementation, 201 counting, 201 and deadlocks, 204 defined, 200 implementation, 202-204 implementation, 202-204 implementation, 202-204 implementation, 203-204 implementation, 204 defined, 200 implementation, 204 defined, 200 implementation, 205-204 implementation,
383 sequential-access devices, 844 sequential devices, 506, 507 serial ATA (SATA) buses, 453 serializability, 225-227 serial schedule, 226 server(s), 5 cluster, 655 defined, 642 in SSL, 586 server, 506, 507 serial ATA (SATA) buses, 453 server subject (Windows XP), 603 services, operating system, session hijacking, 561 session layer, 629 session object, 798
session semantics, 402 session space, 797 shared lock, 378 shared lock, 37
121-123 shell script, 379 shortest-job-first (SJF) scheduling algorithm, 458-459 short-term scheduler, 220 signal handlers, 139-141 signal-safe
functions, 123-124 signatures, 595 simple operating system structure, 58-59 simple endirect blocks, 427 single-level directories, 387 single-level directori
algorithm skeleton, 114 slab allocation, 355-356, 758 Sleeping-Barber Problem, 233 slices, 386 small-area networks, 28 small computer-systems interface, see under SCSI SMB, see server-message-block SMP, see system-on-chip
strategy 915 soft affinity, 170 > soft error, 463 soft real-time systems, 696, 722 software capability, 549 software interrupts (traps), 502 software objects, 533 Solaris: scheduling example, 173, 175-177 swap-space management in, 467 synchronization in, 217-219 virtual memory in, 363-365 Solaris 10 Dynamic Tracing Facility, 52 solid-state disks, 24
sorted queue, 772 source-code viruses, 570 source files, 374 sparseness, 300, 318 special-purpose computer systems, 29-31 handheld systems, 30-31 multimedia systems, 30 real-time embedded systems, 30 speed, relative, 194 speed of operations: for I/O devices, 506, 507 spinlock, 202 spoofed client identification, 398 spoofing, 599 spool, 514
spooling, 514-515, 844-845 spyware, 564 SRM, see security reference monitor SSL 3.0, 585-587 SSTF scheduling algorithms, 335 stack frame, 566-567 stack inspection, 554 stack-overflow attacks, 565-568 stage (magnetic tape), 480 stalling, 276
standby thread state (Windows XP), 789 starvation, see indefinite blocking state (of process), 83 stateless protocols, 727 state restore, 89 static linking, 281-282, 764 static priority, 722 static protection, 534 status information, 55
status register, 498 stealth viruses, 570 storage. Because each active process must have its own copy of the page table, a large page size is desirable. 14,10 Summary Computer systems contain many objects, and they need to be protected from misuse. In fact, some anti-virus programs implement a variety of detection algorithms. The example below
 illustrates the prompt sh> and the user's next command: cat prog. The process is shown in Figure 3.23. Thread libraries provide the application programmer with an API for creating and managing threads. Once a request is received, the server accepts a connection from the client socket to complete the connection. 2.14 What is the main advantage
for an operating-system designer of using a virtual-machine architecture? MORE FROM QUESTIONSANSWERED.NET Seventh Edition ABRAHAM SILBERSCHATZ Yale University PETER BAER GALVIN Corporate Technologies, Inc. A pair of integers, bl and bl, such that bl < bl. A master key is associated with each object; it can be defined or replaced
with the set-key operation. By transferring the files of the project, logging in to each other's remote systems to run programs, and exchanging mail to coordinate the work, users minimize the limitations inherent in longdistance work. Assume that the page to be replaced is modified 70 percent of the time. On the client side, parameter marshalling
involves converting the machinedependent data into XDR before they are sent to the server. If you want to stick to the dozens of free books available, click on the operating system. The current size of the file (in bytes
words, or blocks) and possibly the maximum allowed size are included in this attribute. This execution sequence, which is called a schedule, is represented in Figure 6.22. Restart the process. Information about viruses and worms can be found at , as well as in Ludwig [1998] and Ludwig [2002]. Some systems, including VMS, do not allow a child to
exist if its parent has terminated. A fixed set of possible access rights is known to and interpreted by the system. The CLR is the implementation of the .NET virtual machine. In some instances—such as thread creation—we illustrate a specific concept using all three programming environments, allowing the reader to contrast the three different
libraries as they address the same task. Let's examine what the operating system must do to perform each of these six basic file operations. Photo Courtesy: Westend61/Getty Images The site is filled with some of the most popular kids' books, and rather than read them yourself, you can watch a video of a celebrity like Kevin Costner, Eva Longoria or
Betty White read them to you. This program creates a 4,096-byte shared-memory segment. Security problems associated with the TCP/IP protocol suite are described in Bellovin [1989]. Exercises 123 As noted above, the setup () function loads the contents of the args array with the command specified by the user. The most important property of the
working set, then, is its size. We elaborate on this approach by examining each of the four necessary conditions separately. We present a large number of examples that pertain to the most innovative operating systems, including Sun Microsystems' Solaris; Linux; Mach; Microsystems' Solaris; Linux; Mach; Microsystems and the most innovative operating systems, including Sun Microsystems' Solaris; Linux; Mach; Microsystems and the most innovative operating systems, including Sun Microsystems and the most innovative operating systems.
Windows XP; DEC VMS and TOPS-20; IBM OS/2; and Apple Mac OS X. 2.9 Why is the separation of mechanism and policy desirable? Request and release of resources that are not managed by the operations on semaphores or through acquisition and release of a mutex lock.
The write-ahead log scheme was first introduced in System R by Gray et al. Each entry in this configuration file includes a selection mask to specify the file attributes (inode attributes) that will be monitored for changes. The major difference between this algorithm and the simpler clock algorithm is that here we give preference to those pages that
have been modified to reduce the number of 1/Os required. Alternatively, swap space can be created in a separate raw partition, as no file system or directory structure is placed in this space. Operating-system concepts. This
mechanism allows a client and server on the same host to communicate using the TCP/IP protocol. LRU replacement associates with each page the time of that page's last use. Each computer design has its own interrupt mechanism, but several functions are common. • Allow the system to select arbitrarily which process will receive the message (that
is, either P2 or P3, but not both, will receive the message). • Location. Unfortunately, RC4 as used in WEP (IEEE standard 802.11) has been found to be breakable in a reasonable amount of computer time. r i T #: •: ::: -t\ T": i network host: $" \ .L,..r,$F ":" ••;..: •: ; : . We discuss system I/O in depth, including I/O system design, interfaces, and
internal system structures and functions. 7.4.1 Mutual Exclusion The mutual-exclusion condition must hold for nonsharable resources. Tt then finds a free frame and reads the page in from the backing store. Communication using sockets—although common and efficient—is considered a low-level form of communication between distributed processes
means of communication. One solution to the producer-consumer problem uses shared memory. In this section, we briefly discuss each of them. To overcome this difficulty, we must place a limit on the levels of indirection (for example, limit an instruction to at most 16 levels of indirection). We will call such data thread-specific data. Chapters 1 and 2
explain what operating systems are, what they do, and how they are designed and constructed. If the bit is set to "invalid," the page either is not valid (that is, not in the logical address space of the process) or is valid but is currently on the disk. If you sign up for a free account, you can create a virtual bookshelf with your child's favorites so that you
can find them easily when you want. A strategy that uses the page-fault frequency (PFF) takes a more direct approach. An owner identification and a domain bit (known as the setuid bit) are associated with each file. One protocol that can be used requires each process to request and be allocated all its resources before it begins execution. It did
however, effectively negate the defensive strategy of opening attachments only from people known to the receiver. For example, consider a process 200 KB in size, of which only half (100 KB) is actually used in an execution. • Indirection. 14.8 Capability-Based Systems In this section, we survey two capability-based protection systems. The recovery
 algorithm uses two procedures: • undo(TJ), which restores the value of all data updated by transaction T; to the old values • redo(Tj), which sets the value of all data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transaction T; to the new values The set of data updated by transa
Accordingly, we can ignore hoio a memory address is generated by a program. 8.2 Consider the following process for generating binaries. In general, we want the now ean then take place; wre know that no page fault can
occur, since all the relevant pages are in memory. If the client determines that it does want to send large messages, it asks for a section object to be created. The slab allocator first appeared in the Solaris 2.4 kernel. It copies from the DVD drive and then releases 254 Chapter 7 Deadlocks both the DVD drive and the disk file. Discuss
solutions for preventing this form of attack. After marking the unblocked thread as eligible to run, the application schedule 2 is conflict serializable, because it can be transformed into the serial schedule 1. If a system failure occurs, we restore the state of all updated data by
consulting the log to determine which transactions need to be redone and which need to be undone. If the request cannot be granted immediately (for example, if the resource is being used by another process), then the request cannot be granted immediately (for example, if the resource is being used by another process), then the request cannot be granted immediately (for example, if the resource is being used by another process), then the request cannot be granted immediately (for example, if the resource is being used by another process).
(If we ignore the first three, which all algorithms must suffer, then optimal replacement is twice as good as FIFO replacement.) In fact, no replacement algorithms must suffer, then optimal replacement is twice as good as FIFO replacement.
an "illegal address" fault is generated. The request and release of resources are system calls, as explained in Chapter 2. • Secondary memory. Any process that subsequently sends a message to this mailbox must be notified that the mailbox no longer exists. If we take an average page-fault service time of 8 milliseconds and a memory-access time of
200 nanoseconds, then the effective access time in nanoseconds is 9.3 \text{ Copy-on-Write } 325 \text{ effective access time} = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (8 \text{ milliseconds}) = (1 - p) \times (200) + p \times (200)
task at a time can either own or receive from a mailbox, but these rights can be sent to other tasks if desired. It should be entirely transparent to the user process. A second limitation is that some security-relevant files—are supposed to change over time, and Tripwire does not provide a way to distinguish between an
data item that it locked at an earlier point. The system must also perform various data translations of the two sites involved are not directly compatible (for instance, if they use different character-code representations or representations
system that provides considerable flexibility. The specification for the JVM does not indicate how Java 'threads are to be mapped to the underlying operating system, instead leaving that decision to the particular implementation.of the JVM. One type of social-engineering attack is phishing. \:- : : : : : -• : POSIX also defines several extensions to the
standards, including real-time extensions (POSIXI.c, better known as Pthreads library (POSIXI.c, better known as Pthreads). The original Internet worm turned into a DOS attack when a bug failed to delay its rapid spread. 9.9.3 TLB R e a c h In Chapter 8, we introduced the hit ratio of the TLB. A good example of this is found in Solaris 10. By
rewriting the above command as sh> cat prog.c & the parent and child processes now run concurrently. This system has 128 frames. Perform necessary error checking to ensure that a non-negative number is passed on the command line. Most file operations require the system to modify data within the file. Hence, the write operation is rejected, and
7} is rolled back. Navigating the directory structure and the disk-allocation data structures takes time and (potentially) extra disk accesses. RMI is the Java version of RPCs. RMI allows a thread to invoke a method on a remote object just as it would invoke a method on a local object. A hash table, in contrast, is designed to scatter references,
be hard to detect and prevent. We have rewritten the material in most of the chapters by bringing older material up to date and removing material that was no longer of interest or relevance. The issue of password cracking is examined by Seely [1989]. The first reference to 3 results in replacement of page 0, since 332 Chapter 9 Virtual Memory'
reference string 7 0 1 2 0 3 0 4 0 io LL 0 3 0 3 2 1 7 p ]0' \-J I 2 • 3 '3\ 3 til E 2 31 3 0 0 i 1 7 0 1 P 1 i j || I 1 if page frames Figure 9.12 FIFO page-replacement algorithm. An example using small values is shown in Figure 9.12 FIFO page-replacement algorithm.
execution. If this is set to IPC-PRIVATE, a new shared-memory segment is created. The JVM may be implemented in software on top of a host operating system, such as Windows, Linux, or Mac OS X, or as part of a web browser. Thus, global replacement generally results in greater system throughput and is therefore the more common method. As an
example of how such a strategy works, consider a file system in which each file has an associated access list. Typically, a breach of confidentiality is the goal of an intruder. A typical hard disk has an average latency of 3 milliseconds, and a transfer time of 0.05 milliseconds. Chapters 14 and 15 discuss the processes in an
operating system that must be protected from one another's activities. Most thread libraries—including Win32 and Pthreads—provide some form of support for thread-specific data. N)(m)) provide authentication of the sender? interactive computer systems happened-before relation, 664-666 hard affinity, 170 hard-coding techniques, 100 hard errors,
465 hard links, 394 hard real-time systems, 696, 722 hardware, 4 I/O systems, 496-505 direct memory access, 503-504 interrupts, 499-503 polling, 498-499 for storing page tables, 292-294 synchronization, 197-200 hardware-abstraction layer (HAL), 787, 788 hardware objects, 533 hashed page tables, 300 hash functions, 582 hash tables, 420 hash
value (message digest), 582 heaps, 82, 835-836 heavyweight processes, 127 hierarchical paging, 297-300 hierarchical storage management (HSM), 483 high availability, 14 high performance, 786 hijacking, session, 561 hit ratio, 294, 358 hive, 810 hold-and-wait condition (deadlocks), 253-254 holes, 286 holographic storage, 480 homogeneity, 169
host adapter, 496 host-attached storage, 455 host controller, 453 hot spare disks, 475 hot-standby mode, 15 HSM (hierarchical storage management), 483 human security, 562 Hydra, 547-549 hyperspace, 797 hyperthreading technology, 171 Index I IBM OS/360, 850-851 identifiers: file, 374 group, 27 user, 27 idle threads, 177 IDSs, see intrusion-
detection systems IKE protocol, 585 ILM (information life-cycle management), 483 immutable shared files, 402 implementation: of CPU scheduling algorithms, 184-185 of operating systems, 700-704 and minimizing latency, 702-704 and priority-based scheduling, 700-701 of
transparent naming techniques, 645-646 of virtual machines, 65-66 incremental backup, 436 independent processes, 96 index, 384 index block, 426 indexed disk space allocation, 425-427 index root, 816 indirect blocks, 427 indirect communication, 100
                                        ment (ILM), 483 information-maintenance system calls, 53-54 inode objects, 419, 765 input/output, see under I/O input gueue, 275-276 instruction-execution unit, 811 899 instruction register, 8 » integrity, breach of, 560 intellimirror, 828
Intel Pentium processor, 305-308 interactive (hands-on) computer systems, 16 interface(s): batch, 41 client, 642 defined, 505 intermachine interface, 642 internation, 287, 382 international use, 787 Internat address, 623 Internat Protocol (IP), 584-585 interprocess
communication (IPC), 96-102 in client-server systems, 108-115 remote method invocation, 114-115 remote procedure calls, 111-113 sockets, 108-110 in Linux, 739, 773-774 Mach example of, 105-106 in message-passing systems, 99-102 POSIX shared-memory example of, 103-104 in shared-memory systems, 97-99 Windows XP example of, 106-108
interrupt(s), 7, 499-503 defined, 499 in Linux, 754-755 interrupt-controller hardware, 501 interrupt chaining, 501 interrupt testor, 8, 284, 501
intruders, 560 intrusion detection, 594-596 intrusion-detection systems (IDSs), 594-595 intrusion-prevention systems (IPSs), 595 900 Index inverted page tables, 301-302, 359-360 I/O (input/output), 4, 10-11 memory-mapped, 353 overlapped, 353 overlapped, 353 overlapped, 353 intrusion-detection systems (IDSs), 594-595 intrusion-prevention systems (IDSs), 594-595 intrusion-preventi
362 I/O manager, 805-806 I/O operations (operations (operations, 507-508 blocking and nonblocking I/O, 510-511 clocks and timers, 509-
510 network devices, 508-509 hardware, 496-505 direct memory access, 503-504 interrupts, 499-503 polling, 498-499 kernels, 511-518 buffering, 511-518 protection, 515-516 spooling and device reservation, 514-515 Linux, 770-773 block
devices, 771-772 character devices, 772-773 STREAMS mechanism, 520-522 and system performance, 522-525 transformation of requests to hardware operations, 518-520 IP, see Internet Protocol IPC, see interprocess communication IPSec, 585 IPSs (intrusion-prevention systems), 595 IRP (I/O request packet), 80c ISCSI, 456 ISO protocol stack,
630 ISO Reference Model, 585 Java: file locking in, 377-378 language-based protection in, 553-555 monitors in, 218 Java threads, 134-138 Java Virtual Machine (JVM), 68 JIT compiler, 68 job scheduling, 17 journaling, 768-769 journaling file systems, see
log-based transaction-oriented file systems just-in-time (JIT) compiler, 68 JVM (Java Virtual Machine), 68 K KB (kilobyte), 6 Kerberos, 814 kernel(s), 6, 511-518 buffering, 517-518 Linux, 743, 744 multimedia systems, 720-722
nonpreemptive, 194-195 preemptive, 194-195 preemptive, 194-195 preemptive, 194-195, 701 protection, 515-516 real-time, 698-700 spooling and device reservation, 514-515 task synchronization (in Linux), 753-755 Windows XP, 788-793, 829 Index kernel extensions, 63 kernel memory allocation, 515-516 real-time, 698-700 spooling and device reservation, 514-515 task synchronization (in Linux), 753-755 Windows XP, 788-793, 829 Index kernel extensions, 63 kernel memory allocation, 515-516 real-time, 698-700 spooling and device reservation, 514-515 task synchronization (in Linux), 753-755 Windows XP, 788-793, 829 Index kernel extensions, 63 kernel memory allocation, 515-516 real-time, 698-700 spooling and device reservation, 514-515 task synchronization (in Linux), 753-755 Windows XP, 788-793, 829 Index kernel extensions, 63 kernel memory allocation, 515-516 real-time, 698-700 spooling and device reservation, 515-516 real-time, 698-700 spooling and 698-700 
registration, 746-747 management of, 745-746 kernel threads, 129 Kerr effect, 479 keys, 544, 547, 577 private, 580 key distribution, 583-555 LANs, see local-area networks
latency, in real-time systems, 702-704 layers (of network protocols), 584 layered approach (operating system structure), 59-61 lazy swapper, 319 LCNs (logical cluster numbers), 815 LDAP, see lightweight directory-access protocol LDT (local descriptor table), 306 least-frequently used (LFU) pagereplacement algorithm, 338 least privilege, principle
of, 532-533 least-recently-used (LRU) page-replacement algorithm, 334-336 levels, 719 LFU page-replacement algorithm, 338 libraries: Linux system, 743, 744 shared, 281-282, 318 licenses, software, 235 lightweight directory-access protocol (LDAP), 400, 828 limit register, 276, 277 linear addresses, 306 901 linear lists (files), 420 line discipline, 772
link(s): communication, 99 defined, 392 hard, 394 resolving, 392 symbolic, 794 linked disk space allocation, 423-425 linked lists, 430^131 linked scheme index block, 426^127 linking, dynamic vs. Write a C program that is passed an identifier for a shared-memory segment. This capability follows from the fact that conflicting operations are processed
in timestamp order. This stub locates the port on the server and marshals the parameters. As processes wait for the paging device, CPU utilization decreases. If the user enters, the signal handler will output a list of the most recent 10 commands. The capability list is associated with a domain, but it is never directly accessible to a process executing
in that domain. Next, we explain the operation of the buddy system with a simple example. The producer and consumer—running as separate threads—will move items to and from a buffer that is synchronized with these empty, f ull, and mutex structures. This means that invoking a function in the library results in a local function call in user space
and not a system call. Files may be free form, such as text files, or may be formatted rigidly. 15.4.1 Encryption Because it solves a wide variety of communication security problems, encryption is used frequently in many aspects of modern computing. The file-open counter tracks the number of opens and closes and reaches zero on the last close.
Monitoring the hash of a file for changes is as good as monitoring the files trequires far less room than copying the files themselves. System calls appear as procedure calls to user programs, but result in a change in execution context and privileges. A busy web server may have several (perhaps thousands) of clients
concurrently accessing it. Similarly, authenticators on IP packets detect the modification of contained TCP header information. With this additional knowledge, it can decide for each request whether or not the process should wait. Division-B mandatory-protection systems have all the properties of a classC2 system; in addition, they attach a sensitivity
label to each object. In some early research, investigators noticed that this assumption was not always true. For example, in Figure 7.8, we present a resource-allocation or alteration, and accidental introduction of inconsistency. This information is a
pointer to a device and to the location of the file on that device. Because we save the state (registers, condition code, instruction counter) of the interrupted process when the page fault occurs, we must be able to restart the process in exactly the same place and state, except that the desired page is now in memory and is accessible. When the first
indirection occurs, a counter is set to 16; the counter is then decremented for each successive indirection for this instruction. *; p u b l i c c l a s s DateServer { public static void main(String [] args) { try { ServerSocket (6013); // now listen for connections while (true) { Socket client = sock.accept(); PrintWriter pout = new
PrintWriter(client.getOutputStream(), true); // write the Date to the socket pout.println(ioe); Figure 3.19 Date server. Write a program to coordinate the barber and the customers. 330 Chapter 9 Virtual
Memory Page replacement is basic to demand paging. However, if a process requires its own LDT, it can create one and use that instead of the default LDT. The compiler could generate standard object code as well as a trap door, regardless of the source code being compiled. The operating system abstracts from the physical properties of its storage
devices to define a logical storage unit, the file. This algorithm also was discussed by Dijkstra [1965a]. Consider the first programming exercises in which students learn to create subprocesses or threads. Otherwise, users could arbitrarily kill each other's jobs. A text file is a sequence of characters organized into lines (and possibly pages). • • '- . • '- ': iii
considered how a static access-control scheme can be incorporated in a programming language that supports abstract data types. In this case, an invalid bit is used in the page directory entry to indicate whether the table to which the entry is pointing is in memory or on disk. 5 2. Consider a transaction Tj that committed prior to the checkpoint.
However, Windows XP also provides support for a fiber library, which provides the functionality of the many-to-many model (Section 4.2.3). Mainframe operating systems are designed primarily to optimize utilization of hardware.
management. 15.8 Computer-Security Classifications The U.S. Department of Defense Trusted Computer System Evaluation Criteria specify four security classifications in systems: A, B, C, and D. Various concurrency-control schemes ensure serializability by delaying an operation or aborting the transaction that issued the operation. Unlike network
addresses, however, keys are designed so that it is not computationally feasible to derive them from the messages they were used to generate or from any other public information. [1995]. A digital certificate is a public key digitally signed by a trusted party. In the first, the system can attempt to hide the fact that the process has migrated from the
client. For example, a system may have two printers. After all, we are simply delaying the low-priority process for the benefit of the high-priority process. ER GPU Scheduling CPU scheduling is the basis of multiprogrammed operating systems. However, the cost to service these more frequent interrupts will be correspondingly higher. As a user
process executes, the bit associated with each page referenced is set (to 1) by the hardware. Belady et al. Each word has its own address. But did you notice that with a page size of 1 byte, we would have a page fault for each byte? Read-only files are a good example of a sharable resource. The TLB reach refers to the amount of memory accessible
from the TLB and is simply the number of entries multiplied by the page size. Both the read and write operations use this same pointer, saving space and reducing system complexity. The interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save the address of the interrupt architecture must also save
P. 4.5 Operating-System Examples In this section, we explore how threads are implemented in Windows XP and Linux systems. Then the CPU can transfer the next byte. The full bootstrap program is stored in "the book from the site if you'd like to
own a physical copy. International Children's Digital Library The International Children's Digital Library has one of the biggest selections of kids' books online. (0, 1) not recently used but modified—not quite as good, because the page will need to be written out before replacement 3. The application runs an upcall handler on this new virtual processor,
which saves the state of the blocking thread and relinquishes the virtual processor on which the blocking thread is running. The mapped file represents the shared-memory object that will enable communication to take place between the processes. • To explain the concepts of demand paging, page-replacement algorithms, and allocation of page
frames. 14.8 Discuss the need for rights amplification in Hydra. The segment is initially divided into two buddies—which we will call Ai and AR—each 128 KB in size. If an authentication to be blocked by purposefully causing
incorrect attempts to all accounts. schedule 2 of Figure 6.23. The student process does not need more than 10 frames, so the other 21 are, strictly speaking, wasted. Furthermore, if a permission is changed on a directory, the new permissions do not automatically apply to existing files and subdirectories; the user may explicitly apply them if she so
desires. For LRL replacement, the set of pages in memory would be the n most recently referenced pages. Domain switching in MULTICS occurs when a procedure in a different ring. In a larger sense, however, the storage structure that we have described—consisting of registers, main memory,
and magnetic disks—is only one of many possible storage systems. Each entry in the list has a type, size, and value. Programmers have been arrested for embezzling from banks by including rounding errors in their code and having the occasional half-cent credited to their accounts. An algorithm to detect a cycle in a graph requires an order of n1
operations, where n is the number of vertices in the graph. If there is no free frame, use a page-replacement algorithm toselect a victim frame. But how do we know how many frames it "needs'? If Q is not currently locked, then the lock is granted, and T; can now access it. If the package has not been installed earlier, it can be downloaded from the
ofservice attacks can affect firewalls as much as any other machines. Solaris also allows applications—such as databases—to take advantage of the large 4-MB page size. In this chapter, we discuss virtual memory in the form of demand paging and examine its complexity and cost. [1961] and by Howarth et al. In general, we have no completely
adequate definition of an operating system. However, Linux does not distinguish between processes and threads. InputStream class returns —1 when the client has closed its end of the socket connection. All in all, the ISO Reference Model, which has been almost universally adopted as a model for data networking, defines seven such protocol layers.
In addition to the various physical and logical resources that a process obtains when it is created, initialization data (input) may be passed along by the parent process to the child process. 15.4.1.1 Symmetric Encryption In a symmetric encryption algorithm, the same key is used to encrypt and to decrypt. Signals may be either synchronous or
asynchronous, depending upon the source and the reason for the event being signaled. The j a v a . An I/O-bound program typically has many short CPU bursts. The purpose of this form of page management is to reduce the amount of physical memory needed to track virtual-to-physical address translations. Another popular technique is to run a
program in a sandbox, which is a controlled or emulated section of the systems. In general, the following options exist: 1. 3.5 Examples of I PC Systems In this section, we explore three different IPC systems. 1 7 0 1 9.4 Page Replacement 335 • Counters. Store the sum in C. Facilities are more convenient for users if they do not require the use of a
different set of commands. However, the desired page is read into a free frame from the pool before the victim is written out. The concept of a file is thus extremely general. 6.10 Show how to implement the waitO and signal() semaphore operations in multiprocessor environments using the TestAndSet () instruction. First, RPCs support procedural
programming, whereby only remote procedures or functions can be called. The process attempting access must present a capability for that access. The cache will fulfill the request using a struct task structure to object that has already been allocated in a slab and is marked as free. When multiple systems are involved, especially systems
controlled by attackers, then such tracing is much harder. The method for delivering a signal depends on the type of signal generated. This scheme allows a procedure to be certified as trustworthy to act on a formal parameter of a specified type on behalf of any process that holds a right to execute the procedure. Mutex locks are ^ acquired ;and
released using ptiar:ead.B'U,i:;ex.,lDclc(): ;a;nd p:thre: ad Jmitex.:unlock£X ' respec-: tively. What is required to support dynamic memory allocation In the following schemes? The critical-region concept was suggested by Hoare [1972] and by BrinchHansen [1972]. 0200 Write permission of owner. This is particularly important on systems that
```

```
cannot support a large number of concurrent threads. 15.3.3 Denial of Service As mentioned earlier, DOS attacks are aimed not at gaining information or stealing resources but rather at disrupting legitimate use of a system or facility. A process is thrashing if it is spending more time paging than executing. The memorymapped file serves as the
region of shared meniory between the communicating processes (Figure 9.24). Specifying the desired control of access to a shared resource in a system call is used to create a separate, duplicate process. As
we have seen, resource allocation is especially important where many users access the same mainframe or minicomputer. With a smaller page size, we have better resolution, allowing us to isolate only the memory that is actually needed. This procedure defines the final legal address and hence the amount of available memory. The other two methods
involved operating-system bugs in the UNIX finger and sendmail programs. Each page fault generates the large amount of overhead needed for processing the interrupt, saving registers, replacing a page, queueing for the paging device, and updating tables. Invoking a function in the API for the library typically results in a system call to the kernel.
Initially, all objects in the cache are marked as free. How do user programs and system services interact in a microkernel architecture? This technique also applies to read-only pages (for example, pages of binary code). Ganapathy and Schlmmel [1998] and Navar.ro et al. It is generally more efficient to use one process that contains multiple threads.
Several language constructs have been proposed to deal with these problems. By masquerading, attackers breach authentication, the correctness of identification; they would not normally be entitled. Remember also that we
are looking at only the device-service time. These attacks are launched from multiple sites at once, toward a common target, typically by zombies. 9.8 Allocating Kernel Memory 3s3 reads from shared memory the message "Shared memory the message" that was written by the producer process. For example, assume that A equals 10,000 references and
that we can cause a timer interrupt every 5,000 references. The packets hostX (146.86.5.20) socket (146.86.5.20) socket (146.86.5.20) web server (161.25.19.8) Figure 3.18 Communication using sockets. Modify the solution to Exercise 3.9 so that the echo server services each client in a separate request. The layout for a typical stack bottom frame pointer return
address saved frame pointer grows automatic variables parameter(s) top Figure 15.3 The layout for a typical stack frame. By setting this mutex lock to inherit the handle of the mutex. • We can allow the system to enter a deadlock state, detect it, and recover. • A set C of
ciphertexts. For example, in Solaris 10, the "least privilege" feature implements a list of more than fifty system calls that processes may or may not be allowed to make. The copyright allows the copying of the access right only within the column (that is, for the object) for which the right is defined. The Solaris operating system supported the two-level
model in versions older than Solaris 9. Files are normally organized into directories for ease of use. Such a partition can be treated as a single-site failure. 8. Thus, in schedule 3, TS(T2) < TS(T3), and the schedule is possible under the timestamp protocol. When run subsequently, Tripwire inputs both tw.config and the previously stored database
recomputes the signature for each file or directory named in tw.cprif ig, and compares this signature with the signature (if any) in the previously computed database. 9.7.3 M e m o r y - M a p p e d I/O In the case of I/O, as mentioned in Section 1.2.1, each I/O controller includes registers to hold commands and the data being transferred. These
methods prevent deadlocks by constraining how requests for resources can be made. [1976] used a formal version of this model to enable them to prove properties of a protection system mathematically. Usually, such a system that
support different types of files. Similarly, process Q could, during the course of its execution, send a message to another site, which in turn would create another process. Purchasing unopened software from vendors and avoiding free or pirated copies from public sources or disk exchange offer the safest route to preventing infection. If significant
portions of the file are being accessed, however, it is more efficient to copy the entire file. If your system supports lilo, add an entry to lilo, add an entry to lilo. Pages belonging to libraries that are being shared by several processes—even if they are eligible to be claimed by the scanner—are skipped during the page-scanning process. Alternatively, if a process
 requests some resources, we first check whether they are available. 3.4.2.3 Buffering Whether communication is direct or indirect, messages exchanged by communicating processes reside in a temporary queue. The long-term scheduler executes much less frequently; minutes may separate the creation of one new process and the next. 1, 2, 3, 4, 5, 3,
4,1, 6, 7, 8, 9, 7, 8, 9, 7, 8, 9, 7, 8, 9, 5, 4, 5, 4, 2. r.- r • - [ - .'-. Thus, when one process creates a new process, the identity of the newly created process is passed to the parent. A signaled object is available for ownership; once a dispatcher object (such as a mutex lock) is acquired, it moves to the nonsignaled state. Figure 3.21 shows a sample interaction. Virtual
address spaces that include holes are known as sparse address spaces. Second, an operating system may allow by default more privileges than a normal user needs. Pages that cannot be modified (pages containing executable code) can be shared by the parent and child. In this section, we restrict our attention to two modes: 228 Chapter 6 Process
Synchronization • Shared. In this scenario, the strcpy() function will be gin copying from argv[1] until it encounters a null terminator (\0) or until the program crashes. The FIFO page-replacement algorithm, it is computationally
 infeasible to derive S(/rs) from V(kv); in particular, V is a one-way function. When a page is brought into memory, we insert it at the tail of the queue. The operation of Tripwire is controlled by a configuration file tv.conf ig that enumerates the directories and files to be monitored for changes, deletions, or additions. If I/O performance were the only
consideration, the operating system would gladly turn over the responsibility of disk scheduling to the disk hardware. The security provided by this form of protection rests on the assumption that the code generated by the compiler will not be modified prior to or during its execution. Project: Producer-Consumer Problem In Section 6.6.1, we present a
semaphore-based solution to the producerconsumer problem using a bounded buffer. Because devices are a performance bottleneck, another key is to optimize I/O for maximum concurrency. Synchronous and asynchronous communication b. This client-side stub is responsible for creating a parcel consisting of the name of the method to be invoked on
the server and the marshalled parameters for the method. We first cover the POSIX APT for shared memory and then discuss message passing in the Mach operating system. When a process no longer requires access to the shared-memory segment, it detaches the segment from its address 104 Chapter 3 Processes #include #include *include *inclu
main() { /* the identifier for the shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ const int size = 4096; /* allocate a shared memory segment */ co
memory segment */ shared.memory = (char *) shmat (segment_id, NULL, 0); /* now print out the string from shared memory segment */ shmat (shared.memory); /* now print out the shared memory */ printf ("*%s", shared_memory); /* now print out the shared memory */ printf ("*%s", shared_memory); /* now print out the shared memory segment */ shmat (shared_memory); /* now print out the shared memory segment */ shmat (shared_memory); /* now print out the shared memory segment */ shmat (shared_memory); /* now print out the shared memory segment */ shmat (shared_memory); /* now print out the shared memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_memory segment */ shmat (shared_memory); /* now print out the shared_me
memory segment */ shmctl (segment-Id, IPC RMID, NULL); return 0; Figure 3.16 C program illustrating POSIX shared-memory API. The shm ds structure for a given integer segment i d; shm ds shmbuffer; shmctl
(segmented, IPCSTAT, &shmbuf f e r); If successful, shmctl () returns 0; otherwise, it returns -1. Unfortunately, a page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault as it pages in the external page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now cause the virtual memory manager to generate another page fault may now 
:;: h ::: n hi ;: ;:•;!; Figure 14.9 I;:..;!; Figure 14.9 I;:..;!; Figure 14.9 I;:..;!; Stack inspection. We illustrate this #ir.clude #irdude inn mainfint argc, char *argv[]i HANDLE hFile, hKapFile; LPVCID lpMapAddress; hFile = CreateFile ( "temp, txt" , /,/ file name GENERIC-READ | GENERIC-WRITE, // read/write access 0, // no sharing of the file NULL, // default security OPEN-
ALWAYS, /./ open new or existing file FILE-ATTRIBUTEJSIORMAL, // routine file attributes NULL, /./ default security PAGE-READWRITE, // read/write access; o mapped pages 0, // map entire file 0, TEXT("SharedObject")); // named shared memory object lpMapAddress =
MapViewOfFile(hMapFile, // mapped object handle FILE MAP ALLJ\CCESS, // read/write access 0, // mapped view of entire file 0, 0); /./ write to shared memory using
the Win32 API. Exercises 14.1 Consider the ring protection scheme in MULTICS. Please refer to that chapter for specific instructions regarding created a modification called triple DES, in which the DES algorithm is repeated three times (two
encryptions and one decryption) on the same plaintext using two or three keys—for example, c = E\{k^{\circ}(D\{k2)(E(Ki)(m))). To be useful in practice, it should also be reasonably efficient. For a given virtual memory space, decreasing the page size increases the number of pages and hence the size of the page table. One approach is for the main thread
to create and initialize the matrices A, B, and C. The mutex is acquired and released with the pthread mutex lock() and pthreadjmtexjunlockO functions. Cliff Martin also helped with updating the UNIX appendix to cover FreeBSD. The owner is also allowed to receive from the mailbox. The higher levels are expensive, but they are fast. 15.7
Firewalling to Protect Systems and Networks We turn next to the question of how a trusted computer can be connected by the other processes executing in the system. Installation and out of memory as necessary. Installation and the system is independent if it cannot affect or be affected by the other process is independent if it cannot affect or be affected by the other processes executing in the system. Installation and out of memory as necessary. Installation and out of memory as necessary.
communication costs are relatively low for a tree-structured network. If the same key is used for encrypting an extended amount of data, it becomes vulnerable to attack. This approach defines the locality model of process execution. If another portion is required later, another transfer will take place. When a transaction starts executing, its first
action is to execute wa. ±t(mutex). In some cases, another route through the network may be found, so that the messages are able to authenticate the client computers from which requests are received. This choice, however, is a policy decision that the
protection system can implement but should not define. The types of requests vary according to level. Sharing is a means of running many processes with a limited amount of memory, but shared programs and data must be designed carefully. Thus, its scheduling is central to operating-system design. These security problems are management and
 personnel issues, not problems pertaining to operating systems. The number of kernel threads may be specific to either a particular application or a particular machine (an -user thread Figure 4.3 One-to-one model. Perhaps the most obvious is the need to protect the Tripwire program and its associated files, especially the database file,
 from unauthorized modification. 15.13 Why doesn't D{kt,, N)(E{kd. However, rather than copying all data structures, the new task points to the data structures of the parent task, depending on the set of flags passed to clone (). A p o r t s t a t u s () system call returns the number of messages in a given mailbox. After some time, we can determine
which pages have been used and which have not been used by examining the reference bits, although we do not know the order of use. If the shift register contains 00000000, for example, then the page has not been used for eight time periods; a page that is used at least once in each period has a shift register value of 11111111. If the mailbox is full time periods; a page that is used at least once in each period has a shift register value of 111111111.
the sending thread has four options: 1. How the page to be replaced is selected b. Detach and remove the shared-memory segment. Each file and directory are assigned an owner, a group, or possibly a list of users, and for each of those entities, access-control information is assigned. The implementation of RPCs was discussed by Birrell and Nelson
[1984]. Let's look at a buffer-overflow exploit in more detail. If the value is 0, we proceed to replace this page; but if the reference bit is set to 1, we give the page a second chance and move on to select the next FIFO page. More sophisticated disks, such as the SCSI disks used in high-end PCs and most workstations and servers, are smarter about the page.
bad-block recovery. 7.4 Deadlock Prevention 253 Although this method may not seem to be a viable approach to the deadlock problem, it is nevertheless used in most operating systems, as mentioned earlier. Recent versions of AMD and Intel x86 chips include the NX feature to prevent this type of attack. As an example of a message-based operating systems, as mentioned earlier.
system, we next consider the Mach operating system, developed at Carnegie Mellon University. external fragmentation b. At regular intervals (say, every 100 milliseconds), a timer interrupt transfers control to the operating system. It also provides updated coverage of threading in Linux. 9.17 Consider the parameter A used to define the working-set
window in the working-set model. The main—or parent—thread will initialize the matrices A and B. Authentication is a component of many aspects of security For example, it is the core of nonrepudiation, which supplies proof that an entity performed an
action. How the address space is preserved, and what amount of work is needed to preserve it, depend on the memory-management method of the operating system. By default, threads share the memory and the resources of the process to which they belong. This problem is defined as follows. • Writing a file. While the page swap is taking place, a
replacement can be selected, which is then written to the disk as the user process continues to execute. The data stored in the computer system must be protected from unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency. When we exit the function, the process leaves this locality, since the local
variables and instructions of the function are no longer in active use. The processes are expected to exchange information through the use of these shared wariables. Here, we explore the POSIX API for shared memory. The watchdog is invoked whenever a program requests access to the file. 7.2.1 Necessary Conditions A deadlock situation can arise in a contract the processes are expected to exchange information through the use of these shared wariables.
the following four conditions hold simultaneously in a system: 1. Even so, the full bootstrap code may be small. Therefore, it is imperative that the kernel keep a sufficient amount of free memory available. In Linux on the Intel 386 architecture, a system call is accomplished by storing the system call number into the EAX register, storing arguments to
the system call in other hardware registers, and executing a trap instruction (which is the INT 0x80 assembly instruction). When a process creates a new process, two possibilities exist in terms of execution: 1. When a server receives a message, it services the message using a separate thread. The browser virus installed several back-door programs,
including a keystroke logger, which records all things entered on the keyboard (including passwords and credit-card numbers). The server creates a ServerSocket that specifies it will listen to port 6013. After outputting the contents of the updated memory, it detaches and removes the shared-memory region. CPU-bound, 88-89 job vs., 82 in Linux,
750-751 multithreaded, see multithreaded, see multithreaded, 127 state of, 83 as term, 81-82 threads performed by, 84-85 in Windows XP, 830 process-contention scope (PCS), 172 process control blocks (PCBs, task control blocks), 83-84 process-control
system calls, 47-52 process file systems (Linux), 769-770 process identifier (pid), 90 process management, 20-21 in Linux, 748-750 process management, 20-21 in Linux, 20-
XP), 790 processor affinity, 170 processor scheduling vs., 153 910 Index process scheduling vs., 153 910 Index process scheduling vs., 224-225 concurrent transactions, 225-230 log-based recovery, 223-224
system model, 222-223 bounded-buffer problem, 205 critical-section problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers solution, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 217-219 Windows XP, 220-221 monitors for, 209-217 dining-philosophers problem, 207-209, 212-214 examples of: Java, 218 Linux, 221 Pthreads, 221-222 Solaris, 218 Linux, 221 Pthreads, 221-222 Solaris, 218 Linux, 221 Pthreads, 221-222 Solaris, 221
resumption of processes within, 215-217 semaphores, implementation using, 214-215 usage, 210-212 readers-writers problem, 206-207 semaphores for, 200-204 process termination, deadlock recovery by, 266 production kernels (Linux), 739 profiles, 719 programs, processes vs., 82, 83. (A kilobyte, or KB, is 1,024 bytes; a megabyte, or MB, is 1,0242
bytes; and a gigabyte, or GB, is 1,0243 bytes. 9.10 Operating-System Examples 363 9.10 Operating-System Examples In this section, we describe how Windows XP and Solaris implement virtual memory. They vary greatly in speed. For example, embedded computers in home devices and automobiles may have numeric keypads and may turn indicator
lights on or off to show status, but they and their operating systems are designed primarily to run without user intervention. This array is sometimes called the raw disk, and 1 /O to this array is termed raw I/O. Since authenticators are generally exposed (for example, they are sent on the network with the messages themselves), it must not be feasible
to derive S(k) from the authenticators. Note that although certain applications are more efficient when implementing their own special-purpose storage services. The program shown in Figure 3.16 illustrates the POSIX shared-memory APIdiscussed
 above. The controller maintains a list of bad blocks on the disk. He tries again and is successful. They fall into two categories. 5s4 Chapter 14 Protection It can be complicated for the JVM to determine what class is responsible for a request to access a protected resource. One such representation is known as external data representation (XDR).
 Sobig.F included an attachment for the target e-mail reader to click on, again with a variety of names. These 8-bit shift registers contain the history of page use for the last eight time periods. All this waiting time is wasted; no useful work is accomplished. A user could add a personal firewall to her PC so that a Trojan horse would be denied access to
the network to which the PC is connected. The first WAN to be designed and developed was the Arpanet. Example programs were tested on systems running Windows XP. 15.3 System and Network Threats 575 The code included in the attachment was also programmed to periodically attempt to connect to one of twenty servers
and download and execute a program from them. The Pthreads API provides support for mutexes and condition variables. Keep in mind that developing an ordering, or hierarchy, in itself does not prevent deadlock. direction. Systems with fixed-sized allocation units, such as the single-partition scheme and paging, suffer from internal fragmentation.
568 Chapter 15 Security return address; of; mo(li|jed: shell code::;ii :: " ^: NO "OP copied (a) (b) Figure 15.4 Hypothetical stack frame for Figure 15.2, (a) before and (b) after. Any process that does not share data with any other process is independent. For example, it could modify the read system call so that if the file it has modified is read
the original form of the code is returned rather than the infected code. Hence, the I in RAID now stands for "independent" instead of "inexpensive." 12.7.1 Improvement of Reliability via Redundancy Let us first consider the reliability of RAIDs. The chance that some disk out of a set of N disks will fail is much higher than the chance that a specific
single disk will fail. However, research continues to improve anomalydetection techniques. The logical memory and. 230 Chapter 8 Main Memory logical linear. This mapping allows differentiation between logical memory and. 230 Chapter 8 Main Memory logical linear. This mapping allows differentiation between logical memory and 230 Chapter 8 Main Memory logical linear.
schedule possible under the timestamp protocol. Some operating systems provide memory mapping only through a specific system call and use the standard system call to perform all other file I/O. Modern computer systems use disks as the primary on-line storage medium for information (both programs and data). Other issues include thread
cancellation, signal handling, and thread-specific data. Hosts are generally on LANs, which are, in turn, connected to the Internet via regional networks. Since disk access is much slower than memory access, using swap space significantly decreases system performance. A CPU-bound process, in contrast, generates I/O requests infrequently, using
more of its time doing computations. In addition, the selection mask can instruct that the file be monitored for changes. Whatever file was using that block must be repaired (for instance, by restoration from a backup tape), and that requires manual intervention. The file is automatically closed when the job or program that opened the file terminates.
The timestamp protocol ensures conflict serializability. They 3.5 Examples of IPC Systems 107 are really the same but are given different names according to how they are used. This command displays the file prog. • Theft of service. The procedure-call mechanism of Hydra was designed as a direct solution to the problem of mutually suspicious
subsystems. Operating systems also provide support for synchronization. 5.1.1 CPU-I/O Burst Cycle The success of CPU execution and I/O wait. A serial schedule consists of a sequence of instructions from various transactions wherein the
instructions belonging to a particular transaction appear together. In addition, if a particular site is currently overloaded with jobs, some of them may be moved to other, lightly loaded sites. Replace the page that will not be used for the longest period of time. Triple DES is in widespread use today. By providing the user with access to the various
resources that it maintains, a distributed system can improve computation speed and data availability. Disk I/O is done via clusters, effectively assuring that I/O has more sequential-access and fewer random-access characteristics. See also atomic transactions defined, 768 in Linux, 768-769 in log-
structured file systems, 437-138 Transarc DFS, 654 transfer rate (disks), 452, 453 translation coordinator, 669 translation coordinator, 669 translation thread state (Windows XP), 789 translation coordinator, 669 translation coordinator, 669 translation control protocol (TCP), 823 transparency, 633-634, 642
643 transport driver interface (TDI), 822 transport layer, 629 transport-layer protocol (TCP), 584 traps, 18, 321, 502 trap doors, 564-565 tree-structured directories, 389-391 triple DES, 579 triple indirect blocks, 427 Tripwire file system, 597-598 Trojan horses, 563-564 trusted computer base (TCB), 601 trust relationships, 828 tunneling viruses, 571
turnaround time, 157 turnstiles, 219 two-factor authentication, 591 two-factor authentication, 591 two-phase locking protocol, 669-672 two-phase locking protocol, 669-672 two-phase locking protocol, 689-672 two-phase locking protocol, 689-672 two-phase locking protocol, 28 two-phase locking protocol, 689-672 two-phas
UI, see user interface unbounded capacity (of queue), 102 UNC (uniform naming convention), 824 uniform naming convention (UNC), 824 universal serial buses (USBs), 453 UNIX file system (UFS), 413 UNIX operating system:
consistency semantics for, 401 domain switching in, 535-536 and Linux, 737 permissions in, 406 shell and history feature (project), 121-125 signals in, 123, 139-141 swapping in, 284 unreliable communications, 686-687 upcalls, 143 upcall handler, 143 USBs, see universal serial buses used objects, 356, 759 users, 4-5, 397-398 users
accounts, 602 user authentication, 587-592 with biometrics, 591-592 with passwords, 588-591 user datagram protocol (UDP), 631 user datagram protocol (UDP), 632 user datagram protocol (UDP), 631 user datagram protocol (UDP), 631 user datagram pr
user rights (Linux), 778 Index user threads, 129 utility storage, 476 utilization, 840 VACB, see virtual address control block VADs (virtual address descriptors), 802 valid-invalid bit, 295 variable class, 177 variables, automatic, 566 variable timer, 20 VDM, see virtual DOS machine vector programs, 573 vforkO (virtual memory fork), 327 VFS, see
 program structure, 360-361 pure demand paging, 322 919 and restarting instructions, 322-323 and TLB reach, 358-359 direct virtual memory access, 504 and frame allocation, 340-343 equal allocation, 341 global vs. (If the command is to be run in the background, it will end with '&', and setupO will update the parameter background so the mainO
schedule). This situation would result in unacceptable system performance. We require that every transaction 7} has been assigned timestamp TS(Tj-), and later a new transaction 7) enters the system, then TS(7) < TS(Tj).
In the following sections, we elaborate on each of these issues. Even more restrictive, and thus more protective, are systems that simply do not allow a change of user ID. The child process will then modify its copied page and not the page belonging to the parent process. We look at many issues related to multithreaded programming and how it
memory so that the system does not have to read it from disk for each operation. IVipwire operation of system directories and files. All of the disk-bound bootstrap, artd the operation of system directories and files. Transfer time is proportional to the
 amount transferred (that is, the page size)—a fact that would seem to argue for a small page size. Threads in a task can receive only from a mailbox or mailbox set for which the task has receive access. The general idea behind a thread pool is to create a number of threads at process startup and place them into a pool, where they sit and wait for
via msg receive(). The Internet provides the telnet facility for this purpose. The hardware to support demand paging is the same as the hardware for paging and swapping: • Page table. These are the steps to execute this instruction: 1. More detailed analyses of stack inspection, including comparisons with other approaches to Java security, can be
found in Wallach et al. The page table is held in registers. • The process could create a new subprocess's termination. Thus, a reference to byte 53 of segment at long termination was first discussed by
Dennis [1965]. POSIX-compliant systems must implement the POSIX core standard (POSIX.1)—Linux, Solaris, and Mac OS X are examples of POSIX-compliant systems. Communication in client-server systems may use (1) sockets, (2) remote procedure calls (RPCs), or (3) Java's remote method invocation (RMI). 4.3 Thread Libraries A thread library
provides the programmer an API for creating and managing threads. The controller automatically does the ECC processing whenever a sector is read or written. In this case, the set of objects that can be accessed corresponds to the local variables defined within the procedure. 1.1 What Operating Systems Do 5 In other cases, a user sits at a terminal
 connected to a mainframe or minicomputer. Wait at most n milliseconds. One problem with this method is that if a user manages to create a file with user ID root and what would you lose by using this policy rather than LRLr or
 second-chance replacement? It also provides a basis for application programs and acts as an intermediary between the computer user and the computer user and the computer block of the file should be put. Another problem is the time required to read or
write a page. Trap to the operating system. This approach will ensure that only needed pages are read from the file system but that all subsequent paging is done from swap space. Where remote shells were established, the worm program was uploaded and began executing anew. If P, requests the printer and P. In addition to separating logical
memory from physical memory, virtual memory, virtual memory also allows files and memory to be shared by two or more processes through page sharing (Section 8.4.4). A flag indicating if all objects have been signaled 4. 3.6 Communication in Client-Server Systems 109 traveling between the hosts are delivered to the appropriate process based on the destination
port number. An n x m matrix defines the number of resources of each type currently allocated to each process. Local replacement requires that each process select from only its own set of allocated frames. This virus started by infecting hundreds of Windows servers (including many trusted sites) running Microsoft Internet Information Server (IIS)
At that location is the initial bootstrap program. The structure of local procedure calls in Windows XP is shown in Figure 3.17. Another approach to protecting networks from insider attacks is to secure topology or route discovery. The implementation of these algorithms is expensive, and they do not approximate OPT replacement well. The Win32 AP
for creating threads is covered in Section 4.3.2. Windows XP uses the one-to-one mapping described in Section 4.2.2, where each user-level thread maps to an associated kernel thread maps to an associated kernel thread maps to an associated kernel thread. : If a th;raad .attempts to acquire a . We also consider the problem of selecting an algorithm for a particular system. Asynchronous cancellation. Shared memory is
faster than message passing, as message-passing systems are typically implemented using systems are typically implemented in thus require the more timeconsuming task of kernel intervention. # - . Source code. 6.25 Show that the two-phase locking protocol ensures conflict serializability. Paging and segmentation can be as fast if the .mapping table is implemented in
fast registers. Examples of special privileges include backing up files and directories, shutting down the computer, logging on interactively, and changing the system (NFS) protocol uses this method (Chapter 17), as do newer versions of Andrew. • Selective
Theoretically, some programs could access several new page for the instruction execution (one page for the instruction and many for data), possibly causing multiple page faults per instruction and many for data), possibly causing multiple page faults per instruction. The relationship between slabs, caches, and objects is shown in Figure 9.28. First, the binding information may be predetermined, in the form
of fixed port addresses. 10 Chapter 1 Introduction generally decreases, whereas the access time generally increases. A Windows XP application runs as a separate process, and each process may contain one or more threads. A schedule in which each transaction is executed atomically is called a serial schedule. Multi-factor authentication uses three
or more forms. A companion article (Jacob and Mudge [1998a]) described the hardware support necessary for implementation of virtual memory in six different architectures, including the UltraSPARC. A distributed system must provide various mechanisms for process synchronization and communication and for dealing with the deadlock problem
and a variety of failures that are not encountered in a centralized system. : :: : • • - ; • ;: • locks are created in inhe following cad? • ;;...;;...; Next, two thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and thread.twp—^are;:crea|ed, and both tliese threads have access to both mutex locks, thrfac^-cine and threads have access to both mutex locks are threads have access to both mutex l
do.work^twc (), respectively as: shown in Figure 7.1. 24S Chapter 7 Deadlocks:/; Three instances of resource type R± 250 Chapter 7 Deadloc3 R? If a domain is static., we must define the domain to include both read and write access. Different combinations of send() and receive () are possible. Alternatively, we can use a technique known as copy
associated with the user. A faster software technique is to use a just-in-time (JIT) compiler. If a process is allocated memory starting at location 00000 and continuing until it has as much as it needs, it probably will not end exactly on a page boundary. This process continues as shown in Figure 9.12. GREG GAGNE Westminster College WILEY JOHN
WILEY & SONS. Virtually all contemporary operating systems—including Windows XP, Linux, Mac OS X, Solaris, and Tru64 UNIX (formerly Digital UNIX)—support kernel threads. We accomplish this savings by creating a table that has one entry per page of physical memory, indexed by the pair. UUCP has been superseded by PPP, the point-to-poin
protocol. When a bad block is remapped, the controller uses a spare sector from the same cylinder, if possible. 3.2.3 Context Switch As mentioned in 1.2.1, interrupts cause the operating system to change a CPU from its current task and to run a kernel routine. Accept the parameter passed on the command line and perform error checking to ensure
that the parameter is < MAX_SEQUENCE. More sophisticated thread-pool architectures can dynamically adjust the number of threads in the pool according to usage patterns. For instance, the code might check for a specific user ID or password, and it might circumvent normal security procedures. But do external page tables negate the utility of
inverted page tables? This manager uses algorithms optimized for speed rather than for storage efficiency, because swap space is accessed much more frequently than file systems (when it is used). Under this definition, a subsystem (or partition) may consist of a single node. In this section, we discuss the Intel Pentium architecture, which supports
both pure segmentation and segmentation and disinfection. Because they keep information about which virtual memory page is stored in each physical frame, inverted page tables reduce the amount of physical memory
needed to store this information. To improve this time, we have added an associative memory reference if the page-table entry is in the associative memory. -i ... How can these problems be limited or eliminated? 14.9.2 Protection in Java Because Java was designed to run in a distributed environment, the Java
virtual machine—or JVM—has many built-in protection mechanisms. We discuss these methods in Section 7.4. Deadlock avoidance requires that the operating system be given in advance additional information concerning which resources a process will request and use during its lifetime. 2.13 In what ways is the modular kernel approach similar to these methods in Section 7.4. Deadlock avoidance requires that the operating system be given in advance additional information concerning which resources a process will request and use during its lifetime.
layered approach? Additions include a full description of the WAFL file system and inclusion of Sun's ZFS file system. On the server side, the XDR data are unmarshalled and converted to the machine-dependent representation for the server. For example, a secret-level user could access a file at the confidential level in the absence of other access
controls. Organization of This Book The organization of this text reflects our many years of teaching operating systems courses. The interrupt routine is called indirectly through the table, with no intermediate routine needed. Solaris, for example, sviggests setting swap space equal to the amount by which virtual memory exceeds pageable physical
memory. Linux originally used the buddy system; however, beginning with version 2.2, the Linux kernel adopted the slab allocator. [2002], Kaashoek et al. Then, in Chapter 18, we describe the methods necessary for distributed operating systems to coordinate their actions. The other part, containing the capability list, is accessible only by the
operating system. : •: • •: •-::••;. Then the importance of suitable language notations in which to express protection requirements will be recognized more widely. For example, while it is useful to leave behind a back-door daemon that provides information or allows easy access
even if the original exploit is blocked. In fact, in 2004 a new and widespread virus was detected. If only fixed-sized messages can be sent, the system-level implementation is straightforward. This activity is particularly nefarious, since a search of the program will not reveal any problems. 14.4 Access Matrix ——. Prepaging is an
attempt to prevent this high level of initial paging. Chapter 9, Automatic working-set trimming works by evaluating the number of history bits and the frequency of interrupts (for example, 10 bits and interrupts every 1,000
references). The first concerns the amount of time required to create the thread prior to servicing the request, together with the fact that this thread will be discarded once it has completed its work. They can even bypass the security added by firewalls (Section 15.7). This arrangement allows multiprogramming to maintain CPU utilization but
requires additional time to resume the page-fault service routine when the I/O transfer is complete. We discuss these issues in Section 7.7. If a system neither ensures that a deadlock will never occur nor provides a mechanism for deadlock detection and recovery, then we may arrive at a situation where the system is in a deadlocked
state yet has no way of recognizing what has happened. Each process is actively using the pages in its working set. Note that the laser printer can be accessed only by a process executing in domain Do- Figure 14.3 Access matrix. b. Are there any disadvantages to this address-translation system? Most communication in Mach—including most of the
system calls and all intertask information— is carried out by messages. Discuss two pros and two cons of using watchdogs for security. The principal distinction is that the security of this protection will not be as great as that supported by a protection kernel, because the mechanism must rely on more assumptions about the operational state of the
            ' - : ' - - ' i d ! e - ' ::; :i; :;;;;;; : is written to the log. : i ! : ': ' . If the source code package has been previously installed on your machine, the corresponding files might be available under / u s r / s r c / ! i n u x or / u s r / s r c / ! i r m x - 2 . The header and trailer contain information used by the disk controller, such as a sector number and an
error-correcting code (ECC). This formatting enables the manufacturer to test the disk and to initialize the mapping from logical block numbers to defect-free sectors on the disk. Conversely, if the page-fault rate is too low, then the process may have too many frames. The issue of concurrent reading and writing was discussed by Lamport [1977]. We
mainly use site to indicate the location of a machine and host to refer to a specific system at a site. The operating system acts as the manager of these resources. Such attacks can, for example, result in passing of liability to an innocent party or modification of the source code of an important commercial application. object I laser printer F '3 domain:
read; rti swifcfi ;l :; :| ;pf|n| react vyfilf yfite !;; | swiich swiiah Figure 14.4 Access matrix of Figure 14.3 with domains as objects. Other techniques for enforcing protection include sandboxing (Goldberg et al. How do we resolve conflicting demands for the network's use, given that it is a shared resource? If we allow the two transactions to overlap their
execution, then the resulting schedule is no longer serial. Then, a process executing in domain DT could modify domain D4, as shown in Figure 14.7. The copy and owner rights provide us with a FIFO replacement algorithm. If successful
CreateSemaphoreO returns a HANDLE to the mutex lock; otherwise, it returns NULL. [1987], Schneier [1996], and Stallings [2003] explore the use of cryptography in computer systems. For example, a 12-KB slab (comprised of three continguous 4-KB pages) could store six 2-KB objects. Ultimately, there must exist a relationship between user
threads and kernel threads. WaitForMultipleObjectsO is passed four parameters: 1. This scheme is shown in Figure 8.21. Similarly, the service program may have some private files (for accounting purposes, 14.8 Capability-Based Systems 549 for example) that should not be accessed directly by the calling user program. Typically, RPC servers are
multithreaded. 9.4 Page Replacement In our earlier discussion of the page-fault rate, we assumed that each page faults at most once, when it is first referenced. Otherwise, the effective access time increases, slowing process execution dramatically. Can a subset of the rights associated with an object be revoked, or must we revoke all access rights for
this object? If a page fault occurs while we are fetching an operand, we must fetch and decode the instruction again and then fetch the operand. In 1998, the United States Department of Justice filed suit against Microsoft, in essence claiming that Microsoft included too much functionality in its operating systems and thus prevented application
vendors from competing. If processes are thrashing, they will be in the queue for the paging device most of the time. 14.5 Discuss the strengths and weaknesses of implementing an access matrix using access lists that are associated with objects. Assume that a client wishes to invoke a method on a remote object server with a signature
someMethod(Object, Object) that returns a boolean value. This in turn allows the server to invoke methods on B remotely. The finger utility functions as an electronic telephone directory; the command finger user-name@hostname returns a person's real and login names along with other information that the user may have provided, such as office and
home address and telephone number, research plan, or clever quotation. A final issue with firmware is that it is relatively expensive, so usually only small amounts are available. Each process opens a file in an access mode. Using this approach, the file system itself serves as the backing store. Included are problems and exercises with solutions not
found in the text that should help students master the concepts presented. 8.15 Compare the segmented paging scheme with the hashed page tables scheme for handling large address spaces. These differences imply major variations in the speed and reliability of the communications network, and they are reflected in the distributed operating-system
design. hProcess—that it is waiting for to complete. Fortunately, the servers were disabled before the code could be downloaded. The application programs can be considered clients of the Windows XP subsystem server. •, 1; • i = Examples of synchronous signals include illegal memory access and division by 0. The specific problem is how to prevented.
thrashing. Figure 4.1 illustrates the difference between a traditional single-threaded process and a multithreaded process. Using trial and error, or by examining the source code of the attacker determines the vulnerability and writes a program to do the following: 1. The file system consists of two distinct parts:
a collection of files, each storing related data, and a directory structure, which organizes and provides information about all the files in the system. In a system with many files, the size of the directory itself may be megabytes. Note that this arrangement is not entirely accurate, because we cannot tell where, within an interval of 5,000, a reference
occurred. Chapter 1 Introduction i | 1 • I compiler i user 2 user 3 assembler text editor; user i database system computer hardware Figure 1.1 Abstract view of the components of a computer system and application programs operating system and application programs operating system.
by two transactions, To and T\. Targeting Sun Microsystems' Sun 3 workstations and VAX computers running variants of Version 4 BSD UNIX, the worm quickly spread over great distances; within a few hours of its release, it had consumed system resources to the point of bringing down the infected machines. • Authentication algorithms generally
keeping each routine completely in one page. Readers interested in pursuing the details on process creation and management in the Win32 API are encouraged to consult the bibliographical notes at the end of this chapter. Where should the "salt" be stored, and how should it be used? This combination has given him the peace of mind to focus on the
writing of this text. One solution is to ensure that a critical section of code is in use by only one process or thread at a time. For example, if a client sends the server will respond with the exact data it received from the client—that is, Hello there! the server using the Java networking API described in
allowed. We can achieve this minimization by distributing heavily used pages evenly over all of memory, rather than having them compete for a small number of page frames. This edition has many new exercises and accompanying solutions, which were supplied by Arvind Krishnamurthy. References cannot be forged, and the manipulations are made
only through well-defined interfaces. Chapter 13, I/O Systems, is the old Chapter 13 updated with coverage of new material. Write a monitor using this scheme to implement the readerswriters problem. As this feature becomes prevalent, buffer-overflow attacks should greatly dimmish. Cryptography enables a recipient of a message to verify that the
ability of the access-matrix model to allow the implementation and control of dynamic protection requirements. This timestamp is assigned by the system 6.9 Atomic Transactions 229 before the transaction T, starts execution. 9.8.2 Slab Allocation A second strategy for allocating kernel memory is known as slab allocation. Not all of these steps are
necessary in every case. It would be hard to detect because under normal operations, there would be no security hole. Rather than limiting communication to (and possibly from) a given host. But this requirement means that every segment accessible in D, is also accessible in D. The "." tells the shell
D. To optimize system-call performance, the kernel assembles routines within kernel is 76 Chapter 2 Operating-System Structures the label associated with the new kernel allowing you to choose it dliring bootup process. The first
case is an attack that uses so many facility resources that, in essence, no useful work can be done. Can these be used for memory protection? If successful, CreateMutexO returns a HANDLE to the mutex lock; otherwise, it returns NULL. • Swap the write(B) operation of To with the read(A) operation of To with the read(A) operation of To with the read(B) operation 
messages? ^ r e q u e s t for worm worm sent target system ;: worm infected system Figure 15.6 The Morris Internet worm. Explain your answers. Processes can then exchange information by reading and writing data to the shared region. The main requirement for secondary storage is that it be able to hold large quantities of data permanently.
These shared pages are marked as copy-on-write pages, meaning that if either process writes to a shared page, a copy of the shared page is created. Process P3 is waiting for either process P\ or 7.2 Deadlock Characterization 251 R Figure 7.3 Resource-allocation graph with a deadlock. Chapter 1 Introduction The straightforward method for handling
this transfer would be to invoke a generic routine to examine the interrupt information; the routine, in turn, would call the interrupt information; the may select only one of these three copy rights, or it may provide all three by identifying them as separate rights: copy, transfer, and limited copy. The two-phase locking protocol
ensures conflict serializability (Exercise 6.25). It is this separate program that will run as a child process outputting the Fibonacci sequence. There is still the matter of managing a public key per party to be communicated with, but since public keys need not be secured, simple storage can be used for that key ring. The data structures for swapping on
Linux systems are shown in Figure 12.10. In doing so, we use the reference string 7, 0,1, 2, 0, 3, 0, 4, 2, 3, 0, 3, 2,1, 2, 0, 1, 7, 0,1 for a memory with three frames. • Chapter 22, XP, has been updated. Ready to continue, the low-priority process enters the ready queue and waits for the CPU. However, demand paging is the operating system's attempt
          rove the computer system's utilization and throughput. Consider a schedule S in which there are two consecutive operations O, and Oj of transactions T, and Tj, respectively. Table entry contain the unique name of the object. The skeleton ther
marshals the return value (or exception, if any) into a parcel and returns this parcel to the client. In fact, these so-called "S-boxes" are classified by the United States government. A vector of length m indicates the number of activities to do at
home, sorted by age and grade level. Storyline Online One of the most well-known sites where you'll find free online books for kids is Storyline Online. Global replacement allows a process to select a replacement frame from the set of all frames, even if that frame is currently allocated to some other process; that is, one process can take a frame from the set of all frames.
another. In Chapter 14, we discussed mechanisms that the operating system can provide (with appropriate aid from the hardware) that allow users to protected (that is, a privileged) procedure, which may be written by an application programmer
as part of a subsystem. General discussions concerning the mutual-exclusion problem were offered by Lamport [1986] and Lamport [1991]. The most common is masquerading, in which one participant in a communication pretends to be someone else (another host or another person). [2000] examine the distributed denialof-service attack and propose
IP trace-back solutions to address the problem. Some studies have shown that object-oriented programs also tend to have a poor locality of reference. • receive(A, message)—Receive a message from mailbox A. 14.4 Access Matrix Our model of protection can be viewed abstractly as a matrix, called an access matrix. Aside from explicit loads and
stores, the CPU automatically loads instructions from main memory for execution. The presence of a record in the log allows the system to streamline its recovery procedure. Meanwhile, the CPU is given to other processes. Shared memory allows maximum speed and convenience of communication, as it can be done at memory speeds when within a
computer. We can use demand paging to reduce the number of frames allocated to a process. Dhall, Thomas Doeppner, Caleb Drake, M. There are various modes in which a data item can be locked. CHAPTER OBJECTIVES • To describe the benefits of a virtual memory system. In addition, a B2 system supports covert channels and the auditing of
events that could lead to the exploitation of a covert channel. In contrast, in shared-memory systems, system calls are required only to establish shared-memory regions. The system-wide table contains process-independent information, such as the location of the file on disk, access dates, and file size, provided as either a user- or kernel-level library.
Solomon and Russinovich [2000] and Stevens [1999] outlined interprocess communication in Windows 2000 and UNIX respectively. g. The operating system in such cases is designed to maximize resource utilization—to assure that all available CPU time, memory, and I/O are used efficiently and that no individual user takes more than her fair share.
class files from both the Java program and the Java API for execution by the Java interpreter. If a process has only four LWPs, then the fifth request must wait for one of the LWPs to return from the kernel. We provide a programming exercise at the end of this chapter using shared memory with memory mapping in the Win32 API. In addition to
requiring that we solve the major problems of page replacement and frame allocation, the proper design of a paging system requires that we consider page size, I/O, locking, prepaging, process creation, program structure, and other issues. • POSIX. Exercises 3.1 Describe the differences among short-term, medium-term, and longterm scheduling.
Suppose that a program is provided that can be invoked as a service by a number of different users (for example, a sort routine, a compiler, a game). h. Now, we need to consider only the operations possible on these new objects (domains and the access matrix) and decide how we want processes to be able to execute these operations. • To describe
the various countermeasures to security attacks. Large commercial systems containing payroll or other financial data are inviting targets to thieves. The question is whether the cost of the s*a saved page faults is greater or less than the cost of prepaging s * (1 — a) unnecessary pages. Whenever the paging device is idle, a modified page is selected
and is written to the disk. The producer merely invokes the blocking sendO call and waits until the message is delivered to either the receiver or the mailbox. When process O completes its execution, it sends the needed result back to P via the message system. It's especially important for first graders because they're still learning language, and
reading helps them understand the sounds and patterns words make. 6.9 Atomic Transactions 227 read(A) write(B) read(B) read(B) write(B) read(B) read
program so that execution jumps to its code. For example, in a transaction-processing system, we might service each transaction in a separate thread e. Two parameters passed to CreateProcess () are instances of the STARTUPINFO and PROCESSINFORMATION structures. In addition, a threat is the potential for a security violation, stich as the
discovery of a vulnerability, whereas an attack is the attempt to break secvirity. A design of a reliable RPC mechanism was described by Shrivastava and Panzieri [1982] and Staunstrup [1982] discussed procedure calls versus message-passing communication. Several soft
errors could trigger a process in which a copy of the block data is made and the block is spared or slipped. We can also view a computer system as consisting of hardware, software, and data. Like Mach, Windows XP uses a port object to establish and maintain a connection between two processes. Real-time systems may require not only that
computed results be "correct" but also that the results be produced within a specified deadline period. Knuth [1973] discussed the 50-percent rule. In addition, it is possible that, for a given set of transactions, there are conflict-serializable schedules that cannot be obtained by use of the two-phase locking protocol. The names of user-defined
procedures must be identified to the protection system if it is to deal with objects of the userdefined type. Network packets arrive with a source address, such as an IP address. The long-term scheduler, or job scheduler, or job
across the network to even the workload. If access is denied, an exception condition occurs. As we have already seen, the user's view of memory is not the same as the actual physical memory. An operating system (and, indeed, software in general) should allow fine-grained control of access and security, but it must also be easy to manage and
understand. physical address space, 279-280 paging for management of, 288-302 basic method, 289-295 hashed page tables, 301-302 protection, 295-296 and shared pages, 296-297 segmentation for management of, 302-305 basic method, 302-305 basic method, 302-305 basic method, 302-305 basic method, 289-296 and shared pages, 296-297 segmentation for management of, 288-302 basic method, 289-296 and shared page tables, 301-302 protection, 295-296 and shared pages, 296-297 segmentation for management of, 302-305 basic method, 302-30
304 hardware, 304-305 Intel Pentium example, 305-307 and swapping, 282-284 majority protocol, 673-674 MANs (metropolitan-area networks), 28 mandatory file-locking mechanisms, 379 man-in-the-middle attack, 561 many-to-many multithreading model, 130-131 many-to-one multithreading model, 129-130 marshalling, 825 maskable interrupts,
501 masquerading, 560 mass-storage management, 23-24 mass-storage structure, 451-454 disk attachment: host-attached, 455 network-attached, 455 network-att
-. Restart the user process. Please send correspondence to [email protected] Acknowledgments This book is derived from the previous editions, the first three of which were coauthored by James Peterson. The major problem with message systems has generally been poor performance caused by double copying of messages; the message is copied first
from the sender to the mailbox and then from the mailbox to the receiver. Pages allocated to user-mode processes do not necessarily have to be in contiguous physical memory. This model uses a parameter, A, to define the working-set window. • Learn how to configure, compile, and install the kernel binary. However, the Win32 API also provides the
WaitForMultipleObjectsQ function, which is used when waiting for multiple threads to complete. Java is a widely used programming language with a rich API and built-in language support for thread creation and management. Notice that, with either equal or proportional allocation, a high-priority process is treated the same as a low-priority process.
When the setuid bit is on, the userID is set to that of the owner of the file: B. Examples of such signals iiiclude terminating a process with specific keystrokes (such as ) and having a timer expire. However, POSIX Pthreads also provides the pthreads also pthreads a
specified thread (tid.) Although Windows does not explicitly provide support for signals, they can be emulated using asynchronous procedure calls (APCs). Virtual memory is not easy to implement, however, and may substantially decrease performance if it is used carelessly. For instance, if the attacker sends the part of the protocol that says "I want
to start a TCP connection/ but never follows with the standard "The connection is now complete," the result can be partially started TCP sessions. However, the increased hit ratio and TLB reach offset the performance costs. In this section, we look at three common ways of establishing this relationship. Ideally, the working set for a process is stored
in the TLB. A lazy swapper never swaps a page into memory unless that page will be needed. To see why, let's compute the effective access time for a demand-paged memory. New objects and new domains can be created dynamically and included in the access-matrix model. If the sum of the working-set sizes increases, exceeding the total number of
available frames, the operating system selects a process to suspend. Conversely, if the multiprogramming level decreases, the frames that were allocated to the departed process can be spread over the remaining processes. 12.5.3 Bad Blocks Because disks have moving parts and small tolerances (recall that the disk head flies just above the disk
surface), they are prone to failure. Generally, one host at one site, the server, has a resource that another host at another detailing developments in the relatively new area of multimedia systems, is a new chapter detailing developments in the relatively new area of multimedia systems, and the number of resources and the number of resources are not necessarily.
available resources are declared as follows: #define MAXJIESDURCES 5 int available resources a v a i l a b l e, *//* otherwise return - 1 */ int
decrease.count(int count) { if (available resources -= count; return 0; When a process wants to return a number of resources, it calls the decrease count() function: /* increase available resources += count; return 0; When a process wants to return a number of resources, it calls the decrease count() function: /* increase available resources += count; return 0; When a process wants to return a number of resources.
segment produces a race condition. A process can be restarted only when it is allocated the new resources it is requesting and recovers any resources that were preempted while it was waiting. Research into system-call-based anomaly detection is described in Forrest et al. The server then begins listening to the port with the accept () method. In
contrast, with only one frame available, we would have a replacement with every reference, resulting in eleven faults. : For example, if clone() is passed the flags CLONE FS, CLONEJM, CLONE SIGHAND, and CLONE FILES, the parent and child tasks will share the same file-system information (such as the current working directory), the same
memory space, the same signal handlers, and the same set of open files. In the next two subsections, we look at two higher-level methods of communication: remote procedure calls (RPCs) and remote method invocation (RMI). Think about what might happen if a process had only two frames. Another common form of virus transmission uses Microsoft
Office files, such as Microsoft Word documents. For example, a compiler may produce assembly code, which is consumed by an assembler. Although Robert Morris designed the self-replicating program for rapid reproduction and distribution, some of the features of the UNIX networking environment provided the means to propagate the worm
throughout the system. 376 Chapter 10 File-System must be found for the file system must reuse its open-file table entries, or it could run out of
space in the table. Numerous protocols also have been developed for use by applications, but then the applications, but then the applications themselves must be coded to implement security. Locked pages cannot be replaced. If the number of frames is increased, these n pages will still be the most recently referenced and so will still be in memory. Also, it may be desirable to
guarantee the order of a set of disk writes to make the file system robust in the face of system crashes. Of course, adding physical memory increases the number of frames. Routines that call each other many times can be packed into the same page. The operation returns an index into this table for the newly opened file. In this project, we will design a
programming solution to the bounded-buffer problem using the producer and consumer processes shown in Figures 6.10 and 6.11. Absolute protection of the information stored in a computer system from malicious abuse is not possible; but the cost to the perpetrator can be made sufficiently high to deter most, if not all, attempts to access that
information without proper authority. Reads and writes to these memory addresses cause the data to be transferred to and from the device registers. Numerous systems implement the Pthreads specification, including Solaris, Linux, Mac OS X, and Tru64 UNIX. The sender never blocks. 0002 Write permission of world. The operating system can treat
each partition as though it were a separate disk. In addition, the system administrator can selectively audit the actions of any one or more users based on individual identity. A stack overflow could allow the launching of an unauthorized process. Linux also provides the ability 4.5 Operating-System Examples 145 ETHREAD •\: i :tteeacfi;sfer{;i .\:\
KTHREAD ::;•.;:. sa_handler = handle.SIGINT; sigaction(SIGINT; chandler, NULL)• /* generate the output message */ strcpy(buffer, "Caught Control C"); /* loop until we receive */ while (1) return 0; Figure 3.26 Signal-handling program. Security experts continue to evaluate methods to decrease or eliminate worms. io . Some operating systems are
flexible and can swap both in raw partitions and in file-system space. The two communications models are contrasted in Figure 3.13. satisfies kL.kj mod (p ~ \){q - 1} = 1. In this scheme, a process can communicate with some other process via a number of different mailboxes. The setup () function reads in the user's next command (which can be up
to 80 characters), and then parses it into separate tokens that are used to fill the argument vector for the command to be executed. [1998], Goodman et al. What restrictions need to be put on the await statement so that it can be implemented efficiently? Page 1 is then replaced by page 0. Slab allocators assign kernel data structures to caches
associated with slabs, which are made up of one or more physically contiguous pages. The processes share the following variables: enum pstate {idle, want_in, in_cs}; pstate flag[n]; int turn; All the elements of flag are initially idle; the initial value of turn is immaterial (between 0 and n-1). This allows the server to service several concurrent requests.
The ready queue contains all the processes that are teady to execute and are waiting for the CPU. The algorithm used to determine which page to remove from a working set depends on the type of processor. 1 | «————1 ~~ Figure 9.7 Before process 1 modifies page C. Context-switch times are highly dependent on hardware support. Describe
possible uses for a mechanism that has neither of these guarantees. This allows a thread to check whether it should be canceled at a point when it can be ca
```

```
or nansignaled. The kernel requests memory for data structures of varying sizes, some of which are less than a page in size. It also modified the Windows registry. The classic process-coordination problems that we have described are paradigms for a large class of concurrency-control problems. • Delete a mailbox. 6.6 Explain why interrupts are not
appropriate for implementing synchronization primitives in multiprocessor systems. The first type of authentication algorithm uses symmetric encryption. In between, we are still left with significant choice in frame
allocation. Swap-space allocation is discussed in Chapter 12. In schedule 1 of Figure 6.22, the sequence of instructions of To appearing in the left column and instructions of To appearing in the right column. Even if the sender changes to the ID of someone else, there might be a
record of that ID change. Commonly, the sending thread expects a reply; so the mailbox name of the sender is passed on to the receiving task, which can use it as a "return address." The variable part of a message is a list of typed data items. location that the processor can start executing when powered up or reset. Your task is to incorporate a new
system call into the kernel, thereby expanding the functionality of the operating system. For example, systems commonly keep a pool of free frames. Pure demand paging never brings in a page until that page is referenced. All rights reserved. 15.14 Discuss how the asymmetric encryption algorithm can be used to achieve the following goals. The
program would run within the user's domain, allowing the program to do anything that the user is allowed to do, including deleting the user's files, for instance. bit. 15.6 Implementing Security Defenses 597 THE TRIPWIRE FILE SYSTEM An example of an anomaly-detection tool is the Tripwire file system integritychecking tool for UNIX, developed at
Purdue University. User-level threads are 
needed to record the information that defines the state of the computer system and the status of the system's jobs. In the example given, for instance, we can release the DVD drive and disk file. We generally think of a server as a producer
and a client as a consumer. The Microsoft SMB protocol (running on top of either TCP/IP or the Microsoft NetBEUI protocol) also allows file sharing over a network. The client creates a Socket and requests import java.io.*; public class DateClient { public static void main(String[] args) { try { //make connection to server socket
Socket sock = new Socket("127.0 . Typically, it is stored in read-only memory (ROM) or electrically erasable programmable read-only memory (EPROM), known by the general term firmware, within the computer hardware. It
access(/,/) includes the oivner right, then a process executing in domain D, can add and remove any right in any entry in column /'. On systems that do not include a file offset as part of the readwrite location as a current-file-position pointer. Suppose a user wanted to communicate with
N other users privately. This file operation is also known as a file seek. Because of these capabilities of Java, protection is a paramount concern. The problem is that changing this bootstrap code requires changing the ROM, hardware chips. • Deleting a file. Each such table looks like the traditional per-process page*table and contains information on
where each virtual page is located. Even authorized users, however, may be "encouraged" to let others use their access (in exchange for a bribe, for example). 7.4.3 No Preemption The third necessary condition for deadlocks is that there be no preemption of resources that have already been allocated. An outline of the producer and consumer threads
appears as: #include < s t d l i b . That is, for each k e K, E (k) is a function for generating ciphertexts from messages. The primary distinction between these two schedulers lies in frequency of execution. • To discuss the APIs for Phtreads, Win32, and Java thread libraries. A Hydra subsystem is built on top of its protection kernel and may require
protection of its own components. A program is generally composed of several different localities, which may overlap. Deadlock problems can only become more common, given current trends, including larger numbers of processes, multithreaded programs, many more resources within a system, and an emphasis on long-lived file and database
 servers rather than batch systems. The first approach to meeting this requirement is to place the entire logical address space in physical memory. There are limits to the flexibility of a protection kernel in implementing a user-defined policy, although it may supply adequate facilities for the system to provide enforcement of its own policies. Morris's
legal costs probably exceeded $100,000. We wrote this book as a text for an introductory course in operating systems at the junior or senior undergraduate level or at the first-year graduate level. • We can ignore the problem altogether and pretend that deadlocks never occur in the system. For this reason, most systems store a tiny bootstrap loader
program in the boot ROM whose only job is to bring in a full bootstrap program from disk. For these reasons, protection can no longer be considered a matter of concern to only the designer of an operating system. Although this assumption is true for a non-demand-paging environment, where a page fault represents a fatal error, it is not true where a
page fault means only that an additional page must be brought into memory and the process restarted. SSL (Section 15.4.3), for example, provides security at the transport layer. 538 Chapter 14 Protection The main disadvantage of the ring (or hierarchical) structure is that it ctoes not allow us to enforce the need-to-know principle. All mutex
 functions return a value of 0 with correct operation; if an error occurs, these functions return a nonzero error code. If scanrate is 100 pages per second and lmndspread is 1,024 pages, 10 seconds can pass between the time a bit is set by the front hand and the time it is checked by the back hand. For example, within a computer, the operating system
usually can determine the sender and receiver of a message. Figure 7.4 Resource-allocation graph with a cycle but no deadlock. 10. The highest-level classification is division A. Recent releases of the Solaris kernel have provided enhancements of the paging algorithm. Named 11.c, the grappling hook consisted of 99 lines of C code compiled and run
on each machine it accessed. create a FIFO queue to hold all pages in memory. The type of access, however, is restricted according to the access bits associated with that segment. For instance, if a system wished to allow other systems to be able to list its current users, it would have a daemon supporting such an RPC attached to a port—say, port
3027. For example, the signal SIGINT represents the signal for terminating a program with the control sequence . TER Introduction An operating system is a program that manages the computer system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introduction An operating system is a program with the control sequence . TER Introductio
may be interested in the same piece of information (for instance, a shared file), we must provide an environment to allow concurrent access to such information. Having found the associated directory entry, we release all file space, so that it can be reused by other files, and erase the directory entry. Symmetric encryption requires a shared key, while
asymmetric encryption provides a public key and a private key. At a higher level, the command interpreter or shell provides a mechanism for a user to issue a request without writing a program. This theft of service is not even considered a crime in most countries! Spyware is a micro example of a macro problem: violation of the principle of least
privilege. p» .: All the directories in such a search path must be secure, or a Trojan horse could be slipped into the user's path and executed accidentally. 15.3.2 Port Scanning is not an attack but rather is a means for a cracker to detect a system's vulnerabilities to attack. Second, binding can be done dynamically by a rendezvous
mechanism. We replace the first page encountered in the lowest nonempty class. Although most program examples in this text use C, we will illustrate sockets and has a rich library for networking utilities. Computer break-ins are discussed by Lehmann [1987] and by Reid [1987]. Thus, it
optimizes CPU utilization. Find a free frame: a. If a small student process of 10 KB and an interactive database of 127 KB are the only two processes running in a system with 62 free frames, it does not make much sense to give each process of 10 KB and an interactive database of 127 KB are the only two processes running in a system with 62 free frames, it does not make much sense to give each process of 10 KB and an interactive database of 127 KB are the only two processes running in a system with 62 free frames.
possible to pass objects as parameters to remote methods. The system call numbers for recent versions of the Linux kernel are listed in / u s r / s r c / l i n u x ~ 2 . We find a free frame (by taking one from the free-frame list, for example). See also mass-storage structure holographic, 480 nonvolatile, 10, 223 secondary, 9, 411 stable, 223 tertiary, 24
utility, 476 volatile, 10, 223 storage-area networks (SANs), 15, 455, 456 storage management, 22-26 caching, 24—26 I/O systems, 26 mass-storage management, 23-24 stream head, 520 stream head, 5
114, 281 stub routines, 825 superblock, 414 superblock, 414 superblock objects, 419, 765 supervisor mode, see kernel mode suspended state, 832 sustained bandwidth, 484 swap map, 468 swap-space management, 466^168 switch architecture, 11 switching: circuit,
626-627 domain, 535 message, 627 * packet, 627 symbolic links, 794 symbolic-link objects, 794 symmetric mode, 15 symmetric mode, 16 symmetric mode, 16 symmetric mode, 16 symmetric mode, 16 symmetric mode, 17 symmetric mode, 17 symmetric mode, 17 symmetric mode, 17 symmetric mode, 18 symmetric mode
worm is a process that uses the spawn mechanism to ravage system performance. The receive operation must specify the mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from which a message is to be received- A mailbox set from the 
loads a class in response to a request to create instances (or objects) of that class. A personal firewall is a software layer either included with the operating system or added as an application. (See Bibliographical Notes for references.)
contains. If we want a particular task to run faster, we must break it into subtasks, each of which will be executing in parallel with the others. The disk operation might be read, write, rename, delete, or status, corresponding to the usual file-related system calls. Since only a predefined number of interrupts is possible, a table of pointers to
interrupt routines can be used instead to provide the necessary speed. requests the DVD drive, a deadlock occurs. In addition, if the source and destination blocks overlap, the source and destination blocks overlap, the source and destination blocks overlap, the source block may have been modified, in which case we cannot simply restart the instruction. The object for a 14.8 Capability-Based Systems 547 capability and its table entry
must match. For instance, if there are 93 frames and five processes, each process will get 18 frames. Linux, along with the family of Windows operating systems—including with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the File to be mapped with the Cr e at the F
function, which returns a HANDLE to the opened file. In practice, very few modern operating systems implement swapping in this fashion. It may well be the case that many of the pages brought back into memory by prepaging will not be used. Also, the user should be able to run the most recent command again by just entering V. • The least
frequently used (LFU) page-replacement algorithm requires that the page with the smallest count be replaced. The presentation is motivational and explanatory in nature. If a process does not have enough memory for its working set, it will thrash. Hydra, the Cambridge CAP system, and Mach are capability systems that extend protection to user-
defined software objects. The easiest approach with Pthreads and Win32 is to create a data structure using a structure u
the beginning for both protocols. 15.3 System and Network Threats Program threats typically use a breakdown in the protection mechanisms of a system to attack programs. It then reports a recoverable soft error. • Certain options and features of a program may be used rarely. For most computer systems, the memory-access time, denoted ma,
ranges from 10 to 200 nanoseconds. Here, we explore the most important aspects of the parts of cryptography that pertain to operating systems. • Memory management. However, the number of links grows as the square of the number of sites, resvilting in a huge installation cost. This information may be kept for creation, last modification, and last
use. We can require that the operating system allocate all its buffer and table space from the free-frame list. Each is waiting for the event "CD RVV is released," which can be caused 7.2 Deadlock Characterization 247 only by one of the other waiting processes. 140 Chapter 4 Threads When a signal is generated by an event external to a running
process, that process receives the signal asynchronously. Recall from Chapter 3 that RPCs allow interprocess communication by providing a communication by provid
parameters: (1) the HANDLE of the semaphore, (2) the amount by which to increase the value of the semaphore, and (3) a pointer to the previous value of the semaphore. This loss is only 256 bytes for a page of 512 bytes but is 4,096 bytes for a page of 512 bytes but is 4,096 bytes for a page of 512 bytes.
executed. A Cl environment is one in which cooperating users access data at the same levels of sensitivity. The skeleton is responsible for unmarshalling the memorymanagement unit (MMU) to map logical pages to physical page frames in memory. The message contains the
disk operation to be performed. Once installed, the virus may do any one of a number of things. Hydra solves this problem by restricting amplifications. Message passing is useful for exchanging smaller amounts of data, because no conflicts need be avoided. Specifying the type of operations that a particular process may invoke on an allocated
resource (for example, a reader of a file should be allowed only to read the file, whereas a writer should be impossible for a process to enlarge its set of access rights, except with the authorization of the access-control
mechanism. For multiple CPU systems, each CPU must be described. An alternative to this method used in other operating systems is to place privileged programs in a special directory. The decryption algorithm is then D(kd,N)(c) = ck-> modN. The amount of swap space needed on a system can therefore vary depending on the amount of physical
memory, the amount of virtual memory it is backing, and the way in which the virtual memory is used. These chapters describe the classic internal algorithms and structures of storage management. However, modern systems may now use much larger page sizes, as we will see in the following section. • Alternatively, the address space associated
with a program can be split into two parts. If several processes attempt to open a read-only file at the same time, they can be granted simultaneous access to the file. Object serialization allows the state of an object to be written to a byte stream. The program will then create a separate thread that outputs all the prime numbers less than or equal to
the number entered by the user. Fetch A. This process continues until the user discovers the spyware. External fragmentation can greatly increase swapping times by forcing multiple seeks during reading or writing of a process image. When the buffer-reading subroutine returns from execution, the return address is the exploit code, and the code is
run. We use two complementary techniques to move processes in a computer network. Some versions of the UNIX system use this method in conjunction with the second-chance algorithm. An RPC uses a datagram protocol (UDP on the Internet) to execute a routine on a remote system (Section 3.6.2). Because of the collision resistance in the hash
function, we are reasonably assured that no other message could create the same MAC. The JVM must decide whether or not to open a network connection for this request. Only the source code of the compiler would contain the information. A second option is to create a new file in the source directory and modify /usr/src/linux-2.x/kernel/Makefile to
include the newly created file in the compilation process. In the remainder of this chapter, we address security at the network and operating-system levels. Associated with this list is a threshold value that is used to indicate whether sufficient free memory is available. Message passing is also easier to implement than is shared memory for
intercomputer communication. Such requests will only be granted when an existing license holder terminates the application and a license is returned. If no empty slabs are available, a new slab is allocated from this slab. A networked computer receives bits
fivm the wire with no immediate and reliable way of determining what machine or application sent those bits. Note that the concepts of synchronous and asynchronous occur frequently in operating-system, have noted that the use of
software capabilities allowed them to realize considerable economies in formulating and implementing protection policies commensurate with the requirements of abstract resources. One way to address this problem is for the operating system to ensure that messages are acted on exactly once, rather than at most once. The send and receive
operations themselves are flexible. This scheme allows more processes to be run than can be fit into memory at one time. However, they do not give us the appropriate tools for preventing the propagation (or disclosure) of information. Photo Courtesy: Povilas Baltinas / EyeEm/Getty Images However, if you're reading with your child, you may find that
you want to work your way through all of the books, even the ones for older kids. The segment table has a separate entry for each segment (or limit). The philosophy adopted in Java is to require the library class to explicitly permit the network
 connection to load the requested URL. Permissions are identified according to the following: mode meaning 0400 Read permission of owner. Two processes can communicate only if the processes have a shared mailbox, however. Parts of Chapter 17 were derived from a paper by Levy and Silberschatz [1990]. Two types of buffers can be used. Apply
 the random page-reference string to each algorithm, and record the number of page faults incurred by each algorithm. Swap space is reinitialized at boot time so any fragmentation is short-lived. [1995b]. RC5 can vary in key length, number of transformations, and block size. This segment, BL, can in turn be coalesced with its buddy BR to form a 128-
KB segment. Some systems allocate a fixed percentage of memory for I/O buffers, whereas others allow both user processes and the I/O subsystem to compete for all system memory. At this point, to increase CPU utilization and stop thrashing, we must decrease the degree of multi pro grammi rig. Clearly, any process that shares data with other
processes is a cooperating process. The CPU transfers data through these kinds of devices by reading and wrriting a few device registers, called an I/O port. Java programs run on any operating system supporting a Java virtual machine (or JVM). The average service time for a page fault will increase because of the longer average queue for the paging
device. Because it uses only basic computational operations, it can run on a wide variety of CPUs. RC4 is perhaps the most common stream cipher. The RPC scheme is useful in implementing a distributed file system (Chapter 17). It can monitor the traffic as it forwards the message, watching for and disabling illegal commands, attempts to exploit
bugs, and so on. Threads The process model introduced in Chapter 3 assumed that a process was an executing program with a single thread of control. One solution is to shift the counts right by 1 bit at regular intervals, forming an exponentially decaying average usage count. There is a daemon on the remote site that watches for connection requests
to the system's FTP port. As the write(A) operation of T\ does not conflict with the read(B) operation of To, we can swap these operations to generate an equivalent schedule. No memory is wasted due to fragmentation. Pthreads Thread Creation Creation the disk
into one or more groups of cylinders. Wait indefinitely until there is room in the mailbox. 373 374 Chapter 10 File-System Interface A file is a named collection of related information that is recorded on secondary storage. Memory-mapped I/O is also convenient for other devices, such as the serial and parallel ports used to connect modems and
printers to a computer. Popek [1974] and Saltzer and Schroeder [1975] provided excellent surveys on the subject of protection. We can limit the effects of thrashing by using a local replacement algorithm (or priority replacement algorithm).
The C program shown in Figure 3.10 illustrates the UNIX system calls previously described. [1993b]). Hydra's capabilities c. Either SSTF or LOOK is a reasonable choice for the default algorithm. 16.2.1 Network Operating Systems A network operating system provides an environment in which users, who are aware of the multiplicity of machines, can
 access remote resources by either 614 Chapter 16 Distributed System Structures logging in to the appropriate remote machine or transferring data from the remote machine to their own machines. Thus, we could write to the shared-memory region as follows: sprintf(sharedjnemory, "Writing to shared memory"); Other processes sharing this segment
 would see the updates to the sharedmemory segment. The directory is searched for the appropriate entry, and the current-file-position pointer is repositioned to a given value. Simple possession of the capability means that access is allowed. This vast variety of viruses is likely to continue to grow. With this list, the user can run any of the previous 10
commands by entering r x where 'x' is the first letter of that command. Shared-memory segments can be identified according to a userspecified key or according to a userspecified key or according to the integer value returned from the shared-memory segment created. Look for titles like Judy Moody, Diary of a Wimpy
Kid, Smashie McPerter, Amelia, Stink and more. oceujrs rK! flrig ihis: W i; m[jni0754 ^tj: this .the .; sta:rt;ofoneipeak andithestartiofithe ne:Xt:peak;;iljustifa;t£js; one warkine set to ai 9.7 Memory-Mapped Files Consider a sequential read of a file on disk using the standard system calls openQ, r e a d O , and w r i t e Q . This technique provides for
rapid process creation and minimizes the number of new pages that must be allocated to the newly created process. The code for the producer and consumer processes is shown in Figures 3.14 and 3.15, respectively. To write a file, we make a system call specifying both the name of the file and the information to be written to the file. Most programs
(web browsers, compilers, word processors, spreadsheets, and so on) are stored on a disk until they are loaded into memory. 2.6 What are the advantages and devices? 3.9 An echo server is a server that echoes back whatever it receives from a client. Below, we
provide a brief outline of the major changes to the various chapters: • Chapter 1, Introduction, has been totally revised. The chapter also includes new sections on synchronization in the Linux kernel and in the Pthreads API. It was proved to be optimal by Mattson et al. These methods do not scale well, however. These viruses are triggered when a
program capable of executing the macro is run. Chapter 22 was derived from an unpublished manuscript by Dave Probert, Cliff Martin, and Avi Silberschatz. In this manner, the two processes are able to communicate and then go their separate ways. This approach is particularly appropriate for software or microcode implementations of LRU
replacement. All the sites in such systems are close to one another, so the communication links tend to have a higher speed and lower error rate than do their counterparts in wide-area networks. Second, if we have a reference to a page p, then any immediately following references to page p will never cause a page fault. Within a computer system
each process has a process identifier, and messages may be addressed with the process identifier. Java objects are specified with the classes. When its caller may not be trusted, a method executes an access request within a doPrivileged block to perform the access to a protected resource
 algorithms, there are two main varieties of authentication algorithms. At the lowest level, system calls allow a running program to make requests from the operating system directly. If the signatures match the next time the program is run, it does not need to be virus-scanned again. — f I victim reset page page table table for new page physical
 memory Figure 9.10 Page replacement. Some computer systems, such as PCs, use a two-step process in which a simple bootstrap loader fetches a more complex boot program from disk, which in turn loads the kernel. System and network threats create a situation in which operating-system resources and user files are misused. A generated signal is
delivered to a process. In the IBM PC, each location on the screen is mapped to a memory location. It can be difficult to determine whether a system slowdown is just a surge in system use or an attack. SSTF is common and has a natural appeal because it increases performance over FCFS. Wait for the CPU to be allocated to this process again
Solomon and Russinovich [2000] discuss threading in Windows 2000. The bibliographical notes contain pointers to research papers in which results were first presented and proved, as well as references to material for further reading. When clone 0 is invoked, it is passed a set of flags, which determine how much sharing is to take place between the
function is to carry out the designated task. Each update is a little more expensive, but there is no search for a replacement; the tail pointer points to the bottom of the stack, which is the LRU page. Solaris ini tially implemented the JVM using the many-to-one model (the green thre adslibrary, mentioned-earlier). Another use for a lock bit involves
normal page replacement. If the table is on disk, the operating system can use the other 31 bits to specify the disk location of the table; the table to the general user population. Bibliographical Notes 607 Diffie and
Hellman [1976] and Diffie and Hellman [1979] were tl^e first researchers to propose the use of the public-key encryption scheme. However, for some memory-intensive applications, this may still prove insufficient for storing the working set. Such daemons are installed via two mistakes. Sometimes it is performed out-of-band—say, via a paper
document or a conversation. Policies for resource use may also vary, depending on the application, and they may be subject to change over time. A page with a history register value of 11001101. The C program shown in Figure 3.12 illustrates the CreateProcessO function, which creates the CreateProcessO function, which creates the CreateProcessO function for the application of 11001101.
a child process that loads the application mspaint. The primary modification is to remove unnecessary features of the UNIX network environment that assisted the worm's propagation also helped to stop its advance. Similar viruses install themselves in
device drivers. See also denial-of-service attacks man-in-the-middle, 561 replay, 560 and encryption, 580-583 in Linux, 777 two-factor, 591 in Windows XP), 363 automount feature, 645
autoprobes, 747 auxiliary rights (Hydra), 548 Index back door, 50/ background processes, 166 backing store, 282 backups, 436 bad blocks, 464-465 bandwidth: disk, 457 effective, 484 sustained, 484 banker's algorithm, 259-262 base file record, 815 base register, 276, 277 basic file systems, 412 batch files, 379 batch interface, 41 Bayes' theorem, 596
382 bad, 464-465 boot, 71, 463-464 boot control, 414 defined, 772 direct, 427 file-control, 413 index, 426 index to, 384 indirect, 427 logical, 454 volume control, 415 blocking (synchronous) message passing, 102 block-interleaved
distributed parity, 473 block-interleaved parity organization, 472-473 block, 114 boot disk (system disk), 72, 464 bootstrap programs, 463-464, 573 bootstrap programs (bootstrap programs (bootstrap loaders), 6,
7, 71 boot viruses, 569 bottom half interrupt service routines, 755 bounded-buffer problem, 205 bounded capacity (of queue), 102 breach of availability, 560 breach of confidentiality, 560 breach of integrity, 560 breach of availability, 560 breach of confidentiality, 560 breach of integrity, 560 breach of availability, 560 breach of confidentiality, 560 breach of availability, 560 breach of availability, 560 breach of confidentiality, 560 breach of confidentiality, 560 breach of availability, 560 brea
772 circular, 438 defined, 512 buffer cache, 433 buffering, 102, 512-514, 729 buffer-overflow attacks, 565-568 bully algorithm, 684-685 bus, 453 defined, 496 expansion, 496 PCI, 496 bus architecture, 11 bus-mastering I/O boards, 503 busy waiting, 202, 499 bytecode, 68 Byzantine generals problem, 686 890 Index C cache: buffer, 433 defined, 514 in
Linux, 758 as memory buffer, 277 nonvolatile RAM, 470 page, 433 and remote file access: and consistency, 649-650 location of cache, 647-648 update policy, 648, 649 slabs in, 355 unified buffer, 433, 434 in Windows XP, 806-808 cache coherency, 26 cache-consistency problem, 647 cachefs file system, 648 cache
management, 24 caching, 24-26, 514 client-side, 827 double, 433 remote service vs., 650-651 write-back, 648 callbacks, 657 Cambridge CAP system, 549-550 Cambridge CAP system, 549-550 Hydra, 547-549 capability lists, 543
carrier sense with multiple access (CSMA), 627-628 cascading termination, 95 CAV (constant angular velocity), 454 CD, see collision detection central processing unit, see under CPU certificate authorities, 584 certification, 602 challenging (passwords), 590 change journal (Windows XP), 821 character devices (Linux), 771-773 character-stream
devices, 506-508 checkpoints, 225 checksum, 637? Doubling the page size increases I/O time to only 28.4 milliseconds. • Unbounded capacity...; •... The stub then sends this parcel to the server, where the skeleton for the remote object receives it. In addition to the normal user-namepassword authentication information, the TCB also maintains the
clearance and authorizations of individual users and will support at least two levels of security. However, a subsystem designer who wants to make use of this facility cannot simply study a reference manual, as is the case with Hydra. Despite these problems, LRU replacement with 12 faults is much better than FIFO replacement with 15. One of these
buddies is used to satisfy the 21-KB request. When protection at the instruction after the for k (), with one difference:
The return code for the f o r k O is zero for the new (child) process, whereas the (nonzero) process identifier of the child is returned to the parent. Regardless of how the file is opened, then, Solaris treats all file I/O as memory-mapped, allowing file access to take place via the efficient memory subsystem. A typical bad-sector transaction might be as
follows: The operating system tries to read logical block 87. This eliminates one security problem, with setuid programs in which crackers create and hide (using obscure file or directory names) them for later use. file server '16.3 Network Structure 619 The most common links in a local-area network are twisted-pair and fiberoptic cabling. Some
 antivirus programs also put up a complete shield rather than just scanning files within a file system. How, though, can we define what an operating system is? This is known as cipher-block chaining. This leads to awkward programming for a process that wishes obtain a number of resources: while (decrease count(count) == -1) Rewrite the resource-
manager code segment using a monitor and condition variables so that the decrease count() function suspends the process until sufficient resources are available. The ETHREAD also contains a pointer to the corresponding KTHREAD. 4.2.1 Many-to-one model (Figure 4.2) maps many user-level threads to one kernel thread.
Before we can explore the details of computer system operation, we need to know something about system interacts with the kernel through calls on a set of kernel-defined primitives that define access rights to resources defined by the subsystem interacts with the kernel through calls on a set of kernel-defined primitives that define access rights to resources defined by the subsystem interacts with the kernel through calls on a set of kernel-defined primitives that define access rights to resources defined by the subsystem interacts with the kernel through calls on a set of kernel-defined primitives that define access rights to resources defined by the subsystem interacts with the kernel through calls on a set of kernel-defined primitives that define access rights to resource the call of the calls of the call o
for answers to the exercises. In this chapter, we introduce basic CPU-scheduling concepts and present several CPU-scheduling algorithms. [1996]. Allow the fortunes to contain multiple lines. However, this may lead to an increase in fragmentation for some applications that do not require such a large page size as 32 KB. There are two major classes
of queues in an operating system: I/O request queues 116 Chapter 3 Processes and the ready queue. Another situation might occur when a user presses a button on a web browser that stops a web page from loading any further. Each mailbox has a unique identification. local, 342 LRU-approximation page replacement, 336-338 LRU page replacement
334-336 optimal page replacement, 332-334 and page-buffering algorithms, 338-339 page replacement algorithm, 330 page size, 357-358 page slots, 468 908 Index page table(s), 289-294 hashed, 300 inverted, 301-302, 359-360 page-table base register (PTBR), 293 page-
table length register (PTLR), 296 page-table self-map, 797 paging, 288-302 basic method of, 289-292 hardware support for, 292-295 hashed page tables, 300 hierarchical, 297-300 Intel Pentium example, 306-308 inverted, 301-302 in Linux, 761-762 and memory protection, 295-296 priority, 365 and shared pages, 296-297 swapping vs., 466 paging
files (Windows XP), 797 paging mechanism (Linux), 761 paired passwords, 590 PAM (pluggable authentication modules), 777 parallel systems, set' multiprocessor systems parcels, 114 parent process, 90, 795-796 partition (s), 286, 386, 416-117 boot, 464 raw, 467 root, 417 partition boot sector, 414 partitioning,
disk, 463 passwords, 588-591 encrypted, 589-590 one-time, 590-591 vulnerabilities of, 588-589 path names absolute, 390 relative, 390 path-name translation, 442-443 PCBs, sec process control blocks PCI bus, 496 PCS (process-contention scope), 172! PC systems, 3 PDAs, see personal digital assistants PDEs (page-directory
entries), 799 peer-to-peer computing, 33-34 penetration test, 592-525 with tertiary-storage, 484-488 cost, 485 speed, 484-488 cost, 485 speed, 484-85 of Windows XP, 786 performance improvement, 432-435, 470 periodic processes, 720 periodic processes, 720 permissions, 406 per-processes, 720 periodic processes, 720 permissions, 406 per-processes, 720 periodic processes, 720 periodic processes, 720 periodic processes, 720 permissions, 406 per-processes, 720 periodic processes, 720 permissions, 406 per-processes, 427-429 and 427-429 permissions, 406 per-processes, 427-429 permissions, 406 per-processes, 427-429 permissions, 406 per-processes, 427-429 permissions, 427-429 permi
open-file table, 414 persistence of vision, 716 personal digital assistants (PDAs), 10, 30 personal digital ass
formatting, 462 physical layer, 628, 629 physical memory, 17, 315-316, 756-759 physical security, 562 PIC (position-independent code), 764 pid (process identifier), 90 PIN (personal identification number), 591 pinning, 807-808 PIO, see programmed I/O pipe mechanism, 774 platter (disks), 451 plug-and-play and (PnP) managers, 809-810 pluggable
authentication modules (PAM), 777 PnP managers, see plug-and-play and managers Index point-to-point tunneling protocol (PPTP), 823 policy(ies), 56-57 group, 828 security, 592 policy algorithm (Linux), 761 polling, 498^99 polymorphic viruses, 570 pools: of free pages, 327 thread, 141-142 pop-up browser windows, 564 ports, 353, 496 portability
787 portals, 32 port driver, 806 port scanning, 575 position-independent code (PIC), 764 positioning time (disks), 452 POSIX, 783, 786 interprocess communication example, 103-104 in Windows XP, 813-814 possession (of capability), 543 power-of-2 allocator, 354 PPTP (point-to-point tunneling protocol), 823 P + Q redundancy scheme, 473
preemption points, 701 preemptive kernels, 194-195, 701 preemptive scheduling, 155-156 premaster secret (SSL), 586 prepaging, 357 presentation layer, 629 primary thread, 830 principle of least privilege, 532-533 priority-based scheduling, 700-701 priority-inheritance protocol, 219, 704 priority inversion, 219, 704 priority number, 216 priority
paging, 365 priority replacement algorithm, 344 priority scheduling algorithm, 162-164 private keys, 580 privileged mode, see kernel mode process(es), 17 background, 166 communication between, see 909 interprocess communication components of, 82 context of, 89, 749-750 and context switches, 89-90 cooperating, 96 privileged mode, see kernel mode process(es), 17 background, 166 communication between, see 909 interprocess communication components of, 82 context of, 89, 749-750 and context switches, 89-90 cooperating, 96 privileged mode, see kernel mode process(es), 17 background, 166 communication between see 909 interprocess communication between see 909 interproc
defined, 81 environment of, 749 faulty, 687-688 foreground, 166 heavyweight, 127 independent, 96 I/O-bound vs. The Win32 API is the primary API for the family of Microsoft operating systems (Windows 95, 98, NT, 2000, and XP). However, some systems choose to memory-map a file regardless of whether the file was specified as memory-mapped.
12.6.3 Swap-Space Management: An Example We can illustrate how swap space is used by following the evolution of swapping and paging in various UNIX systems. However, the failure of a single link in such a network can result in the network's becoming partitioned. 350 Chapter 9 Virtual Memory the file. Physical devices are assigned minimum
and maximum security levels that the system uses to enforce constraints imposed by the physical environments in which the devices are located. 9.9 Other Considerations 9.0 Other Considerations 9.0
earlier in this chapter. A default LDT segment 308 Chapter 8 Main Memory(iogica! address) age directory 31 offsei 22 21 Figure 8.23 Paging in the Pentium architecture. Such an event occurred in 1988 to UNIX systems on the Internet, causing millions of
dollars of lost system and system administrator time. 9.9.2 P a g e Size The designers of an operating system for an existing machine seldom have a choice concerning the page size. Thread management is done by the thread library in user space, so it is efficient; but the entire process will block if a thread makes a 130 Chapter 4 Threads •user thread
kernel thread Figure 4.2 Many-to-one model. i o . In a multiprogrammed operating system, two protection domains are insufficient, since users also want to be protected from one another. This is known as priority paging and is covered in Section 11.6.2. 9,11 S It is desirable to be able to execute a process whose logical address space is larger than
the available physical address space. The parent waits for the child process to complete with the wait () system call. The PROCESSJNFORMATION structure contains a handle and the identifiers to the newly created process and its thread. Utilization of multiprocessor architectures. In contrast, RMI is object-based: It supports invocation of methods on
remote objects. To allow more convenient access to I/O devices, many computer architectures provide memory-mapped I/O. Notice that, even if we select for replacement a page that is in active use, everything still works correctly. LPCs are also used in a few other functions that are part of the Win32 API. A process is cooperating if it can affect or be
system allows the creation of access-control lists that denote users or groups not granted access to a given named object. The policy decisions involve which rights should be included in the (z',;')th entry. We next illustrate these steps in more detail. Nessus (from performs a similar function, but it has a database of bugs and their exploits. pointer is
moving fast b. These users have dedicated resources at their disposal, but they also share resources such as networking and servers. R-, Pi Processes P\, P2, and P3 are deadlocked. The p r i n t k O function is used to print messages to a kernel log file and therefore may only be called from the kernel. Revocation is
immediate and can be general or selective, total or partial, and permanent or temporary. For example, since IP packets encapsulate TCP packets, encryption of IP packets (using IPSec, for example) also hides the contents of the encapsulate TCP packets, encryption of IP packets (using IPSec, for example) also hides the contents of the encapsulate TCP packets.
the child thread. For a computer to start running—for instance, when it is powered up or rebooted—it needs to have an initial program to run. If the reference was invalid, we terminate the process. With the expanded privileges, the process can now execute kernel code that might Exercises 75 include privileged instructions that cannot be executed in
user mode. Use of this page-replacement algorithm guarantees the lowest possible pagefault rate for a fixed number of frames. The operating-system kernel consults an internal table to determine where the page is located on the backing store. If we use the recent past as an approximation of the near future, then we can replace the page that has not
been used for the longest period of time (Figure 9.15). The linear address is then given to the paging unit, which in turn generates the physical address in main memory. Free and commercial versions of Tripwire are available from and . 15.4 Cryptography as a Security Tool There are many defenses against computer attacks, running the gamut from
methodology to technology. Generally, the user is allowed to access only those files that are in the directory tree of user "anonymous users, subject to the usual file-protection scheme used on that machine. If a transaction X, has obtained a shared-mode lock (denoted by S) on data item Q, then
7] can read this item but cannot write Q. 3.3.2 Process Terminates when it finishes executing its final statement and asks the operating system to delete it by using the exit() system call. The ten high-order bits reference an entry in the outermost page table, which the Pentium terms the page directory. Knowledge of V(k) and
 knowledge of S(k) are equivalent: One can be derived from the other, so k must be kept secret. Most operating systems provide features for memory access. in etd is responsible for networking services such as telnet and ftp; dtlogin is the process representing a user login
screen. IPSec is becoming widely used as the basis for virtual private networks (VPNs), in which all traffic between two IPSec endpoints is encrypted to make a private network out of one that may otherwise be public. In fact, some architectures provide both. One issue this illustration does not address concerns the situation in which both the producer
process and the consumer process attempt to access the shared buffer concurrently. A subject is used to track and manage permissions for each program that a user runs; it is composed of the user's access token and the program acting on behalf of the user. Because of this replacement, the next reference, to 0, will fault. 96 Chapter 3 Processes 3.4
 Interprocess Communication » Processes executing concurrently in the operating system may be either independent processes. This last policy is usually decided by the operating system. Tf the counter is decremented to 0, a trap occurs (excessive indirection). Various page-replacement algorithms are used. For instance, the
routines on U.S. government computers that balance the budget are only rarely used. The file can be accessed simultaneously by several processes, subject to the following constraint: The sum of all unique numbers associated with all the processes currently accessing the file must be less than n. Designing appropriate algorithms to solve these
problems is an important task, because disk I/O is so expensive. We must solve two major problems to implement algorithm and a page-replacement algorithm and a page-replacement algorithm and a page-replacement algorithm. 14.3 Consider a computer system in which "computer games" can be played by students only between 10 P.M. and 6 A.M., by faculty
members between 5 P.M. and 8 A.M., and by the computer center staff at all times. The bootstrap program must know how to load the operating system and to start executing that system. It does not exploit any known bugs. 9. In this locality, memory references are made to the instructions of
the function call, its local variables, and a subset of the global variables. The sending process sends the message and resumes operation. Creating a Child Process The first part of this project is to modify the mainQ function in Figure 3.25 so that upon returning from s e t u p (), a child process is forked and executes the command specified by the
bakery algorithm, which was developed by Lamport [1974]. Some systems implicitly open a file when the first reference to it is made. long denotes that the entry will occupy the same number of bytes as a data value of type long.) Building a New Kernel Before adding a system call to the kernel, you must familiarize yourself with the task of building
the binary for a kernel from its source code and booting the machine with the newly built kernel. Because no copying of pages takes place, vf ork() is an extremely efficient method of process creation and is sometimes used to implement UNIX command-line shell interfaces. Belady's anomaly was discovered as a result. The default value of siowscan is
be made. That is, sector 202 is copied into the spare, then sector 201 into 202, and then 200 into 201, and so on, until sector 18 is copied into sector 19. There are several reasons for allowing concurrent execution: information sharing, computation speedup, modularity, and convenience. If it will not, then the instances are not identical, and the
resource type classes have not been defined properly. Furthermore, the kernel must inform an application about certain events. Furthermore, the system must provide protection (Chapter 14) to allow the implementation of security features. How does this practice compare with the cross-ring calls in a ring protection scheme? Demand paging requires
this information to process page faults. CLONE_FILES The set of open fifes is shared. Eventually, the final CPU burst ends with a system request to terminate execution (Figure 5.1). If a file is opened and accessed using ordinary system request to terminate execution (Figure 5.1). If a file is opened and accessed using ordinary system request to terminate execution (Figure 5.1). If a file is opened and accessed using ordinary system request to terminate execution (Figure 5.1).
the kernel address space. This process is called low-level formatting, or physical formatting. We see, then, that the effective access time is directly proportional to the page-fault rate. The copy and owner rights allow a process to change the entries in a column. To avoid this constant searching, many systems require that an openO system call be made
before a file is first used actively. Thus, in the worst case, the entire virtual memory must be in physical memory to be executed by other users. The Senior Production Editor was Ken Santor. It does not perform the final step of exploiting the found bugs, but
a knowledgeable cracker or a script kiddie could. 9.20 Consider a system that allocates pages of different sizes to its processes. The new process consists of a copy of the address space of the original process. Throughout the entire operating-system design cycle, we must be careful to separate policy decisions from implementation details
(mechanisms). The kernel then allocates a new virtual processor to the application. In this case, the sender must block until the recipient receives the message. For example, a printer cannot be simultaneously shared by several processes. A domain can be realized in a variety of ways: » Each user may be a domain. What happens during a system call
 when a process executing in a higher-numbered ring invokes a procedure in ring 0? Pthreads names the wait () and signal () operations sem wait () and sem post(), respectively. In this step, the operating system stores the initial file-system data structures onto the disk. Obviously, as the number of frames available increases, the number of page faults
decreases. To ensure serializability when the execution of several transactions overlaps, we must use a concurrency-control scheme. A Cl-class system incorporates some form of controls that allow users to protect private information and to keep other users from accidentally reading or destroying their data. 7.1 System Model A system consists of a
 finite number of resources to be distributed among a number of competing processes. This field is undergoing rapid change, as computers are now prevalent in virtually every application, from games for children through the most sophisticated planning tools for governments and multinational firms. 74 Chapter 2 Operating-System Structures 2.15
 Why is a just-in-time compiler useful for executing Java programs'? Pthreads refers to such points as cancellation points. Assume that s pages are prepaged and a fraction a of these s pages is actually used (0 < a < 1). Optionally, controlled communications may be allowed between the DMZ and one comparations.
demand paging: Never bring a page into memory until it is required. In fact, many early storage devices, including paper tape and core memories, are relegated to museums now that magnetic tape and semiconductor memory have become faster and cheaper. These primitive operations can then be combined to perform other file operations. It does
not allow selective revocation. The selection process is carried out by the appropriate scheduler. 0.1",6013); InputStream in = sock.getInputStream(); English (line = bin.readLine()) != null) System.out.println(line); II close the socket
connection sock.close (); } catch (IOException ioe) { System.err.println(ioe); Figure 3.20 Date client. A process that needs several popular resources may have to wait indefinitely, because at least one of the resources that it needs is always allocated to some other process. A large portion of operating system code is dedicated to managing I/O, both
because of its importance to the reliability and performance of a system and because of the devices. For instance, a T3 is composed of 28 Tl connections and has a transfer rate of 45 megabits per second. What are the disadvantages of using the microkernel approach? This method is usually employed for achieving load balancing
and computation speedup among homogeneous systems, as they do not need user input to help them execute programs remotely. Windows XP allows the creation of any number of user accounts, which can be grouped in any manner. However, this arrangement provides more rights than are needed in each of the two phases, since we have read
access in the phase where we need only write access, and vice versa. At that time, the page will be brought back into memory, perhaps replacing some other page in the process. Domain switching from domain D; to domain D is allowed if and only if the access right switch e access (/,;'). The one-to-one model allows for greater concurrency, but the
developer has to be careful not to create too many threads within an application (and in some instances may be limited in the number of threads she can create). Perhaps the best illustration of a deadlock can be drawn from a law passed by the Kansas legislature early in the 20th century. The freed frames are then distributed to processes with high
page-fault rates. 3.3 Operations on Processes 93 which is a unique integer. Her goal is to replace the return address in the stack frame so that it now points to the code segment containing the attacking program. It does not, however, ensure freedom from deadlock. The lowest-level classification is division D, or minimal protection. After partitioning,
the second step is logical formatting (or creation of a file system). We opt for many of the default values of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten parameters passed to Cre at eProcess of the ten paramet
location (or locations) in the code where the race condition occurs. The second and third parameters indicate the initial value and maximum value of the semaphore. However, because signals need to be handled only once, a signal is typically delivered only to the first thread found that is not blocking it. After that, a consumer process opens a mapping
tp the shared-memory object and reads the message written by the consumer. Process P invokes a predefined procedure at site A. Three different types of models relate user and kernel threads: The many-to-one model maps many user threads to a single kernel thread. We may also want to allow the content of a domain to be changed. The same
situation may arise at other times. Its modify bit is then reset. Furthermore, loss of such data, whether by accident or fraud, can seriously impair the ability of the corporation to function. The buffer is full when ((in + 1) % BUFFER SIZE) == out. The scheme for monitoring the page-fault rate was developed by
VVulf [1969], who successfully applied this technique to the Burroughs B5500 computer system. There are many different memory management, and the effectiveness of a particular algorithm depends on the situation. sclngdiujing:;: 1 :;. These processes cause page faults; and one of
them, using a global replacement algorithm, replaces the page containing the memory buffer for the waiting process. Its speed varies from machine to machi
P(I\A) for the moment, we can compute it using Bayes' theorem: 0.00002 • P(A\I) ~~ 0.0
Dougan et al. Typically, the execO system call is used after a for k O system call by one of the two processes to replace the process's memory space with a new program. Also included under this topic is a discussion of threads. Every signal may be handled by one of two possible handlers: 1. The receive operation attempts to receive from (1) any
mailbox in a mailbox set or (2) a specific (named) mailbox. Each entry in the per-process table in turn points to a system-wide open-file table. The separation of policy and mechanism, is an important design property. If this flag is set, the page directory points directly to the 4-MB page frame, bypassing the inner page table; and the 22 low-order bits in
the linear address refer to the offset in the 4-MB page frame. Thus, we must define an implementation to map twodimensional user-defined addresses into one-dimensional physical addresses. Fortunately, analysis of running processes shows that this behavior is exceedingly unlikely. i l f f f 1.11 "1!; .'- :-: . Kernel memory, however, is often allocated
from a free-memory pool different from the list used to satisfy ordinary user-mode processes. I I 12.4 Disk Scheduling 461 queue 98, 183, 37, 122, 14, 124, 65, 67 head starts at 53 0 14 37 536567 98 122124 183199 1% % Figure 12.8 C-LOOK disk scheduling. Suggest a scheme that will avoid this problem. For example, assume that the child process
attempts to modify a page containing portions of the stack, with the pages set to be copy-on-write. Decrease the degree of multiprogramming. For this project, the execvp () function should be invoked as execvp (args [0], args); be sure to check the value of background to determine if the parent process is to wait for the child to exit or not. Avi is
starting a new chapter in his life, returning to academia and partnering with Valerie. Lempel [1979], Simmons [1979], Denning [1982], Ahituv et al. 9.2 Discuss the hardware support required to support demand paging. Semaphores are acquired with the same WaitForSingleObjectO function as mutex
daemon process may be started at boot time and run as a special user ID. Thus, these systems must provide a mechanism for process creation and termination. Latency time, though, is perhaps 8 milliseconds and seek time 20 milliseconds. Another solution is to allow pages to be locked into memory. For a process to perform an operation on a typed
object, the capability it holds for that object must contain the name of the operation being invoked among its auxiliary rights. Consider a CPU-bound application running on a single process and gives the CPU to another
process. The offset is a 32-bit number specifying the location of the byte (or word) within the segment in question. The virtual memory is implemented by paging, and the page size is 4,096 bytes. We cannot, for example, allocate more than the total number of available frames (unless there is page sharing). It does so in two steps. software, 533 in
 Linux, 758 used, 356 in Windows XP, 793-796 object files, 374 Index object linking and embedding (OLE), 825-826 object serialization, 115 object table, 796 object types, 419, 795 off-line compaction of space, 422 OLE, see object linking and embedding on-demand streaming, 717 one-time pad, 591 one-time passwords, 590-591 one-to-one
multithreading model, 130 one-way trust, 828 on-line compaction of space, 422 open-file table, 376 open() operation, 376 open-file table, 376 open-file tabl
of, 57-58 interrupt-driven, 17-18 mechanisms for, 56-57 network, 28 operations of: modes, 18-20 and timer, 20 policies for, 56-57 real-time, 29-30 as resource allocator, 5 security in, 562 services provided by, 39-41 structure of, 15-17, 58-64 layered approach, 59-61 microkernels, 61-64 modules, 62-63 simple structure, 58-59 system's view of, 5 user
interface with, 4-5, 41-43 optimal page replacement algorithm, 332-334 ordering, event, see event ordering orphan detection and elimination, 652 907 OS/2 operating system, 783 out-of-band key delivery, 583 over allocation (of memory), 327 overlapped I/O, 843-845 overprovisioning, 720 owner rights (Linux), 778 p (page number), 289 packets, 626,
776 packet switching, 627 packing, 382 pages: defined, 289 shared, 296-297 page allocator (Linux), 757 page-fault-frequency (PFF), 347-348 page-fault rate, 325 page-fault traps, 321 page frames, 799 page-frame database, 801 page
number (p), 289 page offset (d), 289 page offset (d), 289 pageout (Solaris), 363-364 pageout (Solaris)
user level, for user threads, or by the kernel, for kernel threads. The one-to-one model maps each user thread to a corresponding kernel thread, what happens when the operating system is using a per-process frame allocation technique and only two pages are allocated, to this process? We then calculate N = 7*13 = 91 and (p-l)(• A). This search would
take far too long. This standard method cannot be used with inverted page tables; because there is only one virtual addresses. This device 1.2 thread of execution 1 ca Computer-System Organization • instruction execution • cycle — data movement — 11
instructions and data CPU (*N) •:, %A:^Z'&iSiS'm%;: ^Wit-A "A ivA:, V hardware CPU memory::: I/O devices j Figure 2.16 VMware architecture. These tasks may take from 1 to 100 microseconds each. Once the system services are defined, the structure of the operating system can be developed. Users then run a separate program, which sends
requests to this process whenever they need to use the facility This method is used by the TOPS-20 operating system. What is needed is a safe, dynamic access-control mechanism for distributing capabilities as necessary.
The ability to copy an access right from one domain (or row) of the access matrix to another is denoted by an asterisk (*) appended to the access right. For instance, some processors (such as the Sun UltraSPARC) provide multiple sets of registers. Revocation was discussed by Redell and Fabry [1974], Cohen and Jefferson [1975], and Ekanadham and
Bernstein [1979]. Security Protection, as we discussed in Chapter 14, is strictly an internal problem: How do we provide controlled access to programs and data stored in a computer system? In addition to containing boot code, the MBR containing boot code, the MBR containing the partitions for the hard disk and a flag indicating which partition the system is to be
booted from. From there, the worm program exploited flaws in the UNIX operating system's security routines and took advantage of UNIX utilities that simplify resource sharing in local-area networks to gain unauthorized access to thousands of other connected sites. An application that is I/Ointensive may require multiple LWPs to execute, however.
1.2.3 I/O Structure Storage is only one of many types of I/O devices within a computer. These matrices will be declared as global data so that each worker thread has access to A, B, and C. Because Linux is designed to run on a variety of processors—many of which may provide only limited support for segmentation—Linux does not rely on
segmentation and uses it minimally- On the Pentium, Linux uses only six segments: 1. The Microsoft Windows NT Workstation Resource Kit (Microsoft Windows NT workstati
operation is called programmed I/O (PIO). Some UNIX systems have chosen to have two versions of forkQ, one that duplicates all threads and another that duplicates only the thread that invoked the forkQ systems—UNIX and MULT1CS—to see how these concepts have
been implemented there. Multimedia data in that multimedia data in that multimedia data—such as frames of video—must be delivered (streamed) according to certain time restrictions. S under the heading ENTRY (sys call table). Some also look for process anomalies. The project for designing and enhancing the UNIX shell interface was
contributed by John Trono of St. Michael's College in Winooski, Vermont. « List of gates. However, in some circumstances, each thread might need its own copy of certain data. The site even has a section on math. Oxford OwlCreated by Oxford University Press, Oxford Owl offers a free site for parents and children to use at home, as well as a
membership version for teachers and schools. A producer can produce one item while the consumer is consuming another item. Therefore, an authentication algorithm takes the message digest and encrypts it. Recent versions of Sun's SPARC chip include this setting, and recent versions of Solaris enable it. Such a function may appear as follows:
DWORD WINAPI PoolFunction(AVOID Param) { /** * this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogramming level is increased, each process */ this function runs as a separate thread. If the multiprogram runs are 
value += 15; } else if (pid > 0) {/* parent process */ wait(NULL); printf("PARENT: value = %d", value); /* LINE A */ exit(0); Figure 3.24 C program. For example, in Figure 3.24 C program. For example, in Figure 4.6(a), domain D| is the owner of F, and thus can add and delete any valid right in column F,. Each swap area consists of a series of 4-KB page slots, which are used to hold
swapped pages. Now, when control returns from mainO, instead of returning to the location specified by the old value of the return address, we return to the modified shell code, which runs with the access rights of the attacked process! Figure 15.4(b) contains the modified shell code. 16.3 Network Structure There are basically two types of
networks: local-area networks (LAN) and wide-area networks (WAN). • Computation speedup. • Breach of confidentiality. The parent may wait for its children may execute concurrently. Create a shared-memory segment of size shared data. Thus, the preceding code zeros one word in each
page, then another word in each page, and so on. This provision introduces a swap-in, swap-out level of intermediate CPU scheduling. A query to a service could reveal passwords. Thelaock© ::mei:ht is used to acquire the lock. (Assume that finding a page-table entry in the TLBs takes zero time, if the entry is there.) 8.10 Why are segmentation and
paging sometimes combined into one scheme? 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. The FDDI network is token-based and runs at over 100 megabits per second. The idea is to examine the most recent A page references. The second partition consists of up to 8 KB segments that are shared among all the
processes. Displaying text on the screen is almost as easy as writing the text into the appropriate memory-mapped locations. Accordingly, service activity has to be carried out across the network; instead of a single centralized data repository, there are multiple independent storage devices. This type of security breach (or trap door) was shown in the
```

```
movie War Games. Because the overhead of creating kernel threads can burden the performance of an application, most implementation operations, as is generally the case for symmetric encryption
transformations. Although they vary greatly from process to process and from computer, they tend to have a frequency curve similar to that shown in Figure 5.2. The curve is generally characterized as exponential or hyperexponential, with a large number of short CPU bursts and a small number of long CPU bursts. Pinilla and Gill [2003]
compare Java thread performance on Linux, Windows, and Solaris. If they are not, we check whether they are allocated to some other process scheduling when discussing general scheduling concepts and thread scheduling to refer to thread-specific ideas. This technique can be
combined with others. d. Fetch B. 9.4.5 LRU-Approximation Page Replacement. This array is sometimes called the raw disk, and I/O to this array is termed raw I/O. There are many other considerations as welt and we discuss several of them here. A process
executing in domain Dk cannot further copy the right R. This will allow a process to invoke decrease count () by simply calling decrease count () by simply calling decrease count (count); The process will only return from this function a specified function. Initially, all bits are cleared
(to 0) by the operating system. Because each small computer is likely to occur in a single enterprise, it was a natural step to connect these small systems into a network. The number of objects to wait for 2.: • •. Of course,
locality of reference is just one measure of the efficiency of the use of a data structure. Thus, the effective access time will increase even for a process that is not thrashing. • A set M of messages. The bootstrap program can perform a variety of tasks. Sometimes the failure is complete; in this case, the disk needs to be replaced and its contents
restored from backup media to the new disk. • Bounded capacity. The ** Figure 12.7 C-SCAN disk scheduling. If a system has two CPUs, then the resource type CPU has two instances. Since the file table is maintained by the operating system, the user cannot accidentally corrupt it. One solution to this problem is for the CPU to have a feature that
disallows execution of code in a stack section of memory. This 354 Chapter 9 Virtual Memory is especially important because many operating system. Again, 'r' alone will be immediately followed by the character if it is wished to execute the most recent command. One protocol that ensures
serializability is the two-phase locking protocol. The FTP mechanism is implemented in a manner similar to telnet implementation. To illustrate these differences, let's first consider the UNIX operating system. There are literally thousands of viruses, but they fall into several main categories. A process never needs to wait for a sharable resource.
Having a large number of disks in a system presents opportunities for improving the rate at which data can be extended or replaced with less disturbance of a system in service than would be caused by the modification of an operating-
system kernel. On return from P, the capability for A is restored to its original, unamplified state. To separate mechanism from policy, we require a more general model of protection. Performance are stored in a. The difficulty with cancellation occurs in situations where resources have been allocated to a canceled thread or where a
thread is canceled while in the midst of updating data it is sharing with other threads. The concept of serializability was formulated by Eswaran et al. We restart the instruction that was interrupted by the trap. Ihg and the concept of paging can be credited to the designers of the Atlas system, which has been described by Kilburn et al. 606 Chapter 15
15.15 Security Consider a system that generates 10 million audit records per day» Also assume that there are on average 10 attacks per day on this system and that each such attack is reflected in 20 records. This scenario is known as a logic bomb. But frequently it is done along with message modification, again to escalate privileges. 8.7.3 Linux on
Pentium Systems As an illustration, consider the Linux operating system running on the Intel Pentium architecture. -; . o Otherwise, the write operation is executed. Most modern operating systems provide kernel support for threads; among these are Windows 98, NT, 2000, and XP, as well as Solaris and Linux. LRU replacement is an approximation
of optimal page replacement, but even it may be difficult to implement. Often, a web page is loaded in a separate threads—each image is loaded in a separate threads. The entry in matrix B. Let's consider a scenario in which the kernel
requests memory from the slab allocator for an object representing a process descriptor. • What CPU is to be used? In a partially connected network, direct links exist between some—but not all—pairs of sites. What options (extended instruction sets, floatingpoint arithmetic, and so on) are installed? When executing the code body of such a
procedure, a process temporarily acquires the right to read or write the contents of a software capability itself. The advantages of distributed systems have resulted in an industry-wide trend toward downsizing. Fetch and decode the instruction (ADD). In fact, look at any process that does not have "enough" frames. The advantage of the first approach
is that by modifying an existing file that is already part of the compilation process, the Makefile does not require modification. The chapter explores how these requirements affect the design of operating systems. Elements within a segment are identified by their offset from the beginning of the segment: the first statement of the program, the seventh
stack frame entry in the stack, the fifth instruction of the Sqrt (), and so on. [2002], and Hu and Perrig [2004] present solutions for secure routing. Then, the protection system needs only to verify that the capability is valid. In i t i a l i z e buffer */ /* 3. (1., 0) recently used but clean—probably will be used again soon 4.
Semaphores are created as follows: #include HANDLE Sem; Sem = CreateSemaphore(NULL, 1, 5, NULL); The first and last parameters identify a security attribute and a name for the semaphore, similar to what was described for mutex locks. The main program proceeded to search for other machines to which the newly infected system could
connect easily. STARTUPINFO specifies many properties of the new process, such as window size and appearance and handles to standard input and output files. Certainly it provides data migration (between a web server and a web server a web server and a web server and a web server and a web serve
The operating system determines where the desired page is residing on the disk but then finds that there are no free frames on the free-frame list; all memory is in use (Figure 9.9). The second main type of authentication algorithm is a digital-signature algorithm, and the authenticators thus produced are called digital signatures. Accounting is
another potential tool in a security administrator's kit. During its lifetime, a process may be either bound to a protection domain or allowed to switch from one domain to another. If these programs are executed in a domain that provides the executing user, the other users may misuse these rights. The next reference (2) replaces
page 7, because page 7 was brought in first. When the process exits, this temporary userlD change ends. Win32 Mutex Locks Mutex locks are a type of dispatcher object, as described in Section 6.8.2. The following illustrates how to create a mutex locks Mutex 
FALSE, NULL); The first parameter refers to a security attribute for the mutex lock. A program reading a contiguously allocated file will generate several requests that are close together on the disk, resulting in limited head movement. Spyware sometimes accompanies a program that the user has chosen to install. 352 Chapter 9 Virtual Memory
sequence in the program shown in Figure 9.25. Can busy waiting be avoided altogether? In a network of computers, the 15.4 Cryptography as a Security Tool 577 situation is quite different. Instead, Linux treats both in the same way, allowing a task to be more akin to a process or a thread depending on the set of flags passed to the clone() system
call. Login authentication is accomplished, and the user is allowed to execute commands remotely. ..-... Such a system can be implemented as a set of RPC daemons and clients. For example, consider a class that is not allowed to open network connections. With demand-paged virtual memory, pages are only loaded when they are demanded during
program execution; pages that are never accessed are thus never loaded into physical memory. Do not wait at all but rather return immediately. Long-term (job) scheduling is the selection of processes that will be allowed to contend for the CPU. For example, given the sequence of memory references shown in Figure 9.20, if A = 10 memory
references, then the working set at time t\ is {1, 2, 5, 6, 7}. Note that k is needed to compute both S(k) and V(k), so anyone able to compute one can compute the other. You can solve this problem using either Pthreads or the Win32 API. When the free-frame list was exhausted, a page-replacement algorithm would be used to select one of the 93 in
memory pages to be replaced with the 94th, and so on. And how is it supposed to provide protection for a request or data when it cannot determine who will receive the response or message contents it sends over the network? For example, a user at site A may be using a laser printer located at site B. If more than one command starts with V, execute the response or message contents it sends over the network?
the most recent one. The certificates can be distributed in a standard X.509 digital certificate format that can be parsed by computer. The operating system monitors the working set of each process and allocates to that working set enough frames to provide it with its working-set size. The instruction is then decoded and may cause operands to be
fetched from memory and stored in some internal register. A slab is made up of one or more physically contiguous pages. The offset d of the logical address must be between 0 and the segment limit. They may also be tricked into allowing access via social engineering. For example, if a request for 11 KB is made, it is satisfied with a 16-KB segment. At
that point, it can execute with no more faults. A firewall the ready queue and a set of device queues are present: the ready queue and a set of device queues the tape
drive is usually needed before the printer, it would be reasonable to define F(tape drive) • R(j and R,, -» P, for some resource 7.6 Deadlock Detection 263 Figure 7.8 (a) Resource-allocation graph, (b) Corresponding wait-for graph. A buffer-overflow attack to a web server will not be stopped by the firewall, for example, because the HTTP connection is
allowed; it is the contents of the HTTP connection that house the attack. Moreover, there is no real file sharing, because a user can only copy a file from one site to another. Domain switching occurs when a procedure call is made. The UltraSPARC, MIPS, and Alpha architectures employ software-managed TLBs. The PowerPC and Pentium manage the
TLB in hardware. In this text, when we refer to Windows XP as an example operating system, we are implying both Windows XP and Windows XP and Windows XP and Windows XP and Windows XP as an example operation of monitors with a single construct await (B),
 where B is a general Boolean expression that causes the process executing it to wait until B becomes true. Various questions about revocation problem. Program errors can be considered implicit requests for service. Add A and B.
With a firewall, however, access is contained, and any DMZ systems that are broken into still are unable to access the company computers. Macro viruses are written in a high-level language, such as Visual Basic. Those pages with at least one bit on will be considered to be in the working set. from these queues in some fashion. This scheme does not
 allowr selective revocation, since only one master key is associated with each object. The hardware must provide appropriate mechanisms to ensure the correct operation of the system. 5. This is similar in functionality to what is illustrated in Figure 3.11
 When a new object for a kernel data structure is needed, the allocator can assign any free object from the cache to satisfy the request. Two approaches are common. The best protection against computer viruses is prevention, or the practice of safe computing. 9.4.4 LRU Page Replacement If the optimal algorithm is not feasible, perhaps an
 approximation of the optima] algorithm is possible. A security kernel for a multiprocessor microcomputer is described by Schell [1983]. Tripwire is a tool to monitor file systems for added, deleted, or changed files and to alert system administrators to these modifications. The bootstrap can execute the operating system directly if the operating system
is also in the firmware, or it can complete a sequence in which it loads progressively smarter programs Exercises 73 from firmware and disk until the operating system itself is loaded into memory and executed. Suppose that a directory for
the named file. Whereas the many-to-one model allows the developer to create as many user thread at a time. By setting the mode to SJRUSR, we are indicating that the owner may read or write to the shared memory segment. Finally, we would
like to add some personal notes. One such enhancement involves recognizing pages from shared libraries. Serializable? If we compute the working-set size, WSSj, for each process in the system, we can then consider that where D is the total demand for frames. Processes are also isolated through the use of
distinct address spaces. All updates are recorded on the log, which is kept in stable storage. Even system calls are made by messages. One such member 142 Chapter 4 Threads in the thread pool API is the QueueUserWorkItemO function, which is passed three parameters: • LPTHREAD_START-ROUTINE Function—a pointer to the function that is to
run as a separate thread • PVOID Param—the parameter passed to Function • ULONG Flags—flags indicating how the thread pool is to create and manage execution of the thread pool to invoke PoolFunction () on behalf of the
programmer. This virus changes each time it is installed to avoid detection by antivirus software. System and a multithreaded program written using the many-to-many threading model. Alternative approaches to enforcing memory protection are
proposed and studied in Wahbe et al. Ease of electronic communication, mechanisms to copy source and binary files to remote machines, and access to both source code and human expertise allowed cooperative efforts to develop solutions quickly. 462 Chapter 12 Mass-Storage Structure Because of these complexities, the disk-scheduling algorithm
 should be written as a separate module of the operating system, so that it can be replaced with a different algorithm if necessary. To contribute to the overall reliability of a system, the access-control mechanism should be safe to use. What would be output from the program at LINE C and LINE P? The subsystem designer can define policies for use of
these resources by user processes, but the policies are enforceable by use of the standard access protection afforded by the capability system. 12.6.2 Swap-Space Location A swap space can reside in one of two places: It can be carved out of the normal file system, or it can be in a separate disk partition. However, by using the sample syllabi, a reader
can select a different ordering of chapters (or subsections of chapters). Optimal page replacement requires future knowledge. All objects in the slab are marked as free. Therefore, if another process also on host X wished to establish another connection with the same web server, it would be assigned a port number greater than 1024 and not equal to
1625. In Solaris, the process at the top of the tree is the sched process, with pid of 0. 2.4 Describe how you could obtain a statistical profile of the amount of time spent by a program executing different sections of its code. The fundamental goal of computer systems is to execute user programs and to make solving user problems easier. We next
illustrate several page-replacement algorithms. Hardware may trigger an interrupt at any time by sending a signal to the CPU, usually by way of the system bus. Dekker's algorithm (Exercise 6.1)—the first correct software solution to the two-process mutual-exclusion problem—was developed by the Dutch mathematician T. Since ciphertexts are
generally exposed (for example, sent 15.4 Cryptography as a Security Tool 579 on the network), it is important that it be infeasible to derive D(k) from the ciphertexts. The owner right controls these operations. The clock is incremented for every memory reference.
reset to the current time. Whenever an operation M is executed on an object O, within domain D-,, the global table is searched for a triple, with M e R/:. The task that creates the mailbox is that mailbox i
registers, saving the current state and the value of the program counter, and jumping to the beginning of the code corresponding to the salled procedure. : : : ; . Most current operating systems do not provide deadlock-prevention facilities, but such features will probably be added soon. A user who wishes to copy the file uses the f t p command as
execute of the individual storage segments associated with the object. The system can transfer the data by one of two basic methods. A logical address consists of two parts: a segment number, s, and an offset into that segment, d. To allow controlled domain switching, we modify the ring field of the segment descriptor to include the following:

•
Access bracket. The date client shown in Figure 3.20 can be used to read the multi-line fortunes returned by the fortune server. DES is now considered insecure for many applications because its keys can be exhaustively searched with moderate computing resources. A multithreaded process contains several different flows of control within the same
address space. Below sdt_shel, a 3.3 Operations on Processes 91 user's command-line shell—the C-shell or csh—is created. However, because access-rights information for a particular domain is not localized, determining the set of access rights for each domain is not localized, determining the set of access rights for each domain is not localized, determining the set of access rights for each domain is not localized.
and to help spread the virus. Our aim is to present these concepts and algorithms in a general setting that is not tied to one particular operating system. Hence, the read operation is rejected, and Tj- is rolled back. 9.12 Suppose that your replacement policy (in a paged system) is to examine each page regularly and to discard that page if it has not
been used since the last examination. For most computers, the bootstrap is stored in read-only memory (ROM). The new chapter provides a grand tour of the major operating-system components, along with basic coverage of computer-system organization. We provide several programming examples written in C illustrating the POSIX base API, as well
as Pthreads and the extensions for real-time programming. Beverly Peavler copy-edited the manuscript The freelance indexer was Rosemary Simpson. The semaphore in this example, by passing the flag 0, we are indicating that this semaphore can only be shared by threads belonging to the
same process that created the semaphore. This port is some arbitrary number greater than 1024. In this scenario, only one thread can run at once, so one LWP is sufficient. Hydra also provides rights amplification. Finally, we can group all keys into one global table of keys. In a large system with long access lists, this search can be time consuming. A
transaction T, that is rolled back as a result of the issuing of either a read or write operation is assigned a new timestamp and is restarted. If a page fault occurs for a process that is below its working-set maximum, the virtual memory manager allocates a page from this list of free pages. Each task in Linux has its own set of page tables and —just as in
Figure 8.23 — the CR3 register points to the global directory for the task currently executing. • Arrays, lists, and tables are often allocated more memory than they actually need. This scheme increases the probability that a page will be clean when it is selected for replacement and will not need to be written out. In a network communication, a man-
in-the-middle attack may be preceded by a session hijacking, in which an active communication session is intercepted. Hence, if we guess right and page in all pages. The first is the integer identifier of the shared-memory segment being
attached, and the second is a pointer location in memory indicating where the shared memory will be attached. As a current example, the installation of an innocuous-seeming program on a Windows system and a host operating system in
a system like VMware? If the lock is in a signaled state, WaitForSingleObjectO returns immediately, and the lock becomes nonsignaled. The critical property that an authenticator a e A such that V(k)(ni.a) - t r u e only if it possesses S(k). 14.10 Discuss which returns immediately, and the lock becomes nonsignaled.
of the following systems allow module designers to enforce the need-to-know principle. [1996]) and software fault isolation (Wahbe et al. Satisfying all these goals is difficult if the flexibility to implement protection policies is restricted by the support mechanisms provided or if protection environments are made larger than necessary to secure greater
operational efficiency. When an interrupt occurs, the system needs to save the current context of the process and then resuming it. However, the echo server cannot guarantee that it will read characters from clients; it may
receive binary data as well. Because the parent and child processes have their own copies of the data, it will be necessary for the child to output the sequence. In addition, a user (of the protection system) can declare other rights. Message passing provides a mechanism to allow processes to communicate and to synchronize their actions without
sharing the same address space and is particularly useful in a distributed environment, where the communicating processes may reside on different computers connected by a network. The system will need to know how to address each device (the device interrupt number), the device is type and model, and any special device
characteristics. We say that a system is secure if its resources are used and accessed as intended under all circumstances. Controllers to memory contents. Responsiveness. Suppose we allocate enough frames to a process to accommodate its current locality. This scheme is called swapping. Once delivered, the signal must be handled. Once A has
been selected, use of the working-set model is simple. Under this approach, to write a block on tape, we lock into memory the pages containing the block. [1976]. Thus, the segmentation and paging units form the equivalent of the memory-management unit (ViMU). When a CPU receives a reset event—for instance, when it is powered up or rebooted-
the instruction register is loaded with a predefined memory location, and execution starts there. Heap memory c. Second, an entry for the new file must be made in the directory. 4.1.1 Motivation Many software packages that run on modern desktop PCs are multithreaded. » Repositioning within a file. The various memory-management algorithms
(contiguous allocation, paging, segmentation, and combinations of paging and segmentation) differ in many aspects. These two processes will invoke wait (), which will cause it to be suspended until the child process exits. In general, sockets use a client-server architecture. This
 approach, though easy to implement, is inefficient. The twofish algorithm is fast, compact, and easy to implement. Prior to the protocol's use, the server s is assumed to have obtained a certificate, denoted cert, from certification authority CA. The virtual-machine concept takes the layered approach and treats both the kernel of the operating system
and the hardware as though they were hardware. This is a case of human error—a common security weakness. in ring /', it cannot access a segment associated, with ring/ (/ < i). When the event that the previously blocked thread is now
locality. Some systems take up less than 1 megabyte of space and lack even a full-screen editor, whereas others require gigabytes of space and are entirely based on graphical windowing systems. Thus, when a page fault occurs, there is a free frame available to page into. A process that is at its working-set minimum may be allocated pages from the
free-page frame list once sufficient free memory is available. The operating system can provide system calls to create, write, read, reposition, delete, and truncate files. Container objects, such as directories, can logically contain other objects. We wrote this book by collaborating in such a manner. Typically, the operating system uses two levels of
internal tables: a per-process table and a system-wide table. For the most part, protection mechanisms are the core of protection from accidents. Modern cryptography is based on secrets called keys that are selectively distributed to computers in a network and used to process messages. What factors need to be considered in choosing the host
operating system? Be sure to include all necessary error checking, including ensuring that the source file exists. If necessary, return values are passed back to the client using the same technique. Whenever a reference to a page is made, the contents of the clock register are copied to the time-of-use field in the page-table entry for that page. The stub
 then transmits a message to the server using message passing. The JVMis a specification for an abstract computer. This implementation suffers from several drawbacks. This program should work as follows: The user will run the program and will enter a number on the command line. As noted, each segment selector includes a 2-bit field for
protection. By default, when an object is created within a container object, the new object inherits permissions from the parent object. In general, most processes can be described as either L/O bound or CPU bound. See also disk(s) second-chance page-replacement algorithm (clock algorithm), 336-338 second extended file system (ext2fs), 766-769
 section objects, 107 sectors, disk, 452 sector slipping, 465 sector sparing, 465, 820 secure single sign-on, 400 secure systems, 560 914 Index security. Of course, not every method is allowed to assert a privilege only if its class is in a protection domain that is itself allowed to exercise the privilege. 9.11 Suppose that a
 machine provides instructions that can access memory locations using the one-level indirect addressing scheme. It is simply this: 9.4 Page Replacement on a reference string. The hardware implementation involves the use of a new bit
in the page tables of the CPUs. This bit marks the associated page as nonexecutable, disallowing instructions to be read from it and executed is unnecessary, as the program specified in the parameters to exec () will replace the
process. Secrecy: only the receiver can decrypt the message. com domain, in particular a proxy server proxy.lucent.com for retrieving URLs. For this reason, the untrusted applet's g e t () method, which performed its openO in a
 doPrivileged block. This initial bootstrap program tends to be simple. First, we begin with a discussion of implementing virtual memorythrough demand paging. Save the registers and process state for the other user (if step 6 is executed). 468 Chapter 12 Mass-Storage Structure - swap area page slot Swap partition 1;!; •!;M;Hi;!M or swap file j::; J j : |
%:\ ill • : • : : : . Even if only a modest change has been made to a large file, all the data must be transferred. Some can be accessed only sequentially, others randomly. Access to the file is carried out at site A and could be initiated by an RPC. signal-safe/ indicating it can be called from inside a signal-handling function; such guarantees cannot be
made of printf().) This program will run in the while (l) loop until the user enters the sequence. When a process is first created, it is assigned a working-set minimum and maximum. One of the most novel and useful features of Java is its support for dynamically loading untrusted classes over a network and for executing mutually distrusting
classes within the same ]"VM. Chapter 7, Deadlocks, is the old Chapter 8. Issues related to trusting computer programs are discussed in Thompson [1984]. The semantics of the f ork() and exec() system calls change in a multithreaded program could take less physical memory, ?inore programs could take less physical memory, ?inore programs could take less physical memory.
be run at the same time, with a corresponding increase in CPU utilization and throughput but with no increase in response time or turnaround time. 16.5 Communication Structure 623 To solve this problem, processes on remote systems are generally identified by the pair This scheme puts policy specification at the disposal of the programmers, while
freeing them from implementing its enforcement. In any of these systems, great care must be taken in writing privileged programs. The producer-consumer problem also provides a useful metaphor for the execvpO function, which has the
following interface: execvp(char *command, char *params[]); where command to be performed and par ams stores the many-to-many model.(such as Tru64 UNIX), a Java thread is mapped according to the many-to-many to-many model.
many model. The process can now access the page as though it had always been in memory. In many systems, deadlocks occur infrequently (say, once per year); thus, this method is cheaper than the prevention, avoidance, or detection and recovery methods, which must be used constantly Also, in some circumstances, a system is in a frozen state but
not in a deadlocked state. A similar protection system would notbe suited to a computer being used for number crunching, in which performance is of utmost importance. Some systems provide no hardware support, and other pagereplacement algorithms (such as a FIFO algorithm) must be used. With symmetric algorithms, both parties need the key
and no one else should have it. Other processes that want to use this region of shared memory must specify this identifier. We thank the following people who reviewed this version of the book: Bart Childs, Don Heller, Dean Hougen Michael Huangs, Morty Kewstel, Euripides Montagne, and John Sterling. When a user creates a new object O-, the
column 0/ is added to the access matrix with the appropriate initialization entries, as dictated by the creator. Here, only the sender names the recipient; the recipient is not required to name the sender names the recipient; the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient; the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the sender names the recipient is not required to name the name that name 
what ways does it differ from the layered approach? ,g Logical to physical address translation in the Pentium. It is important that the long-term scheduler make a careful selection. Thus, if a page was used within the last 10,000 to 15,000
references. 8.8 Summary Memory-management algorithms for multiprogrammed operating systems range from the simple single-user system approach to paged segmentation. Greg would like to acknowledge the continued interest and support from his family. No work is getting done, because the processes are spending all their time paging. More
complete coverage of SSL 3.0 can be found at . If you would like to suggest improvements or to contribute exercises, we must first read the relevant page from disk and then access the desired word. The list is
moderated, so you will receive no inappropriate mail. The following kinds of information must be determined. When this space is not in use by the operating system/ it can be used to support user paging. [1991] by evaluating securely
over an insecure channel. Grosso [2002] discussed RMI in significant detail. When it is determined that a page is going to be duplicated using copyon-write, it is important to note the location from which the free page will be allocated. It enforces the resource requests tlirough sophisticated stack inspection and via the type safety of the language. The
system also may define an algorithm for selecting which process will receive the message (that is, round robin where processes take turns receiving messages). If these two protocols are used, then the circular-wait condition cannot hold. If instead we had pages of only 1 byte, then we could bring in only the 100 KB that are actually used, resulting in
only 100 KB transferred and allocated. This may occur in a system where several different applications open the same file at 
system to another but typically consist of these: s Name. For example, in 2000, the love bug virus became very widespread by appearing to be a love note sent by a friend of the receiver. The architecture of the CLR for the .NET framework is shown in Figure 2.1.8. C++ source VB.Net source MS-IL assembly MS-IL assembly compilation CLR just-in-
time compiler host system Figure 2.18 Architecture of the CLR for the .NET Framework. For example, using the function defined previously, a process that wants to use the tape drive and printer at the same time must first request the printer. 118 Chapter 3 Processes 3.7 Repeat the preceding exercise, this time using
the CreateProcess 0 in the Win32 API. with whether the stack is stored before or after the Sqrt () function. The reference to page 2 replaces page 7, because 7 will not be used at 5, and page 1 at 14. This program will invoke the shmctl () function to obtain its shnuds structure. The loader would take all
these segments and assign them segment 1000; 1400 I 400 \ 6300 i 400 4300 1100 3200 4'-0C0 3200 segment 1 dogical address space 5700 6303 segment i 6700 physical memory Figure
8.20 Example of segmentation. The design of a new operating system is a major task. You can assume that only one space will separate the 'r' and the first letter and Bibliographical Notes 125 that the letter will be followed by ". The system must protect itself from accidental or purposeful security breaches. When the disk read is complete, we modify
the internal table kept with the process and the page table to indicate that the page is now in memory. The detection algorithm 264 Chapter 7 Deadlocks described here simply investigates every possible allocation sequence f is generated. For example, a chat program used on the World Wide Web could be designed so that chat participants
communicate with one another by exchanging messages. As we shall see in Chapters 17 and 18, these actions present difficult problems that have many possible solutions. When a context of the new process scheduled to run. A problem with this
approach is that changing the bootstrap code requires changing the ROM hardware chips. This will involve creating M x N worker threads. However, considering that many child processes invoke the exec() system call immediately after creation, the copying of the parent's address space may be unnecessary. Sometimes the replay comprises the
entire attack— for example, in a repeat of a request to transfer money. Beveridge and Wiener [1997] and Cohen and Woodring [1997] describe multithreading using Win32. These two printers may be defined to be in the same resource class if no one cares which printer prints which output. The system must then be configured or generated for each
specific computer site, a process sometimes known as system generation (SYSGEN). Such a system is designed for one user to monopolize its resources. The symbolic file name is the only information kept in humanreadable form,. With these two bits, we have the following four possible classes: 338 Chapter 9 Virtual Memory 1. Under most
circumstances, a user of an operating system does not need to install network daemons. Once a virus reaches a target machine, a program in execution. Rather, one cracker can determine the bug and then write an exploit. S41: ....:; . h file. These
certificate authorities have their public keys included within web browsers (and other consumers of certificates) before they are distributed. The zero-capacity case is sometimes referred to as a message system with no buffering; the other cases are referred to as systems with automatic buffering. For each use of a kernelmanaged resource by a
process or thread, the operating system checks to make sure that the process has requested and has been allocated the resource. We can see how this allows a fine degree of control over access to objects. j ava that resides on "cs.yale.edu." The user must first invoke the FTP program by executing ftp cs.yale.edu The program then asks the user for a
 login name and a password. Stealth. A multicast socket allows data to be sent to multiple recipients. Why? When counters are decreased 4. 4.5 Operating-System Examples 143 -user thread UWP - lightweight process -kernel thread Figure 4.9 Lightweight process (LWP.) An application may require any number of LWPs to run efficiently. The only of the counters are decreased 4. 4.5 Operating-System Examples 143 -user thread UWP - lightweight process -kernel thread UWP - lightweight process -kernel thread Figure 4.9 Lightweight process -kernel thread UWP - lightweight process (LWP.) An application may require any number of LWPs to run efficiently.
drawback to this model is that creating a user thread requires creating the corresponding kernel thread. What other kinds of waiting are there in an operating system? 4.6 As described in Section 4.5.2, Linux does not distinguish between processes and threads. In what cases it would be impossible for user-level programs to provide these services?
Notice that we may have to scan the circular queue several times before we find a page to be replaced. VIl viii Preface If a feature exists in Windows 2000 but not in Windows XP, then we wili refer specifically, s t r u c t task.struct) exists for each task in the system. 14.7 Revocation of
Access Rights In a dynamic protection system, we may sometimes need to revoke access rights to objects shared by different users. The Intel Pentium address • selector descriptor table 32-bit linear address Figure 8.22 Intel Pentium segmentation. Are packets
sent individually or as a sequence? With this scheme, a key can be associated with several bejects, and several keys can be associated with each object, providing maximum flexibility. We see this situation, for example, with a real-time process running at the highest priority (or any process running on a nonpreemptive scheduler) and never returning
control to the operating system. The segments are stored in physical memory as shown. The program queried finger with a 536-byte string crafted to exceed the buffer allocated for input and to overwrite the stack frame. After this page is brought into memory, the process continues to execute, faulting as necessary until every page that it needs is in
memory. For example, classes loaded from a trusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from an untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows them to access files in the user's home directory, whereas classes loaded from a untrusted server might be placed in a protection domain that allows the user's home directory.
elements. Of the total I/O time (28.2 milliseconds), therefore, only 1 percent is attributable to use the cable exclusively for data network traffic. The new process tries to get started by taking frames from running processes, causing more page faults and a longer queue for the paging device. A common bug
involves spawning subprocesses infinitely. If a stack frame is first found for which access in disallowed based on the protection domain of the method's class, then checkPermissionsO throws an AccessControlException. Because of its general-purpose nature, this allocator is now also used for certain user-mode memory requests in Solaris. Because
up or rebooted—it must have an initial program to run. 9.18 Assume there is an initial 1024 KB segment where memory is allocated using the buddy system. UNIX is representative, providing read, write, and execution protection separately for the owner, group, and general public for each file. Multimedia systems require quality-of-service guarantees
ensuring that the multimedia data are delivered to clients within a specific time frame. [1995] discusses page tables for 64-bit address spaces. When the amount of free memory falls below the threshold, the virtual memory manager uses a tactic known as automatic working-set trimming to restore the value above the threshold. The Ethernet protocol
is defined by the IEEE 802.3 standard. Figure 15.5 shows how a boot virus works. If all licenses are in use, requests to start the application are denied. For example, we are assuming that, in step 6, the CPU is allocated to another process while the I/O occurs. If the queue is not full when a new message is sent, the message is placed in the queue is not full when a new message is sent, the message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is sent, the message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is sent, the message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message is placed in the queue is not full when a new message i
(either the message is copied or a pointer to the message is copied or a pointer to the message is kept), and the sender can continue execution without waiting. We chose Linux and FreeBSD because UNIX—at one time—was almost small enough to understand yet was not a "toy" operating system. For macro viruses, one defense is to exchange Word documents in an alternative file format
called rich text format (RTF). In this example, we considered the possibility that the program being attacked—the code shown in Figure 3.7—ran with system-wide permissions. The operating system must select, for scheduling purposes, processes 88 Chapter 3 Processes I/O request time slice expired fork a child wait for an interrupt Figure 3.7
Queueing-diagram representation of process scheduling. First, the limit is used to check for address validity. For example, SMTP is used for mail transfer. This type of attack can be defeated by having the operating system print a usage message at the end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the c o n t r o l - a l t - d end of an interactive session or by a non-trappable key sequence, such as the content of a l t - d end of an interactive session or by a non-trappable key sequence, such as the content of a l t - d end of a l t - d end
let e combination used by all modern Windows operating systems. A variety of techniques can be provided by a programming-language implementation to enforce protection, but any of these must depend on some degree of support from an underlying machine and its operating systems. It must, however, hold a lock on a data item as long as it
 accesses that item. physically contiguous pages 256KB; '|;|: ; : - | A H i|o;:: • •;; ':; :: ; ';•;; ... Perlman [1988] proposes an approach to diagnose faults when the network contains malicious routers. Note that a parent needs to know the identities of its children. The consumer may have to wait for new items, but the producer can always produce new
items. However, the communication cost is high, since a message may have to cross a large number of links. 6.4 Explain why spinlocks are not appropriate for single-processor systems. While a user process is executing, a page fault occurs. Typically, a separate stub exists for each separate remote
procedure. For example, you could join on ten threads using the Pthread code depicted in Figure 4.12. ;:• ": :: •:• ': •': ; -: -; :: :: •-. This case is a typical one in which the rights held by a process for access to a protected segment must change dynamically, depending on the task to be performed. 14.5.2 Access Lists for
 Objects Each column in the access matrix can be implemented as an access list for one object, as described in Section 10.6.2. Obviously, the empty entries can be discarded. The working-set window is a moving window. Every thread in the JVM has an associated stack of its ongoing method invocations. 9.8 Discuss situations under which the most
frequently used page-replacement algorithm generates fewer page faults than the least recently used page-replacement algorithm. How could the operating system allow access to other memory? Exercises 15.1 Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Attach the
shared-memory segment to its address space. To minimize internal fragmentation, then, we need a small page size. Web-site defacement is a common example of this type of security breach. Consider the simple C program shown in Figure 15.2. This program creates a character array of size BUFFER SIZE and copies the contents of the parameter
provided on the command line—argv[1]. Such an approach is particularly useful for large page sizes. Parnas [1975] discussed some of the flaws in Patil's arguments. Content of This Book The text is organized in eight major parts: • Overview. It can range from a few megabytes of disk space to gigabytes. What are the strengths and weaknesses of the
two approaches? This method is usually employed when the process must be moved to satisfy a hardware or software preference. A paper on the dangers of a computer monoculture can be found at . In addition to differing in speed and cost, the various storage systems are either volatile or nonvolatile. It will then output the following values of the
given shared-memory segment: • Segment ID • Key • Mode Exercises 121 • Owner If ID • Size • Number of attaches Project consists of modifying a C program which serves as a shell interface that accepts user commands and then executes each command in a separate process. 8.7.2 Pentium Paging Theorem
Logic Bomb Consider a program that initiates a security incident only under certain circumstances. The operating system then must provide a mechanism that allows a process to do the following: • Create a new mailbox. onto location
4300 + 53 = 4353. An operating system is a control program. The resulting filename and associated messagedigest list must then be kept free from unauthorized access. These techniques can be used for communication in client-server systems (1.12.2) as well. Because each transaction is atomic, the concurrent execution of transactions must be
 equivalent to the case where these transactions are executed serially in some arbitrary order. Bibliographical Notes Demand paging was first used in the Atlas system, implemented on the Manchester University MUSE computer around 1960 (Kilburn et al. This is a specification for thread behavior, not an implementation. The mainO function will be
passed three parameters on the command line: 1. An object file is a sequence of bytes organized into blocks understandable by the system's linker. Photo Courtesy: Klaus Vedfelt/Getty Images You can also browse by series or Oxford Reading Level. h> sem_t sem mutex; /* create the semaphore */ sem_init(&mutex, 0, 1); /* acquire the semaphore */
sem_wait(&mutex); /*** c r i t i c a l section ***/ /* release the semaphore */ sem_post(femutex); Win32 Details concerning thread creation using a few different techniques. Mailing List We have switched to the mailman system for communication among the users the semaphore */ sem_post(femutex); Win32 Details concerning thread creation using a few different techniques. Mailing List We have switched to the mailman system for communication among the users the semaphore */ sem_post(femutex); Win32 Details concerning thread creation using a few different techniques.
of Operating System Concepts. As they queue up for the paging device, the ready queue empties. Finally, with Java, it provides a form of process migration: Java applets are sent from the server to the client, where they are executed. Because the information in the log is used in reconstructing the state of the data items accessed by the various
transactions, we cannot allow the actual update to a data item to take place before the corresponding log record is written out to stable storage. When it is created, it will use that file name, open the file, and write the contents out. Let the set of processes involved in the
circular wait be {PQ, P\,..., P,,}, where P. 2,500 d. [2000], Hu et al. CHAPTER OBJECTIVES • To develop a description of deadlocks, which prevent a number of different methods for preventing or avoiding deadlocks in a computer system. • To discuss file-system design tradeoffs,
including access methods, file sharing, file locking, and directory structures. Typically, such systems use a notation wherein the data structure for a process contains pointers to the separate threads belonging to the process. •-• ... The class loader loads the compiled . • Java. The purpose of an operating system is to provide an environment in which
a user can execute programs in a convenient and efficient manner. • Each procedure may be a domain. 6.11 The Sleeping-Barber Problem. Furthermore, whereas f ork () is passed no parameters, CreateProcess 0 expects no fewer than ten parameters, convenient and efficient manner.
either the Windows32 or POSIX API. 0 1 0 A 2 valid-invalid 1 B 2 C 4 3 D 5 4 E 6 5 F 7 6 G 8 7 H logical memory Figure 9.5 Page table when some pages are not in main memory. Suppose that a user on "cs.uvm.edu" wants to copy a Java program Server. The broadest tool available
to system designers and users is cryptography. The action has been characterized as both a harmless prank gone awry and a serious criminal offense. Burns [1978] developed the hardware-solution algorithm that satisfies the bounded-waiting requirement. As mentioned above, the pageout process checks memory four times per second. £ , : : . For
 instance, it may be useful to know that, although a new algorithm is not optimal, it is within 12.3 percent of optimal at worst and within 4.7 percent on average. Rather, users prefer to view memory as a collection of variable-sized segments., with no necessary ordering among segments (Figure 8.18). Discussions concerning UNIX security are offered
                and Morris [1984], Wood and Kochan [1985], Farrow [1986a], Far
single disk is 100,000 hours. This memory sharing is illustrated in Figure 9.23. Notice that, in our example, the user at the University of Vermont must have login permission on "cs.yale.edu." FTP also provides a way to allow a user 16.2 Types of Distributed Operating Systems 615 who does not have an account on the Yale computer to copy files
remotely. For each Java class, the compiler produces an architecture-neutral bytecode output (. Disk manufacturers have been alleviating this problem by implementing disk-scheduling algorithms in the controller hardware built into the disk drive. [1991], and Williams [2002] discusses scheduler activations in the NetBSD system. 7.6.2 Several
Instances of a Resource Type The wait-for graph scheme is not applicable to a resource-allocation system with multiple instances of each resource type. The SYSGEN program reads from a given file, or asks the operator of the system for information concerning the specific configuration of the hardware system, or probes the hardware directly to
determine what components are there. Local replacement might hinder a process, however, by not making available to it other, less used pages of memory. For example, a system without memory protection cannot be secure. As might be expected, establishing dynamic protection domains is more complicated than establishing static protection
domains. 15.10 Summary Protection is an internal problem. It is generally considered infeasible to build a network of any scale in which the source and destination addresses of packets can be trusted in this sense. See also directories accessing information on, 382-384 direct access, 383-384 sequential access, 382-383 attributes of, 374-375 batch
379 defined, 374 executable, 82 extensions of, 379-390 internal structure of, 381-382 locking open, 377-379 operations on, 375-377 protecting, 402-406 via passwords/permissions, 406-407 recovery of, 435-437 storage structure for, 385-386 Index file access, 377, 402-406 file-allocation table (FAT), 425 file-control block (FCB)
413 file descriptor, 415 file handle, 415 FileLock (Java), 377 file management, 55 file-management system calls, 53 file mapping, 350 file
file sharing, 397-402 and consistency semantics, 401-402 with multiple users, 397-398 with networks, 398-401 and client-server model, 398-399 and distributed information systems, 399-400 and failure modes, 400-401 file systems, 397-398 with networks, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems, 398-401 and client-server model, 398-399 and distributed information systems.
extended, 412 implementation of, 413-419 mounting, 417 partitions, 416-417 virtual systems, 417-419 levels of, 412 Linux, 764-770 log-based transaction-oriented, 437-438 logical, 412 mounting of, 395-397 network, 438-444 remote, 398 WAFL, 444-446 897 File System Hierarchy Standard f, document, 740 file-system management, 22-23 file-system
manipulation (operating system service), 40 file transfer, 614-615 file transfer protocol (FTP), 614-615 file viruses, 569 filter drivers, 806 firewalls, 31, 599-600 firewall management, 776 firew
scheme, 286 fixed priority (Solaris), 176 fixed routing, 625 floppy disks, 452^153 flow control, 521 flushing, 294 folders, 42 footprint, 697 foreground processes, 166 forests, 827-828 forkO and exec() process model (Linux), 748-750 fork() system call, 138 formatting, 462^163 forward-mapped page tables, 298 fragments, packet, 776
fragmentation, 287-288 external, 287-288, 422 internal 287, 382 frame(s), 289, 626, 716 stack, 566-567 victim, 329 frame allocation, 340-343 equal allocation, 341 global vs. [1981]. Capabilities were originally proposed as a kind of secure pointer, to meet the need for resource protection that was foreseen as multiprogrammed computer systems
came of age. The final option is meant for server tasks, such as a line-printer driver. Usually, one task is to run diagnostics to determine the state of the machine. If revocation is delayed, can we find out when it will take place? To compute the effective access time, we must know how much time is needed to service a page fault. Then, it reverses
direction immediately, without going all the way to the end of the disk. If / < /, then D; is a subset of D; . Part Four Since main memory is usually too small to accommodate all the data and programs permanently, the computer system must provide secondary storage to back up main memory. Suggest a scheme for implementing this policy efficiently
For instance, suppose that the queue usually has just one outstanding request. IP encapsulates the TCP 15.4 Cryptography as a Security Tool 585 packet in an IP packet, which it similarly passes down to the data-link layer t© be transmitted across the network to its IP peer on the destination computer. Instead, data are always copied between system
memory and user memory. Now suppose that processes P\, Vi, and P3 all share mailbox A Process Pi sends a message sent by Pi? Describe the undesirable consequences that could arise from not enforcing either the "at most once" or "exactly once o
semantic. jVM's stack-inspection scheme 14.11 Describe how the Java protection model would be sacrificed if a Java protection model would be sacrificed if a Java protection scheme 14.11 Describe how the Java protection model would be sacrificed if a Java protection model would be sacrificated in the sacrification would be 
\{1,2,5,6,7\} WS(f2) = \{3,4\} Figure 9.20 Working-set modef. Calvertand Donahoo [2001] provided coverage of socket program in Java. This program is to generate. For example, consider the IBM. c to define your system call. When
the file is closed, all the memory-mapped data are written back to disk and removed from the virtual memory of the process; the variable id is set to the name of the process with which communication has taken place. 15.2 Program Threats 565 Trap doors pose a difficult problem
because, to detect them, we have to analyze all the source code for all components of a system. i: .. A clever trap door could be included in a compiler. Indeed, launching an attack that prevents legitimate 5use is frequently easier than breaking into a machine or facility. The full bootstrap program is more sophisticated than the bootstrap loader in the
boot ROM; it is able to load the entire operating system from a non-fixed location on disk and to start the operating system running. This approach, in which the path through the kernel is extended to make building the operating system easier. 8.7 Compare paging with segmentation with respect to the amount
of memory required by the address translation structures in order to convert virtual addresses to physical addresses. The virus dropper is usually a Trojan horse, executed for other reasons but installing the virus as its core activity. Partial. The perprocess table tracks all files that a process has open. Therefore, the chunks are not just encrypted but
also XORed with the previous ciphertext block before encryption. For efficiency, we may check the default set first and then search the access list. In other words, these resources are implicitly released. What the initial value of the counters is 2. The contents of the command entered by the user is loaded into the args array. However, the next-highest
power of 2 from 21 KB is 32 KB so either B; or BR is again divided into two 32-KB buddies, C[. UNIX systems use signals to notify a process that a particular event has occurred. If the parent terminates, however, all its children have assigned as their new parent the init process. 15.4 Cryptography as a Security Tool 583 If encryption can prove the
identity of the sender of a message, then why do we need separate authentication algorithms? As a result, enforcing protection at the granularity of the [VM process is insufficient. The two processes, Pa and Pi, share the following variables: boolean flag[2]; /* in itially false */ int turn; The structure of process P; (i == 0 or 1) is shown in Figure
6.25; the other process is P,- (j == 1 or 0). In this chapter we provide a general overview of the major components of an operating system. By doing so, this method takes responsibility for the request. i ..-•;..: ::: :-.;-.: In the extreme, if A is infinite, the
working set is the set of pages touched during the process execution. A page fault may occur at any memory reference. The procedures that implement such operations are themselves a form of object, and they are accessed indirectly by capabilities. For example, the Internet WAN provides the ability for hosts at geographically separated sites to
communicate with one another. 620 Chapter 16 Distributed System Structures : : ; ;:usef processes :;: • ": • • : • . 310 Chapter 8 Main Memory • Fragmentation. The use of the feature is supported in several x86 operating systems, including Linux and Windows XP SP2. So that the computer system will be convenient to use, the operating systems
provides a uniform logical view of information storage. Restricting a child process to a subset of the parent's resources prevents any process from overloading the system by creating too many subprocesses. This elaborate and efficient three-stage password-cracking algorithm enabled the worm to gain access to other user accounts on the infected
system. See also process synchronization synchronous devices, 506, 507 synchronous message passing, 102 synchronous writes, 434 SYSGEN, see system generation system boot, 71-72 system calls (monitor calls), 7, 43-55 and API, 44-46 for communication, 54-55 for device management, 53 for file management, 53 functioning of, 43-44 for
information maintenance, 53-54 for process control, 47-52 system device, 810 system devic
strategy, 697, 698 system process (Windows XP), 810 system resource-allocation graph, 249-251 system restore, 810 system resto
per-process open-hie, 414 routing, 625 segment, 304 system-wide open-file, 414 tags, 543 tapes, magnetic, 453<sup>54</sup>, 480 target thread, 139 tasks: Linux, 750-751 VxWorks, 710 task control blocks, see process control blocks, see 
driver interface), 822 telnet, 614 Tenex operating system, 853 terminated state, 83 terminated state (Windows XP), 789 termination: cascading, 95 process, 90-95, 266 tertiary-storage, 478^88 future technology for, 480 and operating system support, 480-483 performance issues with, 484-488 removable disks, 478-
480 tapes, 480 tertiary storage devices, 24 text files, 374 text section (of process), 82 theft of service, 560 THE operating system, 846-848 thrashing, 343-345 defined, 345-347 files, 374 text section (of process), 82 theft of service, 560 THE operating system, 846-848 thrashing, 343-348 cause of, 343-345 defined, 343-345 defined, 343-345 defined, 343-345 defined, 345-347 files, 345-347 files, 345-348 thrashing, 343-348 cause of, 345-348 thrashing, 343-348 cause of, 345-348 thrashing, 345-348 thr
(Strangely, if we let S be the reverse of a reference string S, then the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the same as the page-fault rate for the OPT algorithm on 5 is the s
1 " i'; 1!" "; i 1; 1 ••-; •-••• KB: •.-• L:; ; i; ; •; •»: •• 6 4; i KB. The equivalent of the signal () operation on Win32 semaphores is the Release Semaphore of function. Fortunately, except for clogging e-mail systems and users' inboxes, it was relatively harmless. How do we allocate the fixed amount of free memory among the various processes?
The concept of a capability evolved from Iliffe's and Jodeit's codewords, which were implemented in the Rice University computer (Iliffe and Jodeit 129 in Linux, 144-146, 750-751 pools, thread, 141-142 and process model, 84—85
scheduling of, 172-173 target, 139 user, 129 in Windows XP, 144, 145, 789-790, 830, 832-833 thread scheduling, 153 thread scheduling, 153 thread-specific data, 142 threats, 560. Operating systems typically allocate these pages using a technique known
as zero-fill-on-demand. are 1,2, 5,14, 42,132 A formula generating C(i is C = ] (In) — (-"-! 370 Chapter 9 Virtual Memory using the Win32 API as outlined in Section 9.7.2. The producer process will generate the Catalan sequence and write it to a shared memory object. When the I/O is
complete, the pages are unlocked. For example, in an IP network, TCP (a transport-layer protocol) acts as a client of IP (a network-layer protocol): TCP packets are passed down to IP for delivery to the TCP peer at the other end of the TCP connection. When a user process started execution, it would generate a sequence of page faults. The Seventh
Edition As we wrote this seventh edition of Operating System Concepts, we were guided by the many comments and suggestions we received from readers of our previous editions, as well as by our own observations about the rapidly changing fields of operating systems and networking. These options or values might include how many buffers of
which sizes should be used, what type of CPU-scheduling algorithm is desired, what the maximum number of processes to be supported is, and so on. Because we specify 0 as a flag, we provide the thread of control. A thread that is to be
canceled is often referred to as the target thread. Figure 3.11 Process creation. Writes by any of the processes modify the data in virtual memory and can be seen by all others that map the same section of r - i I + • • r r I • . 2.3 Describe three general methods for passing parameters to the operating system. 574 Chapter 15 Security With each new
access, the worm program searched for already active copies of itself. CAP has two kinds of capabilities. Frequently, some or all of the operating systems cannot tolerate a page fault caused by the kernel. Let D, and D- be any two domain rings. c on the terminal using the UNIX cat command.
The cigarette-smokers problem (Exercise 6.8) was developed by Patil [1971]. This restriction, however, makes the task of programming more difficult. Consequently, it quickly faults again, and again, replacing pages that it must bring back in immediately. The memory-mapping system calls can also support copy-on-write functionality,
allowing processes to share a file in read-only mode but to have their own copies of any data they modify. To ensure atomicity despite system failure, we can use a write-ahead log. In this instance we are loading the Microsoft Windows mspaint.exe 3.3 Operations on Processes 95 application. This process might either send a message back to Q or
repeat the cycle. 572 Chapter 15 Security The generalization is that sharing secrets (to prove identity and as keys to encryption) is required for authentication and encryption, and that is easier in environments (such as a single operating system) in which secure sharing methods exist. Alternatively, a program may choose to set up its own signal-
handling function by setting the saJhandler field in struct is gaction to the name of the function, passing it (1) the signal and then invoking the struct is gaction to the name of the function, passing it (1) the signal and then invoking the struction which will handler for, and (2) a pointer to struct is gaction to the name of the function, passing it (1) the signal and then invoking the struct is gaction to the name of the function, passing it (1) the signal we are setting up a handler for, and (2) a pointer to struct is gaction to the name of the function which will handle the signal and then invoking the struct is gaction to the name of the function which will handle for, and (2) a pointer to struct is gaction to the name of the function which will handle for the function which will handle for the signal and then invoking the structure is gaction to the name of the function which will handle for the function which will handle for the signal and then invoking the structure is gaction to the signal and the s
CPU utilization. All messages have the same priority. Issue a read from the disk to a free frame: a. Some of these flags are listed below: flag meaning CLONE FS File-system information is shared. Furthermore, each process has its own task-state segment (TSS), and the descriptor for this segment is stored in the GDT. Most of the file operations
mentioned involve searching the directory for the entry associated with the named file. System-call firewalls sit between applications of the following scenarios. This trade-off is reasonable; if a given storage system were both faster and less expensive than another
```

```
—other properties being the same—then there would be no reason to use the slower, more expensive memory. Under what circumstances is one scheme preferable to the other? Formatting a disk with a larger sector size means that fewer sectors can fit on each track; but it also means that fewer headers and trailers are written on each track and
more space is available for user data. How many page faults occur for your algorithm for the following reference string, with four page frames? Any command that is executed in the history buffer as the next command, (r x does not go into the history list; the actual
command that it specifies, though, does.) It the user attempts to vise this history facility to run a command and the command is detected to be erroneous, an error message should be given to the user attempts to vise this history facility to run a command and the command is detected to be erroneous, an error message should be given to the user and the command and the command is detected to be erroneous, an error message should be given to the user and the command and the command and the command is detected to be erroneous, an error message should be given to the user attempts to vise this history facility to run a command and the command is detected to be erroneous, an error message should be given to the user attempts to vise this history facility to run a command and the command and th
 "infect" other programs. Here is a code sample that shows the simplicity of writing a Visual Basic macro that a virus could use to format the hard drive of a Windows computer as soon as the file containing the macro was opened: Sub AutoOpen() Dim oFS Set oFS = CreateObject("Scripting.FileSystemObject") vs = Shell("c: command.com End Sub /k
format c:'',vbHide) How do viruses work? Vahalia [1996] covers threading in several versions of UNIX. If we decide to prevent replacement this mechanism. Even slight improvements in demand-paging methods yield large gains in system
performance. 6.9.3 Checkpoints When a system failure occurs, we must consult the log to determine those transactions that need to be redone and those that need to be undone. The boundedbuffer problem, and Dijkstra [1965a] and Dijkstra [1971]. If it
is valid, then the value of the offset is added to the value of the base, resulting in a 32-bit linear address. A standard file virus infects a system by appending itself to a file. The second issue is more troublesome: If we allow all concurrent requests to be serviced in a new thread, we have not placed a bound on the number of threads concurrently active
in the system. If the code was malevolent, untold damage to a vast number of machines could have resulted. The computer has 218 bytes of physical memory. [1990] describe 152 Chapter 4 Thread [] workers = new Thread [NUMJTHREADS]
for (inti=0; i < NUM_THREADS; i try { workers[i].join(); } catch (Interrupted Exceptionie) { Figure 4.13 Java code for joining ten threads. SCAM and C-SCAN perform better for systems that place a heavy load on the disk, because they are less likely to cause a starvation problem.. Authentication of a user account is typically
 accomplished via a user name and password, although the modular design of Windows XP allows the development of custom authentication packages. • R-timestamp(Q) denotes the largest timestamp of any transaction that successfully executed read(Q). Notice that, if no frames are free, two page transfers (one out and one in) are required. In
addition, every access to the object must be checked, requiring a search of the access list. This memory holds those pages that are not present in main memory. Specifically address these problems: 1. The number of consumer threads A skeleton for this function appears as: #include int main(int argc, char *argv[]) { /* 1. To resolve differences like
this, many RPC systems define a machine-independent representation of data. With a tagged-capability system, in which all address .552 Chapter 14 Protection computation is performed either by hardware or by a fixed microprogram, even greater security is possible. R,:. Many different types of information may be stored in a file—source programs
object programs, executable programs, numeric data, text, payroll records, graphic images, sound recordings, and so on. In addition, if the function occurs correctly. These systems have specific requirements that differ from those of the general-
purpose systems that are the focus of the remainder of the text. • Disk location of the Internet to the DMZ computers to the Internet to the DMZ computers to the Internet to the DMZ computers to the Internet to the DMZ computers and from the Internet to the DMZ computers to the Internet to the DMZ computers and from the Internet to the DMZ computers to the Internet to the DMZ computers and from the Internet to the DMZ computers and from the Internet to the DMZ computers to the Internet to the DMZ computers and from the Internet to the Internet to the DMZ computers and from the Internet to the DMZ computers and from the Internet to the DMZ computers and from the Internet to the 
from Internet file-sharing services or exchange infected disks. This project is organized into two parts: (1) creating the child process and executing the child process are child process.
store kernel objects. Bibliographical Notes The access-matrix model of protection between domains and objects was developed by Lampson [1971]. One thread immediately terminates the target thread. The child process is a duplicate of the parent process (it has the same program and data as the parent). Hence, the access
matrix of Figure 14.5(a) can be modified to the access matrix shown in Figure 14.5(b). This pointer, not the actual file name, is used in all I/O operations, avoiding any further searching and blocking disallowed or malformed XML
In still other cases, users sit at workstations connected to networks of other workstations and servers. From that point on, all 616 Chapter 16 Distributed System Structures access to the file is local. All of these aspects must be addressed for security to be maintained. A process of 200 KB that used only half of that memory would generate only one
page fault with a page size of 200 KB but 102,400 page faults with a page size of 1 byte. Capon, John Carpenter, Gil Carrick, Thomas Casavant, Ajoy Kumar Datta, Joe Deck, Sudarshan K. In general, resource sharing in a distributed database, printing
 files at remote sites, using remote specialized hardware devices (such as a high-speed array processor), and performing other operations. The Windows 2000 system places its boot code in the first sector on the hard disk (which it terms the master boot record, or MBR). A process may request as many resources as it requires to carry out its
designated task. Most systems, however, require that the programmer open a file explicitly with the openO system call before that file can be used. Short-term (CPU) scheduling is the selection of one process from the ready gueue. To provide inherent protection, we must distinguish capabilities from other kinds of objects and they must be interpreted
by an abstract machine on which higher-level programs run. The devices that attach to a computer vary in many aspects. However, particular attention is paid to the Microsoft family of operating systems (including Windows XP) and Wac OS X). If a page fault
occurs and if the page exists in the free-frame pool, how is the resident page set and the free-frame pool managed to make space for the requested page? In addition, with virtual memory, several processes can share system libraries and memory. If you wish to use this facility, please visit the following URL and follow the instructions there to
subscribe: The mailman mailing-list system provides many benefits, such as an archive of postings, as well as several subscription options, including digest and Web only. • If local objects are to be passed as parameters to remote objects, they must implement the interface j ava. Unfortunately, good bounds checking is the exception rather than the
norm. 8.7 Example: The Intel Pentium Both paging and segmentation have advantages and disadvantages and disadvantages and disadvantages. However, because in most instances the JVM is running on top of a host operating system. Chapters 16 through 18 deal with a collection of
processors that do not share memory or a clock—a distributed system. Programs tend to have locality of reference, described in Section 9.6.1, which results in reasonable performance from demand paging. Ideally, we want the programs and data to reside in main memory permanently. In fact, we cannot guarantee that less than 50 percent of the
 allocated unit will be wasted due to internal fragmentation. • Macro. Each cache is populated with objects that are instantiations of the kernel data structure the cache represents. For example, a macro virus could be contained in a spreadsheet file. In
other cases, however, system performance can be improved if the user (or compiler) has an awareness of the underlying demand paging. The segment table. Finally, we explore how the Windows XP and Linux operating systems support threads at the kernel level. Another variation on the Trojan horse is
spyware. 9.4 A certain computer provides its users with a virtual-memory space of 21" bytes. For example, access rights of a file can be specified to the level of a single individual. In many ways, I/O devices are also the slowest major components of the computer. How does the system process transactions that were issued after the rolled-back
transaction but that have timestamps smaller than the new timestamp of the rolled-back transaction? These faulting processes must use the paging device to swap pages in and out. The content of the program from these servers has not yet been determined. This makes it difficult to detect and contain. However, a computer not holding S(k) cannot
generate authenticators on messages that can be verified using V(k). For the purposes of protection and security, we use mechanisms that ensure that only processes that have gained proper authorization from the operating system can operate on the files, memory, CPU, and other resources. This mechanism must provide a means of specifying the
controls to be imposed, as well as a means of enforcement. If it found one, the new copy exited, except in every seventh instance. Other members in the Win32 thread pool API include utilities that invoke functions at periodic intervals or when an asynchronous I/O request completes. One way of making protection available to the application program
is through the use of a software capability that could be used as an object of computation. Each device (for example, disk drives, audio devices, and video displays). The queue has a maximum length of zero; thus, the link cannot have any messages waiting in it. The traditional UNIX kernel started with
an implementation of swapping that copied entire processes between contiguous disk regions and memory. Since the 9.5 Allocation of Frames 341 instruction is from storage location to storage location to storage location of Frames 341 instruction is from storage location to storage location of Frames 341 instruction is from storage location to st
invoked on the server, then sends this parcel to the server. - ' M - r - '-[-' - : ; :;:|. Since it is a low-priority process, it may not be selected by the CPU scheduler for a time. This program is somewhat simpler than the one shown in Figure 9.25, as all that is necessary is for the process to create a mapping to the existing named shared-memory object. • re
c e i v e (Q, message)—Receive a message from process Q. The virtual address space of a process is stored in memory. A similar function can be added to other aspects of a computer system. The example in Section 15.6.3 illustrating the impact of false-alarm rate on the effectiveness of IDSs is
based on Axelsson [1999]. The JVM also automatically manages memory by performing garbage collection—the practice of reclaiming memory. Thus, such protection decisions are handled within the JVM. Denial-of-service attacks prevent
legitimate use of target systems. Once it does, you can start reading. FunBrain, you'll find a selection of books for elementary and middle grades, including some of the popular books and series that kids love the most. Similarly, if the server decides that replies will be large, it creates a section object. Each device controller is in charge of a
specific type of device. We should then page out its remaining pages, freeing all its allocated frames. (For instance, __NR_close, which corresponds to the system call handlers is typically stored in the file / u s r / s r c / l i m i x - 2. It
commonly is implemented in a semiconductor technology called dynamic random-access memory (DRAM), which forms an array of memory words. 12. x / a r c h / i 3 8 6 / k e r n e l / e n t r y . After we replace an active page with a new one, a fault occurs almost immediately to retrieve the active page. Each file access requires a system call and disk
access. This data structure—typically known as a lightweight process, or LWP—is shown in Figure 4.9. To the user-thread library, the LWP appears to be a virtual processor on which the application can schedule a user thread library, the LWP appears to be a virtual process can switch from, say, domain A to
domain B and enjoy the access privileges of domain B. This scheme allows processes with limited access rights to call procedures in lower rings that have more access rights, but only in a carefully controlled manner. When a task is created, two special mailbox—are also created. Encrypted. A cuirent-ring that have more access rights, but only in a carefully controlled manner.
mtmber counter is associated with each process, identifying the ring in which the process is executing currently. This restriction is necessary with shared code or data and is generally useful in any case to provide simple run-time checks for common programming errors. Security at the first two levels must be maintained if operating-system security is
to be ensured. This becomes especially troublesome with asynchronous cancellation. The use of minimal operating-system support to enforce protection was advocated by the Exokernel Project (Ganger et al. 570 Chapter 15 Security virus copies buo' j sector to unusprt location X virus replaces original boot block with itself whenever new removable
R/W d sk is installed, it infects ^ that as well : :it;btockS:ariy::aftenfi[Dt|df other pifdgrams;|o; yi/rite tHe u P ::; :: boot sector;: n ::: Figure 15.5 (this a tegic;:b6rrtt> to •: N: :•:certain Bate:: :: A boot-sector computer virus. Each object has a list of unique bit patterns, called locks. Many programs then use the disk as both a source and a destination
of the information for their processing. When an operation M on an object 0/ is attempted in domain 14.5 Implementation of Access Matrix 543 Dj, we search the access list for object O., looking for an entry with M e Kj. If the entry is found, we allow the operation; if it is not, we check the default set. Exit */ Producer and Consumer Threads The
producer thread will alternate between sleeping for a random period of time and inserting a random integer into the buffer. The behavior of the program may lead to interesting observations, but it does not provide a sound basis for inferring motive. We examine these operations next. For example, consider a job that needs to access various large files
that reside at different sites, to obtain a summary of those files. To accomplish this goal, the bootstrap program must locate and load into memory the operating systems. In most cases, this requirement is easy
to meet. Therefore, the same process may perform quite 9.6 Thrashing 343 differently (for example, taking 0.5 seconds for one execution) because ROM
 needs no initialization and is at a fixed 464 Chapter 12 Mass-Storage Structure boo' code partition 1 part ten ia.D'e partition 2 partition 2 partition 3 boot partition 4 Figure 12.9 Booting from disk in Windows 2000. These methods greatly decrease the chance of authentication forgery. 4.4 Threading Issues 4.4.2 Cancellation 139? If a stack frame is first
found that has the doPrivileged () annotation, then checkPermissionsO returns immediately and silently, allowing the access. How do we select a particular replacement algorithm? i n i t i a l i z e .the .mut:ex l o c k s */: %'XX^. If the barber is asleep, the customer wakes up the barber. Consider a C program whose function is to initialize to 0 each
element of a 128-by-128 array. 6.14 The strict mutual exclusion within a monitor makes the bounded-buffer monitor of Exercise 6.13 mainly suitable for small portions. is waiting for a resource R,-, which is held by process P/+i. There are different design options for implementing 102 Chapter 3 Processes each primitive. When a frame is needed, the
pointer advances until it finds a page with a 0 reference bit. There are other interesting aspects of DOS attacks. UNIX later evolved to a combination of swapping and paging as paging hardware became available. Depending on the controller, there may be more than one attached device. Because DES works on a chunk of bits at a time, is a known as a
block cipher. [1971]. It may take more than a kilobyte to record this information for each. The first approach is to provide a library entirely in user space with no kernel support. • Relocation. Thus, most computer systems provide a library entirely in user space with no kernel support.
Temporarily cache a message. In some cases, such as a denial-ofservice attack, it is preferable to prevent the attack but sufficient to detect the attack but sufficient to detect the attack so that countermeasures can be taken. In this section, we describe important modern encryption principles and algorithms. 4.2 Describe the actions taken by a thread library to context switch between
user-level threads. If T, requests a shared lock on Q, then 7) must wait if Q is locked in exclusive mode. It clogged e-mail inboxes, slowed networks, and took a huge number of hours to clean up. The home version offers a free eBook library for kids ages 3 to 11, including both fiction and nonfiction. Jacob and Mudge [1998b] compared implementations
of virtual memory in the MIPS, PowerPC, and Pentium architectures.. 8.6 Segmentation An important aspect of memory and the actual physical memory. In this example, a producer process first creates a shared-memory object using the memory.
mapping features available in the Win32 API. Capability lists do not correspond directly to the needs of users; they are useful, however, for localizing information of the openO and close is the simplest case is the sim
may open the file at the same time. '-. But how does the hardware know where the kernel is or how to load that kernel? In this case, the set of objects that can be accessed depends on the identity of the process. Since these tables are referenced only when a page fault occurs, they do not need to be available quickly. However, if amplification may
occur, the right to modify may be reinstated. Preface To obtain restricted supplements, such as the solution guide to the exercises in the text, contact your local John Wiley & Sons sales representative. CHAPTER OBJECTIVES • To introduce CPU scheduling, which is the basis for multiprogrammed operating systems. An I/O-bound process is one that
spends more of its time doing I/O than it spends doing computations. Typically., the open-file table also has an open count associated with each file to indicate how many processes have the file open. It provides a clear description of the concepts that underlie operating systems. The server process sends the date to the client, calling the method prince in the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open. It provides a clear description of the concepts that underlie open.
tlnO. Both methods could be used to access several files residing at various sites. The read() method in the j ava. For the reference string considered previously, for example, if we had three or more frames, we would have only three faults — one fault for the first reference to each page. Such a specification should be given directly as a program is
composed, and in the language in which the program itself is stated.. It is usually possible to choose among a few sizes, such as 256, 512, and 1,024 bytes. ... 15.8 Argue for or against the judicial sentence handed down against Robert Morris/ Jr., for his creation and execution of the Internet worm discussed in Section 15.3.1. 15.9 Make a list of six
security concerns for a bank's computer system. One key goal of an operating system is to provide the simplest interface possible to the rest of the system. application may be allocated more kernel threads on a multiprocessor than on a uniprocessor. I/O subsystem is to provide the simplest interface possible to the rest of the system. application may be allocated more kernel threads on a multiprocessor than on a uniprocessor.
Demand paging is designed to be transparent to the user program. Unlike the telnet daemon, which executes any commands for the user, the FTP daemon responds only to a predefined set of file-related commands. Similarly, we allow for the user, the FTP daemon responds only to a predefined set of file-related commands.
communication. We can improve performance by caching the block location information in physical memory and by using special tools to allocate physically contiguous blocks for the swap file, but the cost of traversing the file-system data structures still remains. The Mach system was especially designed for distributed systems, which we discuss in
Chapters 16 through 18, but Mach is also suitable for singleprocessor systems, as evidenced by its inclusion in the Mac OS X system. File locks are useful for files that are shared by several processes—for example, a system log file that can be accessed and modified by a number of processes in the system. How would the solution to the preceding
exercise differ with the two different ways in which signaling can be performed? You have probably realized that the Web has many aspects of a distributed computing environment. This assembled code fragment is now a binary sequence that will be at the heart of the attack. These problems are used to test nearly every newly proposed
synchronization scheme. We must also allocate at least a minimum number of frames. Thus, a desire to minimize I/O time argues for a larger page size. 138 Chapter 4 Threads The JVM and Host Operating System The JVM is typically implemented on top of a host operating system (see Pigure 2.17). A context switch here simply requires changing the
pointer to the current register set. 9.7.2 Shared Memory in the Win32 API involves first creating a file mapping for the file to be mapped and then establishing a view of the mapped file in a process's virtual address space. A later reference to that
page will cause a page fault. 3.2 Describe the actions taken by a kernel to context-switch between processes. Consider a program that starts with a list of available options from which the user is to select. You can find your representative at the "Find a Rep?" web page: . When a user logs in, dtlog in creates an X-windows session (Xsession), which
in turns creates the sdt shel process. The worst-case scenario occurs in computer architectures that allow multiple levels of indirect indicator). More commonly, however, operating systems are designed to run on any of a class of machines at a variety of sites with a
variety of peripheral configurations. If a process executing in ring /' calls a procedure (or segment) with access bracket (bl,bl), then the call is allowed if bl s ' < bl, and the current ring number of the process remains /'. local, 342-343 proportional allocation, 341-342 frame-allocation algorithm, 330 frame pointers, 567 free-behind technique, 435 free
objects, 356, 758 898 Index free-space list, 429 free-space management (disks), 429-431 bit vector, 429-430 counting, 431 grouping, 431 linked list, 430^31 front-end processors, 523 FTP, see file transfer protocol ftp, 398 full backup, 436 fully distributed deadlock-detection algorithm, 681-683 Gantt chart, 159 garbage collection, 68, 395 gateways,
626 GB (gigabyte), 6 gcc (GNU C compiler), 740 GDT (global descriptor table), 306 general graph directories, 394-395 gigabyte (GB), 6 global descriptor table Threads, 130 graceful degradation, 13 graphs, acyclic, 392 graphical user interfaces (GUIS).
41-43 grappling hook, 573 Green threads, 130 group identifiers, 27 grouping, 431 group policies, 828 group rights (Linux), 778 guest operating systems, 5 handheld computers, 5 handheld systems, 30-31 handles, 793, 796 handling (of signals), 123 handshaking, 498-499,
518 hands-on computer systems, set'? A crucial requirement for demand paging is the need to be able to restart any instruction after a page fault. 12.5 Disk Management, too. The file's owner might write the file to a floppy disk, send it in an e-mail, or copy it across a
network, and it could still be called example.c on the destination system. The separate child process is created using the f ork() system call and the user's command is executed by using one of the system calls in the execO family (as described in Section 3.3.1). For example, suppose a language is used to generate code to run on the Cambridge CAP
system. The Department of Defense Trusted Computer System Evaluation Criteria (DoD [1985]), known also as the Orange Book, describes a set of security levels and the features that an operating system must have to qualify for each security rating. It also shows that as the Internet grows, the damage that even "harmless" worms can do also grows
and can be significant. The slab consists of both used and free objects. Preface xi We have chosen these three programming environments because it, is our opinion that they best represent the two most popular models of operating systems: Windows and UNIX/Linux, along with the widely used Java environment. Performance is, of course, important to
are enough extra frames, another process can be initiated. If a file is specified as memory-mapped (using the mmapO system call), Solaris maps the file into the address space of the process. Consider the damage that could be done if a request for authentication had a legitimate 15.1 The Security Problem 561 user's information replaced with an
 unauthorized user's. 9.14 Consider a demand-paging system with a paging disk that has an average access and transfer time of 20 milliseconds. In this chapter, we discuss the general structure of distributed systems and the networks that interconnect them. • Breach of availability. The system can then continue as usual. It is available to users on the
Internet via the FTP program from host ftp.uu.net in directory /pub/security/cops. The members of this structure are i and j, and the structure for passing data to threads */ struct v { int i; /* row * / int j; /* column */' Both the Pthreads and Win32 programs will create the worker threads using a structure are i and j, and the structure for passing data to threads */ structure for passing data to threads */ structure for passing data to threads using a structure for passing data to threads */ structure for passing data t
strategy similar to that shown below: /* We have to create M * N worker threads */ for (i = 0; i < M, i + + ) for (j = 0,- j < N; j ++ ) { struct v *data = (struct v *) malloc(sizeof(struct v)); data->i = i; data
user therefore specifies each address by two quantities: a segment name and an offset. : . In this way, the most recently used page is always at the bottom (Figure 9.16). In this section, we explore the mechanisms involved in creating processes and illustrate process creation on UNIX
and Windows systems. A control program manages the execution of user programs to prevent errors and improper use of the computer. (By "string", we mean a null-terminated, C-style string variable.) 122 Chapter 3 Processes If include # in
using whitespace as delimiters, setup() modifies the args parameter so that it holds pointers to the null-terminated strings that are the tokens in the most recent user command line as well as a NULL pointer, indicating the end of the argument list, which comes after the string pointers that have been assigned to args. After the transaction either
commits or aborts, it executes signal(/?z«ta')Although this scheme ensures the atomicity of all concurrently executing transactions, it is nevertheless too restrictive. In this case, the bootstrap runs diagnostics and has a bit of code that can read a single block at a fixed location (say block zero) from disk into memory and execute the code from that bootstrap runs diagnostics and has a bit of code that can read a single block at a fixed location (say block zero) from disk into memory and execute the code from that bootstrap runs diagnostics and has a bit of code that can read a single block at a fixed location (say block zero) from disk into memory and execute the code from that bootstrap runs diagnostics are considered.
block. A program illustrating how the consumer process establishes a view of the named shared-memory object is shown in Figure 9.26. For instance, a web server on the DMZ may need to query a database server on the corporate network. Similarly, a firewall that automatically blocks certain kinds of traffic could be induced to block that traffic when
it should not. If paging or segmentation is provided, different sections of a user program can be declared execute-only, read-only, or read-write. • ::: • : • " i ;[ V.. Beyond books, the Oxford Owl site offers a blog with advice for parents and kids on topics like summer reading and what to expect when school starts. The objective of multiprogramming is
to have some process running at all times, to maximize CPU utilization. You may assume the existence of a real hardware clock that invokes a procedure tick in your monitor at regular intervals. The second kind of capability is the so-called software capability, which is protected, but not interpreted, by the CAP microcode. Otherwise, it can obtain the
lock and access Q. • To explain the function of file systems. The process then jumps to this address and the privileges of the process are switched from user to kernel mode. ptiireati.inviuBx^lacikiO blocks the thready until the; ovvner of: the rnufiex :ieok invokes pt:jire:ad.;iinjitexi: : uril5c ; k(). After the trap is executed, the system call number is used
to index into a table of code pointers to obtain the starting address for the handler code implementing the system, every storage reference made on the underlying hardware occurs indirectly through a capability. See also disk(s) magnetic tapes, 453-454, 480 magneto-optic disks, 479 mailboxes, 100 mailbox sets, 106 mailslots, 824
mainframes, 5 Index main memory, 8-9 and address binding, 281-282 and dynamic loading, 280-281 and hardware, 276-278 Intel Pentium example: with Linux, 307-309 paging, 306-308 segmentation, 305-307
and logical vs. This scheme has the advantage that the user does not need to code her program explicitly to accomplish the migration. 7. Briefly describe the two categories and discuss how they differ. Alternatively, process P can send a message to site A. These methods include shared memory and interprocess communications. This main thread will
then create the worker threads, passing the three matrices—along with row i and column j—to the constructor for each worker. The system objects whenever the user, attempts to access to behalf of the user, attempts to access to be object. Few systems could tolerate that level of
overhead for memory management. A network operating system provides most of these features, but a distributed operating system makes them seamless and easily accessible. A typical example of nonrepudiation involves the filling out of electronic forms as an alternative to the signing of paper contracts. However, if the central site fails, every site
in the system becomes disconnected. It watches for other bootable media (that is, floppy disks) and infects them. Another approach to implementing LRU replacement is to keep a stack of page numbers. The consumer then ^include #include int main(int argc, char *argv[]) { HANDLE hMapFile; LPVOID lpMapAddress; hMapFile =
OpenFileMapping {FILEJCAP_fl.LLJ^CCESS, // R/W access FALSE, // no inheritance TEXT("SharedObject handle FILE31AP_ALL_ACCESS, // read/write access 0, // mapped view of entire file 0, 0); // read from shared memory printf("Read message %s"
ipMapAddress); UnmapViewOfFile(IpMapAddress); UnmapViewOfFile(IpMapAddress]; CloseHandle(hMapFile); Figure 9.26 Consumer reading from shared memory using the Win32 API. For example, Solaris, Windows XP, and Linux provide mechanisms such as semaphores, mutexes, spinlocks, and condition variables to control access to shared data. Some are connected to networks
either directly by wire or (more often) through wireless modems and networking. Creating a History Feature The next task is to modify the program in Figure 3.25 so that it provides a history feature that allows the user access up to the number of kernel threads allocated to the program is equal to the number of kernel threads.
of processors. 6.10 Summary Given a collection of cooperating sequential processes that share data, mutual exclusion must be provided. Theoretically, a simple load instruction could reference an indirect address (on yet another page), and so on,
until every page in virtual memory had been touched. Sleep */ * 6...^... The second approach is to implement a kernel-level library supported directly by the operating system. The process then creates a mapping of this file HANDLE using the CreateFileMappingO function. After a class is loaded, the verifier checks that the . A/ is the product of two
large, randomly chosen prime numbers p and q (for example, p andtj are 512bits each). C. 8.7.1 Pentium Segments per process is 16 KB. Viruses and worms are self-perpetuating, sometimes infecting thousands of computers. (It is important
to note that the entire mapping may not be loaded into memory when the mapping is established. The system must have manual recovery. Security protects the information stored in the system (both data and code), as well as the physical resources of the
computer system, from unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency. A variety of disk-organization techniques, collectively called redundant arrays of inexpensive disks (RAIDS), are commonly used to address the performance and reliability issues. 9.6.1 Cause of Thrashing Thrashing results in
severe performance problems. Paged segmentation was first supported in the GE 645, on which MULT1CS was originally implemented (Organick [1972] and Daley and Dennis [1967]). Systems that use inverted page tables have difficulty implemented (Organick [1972] and Daley and Dennis [1967]).
all ages, whether they're reading on their own or hearing stories from teachers, parents and the other adults in their lives. The events with which we are mainly concerned here are resource acquisition and release. If a running program performs either of these actions, a signal is generated. The primary data structures of a thread include:
ETHREAD—executive thread block • KTHREAD—kernel thread block • KTHREAD—kernel thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to which the thread block • KTHREAD include a pointer to the process to the process to the process to the process to t
Finger runs as a background process (or daemon) at each BSD site and responds to queries throughout the Internet. Loading the executable code for all options, regardless of whether an option is ultimately selected by the user or not. Thus, we can directly measure and control the page-fault rate to
prevent thrashing. A capability is valid only if its key matches some key in the global table. The upcall handler thread that is eligible to run on the new virtual processor. Permissions can be accessed by using the bitwise AND operator &. An encryption algorithm enables the sender of a message to ensure that only a computer
possessing a certain key can read the message. Given this standard memory layout, a cracker could execute a bufferoverflow attack. The mainC) function will initialize the buffer and create the separate producer and consumer threads. Antivirus programs in turn now look for families of patterns rather than a single pattern to identify a virus. An
 example of a simple subject is the typical application program that a user executes after she logs on. Because the column defines objects explicitly, we can omit the object name from the access right. It has been updated and an example of Windows XP ACLs has been added. 9.4.1 Basic Page Replacement Page replacement takes the following
approach. In many cases, the user is completely unaware of the paged nature of memory. Hence, the proper management of disk storage is of central importance to a computer system, as we discuss in Chapter 12. The user ID). In a fully connected
network, each site is directly connected to every other site. Processes alternate between these two states. It is likely that Morris chose for initial infection an Internet host left open for and accessible to outside users. The code below illustrates how a semaphore is created: #include sem_t sem; / * Create the semaphore and i n i t i a l i z e it to 5 */
sem_init(&sem, 0, 5); The sem.init () creates and initializes a semaphore. 2.10 Why does Java provide the ability to call from a Java program native methods that are wrritten in, say, C or C++? A suitable verification algorithm is then V(k)(m, a) = (f(k, m) = a). All objects in the slab are marked as used. For completeness, we should note that SSL was provide the ability to call from a Java program native methods that are wrritten in, say, C or C++? A suitable verification algorithm is then V(k)(m, a) = (f(k, m) = a).
designed by Netscape and that it evolved into the industry standard TLS protocol. 10.1.1 File Attributes A file is named, for the convenience of its human users, and is referred to by its name. This program is terminated when the user enters and setup 0 then invokes exit(). General discussions concerning concurrent programming were offered by
Ben-Ari [1990] and Birrell [1989]. The system may identify the receiver to the sender. As you might expect there is no single best page size. ••;!;: H i ;i permission: f:;"?1:;?^,.l',t.i; ^ t ~ class: . That is, for each k e K, D{k} is a function for generating messages from ciphertexts. When they find a known pattern, they remove the instructions,
disinfecting the program. This message-management technique provides a large performance boost but works for only intrasystem messages. It can also provide information about defenses, such as what firewalls are defending the target. With demand paging, the size of the logical address space is no longer constrained by physical memory.
Principally, communication is achieved through two schemes: shared memory and message passing. Initially, the owner is the only process that can receive messages through this mailbox. Clustering handles page faults by bringing in not only the faulting page but also several pages following the faulting page. The hardware topics required for an achieved through this mailbox.
understanding of operating systems are included in Chapter 1. Later releases of the JVM were implemented using the many-to-many model. 9.6.3 Page-Fault Frequency The working-set model is successful, and knowledge of the working set can be useful for prepaging (Section 9.9.1), but it seems a clumsy way to control thrashing. Suppose, for
example, that five different file-read requests occur simultaneously. Add the following code to this file: #include asmlinkage in t sys_helloworld() { printk(KERKLEMERG "hello w o r l d!"); r e t u r n 1; } This creates a system call with the name sysJielloworld().
it has updated by simply executing undo(7}). Process P2 is waiting for the resource R3, which is held by process P3. In this way, both processes share the available frames according to their "needs," rather than equally. When this scheme is used, each page or frame has a modify bit associated with it in the hardware. For e-mail to be secure, the e-
mail message needs to be encrypted so that its security is independent of the transports that carry it. Chapters 21 through 23 in the book, and Appendices A through C on the website, integrate the concepts described in this book by describing real operating systems. The path is searched for a file of that name, and the file is executed. Data and
process migration from one site to another is under the control of the distributed operating system. Swapping in that setting occurs when the amount of physical memory reaches a critically low point and processes (which are usually selected because they are the least active) are moved from memory to swap space to free available memory. So this
 option is not the best choice. dynamic, 534 from viruses, 596-598 protection domain, 534 protection mask (Linux), 778 protection subsystems (Windows XP), 788 protocols, Windows XP networking, 822-824 PTBR (page-table base register), 293 Pthreads, 132-134 scheduling, 172-174 synchronization in, 221-222 Index Pthread scheduling, 708-710
PTLR (page-table length register), 296 public domain, 741 public keys, 580 pull migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 170 pure code, 296 pure demand paging, 322 push migration, 320 push migrati
arrays of inexpensive disks), 468-177 levels of, 470-476 performance improvement, 470 problems with, 477 reliability improvement, 468-470 structuring, 469 RAID levels, 506, 507, 844 random-access memory (RAM), 8 random-access time (disks)
452 rate-monotonic scheduling algorithm, 705-707 raw disk, 339, 416 raw disk space, 386 raw I/O, 508 raw partitions, 467 RBAC (role-based access control), 545 RC 4000 operating system, 848-849 reaching algorithms, 686-688 read-ahead technique, 435 readers-writers problem, 206-207 reader-writer locks, 207 911 reading files, 375
read-modify-write cycle, 473 read only devices, 506, 507 read-only disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write devices, 506, 507 read-write disks, 479 read-write devices, 506, 507 read-write disks, 479 read-write disks, 479 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write devices, 506, 507 read-write disks, 479 read-write disks, 479 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 479 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 479 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 772 read-write disks, 480 read-only memory (ROM), 71, 463-464 read queue, 782 read-only memory (ROM), 71, 463-464 read queue, 782 read-only memory (ROM), 71, 720 read-only memory (ROM), 71, 720 read-
operating systems, 29-30 real-time range (Linux schedulers), 752 real-time streaming, 716, 726-728 real-time systems, 29-30, 695-696 address translation in, 698-699 footprint of, 696, 722 implementation of, 700-704 and minimizing latency
702-704 and preemptive kernels, 701 and priority-based scheduling, 700-701 soft, 696, 722 VxWorks example, 710-712 real-time transport protocol (RTP), 725 real-time t
process termination, 266 by resource preemption, 267 from failure, 633 of files and directories, 435—137 Windows XP, 816-817 redirectors, 826 redundancy, 469. Perform coalescing whenever possible: • release 250 bytes 250 bytes • release 250 bytes 250 bytes 250 bytes 250 bytes 250 bytes
Otherwise, a trap to the operating system occurs, and the situation is handled as follows: If / < bl, then the call is allowed to occur, because we have a transfer to a ring (or domain) with fewer privileges. Each entry in the segment table has a segment table has a segment limit. Because a system is distributed, however, it must provide mechanisms for
process synchronization and communication, for dealing with the deadlock problem, and for handling failures that are not encountered in a centralized system. 9.9.1 Prepaging An obvious property of pure demand paging is the large number of page faults that occur when a process is started. Consider, for example, that the same source block would
result in the same ciphertext if the same key and encryption algorithm were used. Simple Shell A C program that provides the basic operations of a command line shell is supplied in Figure 3.25. A process opening an executable file for writing is suspicious, for example, unless it is a compiler. Some are dedicated, some shared. In this instance, you will
need to specify a separate program to be invoked from CreateProcessC). For example, nmap (from is a very versatile open-source utility for network exploration, produce an output object version of the operating system that is tailored to the
system described. This scheme can significantly reduce the time required to service a page fault, since it reduces I/O time by one-halfif the page has not been modified. Deadlock prevention provides a set of methods for ensuring that at least one of the necessary conditions (Section 7.2.1) cannot hold. Such a redirection by the controller could
invalidate any optimization by the operating system's disk-scheduling algorithm! For this reason, most disks are formatted to provide a few spare sectors in each, cylinder and a spare cylinder as well. 14.14 How can systems that implement the principle of least privilege still have protection failures that lead to security violations? Check that the page
reference was legal and determine the location of the page on the disk. However, even new copies of legitimate software applications are not immune to virus infection: There have been cases where disgruntled employees of a software applications are not immune to virus infection.
software. 4.3.1 Pthreads Pthreads Pthreads refers to the POSIX standard (IEEE 1003.1c) defining an API for thread creation and synchronization. A mechanism is also needed to change the entries in a row. If one access out of 1,000 causes a page fault, the effective access time is 8.2 microseconds. Generally, viruses are the most disruptive security attack; and
because they are effective, they will continue to be written and to spread. 1.1.3 Defining Operating Systems We have looked at the operating system's role from the views of the user and of the system. To write a block on tape, we first copy the block to system memory and then write it to tape. Discussions concerning protection of digital signatures
are offered by Akl [1983], Davies [1983], Davies [1983], Denning [1984]. [1979], Landwehr [1981], Denning [1982], Pfleeger and Pfleeger [2003], Tanenbaum 2003, and Russell and Gangemi [1981]. In addition, we have added several programming projects which are more involved than standard programming exercises. If any are found, the
forking, the separate process should duplicate all threads. These two modes protect the operating system (executing in monitor domain). ! - - . Hence, we are constrained by the hardware available. Release. For example, on our sample reference string, the optimal page-replacement algorithm would
yield nine page faults, as shown in Figure 9.14. The Windows XP security model is based on the notion of user accounts. Many objects in the core Java API implement S e r i a l i z a b l e, allowing them to be used with RMI. In this chapter, we consider the various aspects of files and the major directory structures. For example, a company could be used with RMI. In this chapter, we consider the various aspects of files and the major directory structures.
the client when acting on the client's behalf. Each segment has a name and a length. Three primary threads, Win32 threads, Win32 threads for Windows systems, and Java threads for Windows systems for Windows systems, and Java threads for Windows systems, and Java threads for Windows systems for W
on disk, loads that kernel into memory, and jumps to an initial address to begin the operating-system execution. '::; .... Oaks and Wong [1999], Lewis and Berg [2000], and Holub [2000] discuss multithreading in Java. 234 Chapter 6 Process Synchronization 6.16 How does the signal () operation associated with monitors differ from the corresponding
operation defined for semaphores? Long search paths, such as are common on UNIX systems, exacerbate the Trojanhorse problem. • Identifier. These commands will be numbered 35 commands, the 10 most recent commands should be numbered 26 to 35. •
Swapping. Pages can be reclaimed from the cache list if they are accessed before being moved to the free list. The tool could attempt to connect to every port of one or more systems. After the interrupt address is loaded into the program counter, and the interrupted computation resumes as though the interrupt had not
occurred. ..-... The IPC facility implemented at the user level was described by Bershad et al. Last, we provide two pointers to the STARTUPINFO and PROCESS-INFORMATION structures created at the beginning of the program.
that subprocess may be able to obtain its resources directly from the operatiin system, or it may be constrained to a subset of the parent process. For example, implementations of a. Beyond these two initial parameters, we use the default parameters for inheriting process and thread handles as well as specifying no creation flags.
accomplish this, the server must implement the "at most once" protocol described above but must also acknowledge to the client that the RPC call was received and executed. Finally, computer science classes are notorious sources of accidental system DOS attacks. 15.4.1.2 Asymmetric encryption algorithm, there are
different encryption and decryption keys. Local-area networks are composed 618 Chapter 16 Distributed System Structures of processors distributed over small areas (such as a single building? The user may want to erase the contents of a file but keep its attributes. The Buffer Internally, the buffer will consist of a fixed-size array of type buffer^item.
(which will be defined using a typef def). What is the hardware support required to implement this feature? The system can then remove the entry. The Mach message system attempts to avoid double-copy operations by using virtual-memory-management techniques (Chapter 9). For example, if the set of resource types R includes 7.4 Deadlock
Prevention 255 tape drives, disk drives, and printers, then the function F might be defined as follows: F(tape drive) = 1 F(di.s.k drive) — 5 F (printer) = 12 We can now consider the following protocol to prevent deadlocks: Each process can request resources only in an increasing order of enumeration. can remove any access right from row /'. If the
mailbox is owned by a process (that is, the mailbox), and the user (who can only receive messages through this mailbox) and the were (who can only send messages to the mailbox). Let's assume the size of a memory segment is initially 256 KB and the kernel requests 21 KB of
memory. Individual, school and classroom accounts are all available. Systems with variable-sized allocation units, such as the multiple-partition scheme and segmentation, suffer from external fragmentation. The short-term scheduler, or CPU scheduler, selects from among the processes that are ready to execute and allocates the CPU to one of them
A singlethreaded process can only run on one CPU, no matter how many are available. Sometimes a system and network attack is used to launch a program attack, and vice versa. The controller can be told to replace each bad sector logically with one of the spare sectors. In this instance, we pass no parameters to PoolFunct i o n (). The cost of
                                                                               lication cost. In general, the matrix will be sparse: that is, most of the entries will be empty. A weakness at a high level of security (physical or human) allows circumvention of strict low-level (operating-system) security measures. Of these available pages sizes, Solaris uses both 8-KB and 4-MB pages at a high level of security (physical or human) allows circumvention of strict low-level (operating-system) security measures. Of these available pages sizes, Solaris uses both 8-KB and 4-MB pages at a high level of security (physical or human) allows circumvention of strict low-level (operating-system) security measures.
sizes. Similarly, when we change the content of the access matrix, we are performing an operation on an object: the access matrix. That user would need JV keys and, for more security, would need to change those keys frequently. In addition, no information produced by a prior user is available to another user who accesses a storage object that has
been released back to the system. The pagefault rate increases tremendously As a result, the effective memory-access time increases tremendously As a result, the effective memory-access time increases. The semaphore concept was suggested by Dijkstra [1965a]. pointer is moving slow 9.7 Discuss situations under which the least frequently used pagereplacement algorithm generates fewer page faults than the least
recently used page-replacement algorithm. Furthermore, this setup offers the potential for improving the reliability of data storage, because redundant information can be stored on multiple disks. Also consider the problem of e-mail. 9.2.2 Performance of Demand Paging Demand paging can significantly affect the performance of a computer system.
While the process executes and accesses pages that are memory resident, execution proceeds normally. An unsuspecting user starts to log in at a terminal and notices that he has apparently mistyped his password. How, then, does Linux apply its three-level model on the Pentium 9 In this situation, the size of the middle directory is zero bits,
effectively bypassing the middle directory, concurrent package in Java 1.5 provides a thread pool utility as well. Similarly, a course on operating systems is an essential part of any computer-science education. Note that it may be safer to overestimate than to underestimate the amount of swap space required, because if a system runs out of swap space required.
space it may be forced to abort processes or may crash entirely. An LRU page-replacement algorithm may require substantial hardware assistance. (Contrast this scheme with the paging scheme, in which the user specifies only a single address, which is partitioned by the hardware into a page number and an offset, all invisible to the programmer.)
For simplicity of implementation, segments are numbered and are referred to by a segment name. However, its performance is not always good. The resources (for example, printers, tape drives, memory space, and CPU cycles) or logical resources (for example, files, semaphores, and
monitors). Exercises 6.1 The first known correct software solution to the critical-section processes, some of which are operating-
system processes (those that execute system code) and the rest of which are user processes (those that execute user code). If the modify bit is not set, however, the page has not been modified since it was read into memory. The processors communicate with one another through various communication networks, such as high-speed buses or
telephone lines. 2.2 List five services provided by an operating system that are designed to make it more convenient for users to use the computer system. The exec () system call loads a binary file into memory (destroying the memory image of the program containing the execO system call) and starts its execution. The operating system will then
create a copy of this page, mapping it to the address space of the child process. We can make certain applications more efficient by allowing them to implement their own special-purpose storage services on a raw partition, but most applications more efficient by allowing them to implement their own special-purpose storage services on a raw partition, but most applications more efficient by allowing them to implement their own special-purpose storage services on a raw partition, but most applications more efficient by allowing them to implement their own special-purpose storage services.
generating authenticators from messages. 14.12 How are the access-matrix facility and the role-based access-control facility similar? All requests for synchronization objects must be made in increasing order. Changing the identifier of a process may necessitate examining all other process definitions. .. In Chapter 6, we discuss how synchronization
among cooperating processes can be implemented effectively in a shared memory environment. For example, a high-overhead antivirus scan, such as a sandbox, can be used; and if a program passes the test, a signature can be created for it. If we increase our degree of multiprogramming, we are over-allocating memory. Further, consider that system
memory is not used only for holding program pages. A segmented memory space (Section 8.6) is useful to support this approach. The secondary memory is usually a high-speed disk. When free memory available.
The updating of the clock fields or stack must be done for every memory reference. child processes, 796 children, 90 CIFS (common internet file system), 399 Cincular SCAN (C-SCAN) scheduling algorithm, 460 circular-wait condition (deadlocks), 254-256
claim edge, 258 classes (Java), 553 class loader, 68 CLI (command-line interface), 41 C library, 49 client(s): defined, 642 diskless, 644 in SSL, 586 client interface, 642 client-server model, 398-399 client-side caching (CSC), 827 client systems, 31 clock, logical, 665 clock algorithm, see second-chance pagereplacement algorithm clocks, 509-510 C-
LOOK scheduling algorithm, 461 closeO operation, 376 clusters, 463, 634, 815 clustered systems, 14-15 clustered systems, 14-15 clustering, 634 asymmetric, 15 in Windows XP, 363 cluster remapping, 820 cluster server, 655 CLV (constant linear velocity), 454 code: absolute, 278 reentrant, 296 code books, 591 collisions (of file names), 420 collision
detection (CD), 627-628 COM, see component object model combined scheme index block, 427 command interpreter, 41-42 command-line interface (CLI), 41 commit protocol, 669 Index committed transactions, 222 common interpreter, 41-42 command-line interface (CLI), 41 commit protocol, 669 Index committed transactions, 222 common interpreter, 41-42 command-line interpreter, 41-42 comman
see interprocess communication systems programs for, 55 unreliable, 686-687 communications (operating system service), 40 communication system
administrative, 645 component object model (COM), 825-826 component units, 642 compression units, 821 computation migration, 616 computation migration, 616 computation migration, 618 computation migration, 618 computation migration, 618 computation migration, 618 computation migration, 619 computation migration 
traditional, 31-32 Web-based computing, 34 computer programs, see application programs computer systems, 12-13 single-processor systems, 12-14 distributed systems, 12-13 memory management in, 21-22 operating system
viewed by, 5 operation of, 6-8 891 process management in, 20-21 protection in, 26-27 secure, 560 security in, 27 special-purpose systems, 30 real-time embedded systems, 30 real-time embedded systems, 30 real-time embedded systems, 29-31 handheld systems, 20-31 multimedia system
to, 571-572 computing, safe, 598 concurrency control, 672-676 with locking protocols, 672-675 with timestamping, 675-676 concurrency-control algorithms, 226 conflict phase (of dispatch latency), 703 conflict resolution module
(Linux), 747-748 connectionless messages, 626 connectionless (UDP) sockets, 109 consistency checking, 435^36 consistency semantics, 401 constant angular velocity (CAV), 454 constant linear velocity (CLV), 454 constant linear velocity (CLV), 454 consistency checking, 435^36 consistency semantics, 401 constant linear velocity (CLV), 454 consistency checking, 435^36 consistency semantics, 401 constant linear velocity (CLV), 454 constant linear velocity (CLV), 4
XP), 603 contention, 627-628 contention, 627-628 contention scope, 172 context (of process), 89 context switches, 90, 522-523 contiquous memory allocation, 421-423 controlled access, 402-403 892 Index controlled access, 402-403 892 Index controlled access, 403-403 892 I
direct-memory-access, 503 disk, 453 host, 453 control programs, 5 
channels, 564 CPU (central processing unit), 4, 275-277 CPU-bound processes, 88-89 CPU burst, 154-155 CPU scheduler, sec short-term scheduler, 157-158 evaluation of, 181-185 first-come, first-served scheduling of, 158-159 implementation
of, 184-185 multilevel feedback-queue scheduling of, 168-169 multilevel queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel queue scheduling of, 168-169 multilevel feedback-queue scheduling of, 168-169 multilevel feedback-q
queueing-netrwork analysis, 183 simulations, 183-184 in multimedia systems, 722-723 multiprocessor scheduling, 169-172 approaches to, 169-170 and load balancing, 170-171 and processor affinity, 170 symmetric multithreading, 171-172 preemptive scheduling, 155-156 in real-time systems, 704-710 earliest-deadline-first scheduling, 707
proportional share scheduling, 708 Pthread scheduling, 708-710 rate-monotonic scheduling, 705-707 short-term scheduler, role of, 155 crackers, 560 creation; 193-195 Peterson's solution to, 195-197 and semaphores, 200-204 deadlocks, 204 implementation, 202-204 starvation,
204 usage, 201 and synchronization hardware, 197-200 cross-link trust, 828 cryptography, 576-587 and encryption, 577-584 implementation of, 584—585 SSL example of, 585-587 CSC (client-side caching), 827 C-SCAN scheduling algorithm, 460 CSMA, see carrier sense with multiple access CTSS operating system, 849 current directory, 3900 cross-link trust, 828 cryptography, 576-587 and encryption, 577-584 implementation of, 584—585 SSL example of, 585-587 CSC (client-side caching), 827 C-SCAN scheduling algorithm, 460 CSMA, see carrier sense with multiple access CTSS operating system, 849 current directory, 3900 cross-link trust, 828 cryptography, 576-587 and encryption, 577-584 implementation of, 584—585 SSL example of, 585-587 CSC (client-side caching), 827 C-SCAN scheduling algorithm, 460 CSMA, see carrier sense with multiple access CTSS operating system, 849 current directory, 3900 cross-link trust, 828 cryptography, 576-587 and encryption, 577-584 implementation of, 584—585 SSL example of, 585-587 CSC (client-side caching), 827 C-SCAN scheduling algorithm, 460 CSMA, see carrier sense with multiple access CTSS operating system, 849 current directory, 3900 cross-link trust, 828 cryptography, 576-587 and encryption, 577-584 implementation of, 585-587 CSC (client-side caching), 827 C-SCAN scheduling algorithm, 840 CSMA, see carrier sense with multiple access cross-link trust, 828 cryptography, 576-587 and encryption, 827 C-SCAN scheduling algorithm, 840 CSMA, see carrier sense with multiple access cross-link trust, 828 cryptography, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sense with multiple access cross-link trust, 840 CSMA, see carrier sens
current-file-position pointer, 375 cycles: in CineBlitz, 728 CPU-I/O burst, 154-155 cycle stealing, 504 cylinder groups, 767 Index d (page offset), 289 daemon process, 536 daisy chain, 496 data: multimedia, 30 recovery of, 435-437 thread-specific, 142 database systems, 222 data capability, 549 data-encryption standard (DES), 579 data files, 374 data
fork, 381 datagrams, 626 data-in register, 498 data striping, 470 DCOM, 826 DDOS attacks, 560 deadline I/O scheduler, 772 deadlock(s), 204, 676-683 avoidance of, 252, 256-262 with banker's algorithm, 259-262 with
resource-allocation-graph algorithm, 258-259 with safe-state algorithm, 258-258 defined, 245 detection of, 262-265, 678-683 algorithm usage, 265 several instances of a resource type, 263-265 single instance of each resource type, 263-265 methods for handling, 252-253 with mutex locks, 247-248 necessary conditions for, 247-249
prevention/avoidance of, 676-678 prevention of, 252-256 and circular-wait condition, 254 recovery from, 266-267 by process termination, 266 by resource preemption, 267 system model for, 245-247 system resource-allocation
graphs for describing, 249-251 deadlock-detection coordinator, 679 debuggers, 47, 48 dedicated devices, 506, 507 default signal handlers, 140 deferred procedure calls (DPCs), 791 deferred thread cancellation, 139 degree of multiprogramming, 88 delay, 721 delay-write policy, 648 delegation (NFS V4), 653 deletion, file, 375 demand paging, 319-325
basic mechanism, 320-322 defined, 319 with inverted page tables, 359-360 and I/O interlock, 361-362 and prepaging, 357 and prepaging, 358-359 demand-zero memory, 760 demilitarized zone (DMZ), 599 denial-of-
service (DOS) attacks, 560, 575-576 density, areal, 492 dentry objects, 419, 765 DES (data-encryption standard), 579 design of operating systems; distributed operating systems; distributed operating systems, 633-636 goals, 56 Linux, 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 181-182 894 Index development kernels (Linux), 742-744 mechanisms and policies, 56-57 Windows XP, 785-787 desktop, 42 deterministic modeling, 48-40 desktop, 48-40 deskto
739 device controllers, 6, 518. Optimizing the performance of locking primitives has been discussed in many works, such as Lamport [1987], Mellor-Crummey and Scott [1991], and Anderson [1990]. This situation would require six frames. Using a debugger, the programmer then finds the address of buffer [0] in the stack. Compliance is enforced
through a sophisticated collection of load-time and run-time checks. This approach creates a fixed amount of swap space during disk partitioning. The client has to decide when it sets up the channel whether or not it will need to send a large message. However, the code segment that runs once the value of the return address has been modified might
perform any type of malicious act, such as deleting files, opening network ports for further exploitation, and so on. A computer system has many resources that may be required to solve a problem; we look
more closely at features that characterize deadlocks. Security at the physical and human levels, although important, is for the most part beyond the scope of this text. However, to authenticate a user at a client computer, the server may need to use an application-level protocol—for example, the user may be required to type a password. The other
solution uses temporary registers to hold the values of overwritten locations. 6.5 Explain why implementing synchronization primitives are to be used in user-level programs. As long as the size of this parameter is less than BUFFER^SIZE (we need
one byte to store the null terminator), this program works properly. Some systems attempt to limit the amount of swap space used through demand paging of binary files. LANs, as mentioned, are usually designed to cover a small geographical area (such as a single building or a few adjacent buildings) and are generally used in an office environment.
File systems live on devices, which we explore fully in the following chapters but touch upon here. A source file is a sequence of subroutines and functions, each of which is further organized as declarations followed by executable statements. This medium-term scheduler is
that sometimes it can be advantageous to remove processes from memory (and from active contention for the CPU) and thus reduce the degree of multiprogramming. Several attack methods are depicted in Figure 15.1. As we have already suggested, absolute protection of the system from malicious abuse is not possible, but the cost to the perpetrator
can be made sufficiently high to deter most intruders. Context-switch time is pure overhead, because the system does no useful work while switching. These levels are hierarchical, so that a user may access any objects that carry sensitivity labels equal to or lower than his security clearance. Files in Windows XP may have the following access types:
ReadData, WriteData, AppendData, Execute, ReadExtendedAttribute, WriteExtendedAttribute, and Write and ExtendedAttribute, and WriteBata, AppendData, Execute, ReadExtendedAttribute, WriteExtendedAttribute, and WriteBata, AppendData, Execute, ReadExtendedAttribute, WriteBata, AppendData, AppendData,
used and modified—probably will be used again soon, and the page will be need to be written out to disk before it can be replaced Each page is in one of these four classes. For instance, a multithreaded web browser could still allow user interaction in one thread while an image was being loaded in another thread. This is the job of cryptography.
Thus, when the kernel requests memory for an object, the slab allocator returns the exact amount of memory required to represent the object. '4. Authentication and secrecy: only the receiver knows that only the sender could have generated the message. A simple example of a MAC defines S(k)(m) = f(k,
```

H(m)), where / is a function that is one-way on its first argument (that is, k cannot be derived from f(k, H(m))). It works as follows: The kernel provides an application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processors (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs), and the application with a set of virtual processor (LWPs).

```
a fundamental unit of CPU utilization that forms the basis of multithreaded computer systems. When the doPrivileged block is entered, the stack frame for this method is annotated to indicate this fact. The header indicates the length of the message and includes two mailbox names. If a process wants to use a capability, it may find that that capability and the capability is annotated to indicate this fact.
has been deleted. However, he would like to single out his friend Peter Ormsby who—no matter how busy his life seems to be—always first asks, "How's the writing coming along?" Abraham Silberschatz, New Haven, CT, 2004 Peter Baer Galvin, Burlington, MA, 2004 Greg Gagne, Salt Lake City, UT, 2004 Contents PART ONE Chapter 1 1.1 1.2 1.3 1.4
1.5 1.6 1.7 1.8 Introduction Operating-System Services 39 User Operating-System Interface 41 System Calls 43 Types of System Calls 47 System Programs 55 Operating-System Design and Implementation 56 Chapter 3 1.9 1.10 1.11 1.12 1.13 Protection and Security 26 Distributed Systems 28 Special-Purpose Systems 29 Computing Environments 31
Summary 34 Exercises 36 Bibliographical Notes 38 Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structure 12 Operating-System Operating-System Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.3 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.4 3.5 OVERVIEW What Operating-System Structures PART TWO 3.1 3.2 3.2 3.4 3.5 OVERVIEW What Operating-System Structu
Management 22 Chapter 2 2.1 2.2 2.3 2.4 2.5 2.6 • 2.7 2.8 2.9 2.10 2.11 Operating-System Structure 58 Virtual Machines 64 Operating-System Generation 70 System Boot 71 Summary 72 Exercises 73 Bibliographical Notes 78 PROCESS MANAGEMENT Processes Process Concept 81 Process Scheduling 85 Operations on Processes 90 Interprocess
Communication 96 Examples of IPC Systems 102 3.6 Communication in ClientServer Systems 108 3.7 Summary 115 Exercises 116 Bibliographical Notes 125 XVII xviii Contents Chapter 5 5.1 5.2 5.3 5.4 5.5 4.5 Operating-System Examples
143 4.6 Summary 146 Exercises 146 Bibliographical Notes 151 CPU Scheduling 172 Chapter 6 6.1 6.2 6.3 6.4 6.5 Operating System Examples 173 5.7 Algorithm Evaluation 181 5.8 Summary 185 Exercises
186 Bibliographical Notes 189 Process Synchronization Background 191 The Critical-Section Problems of Synchronization 204 6.7 6.8 6.9 6.10 Monitors 209 Synchronization Examples 217 Atomic Transactions 222 Summary 230 Exercises 231
Bibliographical Notes 242 Chapter 7 Deadlock Prevention 253 Deadlock Prevention 253 Deadlock Prevention 253 Deadlock Prevention 253 Deadlock Prevention 254 Deadlock Prevention 255 Deadlock Prevention 257 Deadlock Prevention 257 Deadlock Prevention 258 Deadlock Prevention 258 Deadlock Prevention 259 Deadlock Prevention 259 Deadlock Prevention 259 Deadlock Prevention 259 Deadlock Prevention 250 Deadlock Preventio
Bibliographical Notes 271 MEMORY MANAGEMENT Main Memory Background 275 Swapping 282 Contiguous Memory Allocation 284 Paging 288 Structure of the Page Table 297 8.6 Segmentation 302 8.7 Example: The Intel Pentium 305 8.8 Summary 309 Exercises 310 Bibliographical Notes 312 Contents Chapter 9 Virtual Memory 9.1 9.2 9.3 9.4
9.5 9.6 9.7 Background 315 Demand Paging 319 Copy-on-Write 325 Page Replacement 327 Allocation of Frames 340 Thrashing 343 Memory-Mapped Files 348 . Frequently, the spyware is not discovered. If the program being attacked runs with system. 4,112 8.13
What is the purpose of paging the page tables? • File pointer. The messages are addressed to the distributed file system onto physical devices. Indeed, much of what is mentioned in this section applies to this entire family of operating systems. In
general, the kernel looks for processes that have been idle for long periods of time. A time line of this operation is shown in Figure 1.3. Interrupts are an important part of a computer architecture. By passing NULL as a second parameter, we initialize the mutex to its default attributes. For example, consider an allocation scheme where we allow high
priority processes to select frames from low-priority processes for replacement. The mainC) function presents the prompt C0MMAND-> and then invokes s e t u p O, which waits for the user to enter a command. The designers of protection systems have drawn heavily on ideas that originated in programming languages and especially on the concepts
of abstract data types and objects. Although redoing the data modifications will cause no harm (due to idempotency), it will nevertheless cause recovery to take longer. Domain switching occurs when the user is changed—generally when one user logs out and another user logs out and another user logs in. This list is typically populated using a page-replacement algorithm such
as those discussed in Section 9.4 and most likely contains free pages scattered throughout physical memory, as explained earlier. A logical address space is a collection of segments. Real systems are much more limited than the generator, which is an
algorithm that attempts to produce random bits. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the
prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center. 6.12 Demonstrate that monitors and semaphores are equivalent insofar as they can be used to implement the same types of synchronization problems. For added cryptographic strength, the session keys are
forgotten once a session is completed. INC EXECUTIVE EDITOR Bill Zobrist SENIOR PRODUCTION EDITOR Ken Santor COVER DESIGNER Madelyn Lesure COVER DESIGNER Judy Allan This book was set in Palatino by the author using LaTeX and printed and bound by Von Hoffmann, Inc. For example, if a client
on host X with IP address 146.86.5.20 wishes to establish a connection with a web server (which is listening on port 80) at address 161.25.19.8, host X may be assigned port 1625. There are four major reasons for building distributed systems: resource sharing, computation speedup, reliability, and communication. :•:.. A process must first create a
shared memory segment using the shmget () system call (shmget () is derived from SHared Memory GET). Create consumer thread(s) */ /* 5. If a process of ten pages actually uses only half of them, then demand paging saves the I/O necessary to load the five pages that are never used. In contrast to the IPC facility, the messages exchanged in RPC
communication are well structured and are thus no longer just packets of data. Wilson et al. In this case, we need at least one frame for the instruction and one frame for the memory reference. As a process executes, it changes state. The programmer first writes a short code segment such as the following: #include int mainfint argc, char *argv[]) {
execvpt"\bin\sh",'v\bin\sh", return 0; NULL); Using the execvpO system call, this code segment creates a shell process. One issue that must be dealt with concerns differences in data representation on the client and server machines. Access to a page marked invalid causes a page-fault trap. In addition to an IP address, an actual host name, such as
ivrvw.westminstercoHege.edu, can be used as well. Most frequently, it comes along with freeware or shareware programs, but sometimes it is included with commercial software. Even an individual user may work on many tasks at the same time. It shares with other threads belonging to the same process its code section, data section, and other
operating-system resources, such as open files and signals. It was disguised as a photo. In general, a file is a sequence of bits, bytes, lines, or records, the meaning of which is defined by the file's creator and user. The scanrate is expressed in pages per second and ranges from siowscan to fastscan. Thread pools offer these benefits: 1. A text-editor
program, for example, may include code to search the file to be edited for certain keywords. We implement such a client in the Java program shown in Figure 3.20. When the program starts executing, the stack is allocated at the other end of the virtual, address space and is allowed to grow towards lower virtual addresses. Termination can occur in
 other circumstances as well. This data structure will contain two items: (1) a fixed-sized array of size MAX SEQUENCE that will hold the Fibonacci values; and (2) the size of the sequence size < MAX..SEQUENCE. From the point of view of a specific processor in a
distributed system, the rest of the processors and their respective resources are remote, whereas its own resources are local. The TCB of a Cl system controls access between users and files by allowing the user to specify and control sharing of objects by named individuals or defined groups. A firewall is a computer, appliance, or router that sits
between the trusted and the untrusted. One reason for allocating at least a minimum number of frames involves performance. process 2-Hs-irnT-rr" i • :i ' ;£: * m. Many systems provide some help, however, in the form of a reference bit. That is, when one protocol generates a message to send to its protocol peer on another machine, it hands its
message to the protocol below it in the network-protocol stack for delivery to its peer on that machine. One of the early UNIX computer break-ins was detected by Cliff Stoll when he was examining accounting logs and spotted an anomaly. The Morris Internet worm used the f inger protocol to break into computers, so f inger would not be allowed to
pass, for example. For example, some database systems prefer raw I/O because it enables them to control the exact disk location where each database record is stored. (See the Bibliographical Notes for appropriate references.) These constructs provide mechanisms for three functions: 14.9 Language-Based Protection 553 1. • Data access. Examples
are the request () and releadlocks () and releadlocks Generally speaking, we can deal with the deadlocks Generally speaking.
deadlock state. 8xaitt|fe,:;a-:s|slejii: "can." fes-e ilisftsMrect& mtycfeti:: t&::itg.bases*; .'lit: Ih'ft:::ca«e*tfit*•: epgiattftg; 'Scte(usually l, SirtdlSkt. However, for applications where security matters, we are asking for trouble if we assume that the source or destination address of a packet reliably determines who sent or received that
packet. 9.2 Demand Paging 321 physical memory Figure 9.6 Steps in handling a page fault. More generally, Java's load-time and run-time checks enforce type safety of Java classes. • Between each pair of communicating processes, there may be a number of different links, with each link corresponding to one mailbox. The < T, commit s> record
appears in the log before the record. Typically, this view is that a process begins at a certain logical address—say, address 0—and exists in contiguous memory, as shown in Figure 9.2. Recall from Chapter 8, though, that in fact physical memory may be organized in page frames arid that the physical page frames assigned to a process may not be
contiguous. 9.4.8 Applications and Page Replacement In certain cases, applications accessing data through the operating system's virtual memory perform, worse than if the operating system provided no buffering at all. stateless service in, 651-652 distributed information systems (distributed naming services), 399 distributed lock manager (DLM), 15
distributed naming services, see distributed information systems, 615-617 distributed operating systems, 615-617 distributed operating systems, 615-617 distributed operating systems as, 615-617 distributed operating systems, 615-617 distributed operati
manager), 15 DMA, see direct memory access DMA controller, see direct-memoryaccess controller DMZ (demilitarized zone), 599 domain switching, 535 domain trees, 827 DOS attacks, see denial-of-service attacks double buffering, 513, 729 double caching, 433 895 double indirect blocks
427 f downsizing, 613 down time, 422 DPCs (deferred procedure calls), 791 DRAM, see dynamic random-access memory driver end (STREAM), 520 driver registration module (Linux), 746-747 dual-booted systems, 417 dumpster diving, 562 duplex set, 820 DVMA (direct virtual memory access), 504 dynamic linking, 764 dynamic link libraries (DLLs),
281-282, 787 dynamic loading, 280-281 dynamic priority, 722 dynamic protection, 534 dynamic random-access memory (DRAM), 8 dynamic routing, 625 dynamic routing, 625 dynamic priority, 722 dynamic protection, 534 dynamic random-access memory (DRAM), 8 dynamic routing, 625 dynamic priority, 722 dynamic protection, 534 dynamic random-access memory (DRAM), 8 dynamic routing, 625 dynamic priority, 722 dynamic priority, 722 dynamic protection, 534 dynamic priority, 722 dynamic priority, 723 ease of use, 4, 784 ECC, see error-correcting code EDF scheduling, 826, 422 earliest-deadline-first
scheduling effective access time, 323 effective bandwidth, 484 effectiv
passwords, 589-590 encrypted viruses, 570-896 Index encryption, 577-584 asymmetric, 580 authentication, 580-583 key distribution, 583-584 symmetric, 579-580 Windows XP, 821 enhanced integrated drive electronics (EIDE) buses, 453 entry section, 193 entry set, 218 environmental subsystems, 786-787 environment vector, 749 EPROM (erasable
programmable readonly memory), 71 equal allocation, 341 error conditions, 316 error conditions, 316 error conditions, 316 error conditions, 316 error detection, 40 escalate privileges, 27 escape (operating systems), 507 events, 220 event latency, 702 event objects (Windows XP), 790
event ordering, 663-666 exceptions (with interrupts), 501 exclusive locks, 378 execution of user programs, 762-764 execution of user progr
ext2fs, see second extended file system extended file system extended file system, 413, 766 external fragmentation, 287-288, 422 failure: detection of, 631-633 mean time to, 468 recovery from, 633 during writing of block, 477-478 failure handling (2PC protocol), 670-672 failure modes
(directories), 400-401 fair share (Solaris), 176 false negatives, 595 fast I/O mechanism, 807 FAT (file-allocation table), 425 fault tolerance, 13, 634, 818-821 fault-tolerant systems, 634 FC (fiber channel), 455 FC-AL (arbitrated loop), 455 FCB (file-control block), 413 FC buses, 453 FCFS scheduling algorithm, see firstcome, first-
served scheduling algorithm fibers, 832 fiber channel (FC), 455 fiber channel (FC), 455 fiber channel (FC) buses, 453 fide (NFS V4), 656 FIFO page replacement algorithm, 331-333 50-percent rule, 287 file(s), 22, 373-374. A network firewall limits network access between the two security domains and monitors and logs all connections. which, the corresponding file or
directory no longer exists (a deleted file). Therefore, there can be no circular wait. It said, in part: "When two trains approach each other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing, both shall come to a full stop and neither shall start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again until the other at a crossing start up again 
it executes, it returns control to the program so that its execution is not noticed. For many hard disks, when the disk controller is instructed to low-level-format the disk, it can also be told how many bytes of data space to leave between the header and trailer of all sectors. 2. One solution to the external-fragmentation problem is compaction. The worm
spawns copies of itself, using up system resources and perhaps locking out all other processes. When a process is submitted for execution, it is not always executed at the site at which it is initiated. The p t h r e a d j n u t e x ^ i a i t D function initializes an unlocked mutex. After it has received the date from the server, the client closes the socket and
exits. Five LWPs are needed, because all could be waiting for I/O completion in the kernel. If the degree of multiprogramming is stable, then the average departure rate of processes leaving the system. Security attributes of an object in Windows XP are described by a security descriptor. The entry
user-level threads. Windows XP classifies objects as either container objects or noncontainer objects or noncontainer objects or noncontainer objects or noncontainer objects as either commands. If no matches the user then invokes various child processes, such as the I s and cat commands. If no matches the user then invokes various child processes, such as the I s and cat commands.
is found, then an illegal address access has been attempted. Distributed operating systems are designed to address this problem. Rather, the capability list is itself a protected object, maintained by the operating system and accessed by the user only indirectly. With indirect communication, the messages are sent to and received from mailboxes, or
ports. The attacks use the same mechanisms as normal operation. In 1999, SSL 3.0 was modified slightly and presented in an IETF Request for Comments (RFC) under the name TLS. 6.7 Describe how the SwapO instruction can be used to provide mutual exclusion that satisfies the bounded-waiting requirement. See also program threats throughput,
157, 720 thunking, 812 tightly coupled systems, see multiprocessor systems time: compile, 278 effective access, 323 effective memory-access, 294 execution, 278 time-out schemes, 632, 686-687 time quantum, 164 timer: programmable interval, 509 variable, 20
timers, 509-510 timer objects, 790 time sharing (multitasking), 16 timestamp-based protocols, 228-230 timestamping, 675-676 timestamps, 665 TLB, see translation look-aside buffer 918 Index TLB miss, 293 TLB reach, 358-359 tokens, 628, 668 token passing, 628, 628 token p
Linus, 737 trace tapes, 184 tracks, disk, 452 traditional computing, 31-32 transactions, 222. What is the sequence of page faults incurred when all of the pages of a program are currently non-resident and the first instruction of the pages of a program is an indirect memory load operation? So that the section object can be used, a small message is sent that
contains a pointer and size information about the section object. During normal operation, the electronic disk stores data in a large DRAM array, which is volatile. What are the drawbacks of making the change that you suggest? 4.5.2 Linux Threads Linux provides the f ork() system call with the traditional functionality of duplicating a process, as
described in Chapter 3. This problem is in general unsolvable (see Bibliographical Notes for references), command line is longer than BUFFER SIZE. These certificate authorities (digitally signing the public keys of these other authorities), and so on, creating a web of trust. The consumer process has a local
variable nextConsumed in which the item to be consumed is stored. The benefit of sharing code and data is that it allows an application to have several different threads of activity within the same address space. Some of the fields of this structure include: • in t shm segsz—size of the shared-memory segment • short shmjiattch—number of attaches
to the shared-memory segment • s t r u c t ipc_perm shm_perm—permission structure (which is available in the file / u s r / i n c l u d e / s y s / i p c .h) contains the fields: • unsigned short uid—identifier of the user of the shared-memory segment •
unsigned short mode—permission modes • key t key (on Linux systems, key)—user-specified key identifier The permission modes are set according to how the shared-memory segment is established with the shared to
authenticate a message. Linux systems provide the ptrace command. We modify the page-fault service routine to include page replacement: 1. Issues concerning the design and verification of secure systems are discussed by Rushby [1981] and by Silverman [1983]. These free pages are typically
allocated when the stack or heap for a process must expand or when there are copy-on-write pages to be managed. It used a variety of subject lines to help avoid detection, including "Thank You!" "Your details," and "Re: Approved." It also used a random address on the host as the "From:" address, making it difficult to determine from the message
which machine was the infected source. A segment for kernel data 3. Higher-level requests, satisfied by the command interpreter or system programs, are translated into a sequence of system calls. InputStream deals with data at the byte level rather than the character level. This scheme is used for secure web communication, as we discuss in
Section 15.4.3. 15.4.2 Implementation of Cryptography Network protocols are typically organized in layers, each layer acting as a client to the one below it. Morris and Thompson [1979] discuss password security. Thus, they provide a much more trustworthy means of constraining senders and receivers of messages. It was the fastest-spreading worm
released to date, at its peak infecting hundreds of thousands of computers and one in seventeen e-mail messages on the Internet. The timestamp-ordering protocol ensures that any conflicting read and write operations are executed in timestamp-ordering protocol ensures that any conflicting read and write operations are executed in timestamp-ordering protocol ensures that any conflicting read and write operations are executed in timestamp-ordering protocol ensures that any conflicting read and write operations are executed in timestamp-ordering protocol ensures that any conflicting read and write operations are executed in timestamp order.
physically contiguous pages. Lipton [1974] discussed the limitations of various synchronization primitives. Essentially, Mach maps the address space containing the sender's message into the receiver's address space containing the sender's message into the receiver's address space. In another example, data warehouses frequently perform massive sequential disk reads, followed by computations and writes. Instead
each processor has its own local memory. Several types of attacks can be launched against programs and against programs a
constructing a multithreaded program that calculates the summation of a nonnegative integer in a separate thread. Main memory is usually too small to store all needed programs and data permanently. More typically, it is simple code (as it fits in a single disk block) and only knows the address on disk and length of the 72 Chapter 2 Operating-System
Structures remainder of the bootstrap program. We can control domain switching by including domains among the objects of the access matrix. Some of these considerations also apply to a softwaresupported protection kernel, but to a lesser degree, since the kernel may reside in fixed physical storage segments and may be loaded from only a
designated file. 14.3 Domain of Protection 535 the need-to-know principle is violated. This semantic can be assured by attaching a timestamp to each message. However, 4.4 Threading Issues 141 whereas UNIX must contend with how to deal with signals in a multithreaded environment, the APC facility is more straightforward, as an APC is delivered
to a particular thread rather than a process. Others include cache memory, CD-ROM, magnetic tapes, and so on. This limitation reduces the maximum number of frames [2002] discussed operating system support for multiple page sizes. Consider a system with a 1-KB frame size.
 Anonymous users, however, cannot access files outside of this directory tree. This virus attempts to bypass detection by an antivirus scanner by installing itself in the interrupt-handler chain. The object assigned from the cache is marked as used. If a process requests a resource that is currently allocated to another process, it can be added to a queue
of processes waiting for this resource. Unfortunately, total security cannot be achieved. Dekker. Here we discuss disk initialization, booting from disk, and bad-block recovery. This approach allows a process to run even though its entire memory image is not in main memory at once. In the remainder of this section, we explore each of these IPC
models in more detail. Another form of nonvolatile storage is NVRAM, which is DRAM with a 64-entry TLB, the TLB reach for Solaris ranges from 512 KB with 4-MB pages, The RSA algorithm is presented in Rivest et al. 5.1 Basic Concepts In a single-processor system, only one process can
run at a time; any others must wait until the CPU is free and can be rescheduled. 15.3 System and Network Threats 573 The worm was made up of two programs, a grappling hook (also called a bootstrap or vector) program and the main programs, a grappling that a process executing in either of these two domains can print object O4. Notice
that the memory unit sees only a stream of memory addresses; it does not know how they are generated (by the instruction counter, indexing, indirection, literal addresses, or some other means) or what they are for (instructions or data). " - - . PPP functions over modem connections, allowing home computers to be fully connected to the Internet. Type
safety' ensures that these restrictions can be enforced. The state of a process is defined by that process's current activity. When the transfer is complete, the CPU is interrupted. The idea of an inherently protected pointer provides a foundation for protection that can be extended up to the applications level. Harrison et al. However, there is not much
communication between the two would require generation of new session keys. Chapter 10, File-System Interface, is the old Chapter 11. Virtual memory techniques in Linux and BSD were described by Bovet and Cesati [2002] and McKusick et al. 6.9.4.2 Locking Protocol One way to ensure serializability is to associate with each data item a lock and
to require that each transaction follow a locking protocol that governs how locks are acquired and released. Thus, the ring network has a higher degree of availability than does a tree-structured network. What is the main advantage for a user? It also features a new section on thread scheduling, including Pthreads, and updated coverage of table
driven scheduling in Solaris. Explain how semaphores can be used by a server to limit the number of concurrent connections. If access has been revoked, the process will not be able to reacquire the capability. 9.4.5.3 Enhanced Second-Chance Algorithm We can enhance the second-chance algorithm by considering the reference bit and the modify bit
(described in Section 9.4.1) as an ordered pair. Connection ports are named objects and are visible to all processes; sthey give applications a way to set up communication channels (Chapter 22). The processors in a distributed system may vary in size and function. 9.4.5.1 Additional-Reference-Bits Algorithm We can gain additional ordering
8.4 311 Most systems allow programs to allocate more memory to its address space during execution. This routing may be either dynamic, to increase communication efficiency, or static, to reduce security risks or to allow communication efficiency, or static, to reduce security risks or to allow communication efficiency.
reference. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011. Each LWP is attached to a kernel thread, and it is kernel threads that the operating system schedules to run on physical processors. 3.11 Most UNIX and Linux
systems provide the ipcs command. Some details of the locking mechanisms used in Solaris were presented in Mauro and McDougall [2001]. Port scanning typically is automated, involving a tool that attempts to create a TCP/IP connection to a specific port or a range of ports. Information about NIST's AES activities can be found at information about
other cryptographic standards for the United States can also be found at that site. What are the advantages of such a paging scheme? Therefore, their operating system is designed to compromise between individual usability and resource utilization. To increase efficiency, most file systems group blocks together into larger chunks, frequently called
clusters. As a result, an object cannot manipulate its run-time stack, because it cannot get a reference to the process can access the address space of the process. The difficulty with the working set.
 Blocking receive. Note that a careful programmer could have performed bounds checking on the size of argv [1] by using the strncpy () function rather than strcpy (), replacing the line "strcpy () function rather than strcpy () function rather than 
different phases and may, for example, need read access in another. The two-phase locking protocol was introduced by Eswaran et al. A process that does not need to spawn other processor state—for instance, by
modifying register values—it must explicitly save the current state and then restore that state before returning. If external power is interrupted, the electronic-disk controller copies the data from RAM to the magnetic disk. Identifies the entry points (or gates) at which the segments may be called. The working set is the set of pages in the current
locality. The simple subject is assigned a security 15.9 An Example: Windows XP 603 context based on the security access token of the application name and command line parameters. They provide a firm practical understanding of the algorithms used—the properties, advantages, and
disadvantages. The access list is searched for any access rights to be revoked, and they are deleted from the list. Weston, and Yang Xiang Parts of Chapter 12 were derived from a paper by Hillyer and Silberschatz [1996]. Language-based protection provides finer-grained arbitration of requests and privileges than the operating system is able to
provide. All signals, whether synchronous or asynchronous or asynchronous, follow the same pattern: 't i I i. More specifically, suppose that 7} requests an exclusive lock on Q. Virtual memory available; she can concentrate instead on
the problem to be programmed. item nextProduced; while ((in + 1) % BUFFER SIZE; Figure 3.14 The producer process. Shared memory is usually implemented as multiple virtual addresses (one for each process
sharing the memory) that are mapped to one physical address. Register values b. Is there a simple method for detecting that such an event has occurred? The file system provides the mechanism for on-line storage of and access to both data and programs residing on the disks. Only secure software is uploaded, and a signature of each program is
taken via a secure message-digest computation. Thus, each memory reference through the page table takes two accesses. The producer then creates a view of the memory-mapped file in its virtual address space. The segments for user code and user data are shared by all processes running in user mode. The resulting list for each object consists of
ordered pairs, which define all domains with a nonempty set of access rights for that object. The suspended process can be restarted later. If CPU utilization is too low, we increase the degree of multiprogramming by introducing a new process to the system. 15.12 Compare symmetric and asymmetric encryption schemes, and discuss under what
circumstances a distributed system would use one or the other. This requires the main thread to wait for all worker threads to finish before it can output the walue of the matrix product. For instance, when a message is sent to a mailbox, the mailbox may be full. The many-to-many model suffers from neither of these shortcomings: Developers can
create as many user threads as necessary, and the corresponding kernel threads can run in parallel on a multiprocessor. do { flag[i] = TRUE; // critical section turn = j) { flag[i] = FALSE; // remainder section } while (TRUE); Figure 6.25 The structure of
process P, in Dekker's algorithm. 9.4 Page Replacement 327 Note, too, that only pages that can be modified need be marked as copy-onwrite. The dynamic adjustment of rights is performed to guarantee consistency of a programmer-defined abstraction. This IP peer then delivers the TCP packet up to the TCP peer on that machine. : j : . To send
messages to the list, send e-mail to: [email protected] Depending on the message, we will either reply to you personally or forward the message to everyone on the mailing list. However, if the parameters are also remote objects, they are passed by reference. Given the mailing list. However, if the parameters are also remote objects, they are passed by reference.
extreme case, the number can be reduced to zero, leaving only the reference bit itself. Other values could be used that would allow the calling thread to time out if the lock did not become available within a specified time. One solution to this issue is to use a thread pool. A producer process produces information that is consumed by a consumer
process. Skinner, Yannis Smaragdakis, Jesse St. Laurent, John Stankovic, Adam Stauffer, Steven Stepanek, Hal Stern, Louis Stevens, Pete Thomas, David Umbaugh, Steve Vinoski, Tommy Wagner, Larry L. • Boot. Therefore, they are suitable for individual readers or for students in lower-level classes who want to learn what an operating system issued to the stepanek.
without getting into the details of the internal algorithms. Sec also frame allocation proxy accepts a connection just as an SMTP server would and then initiates a connection to the original
destination SMTP server. The stability of these systems depends either on a physical limitation (such as the number of available terminals) or on the self-adjusting nature of human users. As the degree of multiprogramming increases, CPU utilization also increases, although more slowly, until a maximum is reached. page 1 page 2 ^ . We may
want to construct the system in a modular fashion, dividing the system functions into separate processes or threads, as we discussed in Chapter 2. But which class should be used to determine if the connection should be allowed, the application or the system functions into separate processes or threads, as we discussed in Chapter 2. But which class should be used to determine if the connection should be allowed, the application or the system functions again, decoding it again, decodin
two operands again, and 9.2 Demand Paging 323 then adding again. However, the inverted page table no longer contains complete information is required if a referenced page is not currently in memory. We assign to each resource type a unique integer number, which, allows us to
compare two resources and to determine whether one precedes another in our ordering. For example, the UltraSPARC supports page sizes of 8 KB, 512 KB, and 4 MB. Would it be possible for the user to develop a new command interpreter using the system-call interface provided by the operations happen frequently on
general-purpose systems. Also, when a thread performs a blocking system call, the kernel can schedule another thread for execution. These storage devices are usually nonvolatile, so the contents are persistent through power failures and system reboots. In comparing different memory-management strategies, we use the following considerations:
Hardware support. 6.2 The first known correct software solution to the critical-section problem for n processes with a lower bound on waiting of n-1 turns was presented by Eisenberg and McGuire. SSL is a complex protocol with many options. 315 316 Chapter 9 Virtual Memory The requirement that instructions must be in physical memory te be
executed seems both necessary and reasonable; but it is also unfortunate, since it limits the size of physical memory. Similarly, the computer sends bits onto the network with no way of knowing who might eventually receive them. For example, a user at the confidential level could not access a file at the more sensitive secre
level. Given our earlier discussions of virtual memory, it should be* clear how the sharing process points to the same page of physical memory—the page that holds a copy of the disk block. Nonetheless, we must have mechanisms to make security
breaches a rare occurrence, rather than the norm. It is the responsibility of the client or server application to impose a structure on the data. 6.20 When a signal is performed on a condition inside a monitor, the signaled. Why is it important for a protection
system to adhere to this principle? 8.16 Consider the Intel address-translation scheme shown in Figure 8.22. A swapper manipulates entire processes, whereas a pager is concerned with the individual pages of a process. Stored in this table is information regarding the use of the file by the process. Unfortunately, this makes it less convenient to
update the database after authorized updates to monitored directories and files. For example, if everyone can read a particular object, it must have a separate entry in every domain. In Pentium systems, the CPU generates logical addresses, which are given to the segmentation unit. 236 Chapter 6 6.28 Process Synchronization The decrease_count()
function in the previous exercise currently returns 0 if sufficient resources are available and -1 otherwise. There are 15 faults altogether. The large blank space (or hole) between the heap and the stack is part of the virtual address Max heap Figure 9.2 Virtual address space. Signals may be handled in different ways. Some systems (known as big-
endian) use the high memory address to store the most significant byte, while other systems (known as little-endian) store the least significant byte at the high memory address. 600 Chapter 15 Security Internet access from company's computers DMZ access from Internet access between DMZ and company's computers Figure 15.10 Domain
separation via firewall. In addition, it includes three access bits to control reading, writing, and execution. Deliver the signal to certain threads in the process model. If so, what are they? it is now first in line. j ava resides and then copy the file by executing get Server. Java In this scheme, the file by execution.
location is not transparent to the user; users must knowexactly where each file is. When an offset is legal, it is added to the segment base to produce the address in physical memory of the desired byte. Another safeguard, although it does not prevent infection, does permit early detection. Buddy system memory allocators were described in Knovvlton
[1965], Peterson and Norman [1977], and Purdom, Jr. and Stigler [1970]. 8.8 Program binaries in many systems are typically structured as follows. Operating systems are now almost always written in a systems implementation language or in a higher-level language. Thus, the access matrix of Figure 14.6(a) can be modified to the access matrix shown
in Figure 14.6(b). - TEB thread identifier user slack -...-. Consequently, it can execute only within its predefined memory space. As long as we have no page faults, the effective access time is equal to the memory space. As long as we have no page faults, the effective access time is equal to the memory space. As long as we have no page faults, the effective access time is equal to the memory access time.
operating system to provide the means for cooperating processes to communicate with each other via a message-passing facility. to release resource Ri. Now consider the resource Ri. Now consider the resource and the resource Ri. Now consider the Ri. Now
read-only memory (EPROM), which is readonly except when explicitly given a command to become writable. The tags themselves must not be directly accessible by an application program. [1990]. If an attempt is made to write onto the file, the system identifies this protection violation by comparing the requested operation with the capability in the
file-table entry. The UNIX news network, UUCP, allows systems to communicate with each other at predetermined times, via modems, to exchange messages. In the latter case, several such requests may be needed if a whole file is to be transferred. Regardless of the initial system state, both schedules produce the same final system state. The code
segment is followed by the data segment that is used for storing the program variables. It will fault for the pages are in memory; then, it will not fault again until it changes locality until all these pages are in memory; then, it will not fault again until it changes locality until all these pages are in memory; then, it will not fault again until it changes locality until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then, it will not fault again until all these pages are in memory; then again until all these pages are in memory; then again until all these pages are in memory; then again until all these pages are in memory; then again until again unt
we cannot compact storage. Linux allows one or more swap areas to be established. Now suppose that a process enters a new phase in its execution and needs more frames. 15.10 What are two advantages of encrypting data stored in the computer system? In other words, a process cannot request three printers if the system has only two. Morris
included in his attack arsenal a call to debug that —instead of specifying a user address, as would be normal in testing—issued a set of commands that mailed and executed a copy of the grappling-hook program. Rather, the mapped file may be demand-paged, thus bringing pages into memory only as they are accessed.) The MapViewDf F i l e ()
function returns a pointer to the shared-memory object; any accesses to this memory location are telephone lines, leased (dedicated data) lines, microwave links, and satellite channels. Fang et al. It starts faulting and taking frames away from other processes. A page fault causes the following
sequence to occur: 1. - - . These items can be represented in a struct { long fib sequence [MAX SEQUENCE]; int sequence size; } shared data; The parent process will progress through the following steps: a. This is the foundation of Java protection, since it enables a class to effectively
encapsulate and protect its data and methods from other classes loaded in the same JVM. With global replacement, a process may happen to select only frames allocated to other processes do not choose its frames for replacement). When a user logs on, Windows XP
creates a security access token that includes the security ID for the user, security IDs for any groups of which the user has. In the following section, we explore a memory allocation scheme where no space is lost due to fragmentation. Security within the operating system and between
operating systems is implemented in several ways, ranging from passwords for authentication through guarding against viruses to detecting intrusions. This example occurred during August 2003. The major problem is how to implement LRU replacement. Another method for determining the serializability order is to select an order in advance. ii 4—r
;' 111 : |. We assume that a transaction is assigned a timestamp immediately before its first instruction. The MULT1CS protection systems when power is turned off or otherwise lost. Thus, we
 want to control the page-fault rate. Output a log record onto stable storage. If the actual page-fault rate exceeds the upper limit, we allocate the process another frame; if the page-fault rate falls below the lower limit, we allocate the process another frame; if the page-fault rate exceeds the upper limit, we allocate the process. Pete would like to thank his family, friends, and coworkers for their support and understanding
during the project. These rights include such basic forms of access as the right to read, write, or execute a memory segment. Some operating systems—notably Solaris—prepage the page frames for small files. For our example reference string, our three frames are initially empty. Windows XP uses two types of ports: connection ports and
communication ports. Then, the contents of the block are execution environment abstracts these details and provides a virtual, machine as an intermediary between the executing program and the underlying a rchitecture At the
core of the .NET Framework is the Common Language Runtime (CLR). The working-set strategy (Section 9.6.2) starts by looking at how many frames a process is actually using. This violation involves unauthorized use of resources. A thread pool limits the number of threads that exist at any one point. 7.2 Deadlock Characterization In a deadlock,
processes never finish executing, and system resources are tied up, preventing other jobs from starting. This approach was used in the Andrew file system, as we discuss in Chapter 17, but it was found to be too inefficient. Hash functions work by taking a message in n-bit blocks and processing the blocks to produce an n-bit hash. Later, the process
can be reintroduced into memory, and its execution can be continued where it left off. These example programs were tested on Debian Linux 2.4 and 2.6 systems, Mac OS X, and Solaris 9 using the gcc 3.3 compiler. Handling signals in single-threaded programs is straightforward; signals are always delivered to a process. How long to sleep before
terminating 2. This page looks like a perfect replacement: It is clean and will not need to be written out, and it apparently has not been used for a, long time. The reference to page 3 replaces page 1, as page 1 will be the last of the three pages in memory to be referenced again. 3.3 Operations on Processes The processes in most systems can execute
concurrently, and they may be created and deleted dynamically. For example, recent security incidents include the use of spyware to provide a conduit for spam through innocent systems (was of spyware to provide a conduit for spam through innocent systems (was conduit for spam through innocent system).
628-631 communication structure of, 622-628 and connection strategies, 626-627 and contention, 627-628 and naming/name resolution, 627-628 and packet strategies, 626 and routing strategies, 626 and routing strategies, 626-627 and contention, 627-628 and packet strategies, 626-627 and contention, 627-628 and routing strategies, 626-627 and routing strategies, 626-627 and routing strategies, 626-627 and routing strategies, 626-628 and routing s
small-area, 28 threats to, 571-572 topology of, 620-622 types of, 617-618 in Windows XP, 822-829 Active Directory, 828 distributed-processing mechanisms, 824-826 domains, 827-828 interfaces, 821 name resolution, 828-829 protocols, 822-824 redirectors, 822 name resolution, 828-829 protocols, 822-824 redirectory, 828 distributed-processing mechanisms, 827-828 interfaces, 821 name resolution, 828-829 protocols, 822-824 redirectory, 828 distributed-processing mechanisms, 827-828 interfaces, 821 name resolution, 828-829 protocols, 822-824 redirectory, 828 distributed-processing mechanisms, 827-828 interfaces, 821 name resolution, 828-829 protocols, 822-824 redirectory, 828 distributed-processing mechanisms, 827-828 interfaces, 821 name resolution, 828-829 protocols, 822-829 protocols, 8
input/output system, see NetBIOS network computers, 32 network devices, 508-509, 771 network device interface specification (NDIS), 822 network file systems (NFS), 438-444 mount protocol, 440-441 NFS protocol, 441-442 path-name translation, 442-443 remote operations, 443^44 network information service (NIS), 399 network layer, 629 in the system of th
network-layer protocol, 584 network login, 399 network information systems, 725-728 network operating systems, 787 network operating systems, 787 network information service), 399 NLS (national-language
support) API, 787 nonblocking I/O, 510-511 nonblocking (asynchronous) message passing, 102 noncontainer objects (Windows XP), 603 nonmaskable interrupt, 501 nonpreemptive kernels, 194-195 nonpreemptive scheduling, 156 non-real-time clients, 728 nonremote (local) objects, 115 nonpreemptive kernels, 194-195 non
 schedule, 226 nonsignaled state, 220 nonvolatile RAM (NVRAM), 10 nonvolatile RAM (NVRAM) cache, 470 nonvolatile RAM), 10 NVRAM (nonvolatile RAM), 23 no-preemption condition (deadlocks), 254 Novell NetWare protocols, 823 NTFS, 814-816 NVRAM (nonvolatile RAM), 10 NVRAM (nonvolatile RAM) cache, 470 objects: access lists for, 542-543 in cache, 355 free, 356
hardware vs. Section 4.3 describes how to wait for a child thread to complete using the Win32, Pthreads, and Java thread libraries. This violation involves unauthorized modification of data. This scheme allows at most BUFFER_SIZE - l items in the buffer at the same time. 4.2.3 Many-to-Many Model The many-to-many model (Figure 4.4) multiplexes
many user-level threads to a smaller or equal number of kernel threads. The algorithm presented in Section 15.4.1 is based on the public-key encryption scheme; it was developed by Rivest et al. Suppose each of three processes holds one of these CD RW drives. They result from abuse of some of the fundamental functionality of TCP/IP. Whenever a
page is referenced, it is removed from the stack and put on the top. At this point, two minimal cycles exist in the svstem: Pi PT P. If the connection was successful, the cracker (or tool) could attempt to communicate with the answering service to determine if it was indeed sendmail and, if so, if it was the version with the bug. The addresses specifyers
 both the segment name and the offset within the segment. 9.6 Thrashing 347 each page. When the JVM loads a class, it assigns the class to a protection domain that gives the permissions of that class. *" Figure 8.21 physical og j address Lti't I n? A mutex is created with the pthread mutex in the permissions of that class. *" Figure 8.21 physical og j address Lti't I n? A mutex is created with the pthread mutex in the permissions of that class. *" Figure 8.21 physical og j address Lti't I n? A mutex is created with the pthread mutex in the permissions of that class to a protection domain that gives the permissions of that class. *" Figure 8.21 physical og j address Lti't I n? A mutex is created with the pthread mutex in the permissions of that class. *" Figure 8.21 physical og j address Lti't I n? A mutex is created with the pthread mutex is cre
a pointer to the mutex. RC4 is used in encrypting steams of data, such as in WEP, the wireless LAN protocol. It could instead have passed values specifying an offset and size, thus creating a view containing only a subsection of the file. Once the connection is made, the client can read front the socket using normal stream I/O statements. This pointer
is unique to each process operating on the file and therefore must be kept separate from the on-disk file attributes. This extra copying may result in unacceptably high overhead. In fact, an examination of real programs shows us that, in many cases, the entire program is not needed. This means that on Windows systems, Java threads are typically
implemented using the Win32 API; UNIX and Linux systems often use Pthreads. 90 Chapter 3 Processes Switching the CPU to another process requires performing a stat a state restore of a different process. Typically, a directory entry consists of the file's name and its unique identifier. One such situation occurs
when I/O is done to or from user (virtual) memory. The final result of these swaps is schedule 1 in Figure 6.22, which is a serial schedule. For many enterprises, it is more economical to have a number of small computers, each with its own self-contained applications, than to have a single large system. The process may require software that is
available at only a particular site, and either the software cannot be moved, or it is less expensive to move the process. It exploited three separate bugs for its operation. • Request. If none exist, a free object is assigned from an empty slab. This implementation approach is called stack inspection. Keys. For example, a web browser was an integral part
of the operating system. Using the log, the system can handle any failure that does not result in the loss of information on nonvolatile storage. This technique allows the child to write the contents of the Fibonacci sequence to the sharedmemory segment and has the parent output the sequence when the child completes. 3.4 Using the program shown
in Figure 3.24, explain what will be output at Line A. One solution is the use of a firewall to separate trusted and untrusted systems. Looking for a replacement, the paging system sees a page that is in memory but has not been referenced or modified: Tt is the paging system sees a page that the low-priority process just brought in. Restore the user registers, process state
and new page table, and then resume the interrupted instruction. Chapter 12, Mass-Storage Structure, is the segment allocated to the 21 KB request. A FIFO replacement algorithm associates with each page the time when that page was brought into memory. Once it has
written the date to the socket, the server closes the socket to the client and resumes listening for more requests. Many companies are replacing their mainframes with networks of workstations or personal computers. Novel hardware instructions and their utility in implementing Bibliographical Notes 243 synchronization primitives have been
described in works such as Culler et al. When a file is named, it becomes independent of the parent once it resumes. Which of the two versions
of f orkO to use depends on the application. In this way, the RPC models a typical subroutine procedure call but can work between systems—hence the term remote. In our example, if A is a local object and B a remote object, A is serialized and passed by reference. The third parameter identifies a mode flag. A flag indicating
the level of sharing 3. The designer of a communication network must address five basic issues: • Naming and name resolution. POSIX (which stands for Portable Operating Systems. The occurrence of an event is usually signaled by an interrupt from
either the hardware or the software. Chapters 8 and 9 deal with main memory management during the execution of a process. • Nonblocking send. Messages are sent to and received from mailboxes, called ports in Mach. Virtual memory involves the separation of logical memory as perceived by users from physical memory. It may also include various
data structures: objects, arrays, stacks, variables, and so on. If we must suspend a process (due to an I/O wait or a lack of free frames), we remember the working set for that process. We also discuss the semantics of sharing files among multiple processes, users, and computers. A file is a collection of related information defined by its creator. The
new procedure executed /bin/sh, which, if successful, gave the worm a remote shell on the machine under attack. Note that the locality model is the unstated principle behind the caching discussions so far in this book. 14.3.3 An Example: MULTICS system, the protection domains are organized hierarchically into a ring structure. A
nonprocedural or declarative notation seems a preferable way to make protection available to the application programmer. Encryption limits the domain of senders. Generally, if the time to transfer the data is longer than the time to execute the remote command, the remote command should
be used. Operating systems exist because they offer a reasonable way to solve the problem of creating a usable computing system. Fork the child process and invoke the wait () systems are previously compromised, independent systems that are serving their owners while being used for nefarious
purposes, including denial-of-service attacks and spam relay. 9.4 Page Replacement 329 b. Save the user registers and process state. The server would create a separate thread to service the request. The
entire process, or parts of it, may be executed at different sites. This is one of the most important differences between Java and many other languages (including C++). It includes new coverage of shared memory is enhanced
with a program illustrating the shared-memory API available for POSIX systems. As we move down the hierarchy, the cost per bit legislorr, cache :t[ 3 mam niomory electronic disk magnetic disk oplic.il dink magnetic tapes Figure 1.4 Storage-device hierarchy, the cost per bit legislorr, cache :t[ 3 mam niomory electronic disk magnetic disk oplic.il dink magnetic tapes Figure 1.4 Storage-device hierarchy, the cost per bit legislorr, cache :t[ 3 mam niomory electronic disk magnetic disk oplic.il dink magnetic tapes Figure 1.4 Storage-device hierarchy, the cost per bit legislorr, cache :t[ 3 mam niomory electronic disk magnetic disk oplic.il dink magnetic disk oplic.il dink magnetic tapes Figure 1.4 Storage-device hierarchy, the cost per bit legislorr, cache :t[ 3 mam niomory electronic disk magnetic disk oplic.il dink magnetic disk oplic.il disk oplic.il dink magnetic disk oplic.il disk op
by B, whose associated domain bit is off, the userlD of the process is set to A. Suggestions We have attempted to clean up every error in this new edition, but—as happens with operating systems—a few obscure bugs may remain. These mechanisms work well only as long as the users conform to the intended use of and access to these resources. It
initializes all aspects of the system, from CPU registers to device controllers and the contents of main memory, and then starts the operating system. CLONE SIGHAND Signal handlers are shared. The key ks again is a pair (d, N), where N is the product of two large, randomlychosen prime numbers p and q. In this case, ranges of memory addresses
are set aside and are mapped to the device registers. 9.5.3 Global versus Local Allocation Another important factor in the way frames are allocated to the various processes is page replacement. 1.1 What Operating Systems Do We begin our discussion by looking at the operating system's role in the overall computer system. (Digital signatures are
covered in Section 15.4.1.3.) A configurable policy file determines the permissions granted to the domain (and its classes). Every client that calls a subsystem needs a communication channel, which is provided by a port object and is never inherited. The worm program took elaborate steps to cover its tracks and to repel efforts to stop its spread. The
code 2. When we select a page for replacement, we examine its modify bit. When the user is asked for the login name, the user supplies the name "anonymous" and an arbitrary password. • To discuss the principles of the working-set model. We check an internal table (usually kept with the process control block) for this process to determine whether
the reference was a valid or an invalid memory access. This result implies that, regardless of the initial system state, schedule 2 will produce the same final state as will some serial schedule. Stack memory 4.5 Can a multiprocessor system than on a
single processor system? For example, suppose that, in Figure 14.4, we include the control right in access(D2, D4). • Partial versus total. Moreover, it is not always desirable for a transaction to unlock a data item immediately after its last access of that data item, because serializability may not be ensured. The file to be copied (that is, Server Java)
rmist be placed in a special subdirectory (say, ftp) with the protection set to allow the public to read the file. Although a programmer can define her own protected procedures (any of which might be incorrect), the security of the overall system cannot be compromised. When the process is to be resumed (because I/O has finished or enough free
frames have become available), we automatically bring back into memory its entire working set before restarting the process. Empirically gauging the difference in overhead can be difficult, but in general it is much more time consuming to create and manage processes than threads. The first three references (7.0.1) cause page faults and are brought
into these empty frames. 8.11 Explain why sharing a reentrant module is easier when segmentation, is used than when pure paging is used. The access matrix can implement policy decisions concerning protection. To reduce the number of data, we use two facts. Under direct communication, each process that wants to communicate must explicitly
name the recipient or sender of the communication. We can approximate the working-set model with a fixed-interval timer interrupt and a reference bit. The users normally decide the contents of the access-matrix entries. A smaller page size allows each page to match program locality more accurately, pure segmentation c. The process's pages are
written out (swapped), and its frames are reallocated to other processes. Furthermore, Windows 2000 allows a hard disk to be divided into one or more partition, identified as the boot partition.
following sections, we examine two strategies for managing free memory that is assigned to kernel processes. When the RPC is being invoked on a process on the same system, the RPC is indirectly handled through a local processes. When the RPC is being invoked on a process on the same system, the RPC is being invoked on a process on the same system, the RPC is being invoked on a process on the same system.
kbad "*j algorithm 0 attacker - read 1 messagem- decryption key kd Figure 15.9 A man-in-the-middle attack on asymmetric cryptography. Before it can request any additional resources, however, it must release all the resources that it is currently allocated. 6.26 What are the implications of assigning a new timestamp to a transaction that is rolled
back? This action restores memory to its state before the instruction was started, so that the instruction can be repeated. Designing a system as a sequence of layers or using a microkernel is considered a good technique. Can access be revoked and
later be obtained again? Exercises 9.6 367 Assume that you are monitoring the rate at which the pointer isi the clock algorithm (which indicates the candidate page for replacement) moves. This scheme requires a search of the page table to find the LRU page and a write to memory (to the time-of-use field in the page table) for each memory access.
This scheme is called equal allocation. For example, a server may wish to have only N socket connections at any point in time. The interrupt must transfer control to the appropriate interrupt must transfer cont
Sockets A socket is defined as an endpoint for communication. In this chapter, we start by examining ways in which resources may be accidentally or purposefully misused. These communication links are controlled by special communication processors (Figure 16.3), which are responsible for defining the interface through which the sites
communicate over the network, as well as for transferring information among the various sites. ".:" ".::." \:\ Figure 2.17 The Java virtual machine. The number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the program is less than the number of kernel threads allocated to the number of kernel threads allocated threads 
shmat () returns a pointer to a character string. Systems that contain data pertaining to corporate operations may be of interest to unscrupulous competitors. The second parameter specifies the size (in bytes) of the shared memory segment. Once a victim page is found, the page is replaced, and the new page is inserted in the circular queue in that
position. Of course, for stack inspection to work, a program must be unable to modify the annotations on its own stack frame or to do other manipulations of stack inspection. The pages are paged out. It is difficult for the operating system to schedule for improved rotational latency, though, because modern disks do not disclose the physical location of
logical blocks. You can narrow the selections down by age, length of book, topic and other categories. [1991], Govindan and Anderson [1991], Draves et al. The rows of the access matrix represent domains, and the columns represent objects. If this triple is found, the operation is allowed to continue; otherwise, an exception (or error) condition is
raised. A general structure of a distributed system is shown in Figure 16.1. 611 612 Chapter 16 Distributed system. 9.4.6 Counting-Based Page Replacement There are many other algorithms that can be used for page replacement. Indeed, this sharing of data
provides one of the benefits of multithreaded programming. This procedure allows the process to restart as soon as possible, without waiting 9.4 Page Replacement 339 for the victim page to be written out. The scheduling algorithms described here consider only the seek distances. We now consider the possible security vulnerabilities of a buffer
overflow. On Windows NT, 2000, and XP systems, however, shared memory is accomplished by memory mapping files. • Multipartite. The extent to which data can be accessed despite the failure of some links or sites. This approach would multithread the
web-server process. Thus, running a program that is not entirely in memory would benefit both the system and to set file stributes, such as the file's owner. Also note that the function F should be defined according to
the normal order of usage of the resources in a system. 3.5 What are the benefits and the disadvantages of each of the following? The changes do not affect the virus's functionality but rather change the virus's signature. One option is to load the entire program in physical memory at program execution time. That is, all transactions share a common
semaphore mutex, which is initialized to 1. Clean pages do not have to be paged out to be replaced. A page is in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working set if it is referenced anywhere in the working s
the capability for access to A may be amplified as control passes to the code body of P. When the definition of an object is made known to Hydra, the 548 Chapter 14 Protection names of operations on the type become auxiliary rights. A successful call to shmget () returns an integer identifier for the shared-memory segment. The Bl-class TCB
maintains the security label of each object in the system; the label is used for decisions pertaining to mandatory access control. The procedure for handling this page fault is straightforward (Figure 9.6): 1. In this instance, the producer process writes the message "Shared memory message" to shared memory. Physical. 16.2.1.2 Remote File Transfer
Another major function of a network operating system is to provide a mechanism for remote file transfer from one machine to another. The watchdog then either grants or denies access to the file. 3.10 In Exercise 3.6, the child process must output the Fibonacci sequence, since the parent and child have their own copies of the data. For example, a
web-site click could download a Java applet that proceeds to vise all available CPU time or to infinitely pop up windows. Where, then, should a signal be delivered? This remote copying is accomplished through the "anonymous FTP" method, which works as follows. internal fragmentation c. - ' - - ' - . Multithreaded programs introduce many challenges
for the programmer, including the semantics of the fork() and exec() system calls. Most people would say no. A task-state segment (TSS) 6. The structure of a Windows XP thread is illustrated in Figure 4.10. This scheme was adopted in the CAL system. Protection is a mechanism for controlling the access of programs, processes, or users to the
resources defined by a computer system. A condition variable provides a method by which a monitor procedure can block its execution until it is signaled to continue. (In some circumstances, a process may be allowed to exceed its working-set maximum.)
effective and flexible, depending on the length of the keys. This procedure is known as an upcall. The KTHREAD includes scheduling and synchronization information for the untrusted applet's openO invocation will result in an exception, because the
checkPermissionsO call finds no doPrivileged annotation before encountering the stack frame of the gui 0 method. physical, 279-280 virtual, 317, 760-761 address-space identifiers (ASIDs), 293-294 administrative complexity, 645 admission control, 721, 729 admission-control algorithms, 704 advanced encryption standard (AES), 579 advanced
technology attachment (ATA) buses, 453 advisory file-locking mechanisms, 379 AES (advanced encryption standard), 579 affinity, processor, 170 887 888 Index aging, 163-164, 636 allocation, 421-423 indexed allocation, 425^427 linked allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 425^427 linked allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 425^427 linked allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 421-423 indexed allocation, 425^427 linked allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 425^427 linked allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 421-423 indexed allocation, 421-423 indexed allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 421-423 indexed allocation, 421-423 indexed allocation, 423^125 and performance, 427-429 contiguous allocation, 421-423 indexed allocation, 421-423 indexed allocation, 421-423 indexed allocation, 423^125 and performance, 421-429 contiguous allocation, 421-423 indexed allocation, 421-423 indexed allocation, 421-423 indexed allocation, 423^125 and 421-423 indexed allocation, 421
429 equal, 341 as problem, 384 proportional, 341 slab, 355-356 analytic evaluation, 181 Andrew file system (AFS), 653-659 file operations in, 657-658 implementation of, 658-659 shared name space in, 656-657 anomaly detection, 595 anonymous memory, 467 APCs, see asynchronous procedure calls API, see application
```

```
program interface Apple Computers, 42 Application Domain, 69 application interface (I/O systems), 505-511 block and character devices, 507-508 blocking and nonblocking I/O, 510-511 clocks and timers, 509-510 network devices, 508-509 application programs, 4 disinfection of, 596-597 multistep
processing of, 278, 279 processes vs., 21 system utilities, 55-56 application program interface (API), 44-46 application proxy firewalls, 600 arbitrated loop (FC-AL), 455 architecture (s), 12-15 clustered systems, 12-14 of Windows XP, 787-788 architecture (s), 12-15 clustered systems, 12-18 ingle-processor systems, 12-19 of Windows XP, 787-788 architecture (s), 12-19 clustered systems, 12-19 c
areal density, 492 argument vector, 749 armored viruses, 571 ARP (address resolution protocol), 636 arrays, 316 ASIDs, see address-space identifiers assignment edge, 249 asymmetric clustering, 15 asymmetric encryption, 580 asymmetric multiprocessing, 102
asynchronous procedure calls (APCs), 140-141, 790-791 asynchronous thread cancellation, 139 asynchronous writes, 434 ATA buses, 453 Atlas operating system, 845-846 atomicity, 669-672 atomic transactions, 198, 222-230 and checkpoints, 224-225 concurrent, 225-230 and locking protocols, 227-228 and serializability, 225-227 and timestamperating system, 845-846 atomicity, 669-672 atomic transactions, 198, 222-230 and checkpoints, 224-225 concurrent, 225-230 and locking protocols, 227-228 and serializability, 225-227 and timestamperating system, 845-846 atomicity, 669-672 atomic transactions, 198, 222-230 and checkpoints, 224-225 concurrent, 225-230 and locking protocols, 227-228 and serializability, 225-227 and timestamperating system, 845-846 atomicity, 669-672 atomic transactions, 198, 222-230 and checkpoints, 224-225 concurrent, 225-230 and locking protocols, 227-228 and serializability, 225-227 and timestamperating system, 845-846 atomicity, 845-846 
based protocols, 228-230 system model for, 222-223 write-ahead logging of, 223-224 attacks, 560. To do so, the user must have a valid account on that machine. Linux is similar to Solaris in that swap space is only used for anonymous memory or for regions of memory shared by several processes. Upon execution of a program, the CLR loads
assemblies into what is known as the Application Domain. For this reason, Tripwire and its associated files should be stored on some tamper-proof medium, such as a write protected disk or a secure server where logins can be tightly controlled. By the evening of the next day, November 3, methods of halting the invading program were circulated to
system administrators via the Internet. The type of system desired is the foundation for choices among various algorithms and strategies that will be needed. Initially, a transaction is in the growing phase. 1 7 0 1 334 Chapter 9 Virtual Memory Section 5.3.2.) As a result, the optimal algorithm is used mainly for comparison studies. The site or sites
containing the computer systems must be physically secured against armed or surreptitious entry by intruders. 8.8 Summary 309 {linear address) llobal directory • page table offset CR3 — register Figure 8.24 Three-level paging in Linux. • To describe the interfaces to file systems. Another early demand-paging system was
MULTICS, implemented on the GE 645 system (Organick [1972]). Each of the summation of the s
writes one data byte to the data register and sets a bit in the control register to signal that the byte is available. The working-set model assumes that processes execute in localities. With local replacement, if one process starts thrashing, it cannot steal frames from another process and cause the latter to thrash as well. We acquire the semaphore Sem
created in this example by using the statement: WaitForSingleObj ect(Semaphore is in the signaled state and thus is acquired by the calling thread. Random numbers will 238 Chapter 6 Process Synchronization be produced using the rand() function, which produces random irttegers
between 0 and RANDJvlAX. 3.5 Examples of IPC Systems 3.5.1 An Example: POSIX Shared Memory 103 * Several IPC mechanisms are available for POSIX systems, including shared memory and message passing. Upcalls are handled by the thread library with an upcall handler, and upcall handlers must run on a virtual processor. Versions of SCAN
and C-SCAN that follow this pattern are called LOOK and C-LOOK scheduling, because they look for a request before continuing to move in a given direction (Figure 12.8). The receiver blocks until a message is available. We attach a region of shared memory using shmat () as follows: shared memory = (char *) shmat(id, NULL, 0); If successful
shmat () returns a pointer to the beginning location in memory where the shared-memory region has been attached. The kernel messages specified in the parameter to p r i n t k O are logged in the file /var/log/kernel/warnings. Using a lock bit can be dangerous: The lock bit may get turned on but never turned off. To illustrate this protocol, consider
schedule 3 of Figure 6.24, which includes transactions % and T3. An alternative strategy is to initially load pages only as they are needed. Some operating systems give special programs the ability to use a disk partition as a large sequential array of logical blocks, without any file-system data structures. 604 Chapter 15 Security For a real multiuser
environment, the system administrator should formulate a security plan and implement it, using the features that Windows XP provides and other security tools. and CR. This is a case of poor operating-system design decisions. An RPC occurs when a process (or thread) calls a procedure on a remote application. Memory is allocated from this segment
using a power-of-2 allocator, which satisfies requests in units sized as a power of 2 (4 KB, 8 KB, 16 KB, and so forth). Refer again to the program shown in Figure 15.4(a). [1997]. Exercises 233 6.3 What is the meaning of the term
busy 'waiting? The ability to execute a program that is only partially in memory would confer many benefits: • A program would no longer be constrained by the amount of physical memory that is available. The attacker then happily decrypts it. It would be more efficient to access the files at the sites where they reside and return the desired results to
the site that initiated the computation. Also, the more complex the operating system, the more work must be done during a context switch. This platform allows programs to be written to target the .NTT Framework instead of a specific architecture. The operating-system kernel supports and manages kernel-level threads. Typically, a process using an
existing shared-memory segment first attaches the shared-memory region to its address space and then accesses (and possibly updates) the region of shared memory. To reduce the overhead in searching the log after a system failure has occurred, we can use a checkpoint scheme. As you might expect, neither MFU nor LFU replacement is common. A
CPU-bound load store add store add store read from file • CPU burst • I/O burst wait for I/O load store read from file • CPU burst • I/O burst wait for I/O load store add store read from file • CPU burst • I/O load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store add store read from file • CPU load store read from f
have not yet been overwritten. As a general rule, we encourage readers to progress sequentially through the chapters, as this strategy provides the most thorough study of operating systems. In this example, we initialize the semaphore to the value 5. However, certain hardware devices interact directly with physical memory—without the benefit of a
more storage is needed, both for the data themselves and for the log recording the changes. • Hardware preference. The advantage of a distributed system is that these functions can be carried out over great distances. In summary, the specification of protection in a programming language allows the high-level description of policies for the allocation
and use of resources. Exercises 605 15.3 The list of all passwords is kept within the operating system. Also growing is the use of optical-fiber-based FDDI networking. The bug exploited in sendmail also involved using a daemon process for malicious entry, sendmail sends, receives, and routes electronic mail. The act of allocating—and releasing—
memory can be a time-consuming process. The full bootstrap program can be changed easily: A new version is simply written onto the disk. 9.6.2 Working-Set Mode! As mentioned, the working-set model is based on the assumption of locality. Furthermore, lack of bounds checking is not the only possible cause of the behavior of the program in Figure
15.2. The program could instead have been carefully designed to compromise the integrity of the system. 16.2.2. Computation In some circumstances, we may want to transfer the computation. If one thread in a program calls f ork(), does the new
process duplicate all threads, or is the new process single-threaded? An additional aspect of demand paging is the handling and overall use of swap space. Two-factor authentication requires two forms of authentication requires two forms of authentication pink. This approach is the least-recently-used (LRU) algorithm. Swapping may be
necessary to improve the process mix or because a change in memory, requirements has overcommitted available memory to be freed up. When the setuid bit is on, and a user executes that file, the user ID is set to that of the owner of the file; when the bit is off however, the user ID does not change. (Hint: Use different internal and
external representations.) 15.4 What is the purpose of using a "salt" along with the user-provided password? !.; « ..-.- .. In particular, if an object must be accessible in domain Du then we must have / < i. The effective access time = (1 - p) x ma + p x page fault time. See also RAID 912 Index
redundant arrays of inexpensive disks, set' RAID Reed-Solomon codes, 473 reentrant code (pure code), 296 reference bits, 336 Reference Model, ISO, 585 reference string, 330 register(s), 47 base, 276, 277 memory-address, 279 page-table base, 293 page-table length, 296 for page tables, 292-293 relocation, 280 registry, 55, 810
relative block number, 383-384 relative path names, 390 relative speed, 194 releaseO operation, 377 reliability, 626 of distributed operation systems, 612-613 in multimedia systems, 616-651 basic scheme for, 647 and cache location
647-648 and cache-update policy, 648, 649 and caching vs. A process executing in domain D\ can read file in its virtual address space with the MapViewOf FileC) function. This algorithm is called the second-chance pagereplacement algorithm. 9.7.1
Basic Mechanism Memory mapping a file is accomplished by mapping a disk block to a page (or pages) in memory. In the absence of expensive battery and generator backup systems, data must be written to nonvolatile storage for safekeeping. If the swap space is simply a large file within the file system, normal file-system routines 12.6 Swap-Space
Management 467 can be used to create it, name it, and allocate its space. Signals may be handled by first setting certain fields in the C structure s t r u c t sigaction and then passing this structure to the sigaction fields in the C structure s t r u c t sigaction and then passing this structure s t r u c t sigaction and then passing this structure to the sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction and then passing this structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t r u c t sigaction fields in the C structure s t u c t sigaction fields in the C structure s t u c t sigaction fields in the C structure s t u c t sigaction fields in the C structure s t u c t sigaction fields in the C structure s t u c t sigaction fields in the C structure s t u c t sigaction fi
inexpensive digital books for kids online. Bershad et al. For example, one of the fields in a TLB entry must indicate the size of the page frame corresponding to the TLB entry. This classification of transactions is accomplished as follows: • Transaction 7, needs to be undone if the log contains the < T, s t a r t s > record but does not contain the < T-,
commits record. Both of the models just discussed are common in operating systems, and many systems, and worst-fit, best-fit, best-fit, best-fit, best-fit, best-fit, best-fit, and worst-fit algorithms place processes of 212 KB, 417 KB, 112 KB, and 426 KB (in order)? 9.8
Allocating Kernel Memory When a process running in user mode requests additional memory, pages are allocated from the list of free page frames maintained by the kernel. This pattern continues. 4.6 Summary A thread is a flow of control within a process. Define a page-replacement algorithm using this basic idea. The controller calculates the ECC
and finds that the sector is bad. 0040 Read permission of group. The Hydra system was described by Wulf et al. Certain computing environments may require other certification, such as that supplied by TEMPEST, which guards against electronic eavesdropping. The system's free memory and CPU resources don't stand a chance. In UNIX, as we've
seen, each process is identified by its process is identified by its process identifier, #include #inc
complete */ wait(NULL); printf("Child Complete"); exit (0); Figure 3.10 C program forking a separate process. • Nonblocking receive. Such a computation can be carried out in different ways. You can purchase a print copy of this supplement at Wiley's website by going to and choosing the Student Solutions Manual link. On operating systems that
support them, it is kernel-level threads—not processes—that are in fact being scheduled by the operating system. One scheme for communication between the user-thread library and the kernel is known as scheduled by the operating system. One scheme for communication between the user-thread library and the kernel is known as scheduled by the operating system.
row i and column / that it is to use in calculating the matrix product.: 68 Chapter 2 Operating-System Structures 2.8.3.2 The Java Virtual Machine * Java is a popular object-oriented programming language introduced by Sun Microsystems in 1995. One-time passwords, for example, change from session to avoid replay attacks. Provide an
example of a situation in which a native method is useful, 2.11 It is sometimes difficult to achieve a layered approach if two components of the operating system are dependent on each other. This is possible because all processes use the same logical address space and all segment descriptors are stored in the global descriptor table (GDT). Based on
the complexity of starting the attack, it is unlikely that the worm's release or the scope of its spread was unintentional. Here, a lock bit is associated with every frame. For instance, a web client could trigger a database operation on a web server. MULTICS has a segmented address space; each segment is a file, and each segment is associated with
one of the rings. 15.2 Program Threats Processes, along with the kernel, are the only means of accomplishing work on a computer. : : : : ; iiiii iiiii • : - . Every memory address generated by the CPU must be checked for legality and possibly mapped to a physical address. Identify a scenario in which it is unclear how to layer two system components
that require tight coupling of their functionalities. Install a bigger paging disk. The third parameter allows naming of the mutex. In a compiler-supported scheme, security rests on correctness of the translator, on some underlying mechanism of storage management that protects the segments from which compiled code is executed, and, ultimately,
on'the security of files from which a program is loaded. The most common configurations are multiaccess bus, ring, and star networks. Most of its internal algorithms were selected for simplicity, rather than for speed or sophistication. When the sector is read, the ECC is recalculated and is compared with the stored value. The server listens to port
6013, although the port could have any arbitrary number greater than 1024. Multithreaded program execution, 55 program mable interval
timer, 509 programmed I/O (PIO), 353, 503 programming-language support, 55 program threats, 563-564 * viruses, 563-564 * viruses, 563-564 * viruses, 563-568 trap doors, 564-565 Trojan horses, 563-564 * viruses, 563-568 trap doors, 564-565 Trojan horses, 563-564 * viruses, 563-568 trap doors, 564-565 Trojan horses, 563-568 trap doors, 564-568 t
access control for, 402-406 access matrix as model of, 538-542 control, access, 545-546 implementation, 542-545 capability-based systems, 547-550 Cambridge CAP system, 549-550 Hydra, 547-550 Cambridge CAP systems, 547
file systems, 402-407 goals of, 531-532 I/O, 515-516 language-based systems, 550-555 compiler-based enforcement, 550-555 as operating system service, 41 in paged environment, 295-296 permissions, 406 and principle of least privilege, 532-533 retrofitted, 407 and revocation of access rights, 546-547 security vs., 559 static vs. A user
of the Hydra system would explicitly incorporate calls on these system procedures into the code of her programs or would use a program translator that had been interfaced to Hydra. So that access to the shared data is coordinated, the processes involved might use one of the mechanisms for achieving mutual exclusion described in Chapter 6. As an
example, many commercial software packages provide a given number of licenses, indicating the number of application is started, the license count is decremented. x/kernel directory, although that location may differ in your Linux distribution. Distributed systems. We can now use the freed frame to
hold the page for which the process faulted. Another approach for increasing the TLB reach is to either increase the size of the page or provide multiple page sizes. Ann x in matrix indicates the current request of each process. 6.9.4.3 Timestamp-Based Protocols In the locking protocols described above, the order followed by pairs of conflicting
transactions is determined at execution time by the first lock that both request and that involves incompatible modes. 320 Chapter 9 Virtual Memory 9.2.1 Basic Concepts When a process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped in, the pager guesses which pages will be used before the process is to be swapped out again. The RPC scheme requires a similar binding of the client
and the server port, but how does a client know the port numbers on the server? Now that the full bootstrap program has been loaded, it can traverse the file system to find the operating system kernel, load it into memory, and start its execution. Set the value of sequence_size to the parameter on the command line. 4.1.2 Benefits The benefits of
multithreaded programming can be broken down into four major categories: 1. Messages longer than 64 bits are broken into 64-bit chunks, and a shorter block is padded to fill out the block. MULTJCS uses a ring structure in addition to file access. The search path lists the set of directories to search when an ambiguous program name is given. In
addition, if a page is used often enough to keep its reference bit set, it will never be replaced. 362 Chapter 9 Virtual Memory We must be sure the following sequence of events does not occur: A process issues an I/O request and is put in a queue for that I/O device. The latter choice produces a large number of data (on the order of 1 million addresses
per second). The write pointer must be updated whenever a write occurs. When a page fault occurs, we first check whether the desired page is in the free-frame pool, if it is not, we must select a free frame and read into it. These are the very reasons for efforts to create asymmetric key algorithms. For instance, demand paging may take priority over
application I/O, and writes are more urgent than reads if the cache is running out of free pages. If the intrusion-detection system has a true-alarm rate of 0.0005, what percentage of alarms generated by the system correspond to real intrusions? The main difference between the two is the way in which they are
 geographically distributed. In previous editions, the chapter gave a historical view of the development of operating systems. If a is close to 0, prepaging loses; if a is close to 1, prepaging wins. The principle of separation of policy and mechanism was advocated by the designer of Hydra (Levin et al. A swap area may be in either a swap file on a regular
 file system or a raw swap partition. Some systems recommend the amount to be set aside for swap space. • Sometimes, we want authentication but not confidentiality. Deferred cancellation. The APC facility allows a user thread to specify a function that is to be called when the user thread receives notification of a particular event. Kent et al. This
requires passing two parameters to each thread. The control right is applicable only to domain objects. Two implementations are feasible: reference string 7 0 7 1 2 0 3 0 4 2 3 0 3 i- A 0 5 0i 3} t 2 7 7 2 2 A 0 0 0 0 - 3 0 3 1 i '• 2 1 2 0 page frames Figure 9.15 LRU page-replacement algorithm. To illustrate process execution and termination, consider
that, in UNIX, we can terminate a process by using the exit Q system call; its parent process may wait for the termination of a child process by using the wait O system call; its parent process may wait for the termination of a child process by using the wait O system call; its parent process may wait for the termination of a child process by using the wait O system call; its parent process by using the exit Q system call; its parent process may wait for the termination of a child process by using the wait O system call; its parent process by using the exit Q system call; its parent process by using the exit Q system call; its parent process by using the exit Q system call; its parent process by using the wait O system call of the control of the 
service only one client at a time. Although each process considers the shared libraries reside in physical memory are shared by all the processes (Figure 9.3). Information about the first partition is kept in the local descriptor table (LDT); information about the second partition
is kept in the global descriptor table (GDT). A nonzero value would allow other processes to access the semaphore as well. The minimum number of frames is defined by the computer architecture. The access matrix provides an appropriate mechanism for defining and implementing strict control for both the static and dynamic association between
processes and domains. 15.4.3 An Example: SSL SSL 3.0 is a cryptographic protocol that enables two communicate securely—that is, so that each can limit the sender and receiver of messages to the other. In this case, the undetected deadlock will result in deterioration of the system's performance, because resources are being held by
processes that cannot run and because more and more processes, as they make requests for resources, will enter a deadlocked state. In the first two cases, the process eventually switches from the waiting state to the ready queue. Data allocated in the heap segments of programs is an example of such allocated
memory. In general, Windows XP does a good job of providing features to help ensure a secure computing environment. needs to execute. To illustrate the concept of cooperating processes, let's consider the producer-consumer problem, which is a common paradigm for cooperating processes. Rather, systems now combine swapping with virtual
memory techniques (Chapter 9) and swap pages, not necessarily entire processes. However, closer examination shows that it, too, can be used to provide secure protection of user-defined objects. Details of Windows 2000 synchronization can be found in Solomon and Russinovich [2000]. We can implement this provision by requiring that system calls
requesting resources for a process precede all other system calls. All connections must be unique. Often, in a batch system, more processes are submitted than can be execution) to guarantee correct behavior,
even if a failure occurs during the recovery process. To allow producer and consumer processes to run concurrently, we must have available a buffer of items that can be filled by the producer and emptied by the consumer. The system administrator can prohibit printing to a printer on the system for all or part of a day and can use the Windows XP
Performance Monitor to help her spot approaching problems. Most disks even come from the factory with bad blocks. The monitor concept was developed by Brinch-Hansen [1973]. AES is another symmetric block cipher. These algorithms are described below. A key is a unique bit pattern that can be associated with a capability. Global variables d.
For a given set of processes, we can increase the multiprogramming level only by packing more process is suspended, and the child process uses the address space of the parent. For
most applications, the value of working-set minimum and working-set minimum is 50 and 345 pages, respectively. If we were to use an interrupt for every memory reference by a factor of ten. Since the frame
contents are not modified when a frame is written to the disk, the old page can be reused directly from the free-frame pool if it is needed before that frame is reused. Data that resided on the bad blocks usually are lost. It is independent and is not attached to any particular processes, the operating system can
make the computer more productive. 344 Chapter 9 Virtual Memory degree of multiprogramming Figure 9.18 Thrashing. A refinement of Knuth's algorithm by deBruijn [1967] reduced the waiting time to n2 turns, after which Eisenberg and McGuire [1972] (Exercise 6.4) succeeded in reducing the time to the lower bound of n—1 turns. A client then
sends a message containing the name of the RPC to the rendezvous daemon requesting the port address of the RPC it 3.6 client Communication in Client-Server Systems message, looks up answer ^ 113 j user calls kernel | to send RPC message to procedure X kernel sends message to
matchmaker to find port number kernel places port Pin user RPC message Pprtt kernel Pie: fiPG? The association between the FIFO and OPT algorithms (other than looking backward versus forward in time) is that the FIFO algorithm uses the
time when a page was brought into memory, whereas the OPT algorithm uses the time when a page is not modified and 20 milliseconds if the replaced, page is modified. The attack via remote access was one of three infection methods
 AccessAUowed or AccessDenied for each action. Virtual memory allows one process to create a region of memory that it can share with another process. • - • : ..;;.' . A system table records whether each resource is free or allocated; for each resource that is allocated, the table also records the process to which it is allocated. If format finds a bad
block, it writes a special value into the corresponding FAT entry to tell the allocation routines not to use an efficient type of process creation known as copy-on-write, wherein parent and child processes share actual pages of memory. A new process is initially put in the ready queue. Typically, an
asynchronous signal is sent to another process. Virtual memory techniques are often used for managing this table. Since we are now viewing a process as a sequence of pages, rather than as one large contiguous address space, use of the term swapper is technically incorrect. The former is an invocation of the g e t () method of a class in the URL
loader protection domain, which is permitted to openO sessions to sites in the lucent addasse and one thread returns the result, the remaining threads
might be canceled. • Packet strategies. The confinement problem was first discussed by Lampson [1973] and was further examined by Lipner [1975]. We also describe the basic computer architecture that makes it possible to write a functional operating system. The call to shmat () expects three parameters as well. The bounded buffer assumes a fixed
buffer size. Operating system designers may implement the specification in any way they wish. Let p be the probability of a page fault (0 s p 5 1). Frequently, the bugs are buffer overflows, allowing the creation of a privileged command shell on the system. For instance, we can create a copy of a file, or copy the file to another I/O device, such as a
printer or a display, by creating a new file and then reading from the old and writing to the manufacturing process. 16.4 Network Topology The sites in a distributed system can be connected
physically in a variety of ways. While it is waiting, some of its resources may be preempted, but only if another process requests them. A stream of bytes or bits rather than a block. The security descriptor contains the security ID of the owner of the object (who can change the access permissions), a
group security ID used only by the POSIX subsystem, a discretionary access-control list that identifies which atiditing messages the system will generate. iii iii II..Iii ::; :. Empty. Therefore, any data that it must access in your
program must be declared globally, i.e. at the top of the source file before your function declarations. 106 Chapter 3 Processes 3. 3.8 Modify the date server shown in Figure 3.19 so that it delivers random fortunes rather than the current date. This table has the ability to mark an entry invalid through a valid-invalid bit or special value of protection
global table is simple; however, the table can be quite large and often cannot take advantage of special groupings of objects or domains. They might copy the data structure or pass its address to other program components, but they could not gain access to its contents. Within days, specific software patches for the exploited security flaws were
available. Stack- and buffer-overflow techniques allow successful attackers to change their level of system access. While the low-priority process faults. If we have only one large page, we must bring in the entire page, a total of 200 KB transferred and allocated. However, as described earlier in this section, the Pentium
architecture only uses a two-level paging model. In the message exchanged between the cooperating processes. Typically, a library is mapped read-only into the space of each process that is linked with it. Design a new scheme that is suitable for larger portions. Most local procedure
calls have the "exactly once" functionality, but it is more difficult to implement. Other mechanisms by which the user-level thread library and the kernel cooperate with each other threads in the process. Scheduler
activations were first presented in Anderson et al. 15.2.5 Viruses Another form of program threat is a virus. Then, in Sections 7.4 through 7.7, we present detailed algorithms. of a process is divided into two partitions. The interrupt service routine executes; on completion, the CPU resumes the interrupted computation. Applications like this
understand their memory use and disk use better than does an operating system that is implementing algorithms for general-purpose use. There are two fundamental models of interprocess communication: (1) shared memory and (2) message passing. Describe all the steps taken by the Intel Pentium in translating a logical address into a physical
 address. CLONE_VM The same memory space is shared. The load instruction moves a word from main memory to an internal register within the CPU, whereas the store instruction moves the content of a register to main memory to an internal register within the CPU.
it contains enough information that, if only a few 12.5 Disk Management 463 bits or data have been corrupted, the controller can identify which bits, have changed and can calculate what their correct values should be. 14.9 Language-Based Protection To the degree that protection is provided in existing computer systems, it is usually achieved
through an operating-system kernel, which acts as a security agent to inspect and validate each attempt to access a protected resource. This time, however, when this bit is set to "valid," the associated page is both legal and in memory. Raw I/O bypasses all the file-system services, such as the buffer cache, file locking, prefetching, space allocation
file names, and directories. The machine has six segment registers, allowing six segments to be addressed at any one time by a process. There are several other symmetric block encryption algorithms in use today that bear mentioning. Chapter 14, Protection, is the old Chapter 18 updated with coverage of the principle of least privilege. A user
process generates the virtual address 11123456. Some devices transfer a character or a block of charac
shared areas. In addition to a language specification and a large API library, Java also provides a specification for a Java virtual machine—or JVM. When the client invokes a remote procedure, the RPC system calls the appropriate stub, passing it the parameters provided to the remote procedure. Unlike the native Word format, RTF does not include
the capability to attach macros. Once the child process exits, control returns from the WaitForSingleOb j ect () function in the parent process. This scheme may be used for several reasons: • Load balancing. 10,1.2 File Operations A file is an abstract data type. RPCs are another form of distributed communication. The CAP system was described by
Needham and Walker [1977]. The write(A) operation of To conflicts with the read(B) operation of To conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read(B) operation of To does not conflict with the read (B) operation of To does not conflict with the read (B) operation of To does not conflict with the read (B) operation of To does not confli
memory access. There are several reasons for providing an environment that allows process cooperation: • Information sharing. Authentication: the receiver knows that only the sender could have generated the message. The LRU algorithm would be removing old pages and preserving new ones, while the application would more likely be reading
older pages than newer ones (as it starts its sequential reads again). A pointer to the semaphore 2. 9.22 The Catalan numbers are an integer sequence C,, that appear in treeenumeration problems. To determine the number of page
frames available. • Suppose that transaction 7} issues write(Q): o If TS(T,) < R-timestamp(Q), then the value of Q that 7} is producing was needed previously and T,- assumed that this value would never be produced. However, many operating systems—such as Windows XP and Solaris—treat processes and threads differently. These compiled files
called assemblies, include MS-IL instructions and metadata. In this instance, the producer process will be passed an integer parameter on the command line means the producer process will generate the first 5 Catalan numbers. How are messages sent
through the network? process Pi to release resource Ri. In addition, process Pi is waiting for process P? As the number of frames increases, the number of page faults drops to some minimal level. A user-defined signal handler Every signal has a default signal handler that is run by the kernel when handling that signal. We discuss these schemes in
Section 7.5. If a system does not employ either a deadlock-prevention or a deadlockavoidance algorithm, then a deadlock situation may arise. Why did Morris unleash the worm? It should also be available as a tool for use by the application designer, so that resources of an applications subsystem can be guarded against tampering or the influence of
an error. The third solution is the one used by most operating systems, including LJMTX and Windows; it is then up to the application developer to write programs that handle deadlocks. io. InputStream. A runaway process could constitute an accidental denial-of-service attack. Programs written in languages such as C# (pronounced C-sharp) and
VB.NET are compiled into an intermediate, architecture-independent language (MS-1L). In addition, if one-level indirect addressing is allowed (for example, a load instruction on page 23), then paging requires at least three frames per
process. More generally, in order to access a protected resource, some method in the calling sequence that resulted in the request must explicitly assert the privilege to access the resource. 9.4.2 FIFO Page Replacement The simplest page-replacement algorithm is a first-in, first-out (FIFO) algorithm. In a shared-memory system, the responsibility for
When a user creates an object, he can specify which domains can access the object, as well as the operations allowed. [1995a], and Thorn [1997]. Explain your answer. The upcall handler for this event also requires a virtual processor, and the kernel may allocate a new virtual processor or preempt one of the user threads and run the upcall handler on
its virtual processor. After that, whenever the system requests logical block 87, the request is translated into the replacement sector's address by the controller. memory was a set of accesses by the controller. memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller. The memory was a set of accesses by the controller was a set of accesses by t
rights. [1997] and Gong etal. File "locks allow one process to lock a file and prevent other processes from gaining access to it. - - - - . Hennessy and Patterson [2002] discussed the hardware aspects of TLBs, caches, and MM Us. Talluri et al. The producer and consumer must 98 Chapter 3 Processes be synchronized, so that the consumer does not try
to consume an item that has not yet been produced. for responding to keystrokes from the user, and a third thread for performing spelling and grammar checking in the background. If there are no customers to be served, the barber goes to sleep. On Mac OS X, the ktrace are no customers to be served, the barber goes to sleep. On Mac OS X, the ktrace are no customers to be served, the barber goes to sleep.
returns a pointer to the entry in the open-file table. The port number is returned, and the RPC calls can be sent to that port until the process terminates (or the server crashes). These include the following: • g e t : Transfer a file from the remote machine to the local machine. Let's look at a contrived but informative example. Here, however, because
we are dealing with an environment in which the processes are executing on separate systems, we must use a message-based communication scheme to provide remote service. Intercepting these data could be just as harmful as breaking into a computer; and interruption of communications could constitute a remote denial-of-service attack,
diminishing users' use of and trust in the system. For example, we illustrate shared memory using just the POSIX API; socket programming in TCP/IP is highlighted using the Java API. If we add TLBs, and 75 percent of all page-table references are found in the TLBs, what is the effective memory reference time? Segmentation is a memory
management scheme that supports this user view of memory. Once the read has taken place, the read pointer is updated. All references to the old identifier must be found, so that they can be modified to the new identifier. Deciding how much to program pages is a significant challenge. Bovet and Cesati
[2002] explain how Linux handles threading. We can accomplish this scheme in an application program by developing an ordering among all synchronization objects in the system. More recent architectures store the return address on the system stack. 9.8 9.9 9.10 9.11 Allocating Kernel Memory 353 Other Considerations 357 Operating-System
Examples 363 Summary 365 Exercises 366 Bibliographical Notes 370 PART FOUR • STORAGE MANAGEMENT Chapter 10 10.1 10.2 10.3 10.4 11.5 11.6 11.7 File-System Interface 10.6 Protection 402 10.7 File-System Mounting 395 File Sharing 397 Chapter 11 11.1 11.2 11.3 11.4 11.5 11.6 11.7 File-System Interface 10.6 Protection 402 10.7
Summary 407 Exercises 408 Bibliographical Notes 409 File-System Implementation 413 Directory Implementation 415 Log-Structured File Systems 437 NFS 438 Example:
The WAFL File System 444 Summary 446 Exercises 447 Bibliographical Notes 449 Chapter 12 Mass-Storage Structure 451 12.2 Disk Structure 451 12.2 Disk Structure 451 12.2 Disk Structure 451 12.3 Disk Attachment 455 12.4 Disk Structure 451 12.2 Disk Structure 451 12.3 Disk Attachment 455 12.4 Disk Structure 451 12.7 Disk Structure 451 12.8 Disk
Stable-Storage Implementation 477 Tertiary-Storage Structure 478 Summary 488 Exercises 489 Bibliographical Notes 493 Chapter 13 I/O Systems 13.1 13.2 13.3 13.4 13.5 Overview 495 I/O Hardware 496 Application I/O Interface 505 Kernel I/O Subsystem 511 Transforming I/O Requests to Hardware Operations 518 13.6 STREAMS 520 13.7
Performance 522 13.8 Summary 525 Exercises 526 Bibliographical Notes 527 xx Contents PART FIVE • PROTECTION AND SECURITY* Chapter 14 Protection 531 14.7 Revocation 532 14.8 Capability-Based Systems 547 Domain of Protection 533 14.9
Language-Based Protection 550 Access Matrix 542 Exercises 556 Access Matrix 542 Exercises 556 Access Control 545 Bibliographical Notes 557 Chapter 15.2 15.3 15.4 15.5 15.6 15.7 The Security Problem 559 15.8 Computer-Security Program Threats 563 Classifications 600 System and Network Threats
611 16.2 Types of Distributed Operating Systems 613 16.3 Network Structure 622 16.6 Communication Protocols 628 16.7 16.8 16.9 16.10 Robustness 631 Design Issues 633 An Example: Networking 636 Summary 637 Exercises 638 Bibliographical Notes 640 Chapter 17 Distributed
File Systems 17.1 17.2 17.3 17.4 17.5 Background 641 Naming and Transparency 643 Remote File Access 646 Stateful Versus Stateless Service 651 File Replication 652 17.6 An Example: AFS 654 17.7 Summary 659 Exercises 660 Bibliographical Notes 661 Contents Chapter 18 18.1 18.2 18.3 18.4 18.5 Distributed Coordination Event Ordering 663
Features of Real-Time Kernels 698 Implementing Real-Time Operating Systems 700 19.5 Real-Time Operating Systems 700 19.5 Real-Time Operating Systems 710 19.7 Summary 712 Exercises 713 Bibliographical Notes 713 Chapter 20 Multimedia Systems 20.6 Network Management 725 20.7 An Example: CineBlitz 728 20.8 Summary 730 Exercises 731 Bibliographical
Notes 733 20.1 What Is Multimedia? System generation involves simply creating the appropriate tables to describe the system. Both V and V(k) for any k should be efficiently computable functions. In such a case, on a UNIX system, the setuid bit on a networking program would be set, causing the user ID to change when the program was run. A
request in units not appropriately sized is rounded up to the next highest power of 2. The benefits of a distributed system and thereby speeding up computation and improving data availability and reliability. The IP address 127.0.0.1 is a special IP address known as the loopback
Schlichting and Schneider [1982] discussed asynchronous message-passing primitives. If we have multiple processes in memory, we must decide how many frames to allocate to each process. Similarly, domain D2 is the owner of F2 and F3 and thus can add and remove any valid right within these two columns. call ita X.. There are also various
commands to change transfer modes (for binary or ASCII files) and to determine connection status. 9.3 What is the copy-on-write feature? Unfortunately, the optimal page-replacement algorithm is difficult to implement, because it requires future knowledge of the reference string. That
is, E(k) can be derived from D(k), and vice versa. • If the marshalled parameters are local (or nonremote) objects, they are passed by copy using a technique known as object serialization. In fact, there is currently much debate in the Linux community about whether to set aside swap space at all! Some operating systems—including Linux—allow the
use of multiple swap spaces. These modules are linked together to form the generated operating system. The processes or cooperating processes or cooperating processes or cooperating processes or cooperating system. The processes or cooperating system may be either independent processes or cooperating system. The processes or cooperating processes or cooperating system may be either independent processes.
reach. The segmentation unit produces a linear address for each logical address. Inconvenient or inadequate security measures are bound to be circumvented, causing an overall weakening of the security measures are bound to be circumvented, causing an overall weakening of the security measures are bound to be circumvented.
b in / Is (used to get a directory listing) using the execlpO system call (execlpO is a version of the execlpO system call). Process creation is time consuming and resource intensive, as was shown in the previous chapter. Request. It works by performing 10 to 14 rounds of transformations on a matrix formed from a block. This is useful when the length
a communication would make a block cipher too slow. '-: • • - '-. Therefore, Linux has adopted a threelevel paging strategy that works well for both 32-bit and 64-bit architectures. Chapter 6, Process Synchronization, is the old Chapter 7. As soon as N connections are made, the server will not accept another incoming connection until an existing
connection is released. Although the Pentium uses a two-level paging model, Linux is designed to run on a variety of hardware platforms, many of which are 64-bit platforms where two-level paging is not plausible. Ng, Banu Ozden, Ed Posnak, Boris Putanec, Charles Qualline, John Quarterman, Mike Reiter, Gustavo RodriguezRivera, Carolyn J. They
can decompress compressed viruses before checking for a signature. The FunBrain site also has games for kids of ages and videos like Kidz Bop, Teen Titans Go! and Highlights Kids. Deliver the signal to every thread in the process. Removing a page and putting it on the top of the stack then requires changing six pointers at worst. The standard C
library 304 Chapter 8 [emery Libraries that are linked in during compile time might be assigned separate segments. m Chapter 2, Operating-System Structures, is a revised version of old Chapter 3, with many additions, including enhanced discussions of system calls and operating-system structure. 3.2 Process Scheduling queue header PCB7 87
PCBZ ready queue mag tape unit 0 mag tape unit 0 mag tape unit 1 disk unit 0 PCB, terminal unit 0 head tail Figure 3.6 The ready queue and various I/O device queues. Protection needs are simply declared, rather than programmed as a sequence of calls on procedures of an, operating system. Subsequent reads and writes to the file are handled as routine memory
 accesses, thereby simplifying file access and usage by allowing the system to manipulate files through memory rather than incurring the overhead of using such a system for security? This shielding ensures that equipment outside the room or building where the terminal is
housed cannot detect what information is being displayed by the terminal. The maximum size of the message queue defaults to eight messages. A programmer can make direct use of the protection system after acquainting herself with its features in the appropriate reference manual. How many memory operations are performed when an user
program executes a memory load operation? For instance, consider the use of the "." character in a search path. This working-set strategy prevents thrashing while keeping the degree of multiprogramming as high as possible. Notice that it is not strictly necessary to record the time when a page is brought in. 14.6 Discuss the strengths and
weaknesses of implementing an access matrix using capabilities that are associated with domains. If the total demand is greater than the total number of available frames (D > m), thrashing will occur, because some processes will not have enough frames. c), and then create a separate child process that performs the command- Unless otherwise
specified, the parent process waits for the child to exit before continuing. • put: Transfer from the local machine to the remote machine to the remote machine. When counters are increased 3. This phenomenon is illustrated in Figure 9.18, in which CPU utilization is plotted against the degree of multiprogramming. First, generate a random pagereference string where page
numbers range from 0 to 9. 7.4 Deadlock Prevention As we noted in Section 7.2.1, for a deadlock to occur, each of the four necessary conditions must hold. For instance, when a swapped-out process is restarted, all its pages are on the disk, and each must be brought in by its own page fault. Morshedian [1986] presents methods to fight password
pirates. The mailbox has an initially empty queue of messages. locked niutex,;-. We can try to keep three free frames reserved on the free-frame list at all times. ' - " ' . For every service that answered, it could try to use each known bug. More changes were made in later versions of Solaris. 9.6 Thrashing 345 34 32 30 28 en , 26 b CD E 24 ....ll!!,.l. _\
virtual memory Figure 9.1 - • : • a memory map page v • physica memory Diagram showing virtual memory that is larger than physical memory. The fully connected network. A disk
that has a boot partition (more on that in section 12.5.1) is called a boot disk or system disk. The producer then writes a message process-] • shared-;: %riet?nery v process2 ~ - -.. A P r i n t W r i t e r object allows the server to write to the socket using the routine p r i n t () and p r i n t In () methods for output. This is one of many reasons that
 "inconsequential" systems should also be secured, not just systems containing "valuable" information or services. [1975]). In this context, we can view an operating system as a resource allocator. Suppose that these transactions are executed atomically in the order To followed by T\. One way to implement the second-chance algorithm (sometimes
referred to as the dock algorithm) is as a circular queue. Details of interprocess communication in UNIX systems were presented by Gray [1997]. A process is the unit of work in a system. This requirement has led to the development of a number of language constructs that allow the programmer to declare various restrictions on the use of a specific
managed resource. Another reason is the vast number of services Windows XP system. The view of the mapped in the virtual address space of the process —the entire file or only a portion of it may
be mapped. The queue has finite length n; thus, at most n messages can reside in it. Receive an interrupt from the disk I/O subsystem (I/O completed). Amplification allows implementation procedures access to the representation variables of an abstract data type. Other factors must be considered as well (such as the relationship between page size
                                      ing device). 92 Chapter 3 Processes terminal. If we increase the page size—say, from 8 KB to 32 KB—we quadruple the TLB reach. Because networked systems share no memory, a host within the system initially has no knowledge about the processes on other hosts. This means that references to virtual addresses that are not
mapped result in page faults.;:. This protocol operates as follows: • Suppose that transaction T,- issues read(Q): o If TS(T,) < W-timestamp(), then T, needs to read a value of Q that was already overwritten. When pointed at a target, it will determine what services are running, including application names and versions. Examples include failure
auditing for login and logoff events to detect random password break-ins, success auditing for executable files to track a virus outbreak, and success and failure auditing for file access to detect access to sensitive files. If another process
requests that resource, the requesting process must be delayed until the resource has been released. What has happened is that his authentication key and password have been stolen by the child to complete by invoking the wait to
system call. The main differences among the various storage systems lie in speed, cost, size, and volatility. 2.5 What are the five major activities of an operating system with regard to file management? The server must keep a history of all the timestamps of messages it has already processed or a history large enough to ensure that repeated messages
are detected. Protection and security. Low-level formatting also sets aside spare sectors not visible to the operating system. A typical LAN may consist of a number of different computers (from mainframes to laptops or PDAs), various shared peripheral devices (such as laser printers and magnetic-tape drives), and one or more gateways (specialized
processors) that provide access to other networks (Figure 16.2). In the following section, we illustrate support in the Win32 API for shared memory using memory-mapped files. For each item on your list, state whether this concern relates to physical, human, or operating-system security. 9.10.1 Windows XP Windows XP implements virtual memory-mapped files.
using demand paging with clustering. To order books or for customer service please, call l(800)-CALL-WILEY (225-5945). As intruders exploit security vulnerabilities, security vulnerabilities, security vulnerabilities, security vulnerabilities, security vulnerabilities.
scheduling queues throughout its lifetime. Rather, Client Server Connection Port Handle Client Communication Port Handle Client Communication Port Handle Server Connection Port Handle Server Connection Port Handle Server Communication Port Handle Server Connection Port Handle
syllabi that suggest various approaches for using the text in both introductory and advanced operating systems courses. It provides the mechanism for on-line storage of and access to both data and programs of the operating systems courses. It provides the mechanism for on-line storage of and access to both data and programs of the operating systems courses.
to run a program to accomplish a specific task, as depicted in Figure 14.8. This implementation of privileges decreases the security risk associated with superusers and setuid programs. Explain why this is true. The access matrix is sparse. The entry in the file table then points to the file and its buffers. Mauro and McDougall [2001] describe recent
developments in threading the Solaris kernel. This action is a transfer of a right, rather than a copy. In this case, the consumer must wait if the buffer is empty, and the producer must wait if the buffer is full. There are many variations on this simple strategy.
Figure 16.4 Network topology. It can determine the host operating system. Most modern operating systems now provide features enabling a process to contain multiple threads of control. Sometimes a site does not even know it is under attack. What is not open to speculation, however, is the legal outcome: A federal court convicted Morris and
handed down a sentence of three years' probation, 400 hours of community service, and a $10,000 fine.; . The process continues to have the same privileges as before. The operating system lacks this knowledge. 9.3 Copy-on-Wrste In Section 9.2, we illustrated how a process can start quickly by merely demandpaging in the page containing the first
instruction. First, consider "at most once". Hydra provides a large library of system-defined procedures that can be called by user programs. This movement of jobs is called load sharing. • Security. 3.5.3 An Example: Windows XP The Windows XP Th
decrease the time needed to implement new features. Consider the cost of modifying the system to support a newly acquired graphics terminal or another representing code? 108 Chapter 3 Processes applications using the Win32 API invoke
standard remote procedure #calls. This will vary between the different kernel distributions, but some typical commands for building the kernel source code is stored) include: c make xconfig o make bzlmage • Add a new entry to the set of bootable kernels supported by the system. In general,
we expect a curve such as that in Figure 9.11. The openO operation takes a file name and searches the directory, copying the directory entry into the open-file table. When a process executes in monitor mode, it can execute privileged instructions and thus gain complete control, of the computer system. This solution, however does not have an upper
bound on the amount of time a process must wait before it is allowed to enter the critical section. We next see the frame pointer, which is the address of the beginning of the stack frame. • Use a logical counter as the timestamp; that is, a transaction enters the system. A language
implementation can provide software for protection enforcement when automatic hardware-supported checking is unavailable. We can increase Sem by 1 using the following statement: ReleaseSemaphore(Sem, 1, NULL); Both ReleaseSemaphore(Sem, 1, NULL); Both ReleaseSemaphore(Sem, 1, NULL); Both ReleaseSemaphore(Sem, 2, NULL); Both ReleaseSemaphore(Sem, 3, NULL); Both ReleaseSemaphore(Sem, 4, NULL); Both ReleaseSemaphore(S
allow the child process to run in the background—or concurrently—as well by specifying the ampersand (&) at the end of the command. In the hierarchy shown in Figure 1.4, the storage systems above the electronic disk are volatile, whereas those below are nonvolatile. Code is stored starting with a small fixed virtual address such as 0. We start with
an exploration of security threats. And when a computer sends a message, it names the intended receiver by specifying a destination on threads programming in Solaris can be found in Sun Microsystems [1995]. If the association is
dynamic, a mechanism is available to allow domain switching, enabling the process to switch from one domain to another. IVM for the Windows family of operating systems might use the Pthreads -APL 4.4 Threading Issues In this section, we discuss some of the issues to
consider with multithreaded programs. We also want to have operations that allow a user to get and set the various attributes of a file. Photo Courtesy: Catherine Falls Commercial/Getty Images Many of the books are free to read online. 6.9 Show that, if the waitO and signal () semaphore operations are not executed atomically, then mutual exclusion
may be violated. Paging is added between the CPU and the memory in a computer system. Some computers have little or no user view. The common functions of controlling and allocating resources are then brought together into one piece of software: the operating system. As we shall see, in many cases we can allow transactions to overlap their
execution while maintaining serializability. The biggest change is first created by the communication works as follows: • The client opens a handle to the subsystem's connection port object. Therefore, we now provide
an overview of I/O. We have added over 15 new programming exercises that emphasize processes, threads, shared memory, process synchronization, and networking. Virtual memory is a technique that enables us to map a large logical address space onto a smaller physical memory. Rather than swapping the entire process into memory, however, we
use a lazy swapper. FTP requires the user to know a command set entirely different from the normal operating-system commands. Note that writes to the file on disk. Consider how you think of a program when you are writing it. • cd: Change the current directory on
the remote machine. By transitivity, F(Ro) < F(RQ), which is impossible to design, code, and implement an operating-System Structures 2.9 Operating-System Generation It is possible to design, code, and implement an operating system specifically for one machine at one site. It is only at this point that the system is said to be running. In addition, there may be a
relationship between the Java thread library and-the-thread library on the host operating system. Had the worm exited on all duplicate sightings, it might have remained undetected. In principle, we need to search the entire log to make these determinations. What does the system degenerate to if the number of pages in the free-frame pool is zero?
The operating system is normally distributed on disk or CD-ROM. The MULTICS ring protection scheme b. or a number of adjacent buildings), whereas wide-area networks are composed of a number of adjacent buildings), whereas wide-area networks are composed of a number of adjacent buildings.
inconsistencies (for example, if the log file shrinks). These ACK messages are common throughout networking. More frequently, one or more 12.5 Disk Management 465 sectors become defective. If the stack inspection exhausts the stack without finding either type of frame, then whether access is allowed depends on the implementation (for example,
some implementations of the JVM may allow access, other implementations may disallow it). The creating process is called a parent process, and the new processes are called the children of that process, and the new processes are called the children of that process. The mechanism notifies the security administrator a a led to receive the new process. The mechanism notifies the security administrator a led to receive the new process.
computer system consists of CPUs and multiple device controllers that are connected through a common bus. This kind of statement can be integrated into a language by an extension of its typing facility. know we can trust the certifier? Assume that demand paging is used. To illustrate, we let R = {R\, Ri, ..., Rm} be the set of resource types. In
addition, the system periodically performs checkpoints that require the following sequence of actions to take place: 1. Of these four levels, Linux only recognizes two: user mode and kernel mode. If so, we preempt the desired resources from the waiting process and allocate them to the requesting process. The varying level of sharing is possible
because of the way a task is represented in the Linux kernel. We are concerned here not with the link's physical implementation. In fact, Linux generally uses the term task—rather than process or thread—when referring to
a flow of control within a program. Win32 provides the WaitForSingleObjectO function, whereas Pthread join() and join() a
and unseal operations takes a procedural approach to specifying protection. See also mass-storage structure allocation, 421-429 contiquous allocation, 421-429 contiquous allocation, 421-429 indexed allocation, 421-429 contiquous allocation, 421-429
452-453 formatting, 462-463 free-space management for, 429^31 host-attached, 455 low-level formatted, 454 » magneto-optic, 479 removable, 478-480 scheduling algorithms, 456^62 C-SCAN, 460 FCFS, 457-458 formatting, 462-463 free-space management for, 429^31 host-attached, 455 low-level formatted, 454 » magneto-optic, 479 removable, 478-480 scheduling algorithms, 456^62 C-SCAN, 460 FCFS, 457-458 formatting, 462-463 free-space management for, 429^31 host-attached, 455 low-level formatted, 454 » magneto-optic, 479 removable, 478-480 scheduling algorithms, 456^62 C-SCAN, 460 FCFS, 457-458 formatting, 462-463 free-space management for, 429^31 host-attached, 455 low-level formatted, 454 » magneto-optic, 479 removable, 478-480 scheduling algorithms, 456^62 C-SCAN, 460 FCFS, 457-458 formatting, 462-463 free-space management for, 429^31 host-attached, 455 low-level formatted, 455 low-level formatted, 455 low-level formatted, 455 low-level formatted, 456 formatted, 455 low-level formatted, 455 low-level formatted, 456 formatted, 456 formatted, 456 formatted, 457 low-level formatted, 457 low-level formatted, 458 low-
458 LOOK, 460^61 SCAN, 459-460 selecting, 461-462 SSTF, 458-459 solid-state, 24 storage-area network, 456 structure of, 454 system, 464 WORM, 479 disk scheduling: CineBlitz, 728 in multimedia systems, 723-724 disk striping, 818 dispatched process, 87 dispatcher, 157
dispatcher objects, 220 Windows XP, 790 in Windows XP, 793 dispatch latency, 157, 703 distributed coordination: and atomicity, 669-672 and concurrency control, 672-676 and deadlocks, 676-683 prevention/avoidance, 676
algorithms for, 686-688 distributed denial-of-service (DDOS) attacks, 560 Index distributed file system (DFS), 398 stateless, 401 Windows XP, 827 distributed file systems (DFSs), 641-642 AFS example of, 653-659 file operations, 657-658 implementation, 658-659 shared name space, 656—657 defined, 641 naming in, 643-646 remote file access in,
646-651 basic scheme for, 647 and cache location, 647-648 and cache-update policy, 648, 649 and 648, 
multiprogramming by running twice as many processes. If no message is waiting to be received, the receiving thread can either wait at most n milliseconds or not wait at all. 328 Chapter 9 Virtual Memory valid—invalid bit frame \M\ physical memory i 2 v 7
logical memory for user 2 V page table for user 2 V page table for user 2 Figure 9.9 Need for page replacement. database. Hardware protection features are needed to support an overall protection scheme. Since it was used heavily, it has a large count and remains in memory even though it is no longer needed. To detect deadlocks, the system needs to maintain the wait-for
graph and periodically invoke an algorithm that searches for a cycle in the graph. For example, a web server produces (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that is, provides) HTML files and images, which are consumed (that 
telnet server listens to port 23, an ftp server listens to port 21, and a web, or http, server listens to port 80). We also use the parent's existing environment block and starting directory. It could terminate the user process. Connections between networks frequently use a telephone-system service called Tl, which provides a transfer rate of 1.544
megabits per second over a leased line. The text also provides several example programs written in C and Java. Suggest how the implementation described in Section 6.7 can be simplified. [1995] presented several algorithms for dynamic memory allocation. Memory space, CPU cycles, files, and I/O devices (such as printers and DVD drives) are
examples 245 246 Chapter 7 Deadlocks of resource types. When a page fault occurs, a victim frame is chosen as before. 9.1 Background The memory-management algorithms outlined in Chapter 8 are necessary because of one basic requirement: The instructions being executed must be in physical memory. The segment table is thus essentially an
array of base-limit register pairs. o If TS(TJ) > W-timestamp(Q) and TS(T,). If all capabilities are secure, the object they protect is also secure against unauthorized access. A parent may terminate the execution of one of its children for a variety of
reasons, such as these: • The child has exceeded its usage of some of the resources that it has been allocated. WTe evaluate an algorithm by running it on a particular string of memory references and computing the number of page faults. In addition to the most common network firewalls, there are other, newer kinds of firewalls, each with its pros
and cons. The means for enforcement need not be provided by the designer of a subsystem. Software may trigger an interrupt by executing a special operation called a monitor call). You can also sort their books by collection or series. [1994], Bershad et al. It also allows processes to be run even though their memory
```

```
requirements exceed the total available physical memory Such processes run in virtual memory. When the operating system sets the instruction pointer to the first 322 Chapter 9 Virtual Memory instruction of the process, which is on a non-memory-resident page, the process immediately faults for the page. • Stack. A process requests resources; and
if the resources are not available at that time, the process enters a waiting state. As messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free, we find one that is not currently being used and free it. 3. The messages are copied into the mailbox. If no frame is free it. 3. The messages are copied into the 
hard error, however, results in lost data. This buffer will reside in a region of memory that is shared by the producer and consumer processes. The base and limit information about the segment in question is used to generate a linear address. Consider the man-in-the-middle attack shown in Figure 15.9. Here, the person who wants to receive an
encrypted message sends out his public key, but an attacker also sends her "bad" public key (which matches her private key). Of course, this provision could result in multiple receivers for each mailbox. There are three primary reasons. One way to ensure that this condition never holds is to impose a total ordering of all resource types and to require
that each process requests resources in an increasing order of enumeration. The consumer will also sleep for a random period of time and, upon awakening, will attempt to remove an item from the buffer. To alleviate this problem, we use a hash table, as described in Section 8.5.2, to limit the search to one—or at most a few—page-table entries. As
mentioned earlier, volatile storage loses its contents when the power to the device is removed. Once the correct information has been received, the process acts as a proxy for the user, who can compute on the remote machine just as any local user can. Racsit Eskicioglu, Hans Flack, Robert Fowler, G. (Generation of these timestamps is discussed in
Section 18.1.) For "exactly once," we need to remove the risk that the server never receives the request. The page-switch time, however, will probably be close to 8 milliseconds. They all behave like FCFS scheduling. This program is
in the form of read-only memory (ROM), because the RAM is in an unknown state at system and network threats involve the abuse of services and network connections. Alternatively, we can require that, whenever a process requests an instance of
resource type R,, it has released any resources R. • I s or d i r: List files in the current directory on the remote machine. The list is initialized during the low-level formatting at the factory and is updated over the life of the disk. Part Six Distributed A distributed system is a collection of processors that do not share memory or a clock. The message-
passing method allows the processes to exchange messages. The algorithm employs several time-varying data structures that are similar to those used in the banker's algorithm (Section 7.5.3): » Available. To illustrate this facility, lets suppose that a user at Westminster College wishes to compute on "cs.yale.edu," a computer that is located at Yale
University. A port is simply a number included at the start of a message packet. If a remote process needs a service, it addresses a message to the proper port. Which algorithm makes the most efficient use of memory? kernel. Connectionless (UDP) sockets use the DatagramSocket class. • Flexibility. To understand more fully the operating system's
role, we next explore operating systems from two viewpoints: that of the user and that of the system. A distributed secure system is described by Rushby and Randell [1983]. For 4-KB pages, the Pentium uses a two-level paging scheme in which the division of the 32-bit linear address is as follows: page number 10 10 page offset 12 The address-
translation scheme for this architecture is similar to the scheme shown in Figure 8.15. Once the region of shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! to shared memory is attached, the process writes the message Hi There! The message Hi There! The message Hi There! The message Hi There! The message Hi There!
devices. CPU user process I/O interrupt process I/O interrupt process doing output. Ultimately, we can end up with the original 256-KB segment. Another enhancement concerns distinguishing pages that have been allocated to processes
from pages allocated to regular files. A signal may be received either synchronously, depending on the source of and the reason for the event being signaled. Find the location of the desired page on the disk. Sobig.F was launched by being uploaded to a pornography newsgroup via an account created with a stolen credit card. 4.10
Modify the socket-based date server (Figure 3.19) in Chapter 3 so that the server services each client request in a separate thread. The table is usually large and thus cannot be kept in main memory, so additional I/O is needed. When a server receives a request, it awakens a thread from this pool—if one is available—and passes it the request to
service. As a result, the kernel must use memory conservatively and attempt to minimize waste due to fragmentation. The operating system may take 35 KB, leaving 93 frames for the user process. A simple viewpoint is that it includes everything a vendor ships when you order "the operating system." The features included, however, vary greatly
across systems. We will call this the helloioorld system call. As a worst-case example, consider a three-address instruction such as ADD the content of A to B, placing the result in C. A collection of algorithms for mutual exclusion was given by Raynal [1986]. ROM is convenient because it needs no initialization and cannot be infected by a computer
virus. These systems include Linux, Windows Preface XP, FreeBSD, Mach, and Windows 2000. If we have 93 free frames and two processes, how many frames does each process get? Both these protocols have two main disadvantages. If a process requests an instance of a resource type, the allocation of any instance of the type will satisfy the request
When an access right to an object is revoked, does it affect all the users who have an access rights should be revoked? After this connection has been established, the networking software creates a transparent, bidirectional link so that all characters entered by the user are
sent to a process on "cs.yale.edu" and all the output from that process is sent back to the user. Explain. Four times per second, the kernel checks whether the amount of free memory is less than lotsfree. Extensibility of system code through language-based protection mechanisms was discussed in Bershad et al. 8.14 Consider the hierarchical paging
scheme used by the VAX architecture. Exercises 6.27 235 Assume that a finite number of resources of a single resource type, must be managed. Where is cryptographic protection best placed in a protocol stack? A computer system, the application programs, and the
users (Figure 1.1). Let Oj and Oj be consecutive operations of a schedule S. However, we have shown only that the basic mechanism 542 Chapter 14.7 Modified access matrix of Figure 14.4. is here; system designers and users must make the policy decisions concerning which domains are to have access to which objects in which
ways. As with capability lists, the list of keys for a domain must be managed by the operating system on behalf of the domain. The procedure of starting a computer by loading the kernel is known as booting the system. To what uses can such an encryption be put? The process must then again request the disk file and the printer. A C2-class system
adds an individual-level access control to the requirements of a Cl system. To improve both the utilization of the CPU and the speed of its response to its users, the computer must keep several processes in memory used to construct
the TLB is both expensive and power hungry. Over-allocation of memory manifests itself as follows. At intervals determined by the operating system, usually dictated by CPU-scheduling policies, processes are copied from main memory to a backing store and laterare copied back to main memory. If the resources are neither available nor held by a
waiting process, the requesting process must wait. A virus of this type is able to infect multiple parts of a system, including boot sectors, memory, and files. Such functions include file transfer, login, mail, and remote procedure calls (RPCs). With slab allocation, no memory is wasted due to fragmentation, and memory requests can be satisfied quickly
We can implement this restriction readily by passing an access right that does not have the modification (write) right. An Ethernet scheme is commonly vised to construct LANs. An Ethernet network has no central controller, because it is a multiaccess bus, so new hosts can be added easily to the network. The output of the generator 580 Chapter 15
Security when fed a key is a keystream. Why should it or should it not? In both cases, a callback mechanism can be used when either the client or the server cannot respond immediately to a request. But consider what happens if the parameter provided on the 566 Chapter 15 Security #include #define BUFFER^SIZE 256 int main(int argc, char
 *argv[]) { char buffer [BUFFER SIZE]; if (argc < 2) return -1; else { strcpy(buffer, argv[1]); return 0; Figure 15.2 C program with buffer-overflow condition. Thus, if TS(T,) < TS(T,), then the system must ensure that the produced schedule in which transaction T, appears before transaction T, appears bet
involves packaging the parameters into a form that can be transmitted over 112 Chapter 3 Processes a network. • To examine the uses of cryptography in computing. What is the significance of the above structure on the following schemes? On the other hand, it could contain a heavily used variable that was initialized early and is in constant use.
Stack inspection is illustrated in Figure 14.9. Here, the gui() method of a class in the tmtrusted applet protection domain performs two operations, first a get O and then an open(). 2.8 Virtual Machines THE .NET FRAMEWORK The .MET Framework is a collection of technologies, including a set of class libraries, and an execution environment that
come together to provide a platform for developing software. Copy-on-write is illustrated in Figures 9.7 and Figure 9.8, which show the contents of the physical memory before and after process 1 modifies page C. Even if a system does not provide a protection kernel as powerful as those of Hydra or CAP, mechanisms are still available for
implementing protection specifications given in a programming language. This use can increase the strain on memory-placement algorithms. 2.10 System Boot 71 The major differences among these approaches are the size and generality of the generated system and the ease of modification as the hardware configuration changes. Allocation can be
fixed, suggesting local page replacement, or dynamic, suggesting global replacement. What is the effective memory access time? The primary programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows systems is the Win32 API (application programming environment for Windows environment for
peripheral devices. S. For example, consider a process whose function is to display the contents of a file—say, img.jpg—on the screen of a Figure 3.9 A tree of processes on a typical Solaris system. Thus, it avoids reading into memory pages that will not be used anyway, decreasing the swap rime and the amount of physical memory needed. The RPC
system hides the details that allow communication to take place by providing a stub on the client side. They search boot sectors, memory, inbound and outbound e-mail, files as they are downloaded, files on removable devices or media, and so on. Of course, the code segment could do anything allowed by the privileges of the attacked process.
Assuming independence 358 Chapter 9 Virtual Memory of process size and page size, we can expect that, on the average, half of the final page of each process will be wasted. Companies get a bigger bang for the buck (that is, better functionality for the cost), more flexibility in locating resources and expanding facilities, better user interfaces, and
 easier maintenance. Reading it is a good starting point for understanding security concerns. • To provide coverage of basic computer system organization. The Mach operating system is discussed in an extra chapter posted on our website. It is also used in communications between web browsers and web servers, as we discuss below. For instance, a
viser on a Windows machine who telnets to a UNIX machine must switch to UNIX commands for the duration of the telnet session. This .mapping is effected by a segment table. 110 Chapter 3 Processes the server. Any oversight can result in a total lack of protection on the system. Allowing every seventh duplicate to proceed (possibly to confound
efforts to stop its spread by baiting with fake worms) created a wholesale infestation of Sun and VAX systems on the Internet. Yet the program contained no code aimed at damaging or destroying the systems on which it ran. The procedure executes appropriately and then returns the results to P. Access rights to the file and accounting information
can also be included. A stub is a proxy for the remote object; it resides with the client. Sooner or later, it starts the operations yestem. We can demonstrate this fact by assuming that a circular wait () and signal () semaphore operations
This packaging is a variant of the bin-packing problem of operations research: Try to pack the variable-sized load segments into the fixed-sized pages so that interpage references are minimized. The queues length is potentially infinite; thus, any number of messages can wait in it. On these systems, processes can communicate using shared memory by
having the communicating processes memory-map the same file into their virtual address spaces. (You will read more about the ISO model of networking in Chapter 16; Figure 16.6 shows a diagram of the model.) Cryptography can be inserted at almost any layer in the ISO model. Just as in computation migration, if the data being used in the
computation are numerous, it may be more efficient to have a process run remotely than to transfer all the data. Rather, a separate swap-space storage manager is used to allocate and deallocate the blocks from the raw partition. i; : ; : . We must allow the contents of a domain to be modified so that it always reflects the minimum necessary access
rights. 3.6.2 Remote Procedure Calls One of the most common forms of remote service is the RPC paradigm, which we discussed briefly in Section 3.5.2. The RPC was designed as a way to abstract the procedure-call mechanism for use between systems with network connections. A barbershop consists of a waiting room with n chairs and a barber
room with one barber chair. With a programming language, protection policy can be declared and enforcement provided as needed by an implementation. Begin the transfer of the page to a free frame. See also virtual memory logical records, 383 logical units, 455 login, network, 399 long-term scheduler (job scheduler), 88 LOOK scheduling
algorithm, 460-461 loopback, 111 lossless compression, 718 lossy com
system, 61, 105-106, 851-853 Macintosh operating system, 381-382 macro viruses, 569 magic number (files), 381 magnetic disk(s), 9, 451-453. This is also illustrated in Figure 3.11. We schedule a disk operation to read the desired page into the newly allocated frame. • For all transactions Tj- in T that have no < Ti- commits> record in the log,
execute undo(TO6.9.4 Concurrent Atomic Transactions We have been considering an environment in which only one transaction can be executing at a time. The default LDT segment is normally shared by all processes and is usually not used. In Linux systems, a process descriptor is of the type s t r u c t t a s k ^ s t r u c t , which requires
approximately 1.7 KB of memory. Network. For code examples, we use predominantly C, with some Java, but the reader can still understand the algorithms without a thorough knowledge of these languages. The operation allows clients to request the current date and time from import java.net.*; import java.net.*; import java.net.*; import java.net.*
provide an algorithm that examines the state of the system to determine whether a deadlock has occurred and an algorithm to recover from the deadlock has indeed occurred). The question is simply whether the cost of servicing the corresponding page faults. Some asynchronous signals—such as
a signal that terminates a process (, for example)—should be sent to all threads. Values greater than 0 indicate that the page slot is occupied by a swapped page. Since bare hardware alone is not particularly easy to use, application programs are Chapter 1 Introduction developed. If the degree of multiprogramming is increased even further, thrashing
sets in, and CPU utilization drops sharply. For a computer system to begin running, the CPU must initialize and start executing the bootstrap program in firmware. We can free a frame by writing its contents to swap space and changing the page table (and all other tables) to indicate that the page is no longer in memory (Figure 9.10). Wear, John
Werth, James M. The first is to add the system call to an existing source file in this directory. Further, it frees application programmers from worrying about memory availability. We also see a csh process with pid of 7778 representing a user who has logged onto the system using tell net. Under this method, messages of up to 256 bytes can be sent
Thus, the user can access only those files that have been opened. For example, an attacker might modify the system programs into directories commonly found in user-shell search paths, Or an intruder might remove system log'files to cover his tracks. 2.17 The experimental
Synthesis operating system has an assembler incorporated in the kernel. When a user presses the stop button on the browser, all threads loading the page are canceled. Bershad and Pinkerton [1988] present the watchdog extension to BSD UNIX. 9.4.5.2 Second-Chance Algorithm The basic algorithm of second-chance replacement is a FIFO
replacement algorithm. Rather, there is a set of factors that support various sizes. Write a monitor that allocation. Antivirus programs are often used to provide this protection. Another approach to designing this program is to establish a
shared-memory segment between the parent and child processes. More typically, suspicious events are logged. First, resource utilization may be allocated but unused for a long period. The semantics of RPCs allow a client to invoke a procedure on a remote host as it would invoke a procedure locally. This leads to the
following benefits: • System libraries can be shared by several processes through mapping of the shared object into a virtual address space. Each title gives a suggested grade level range. Another important issue concerns the communication between a server and a client. contiguous-memory allocation b. Obviously, this switch must be done in address space.
controlled manner; otherwise, a process could start executing in ring 0, and no protection would be provided. One solution is never to execute I/O to user memory, and thrown away if selected for pageout. These processors are
referred to by a number of names, such as sites, nodes, computers, machines, and hosts, depending on the context in which they are mentioned. In this exercise, the parent and child finishes generating the sequence. [1961]). For example,
segment 2 is 400 bytes long and begins at location 4300. Telnet requires a smaller shift: The user must know appropriate commands on the remote system. A rogue computer can send a message with a falsified source address, and numerous computers other than the one specified by the destination address can (and typically do) receive a packet
Some special, secure versions of UNIX have been certified at the C2 level. Like optimal replacement, LRL replacement does not suffer from Belady's anomaly. 114 Chapter 3 Processes 3.6.3 Remote method invocation •• Remote method invocation (RMI) is a Java feature similar to RPCs. RMI allows a thread to invoke a method on a remote object.
Users would be able to write programs for an extremely large virtual address space, simplifying the programming task. These programs are intended to run in the following programming environments: • Windows systems. Ten megabit:
per second is most common and is the speed of lOBaseT Ethernet. Write a monitor to coordinate access to the file. However, a problem with this approach, is that we may not initially need the entire program. The system can therefore gair
better paging throughput by copying an entire file image into the swap space at process startup and then performing demand paging from the swap space. Both E and E(k) for any k should be efficiently computable functions. • Denial of service. The scheme requires that these processes share a region of memory and that the code for accessing and
manipulating the shared memory be written explicitly by the application programmer. (We must use the write () function for performing output rather than the more common printf() as the former is known as being 124 Chapter 3 Processes #include #in
function */ void handle SIGINT () write (STDOUT FILENO, buffer, s t r l e n (buf f er)); exit (0); int mainfint argc, char *argv[]) /* set up the signal handler */ struct sigaction handler; handler. The figure shows two kernel objects 3 KB in size and three objects 7 KB in size. Messages sent by a process can be of either fixed or variable size. The
program stored in the boot block may be sophisticated enough to load the entire operating system into memory and begin its execution. This restriction prevents any process from accessing a resource outside of its protection environment at any time. If / > bl, then the call is allowed to occur only if b3 is greater than or equal to / and the call has been
directed to one of the designated entry points in the list of gates. This activity comprises the following tasks, some of which are dependent on the particular installation of the Linux operating system. Actually, since each entry in the access matrix as an object to be
protected. A variation of the Trojan horse is a program that emulates a login program. Servicing a request with an existing thread is usually faster than waiting to create a thread. Chapter 11, File-System Implementation, is the old Chapter 12. 622 Chapter 16 Distributed System Structures If a communication link fails, messages that would have been
 transmitted across the link must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted. It can use a variable key length of up to 256 bits and works on 128-bit blocks. Because directories, like files, must be rerouted as a variable key length of up to 256 bits and up to 256 bits an
static access enforcement can be verified off-line at compile time. An analysis of an optimal thread-pool size can be found in Ling et al. A mailbox may be owned either by a process or by the operating system. This account crediting can add up to a large amount of money, considering the number of transactions that a large bank executes. Up
the, chain, the user-level thread attached to the LWP also blocks. Enforcement by a kernel provides a greater degree of security of the protection systems are now
concerned not only with the identity of a resource to which access is attempted but also with the functions, such as standard file-access methods, to include functions that may be user-defined as well
Pthreads, the threads extension of the POSIX standard, may be 132 Chapter 4 Threads - user thread figure 4.5 Two-level model. [1969] were the first researchers to observe that the FIFO replacement strategy may produce the anomaly that bears Belady's name. As it advances, it clears the reference bits (Figure 9.17). Spafford [1989]
presents a detailed technical discussion of the Internet worm. Here, we look more closely at the latter requirement. Other web sites containing up-to-date security information include and httpd://www.eeye.com. [1970]. The operating system has several options at this point. We have five segments numbered from 0 through 4. The reason for this
selection is that an actively used page should have a large reference count. The mechanism consists of implementing the access matrix and ensuring that the semantic properties we have outlined indeed, hold. If all processes are CPU bound, the I/O waiting queue will almost always be empty, devices will go unused, and again the system will be
unbalanced. When a process is executing 14.3 Domain of Protection S37 ring 1 ring N- 1 Figure 14.2 MULTICS ring structure. When the message can be put in the mailbox, a message is sent back to the sender; only one such message to a full mailbox can be pending at any time for a given sending thread. If a single process can be divided into a
number of subprocesses that can run concurrently on different sites, then the total process turnaround time can be reduced. Depending on the disk and controller in use, these blocks are handled in a variety of ways. Propagation of the copy right may be limited. Universal trust is not placed in any code other than the CAP machine's microcode. This process turnaround time can be reduced.
employed when the thread is running in kernel mode • A private storage area used by various run-time libraries (DLLs) The register set, stacks, and private storage area are known as the context of the thread. For example, a 33-KB request can only be satisfied with a 64KB segment. The client executes the statement boolean
      = server.someMethod(A, B); The call to someMethod() with the parameters A and B invokes the stub for the remote object. If protection interferes with the ease of use of the system or significantly decreases system performance, then its use must be weighed carefully against the purpose of the system. File viruses are sometimes known as
parasitic viruses, as they leave no full files behind and leave the host program still functional. Consider as an example the RSA digital-signature algorithm. Although this scheme decreases the amount of memory needed to store each page table, it increases the amount of time needed to search the table when a page reference occurs. Bibliographical
Notes Interprocess communication in the RC 4000 system was discussed by BrinchHansen [1970]. Exercises 2.1 The program shown in Figure 4.11 uses the Pthreads API. Nonrepudiation assures that a person filling out an electronic form cannot
Structures A distributed system is a collection of processors that do not share memory or a clock. Because the inverted page table is sorted by physical address, but lookups occur on virtual addresses, the whole table might need to be searched for a match. A default signal handler 2. Such attacks, which can last hours or days, have caused partial or
full failure of attempts to use the target facility. These attacks are usually stopped at the network level until the operating system ;:-•:'- communication processor Figure 16.3 Communication processors in a wide-area network. The
primary distinction between RPCs and RMI is that in RPCs data are passed to a remote procedure in the form of an ordinary data structure, whereas RMI allows objects to be passed in remote method calls. Second, starvation is possible. Their operating systems are designed mostly for individual usability, but performance per amount of battery life is
important as well. We now turn to the case where multiple transactions are active simultaneously. Java's RMI systems work similarly. An encrypted virus includes decryption code along with the encrypted virus, again to avoid detection. Associated with this list of free pages is a parameter—that represents a threshold to begin paging. What
does the system degenerate to if the number of resident pages is set to one? Both D and D(k) for any k should be efficiently computable functions. 312 Chapter 8 8.12 Main Memory Consider the following segment table: Segment 0 1 2 3 4 Base Length 219 600 14 100 580 96 2300 90 1327 1952 What are the physical addresses for the following logical
 addresses? Each serial schedule is correct, because it is equivalent to the atomic execution of the various participating transactions in some arbitrary order. As instructions are requested by the executing program, the CLR converts the MS-IL instructions inside the assemblies into native code that is specific to the underlying arcliitecture using just-in-
time compilation. If the diagnostics pass, the program can continue with the booting steps. The mechanisms commonly used to prevent such attacks are discussed in Cheswick et al. 14.13 How does the principle of least privilege aid in the creation of protection systems? file. For instance, Solaris allows locking "hints," but it is free to disregard these
hints if the free-frame pool becomes too small or if an individual process requests that too many pages be locked in memory. We have removed the coverage of two-process solution, as the two-process solution, as the two-process solution, as the two-process solution and now discuss only Peterson's solution, as the two-process solution and now discuss only Peterson's solution, as the two-process solution and now discuss only Peterson's solution.
thread that will generate the Fibonacci numbers, placing the sequence in data that is shared by the threads (an array is probably the most convenient data structure). A programmer, for example, might write code to detect if she is still employed; if that check failed, a daemon could be spawned to allow remote access, or code could be launched to
cause damage to the site. The capabilities point indirectly, not directly, to the objects. [2000]. The code example below creates a binary semaphore mutex with an initial value of 1 and illustrates its use in protecting a critical section: #include < semaphore mutex with an initial value of 1 and illustrates its use in protecting a critical section: #include < semaphore mutex with an initial value of 1 and illustrates its use in protecting a critical section: #include < semaphore mutex with an initial value of 1 and illustrates its use in protecting a critical section.
some combination of the two. [1961]. If the operating system is buffering I/O, and the application is doing so as well, then twice the memory is being used for a 'JVVI running on such a system maps to a kernel thread. Personal
computer (PC) operating systems support complex games, business applications, and everything in between. Service the page-fault interrupt. Rather, we present the major ideas on which it is based. Thus, this program suffers from a potential buffer-overflow problem in which copied data overflow the buffer array. The process releases the resource
598 Chapter 15 Security Both viruses and antivirus software continue to become more sophisticated. The system with the best performance will thus have a combination of CPU-bound and I/O-bound processes. We conclude with Windows XP, which interestingly uses shared memory as a mechanism for providing certain types of message passing. 2.8
What are the two models of interprocess communication? This causes intruders to become more sophisticated in their attacks. Periodically, capabilities are deleted from each domain. Access to system objects can then be permitted or denied as desired. In this scheme, process P may execute concurrently with process Q and, in fact, may have several
processes running concurrently on several sites. The target thread periodically checks whether it should terminate, allowing it an opportunity to terminate itself in an orderly fashion. We can implement can increase the degree of multiprogramming
(allowing more processes to be available for execution at one time) and—in theory, at least—the CPU utilization of the system. 4.4.6 Scheduler Activations A final issue to be considered with multithreaded programs concerns communication between the kernel and the thread library, which may be required by the many-to-many and two-level models
discussed in Section 4.2.3. Such coordination allows the number of kernel threads to be dynamically adjusted to help ensure the best performance. Resource sharing. To generate a system, we use a special program. The skeleton on the server unmarshals the parameters and invokes the method someMethod(). 148 Chapter 4 Threads #include
#include (int value = 0; void *runner(void *param); /* the thread */ int main (int argc, char *argv[]) { int pid; pthread attr init (&attr); pthread attr init (&attr); pthread attr init (attr); pthrea
0) {/* parent process */ wait(NULL); printf("PARENT: value = %d",value); /+ LINE P */ void *runner(void *param) value = 5; pthread exit (0); Figure 4.11 C program for question 4.7. 4.11 The Fibonacci sequence is the series of numbers 0,1,1,2,3,5, Formally, it can be expressed as: fih = 0 fib, = 1 fib,, = fib,, -2 Write a multithreaded program
that generates the Fibonacci series using either the Java, Pthreads, or Win32 thread library. The TEB is a user-space data structure that is accessed when the standard UNIX function for delivering a signal is kill (aid to
a i d, intsignal); here, we specify the process (aid) to which a particular signal is to be delivered. If not, the process will spend a considerable amount of time resolving memory references in the page table rather than the TLB. Many old designs simply stored the interrupt address in a fixed location or in a location indexed by the device number.
If we fault when we try to store in C (because C is in a page not currently in memory), we will have to get the desired page, bring it in, correct the page table, and restart the instruction. c l a s s file is valid Java bytecode and does not overflow or underflow the stack. We turn now to a deadlockdetection algorithm that is applicable to such a system.
This scheme was adopted in the MULTICS system. An authorized user of the system may also use this exploit for privilege escalation. Any vulnerable Microsoft Explorer web browser virus with any download. Here, we discuss some examples of these threats, including worms, port scanning, and denial-of-service
attacks. 366 Chapter 9 Virtual Memory In addition to a page-replacement algorithm, a frame-allocation policy is needed. The buffer will also require an initialization function that initializes the mutual exclusion object mutex along with the empty and full semaphores. [1996], respectively. Johnstone and Wilson [1998] described various memory-
fragmentation issues. In summary, several pieces of information are associated with an open file. Java provides three different types of sockets. The heap, from which memory is allocated 4. For any particular list of requests, we can define an optimal order of retrieval, but the computation needed to find an optimal schedule may not justify the savings and the computation are associated with an open file.
over SSTF or SCAN. The process on the remote machine asks the user for a login name and a password. Patil [1971] examined the question of whether semaphores can solve all possible synchronization problems. • Armored. In place of proofs, figures and examples are used to suggest why we should expect the result in question to be true. A problem
with firmware in general is that executing code in RAM. In a ring network, at least two links must fail for partition, however, we may want to give the high-priority process more memory to speed its execution, to the detriment of low-priority processes. Although only 1 bit is necessary to
distinguish between capabilities and other objects, more bits are often used. M'.-... o'to -: o; ;; o o; ;; o of the ECC is updated with a value calculated from all the
bytes in the data area. In Figure 4.6, this is the runner () function. Some firewalls are designed for one specific protocol. Inherent in this concept is the idea that certain program components might have the privilege of creating or examining these software capabilities. The solution presented in Section 6.6.1 uses three semaphores: empty and full,
which count the number of empty and full slots in the buffer, and mutex, which is a binary (or mutual exclusion) semaphore that protects the actual insertion or removal of items in the buffer. A typical instruction from memory and stores that
instruction in the instruction register. We now have two different processes running a copy of the same program. To execute operation M on object O/ as a parameter. Again, we can control these changes by including the access matrix itself as an object. For
example, a controller for a USB storage device is generally given the number of bytes to transfer and a memory address for the buffer (Figure 9.29). • Shrinking phase. But this condition means that F(R()) < F(R^) < ••• < F(R,) < F(R). If the operating system allocates fewer than 128 frames to the entire program, then its execution will result in 128 frames.
x 128 = 16,384 page faults. What information needs to be passed from the compiler to the linkage editor? As prerequisites, we assume that the reader is familiar with basic data structures, computer organization, and a high-level language, such as C. This scheme exhibits symmetry in
addressing; that is, both the sender process and the receiver process and the receiver process are used to infer the potential senders and receivers of
network messages. static, 281-282, 764 Linux, 737-780 adding system call to Linux kernel (project), 74-78 design principles for, 742-744 file systems, 764-770 ext2fs, 766-768 journaling, 768-769 process, 769-770 virtual, 765-766 history of, 737-742 distributions, 740-741 first kernel, 738-740 licensing, 741-742 system description, 740 interprocess
communication, 773-774 I/O system, 770-773 block devices, 771-772 character devices, 771-773 kernel modules, 745-748 memory, 756-759 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-759 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-759 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-759 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-765 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-765 virtual memory, 756-765 virtual memory, 756-765 virtual memory, 756-765 virtual memory, 756-766 virtual memory, 756-766 virtual memory, 756-766 virtual memory, 756-767 virtual memory, 756-768 virtual mem
and execO process model, 748-750 processes and threads, 750-751 process representation in, 86 real-time, 711 scheduling, 751-756 kernel synchronization, 753-756 scheduling example, 179-181 security model, 777-779 access control, 778-779 authentication, 777-779 access control, 778-779 access co
swap-space management in, 468 synchronization in, 221 threads example, 144-146 Linux distributions, 738, 740-741 Linux kernel, 738-740 Linux system, components of, 738, 743-744 lists, 316 Little's formula, 183 live streaming, 717 load balancers, 34 load balancing, 170-171 loader, 842 loading: dynamic, 280-281 in Linux, 762-764 load sharing
169, 612 load time, 278 local-area networks (LANs), 14, 28, 618-619 local descriptor table (LDT), 306 locality model, 344 locality of reference, 322 local name space, 655 local (nonremote) objects, 115 local playback, 716 local procedure calls (LPCs), 786, 804-805 local replacement, 342 local replacement algorithm (priority replacement algorithm)
344 location, file, 374 location independence, 643 location-independence, 643 location-transparency, 379 mutex, 201, 251-252 reader-writer, 207 shared, 378 locking protocols, 227-228, 672-675 '> lock-key scheme, 544 lockO operation, 377 log-based
transaction-oriented file systems, 437-438 log-file service, 817 logical clock, 665 logical address space, 279-280 logical formatting, 463 logical memory, 17, 317. Disk I/O to swap space is generally faster
than that to the file system. See also I/O systems device directory, 386. One entry in the page directory is the Page Size flag, which—if set—indicates that the size of the page frame is 4 MB and not the standard 4 KB. A programmer who is developing multithreaded applications must pay particular attention to this problem. The execO system call
typically works in the same way as described in Chapter 3. Domain switching occurs when one process sends a message to another process and then waits for a response. Much of the information for the command comes from the data structure s t r u c t shmicLds, which is available in the / u s r / i n c l u d e / s y s / s h m . So, for example, an attack
that modifies (without deleting) a system log that would normally change anyway would escape Tripwire's detection capabilities. Then the mean time to failure of some disk in an array of 100 disks 12.7 RAID Structure 469 |ptpgg § | | j ^ f Idi? Because the child process is a copy of the parent, the shared-memory region will be attached to the child's
address space as well. This latter mode is an example of a general category of attacks known as covert channels, in which surreptitious communication occurs. Logging can be general or specific. This restriction enables discrimination of access rights to be made on an instance-by-instance and process-by-process basis. It can also initialize all aspects
f[ag[turn] = idle) break; // critical section j = (turn + 1) \% n; while f[ag[j] = idle); // remainder section g[turn] 
types of locks are available inside and outside the kernel. For most users, the file system is the most visible aspect of an operating system. Even more difficult to prevent and resolve are distributed denial-of-service attacks (DDOS). If there is a cycle, then the system may or may not be in a deadlocked state. A more complete description of the swatch
program and its use with syslog can be found in Hansen and Atkins [1993]. Important theoretical results are covered, but formal proofs are omitted. Observe that process P4 may release its instance of resource type R?. If the application name is NULL (which in this case it is), the command line parameter specifies the application to load. In both
methods, data migration includes more than the mere transfer of data from one site to another. Dynamic loading can help to ease this restriction, but it generally requires special precautions and extra work by the programmer. When it is too high, we know that the process needs more frames. blocking system call. M syrjeKronizatitin!:: :;! : : 3,400 e
An assembler symbol table may have room for 3,000 symbols, although the average program has less than 200 symbols. Internally, operating systems vary greatly in their makeup, since they are organized along many different lines. Because an operating system is large and complex, it must be created piece by piece. We discuss how to allocate space
for the file in Chapter 11. When a system is split into two (or more) subsystems that lack any connection between them, it is partitioned. If a schedule S can be transformed into a serial schedule S can be transformed into a serial schedule S can be transformed into a serial schedule S. is conflict serializable. Each process may be in one of the following states: new,
ready, running, waiting, or terminated. Others who helped us with previous editions include Hamid Arabnia, Rida Bazzi, Randy Bentson, David Black, Joseph Boykin, Jeff Brumfield, Gael Buckley, Roy Campbell, P. A compiler is used to generate the object modules into
a single program binary. The CPU scheduler sees the decreasing CPU utilization and increases the decreasing CPU utilization and increases the decreasing the specified need, the fixed
overhead of kernel calls can often be avoided. An armored virus is coded to make itself hard for antivirus researchers to unravel and understand. We'll call these transactions set T. There is a single cache for each unique kernel data structure —for example, a separate cache for the data structure representing process descriptors, a separate cache for
file objects, a separate cache for semaphores, and so forth. Accordingly, each process should be allocated enough frames for its current working set. Some other page will need to be replaced to bring the active page back into memory. Do the following: a. Let's take Solaris as an example. Dijkstra [1965b] presented the first solution to the mutual-
exclusion problem for n processes. The messages themselves consist of a fixed-length header followed by a variable-length data portion. If it takes 10 milliseconds, then 10/(100 + 10) = 9 percent of the CPU is being used (wasted) simply for scheduling the work. A socket is defined as an endpoint for
communication. Is this approach equivalent to including the access privileges of domain A? There are many different page-replacement algorithms. A demand-paging system is similar to a paging system with swapping (Figure 9.4) where processes reside in secondary memory (usually a disk). An expansion of this idea is to
maintain a list of modified pages. Hydra provides mechanisms for directly dealing with this problem. If the barber is busy but chairs are available, which in turn points to the object. The return address of the overflowed routine can still be
modified; but when the return address is within the stack and the code there attempts to execute, an exception is generated, and the program is halted with an error. To associate each thread with its unique identifier, we could use thread-specific data. It is more efficient to reread a page from the file system than to write it to swap space and then
reread it from there. The device takes the data byte and then clears the bit in the control register to signal that it is ready for the next byte. A number of different concurrency-control algorithms ensure serializability. When a page is selected for replacement, its lock bit is turned on; it remains on until the faulting process is again dispatched. The
parent can then create more children; or, if it has nothing else to do while the child runs, it can issue a wait () system call to move itself off the ready queue until the termination of the child. If the performance declines to unacceptable levels on a multiuser system, some users will simply quit. [1970] demonstrated that stack algorithms are not subject
to Belady's anomaly. When we want to execute a process, we swap it into memory. Multithreading an interactive application may allow a program to continue running even if part of it is blocked or is performing a lengthy operation, thereby increasing responsiveness to the user. This protocol requires that each transaction issue lock and unlock
requests in two phases: • Growing phase. If they are, we allocate them. What is the minimum number of page faults for an optimal pagereplacement strategy for the reference string in part b with four page frames? Using the thread pool API is similar to creating a thread with the Thread Create() function, as described in Section 4.3.2. Here, a
function that is to run as a separate thread is defined. 9.21 Write a program that implements the FIFO and LRU page-replacement algorithms presented in this chapter. A technique that is potentially even faster is to run the JVM in hardware on a special Java chip that executes the Java bytecode operations as native code, thus bypassing the need for
 either a software interpreter or a just-in-time compiler. An amazing aspect of operating systems is how varied they are in accomplishing these tasks. It also has six 8-byte microprogram registers to hold the corresponding descriptors from either the LDT or GDT. Allocating memory and resources for process creation is costly. Another means of
increasing the multiprogramming level is to share code and data among different users. It's won several awards, including an Emmy, and it's been endorsed by the American Library Association. In general, a process will need certain resources (CPU time, memory, files, I/O devices) to accomplish its task. Yet the fundamental concepts remain fairly
clear, and it is on these that we base this book. Java provides support as well. Implement the replacement algorithms so that the number of page frames can vary from 1 to 7. Finally, when the failed site recovers or is repaired, mechanisms must be available to integrate it back into the system smoothly. Here, we first describe several methods of
implementing the access matrix and then compare the methods. (To determine whether this has occurred, the parent must have a mechanism to inspect the state of its children.) • The task assigned to the child is no longer required. 1.2.2 Storage Structure Computer programs must be in main memory (also called random-access memory or RAM) to
be executed. The client must resend each RPC call periodically until it receives the ACK for that call. Because, the system may be overly general. In other cases, a failure may mean that no connection exists between some pairs of sites. Users are not allowed to examine or modify
the list of keys (or locks) directly. Siblsographical SMotes Dynamic storage allocation was discussed by Knuth [1973] (Section 2.5), who found through simulation results that first fit is generally superior to best fit. The interpretation of user-defined rights is performed solely by the user's program, but the system provides access protection for the user
of these rights, as well as for the use of system-defined rights. There have been several successful denial-of-service attacks of this kind against major web sites. Once transaction Tj and all transactions Tj that started executing after transaction Tj-. • Temporary
versus permanent. DES works by taking a 64-bit value and a 56-bit key and performing a series of transformations. This representation is not strictlyaccurate, however. We illustrate various operating system and networking concepts with several Java programs tested using the Java 1.4 JVM. Ortiz [2001] described virtual memory used in a real-time
embedded operating system. The choice of programming language can affect paging as well. There is no such tool, but there are tools that perform subsets of that functionality. Thus, a page that is given a second chance will not be replaced until all other pages have been replaced (or given second chances). If the mailbox is not full, the message is
copied to the mailbox, and the sending thread continues. This default action can be overridden by a user-defined signal handler that is called to handle the signal. Cooperating processes require an interprocess communication (IPC) mechanism that will allow them to exchange data and information. Automated load sharing, in which the distributed
operating system automatically moves jobs, is not yet common in commercial systems. This identification is accomplished via a protected mechanism or password; the TCB protects the authentication data so that they are inaccessible to unauthorized users. A simple technique for addressing this issue is to allow the page table to contain only one
         ng of a virtual address to the shared physical address. • Contention, Recently, many varieties of handheld computers have come into fashion. The operating system controls and coordinates the use of the hardware among the various application programs for the various users. That is, a process executing in domain D, has more privileges than
does a process executing in domain D,\ A process executing in domain Do has the most privileges. unit it was allocated, the system can coalesce C-L and CR into a 64-KB segment. Because the sites in a WAN are physically distributed over a large geographical area, the communication links are, by default, relatively slow and unreliable. In sum, it is
important to keep the page-fault rate low in a demand-paging system. Only three system calls are needed for message transfer. Protection requirements can be stated independently of the facilities provided by a particular operating system. Install a faster CPU. Increase the page size. For pages of 128 words, each row takes one page. 1.2.1 Computer
System Operation A modern general-purpose computer system consists of one or more CPUs and a number of device controllers connected through a common bus that provides access to shared memory (Figure 1.2). A process executing in domain D4 has the same privileges as one executing in domain D4; but in addition, it can also write onto files F
and F?. It is known as the swap device, and the section of disk used for this purpose is known as swap space. processes may have opened a file, the system must wait for the last file to close before removing the open-file table entry. • Connection strategies. The working-set minimum is the minimum number of pages the
process is guaranteed to have in memory. Notice that the first 5 faults are the same as those for optimal replacement, Architecturally, a class-Al system, but it uses formal design specifications and verification techniques, granting a high degree of assurance that the TCB has been implemented correctly. If this
payload was executed, it stored a program called W1NPPR32.EXE in the default Windows directory, along with a text file. However, because of the demands placed on the memory system, a scanrate of several thousand is not uncommon. Capabilities, however, present a much more difficult revocation problem. The accuracy of the working set
depends on the selection of A. What is the effect of setting A to a small value on the page fault frequency and the number of active (non-suspended) processes currently executing in the system? conf, such as: image=/boot/bzImage. Security, in contrast, must consider both the
computer system and the environment—people, buildings, businesses, valuable objects, and threats—within which the system is used. Recall that, normally, the operating system tries to prevent one process from accessing another process's memory. • ':.; * . The U.S. government is, of course, concerned about security. Savage et al. The keys can be
passed freely from domain to domain to domain. Abstractly, cryptography is used to constrain the potential senders and/or receivers of a message. (We eliminate much of the error checking for code brevity.) The call to CreateFileMapping O creates a named shared-memory object calledSharedObject. Shareware implementations are available in the public
domain for the various Windows operating systems as well. For example, an intruder (or intrusion program) may install a daemon on a system that acts as a file server. The server waits for incoming client requests by listening to a specified port. A word processor may have a thread for displaying graphics, another thread 127 128 Chapter 4 Threadsen, another thread for displaying graphics.
code registers data files code data files code data files stack • thread threaded process Figure 4.1 Single-threaded proc
attempts to breach security. The checking cannot be implemented (efficiently) in software. • Protection. The problem of synchronization of independent processes was discussed by Lamport [1976]. Once shared memory is established, all accesses are treated as routine memory accesses, and no assistance from the kernel is required. We begin by
discussing the basic functions of system startup, I/O, and storage. • What operating-system options are desired, or what parameter values are to be used? SMB is described in Appendix C.6.1. Clearly, if only a small part of a large file is being accessed, the latter approach is preferable. The pageout algorithm uses several parameters to control the rate
at which pages are scanned (known as the scanrate). 318 Chapter 9 Virtual Memory space but will require actual physical pages only if the heap or stack grcfvvs. It generates reports about the results. The value of pid for the child process is zero; that for the parent is an integer value greater than zero. doPrivileged() is a static method in the
AccessController class that is passed a class with a run() method to invoke. Under the normal mode of operation, a process may utilize a resource in only the following sequence: 1. Another modification is to keep a pool of free frames but to remember which page was in each frame. To detach a region of shared memory, the process can pass the
pointer of the shared-memory region to the shared segment along with the flag IPCJRMID. • The client sends a connection request. An access right is
permission to perform an operation on an object. This memory can be as fast as DRAM but has a limited duration in which it is nonvolatile. Recall that the hit ratio for the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the percentage of virtual address translations that are resolved in the TLB refers to the translation translation translations that are res
requests can be satisfied quickly. These objects are stored in their respective caches. It reports this finding to the operating system. Barrera [1991] and Vahalia [1996] described interprocess communication in the Mach system. Barrera [1991] and Vahalia [1996] described interprocess communication in the Mach system.
interrupt, and be put back in the ready queue. First, for a given page size (and the page size is generally fixed by the hardware or system), we need to consider only the page number, rather than the entire address. One RPC might result in the invocation of another RPC or even in the transfer of messages to another site. This key is defined when the
capability is created, and it can be neither modified nor inspected by the process owning the capability. [2003]. 9.2 Demand Paging Consider how an executable program might be loaded from disk into memory. Under local replacement, the set of pages in memory for a process is affected by the paging behavior of only that
process. By setting up special files that list host-login name pairs, users can omit entering a password each time they access a remote account on the paired list. Assume that pages are 128 words in size. 6.23 Why do Solaris, Linux, and Windows 2000 use spinlocks as a synchronization mechanism only on multiprocessor systems and not on single-
processor systems? A pointer (that is, a hand on the clock) indicates which page is to be replaced next. Special-purpose systems. However, when a predefined set of parameters were met, the security hole would be created. For example, time-sharing systems such as UNIX and Microsoft Windows systems often have no long-term scheduler but simply
put every new process in memory for the short-term scheduler. bad blocks, 464-46 boot block, 463-464 formatting of disks, 462^163 disk scheduling algorithms, 456-462 C-SCAN, 460 FCFS, 457^158 LOOK, 460^161 SCAN, 459-460 selecting, 461-462 SSTF, 458^59 disk structure, 454 extensions, 476 magnetic disks, 451^453 magnetic tapes, 453-454 magnetic tapes, 453-454 magnetic disks, 462^163 disk scheduling algorithms, 456-462 C-SCAN, 460 FCFS, 457^158 LOOK, 460^161 SCAN, 459-460 selecting, 461-462 SSTF, 458^59 disk structure, 454 extensions, 476 magnetic disks, 451^453 magnetic tapes, 453-454 magnetic disks, 462^163 disk scheduling algorithms, 456-462 C-SCAN, 460 FCFS, 457^158 LOOK, 460^161 SCAN, 459-460 selecting, 461-462 SSTF, 458^59 disk structure, 454 extensions, 476 magnetic disks, 451^453 magnetic tapes, 453-454 magnetic disks, 451^453 ma
454 RAID structure, 468^77 performance improvement, 470 problems with, 477 RAID levels, 470-476 reliability improvement, 468-470 stable-storage implementation, 477-478 swap-space management, 460-468 tertiary-storage, 478-488 future technology for, 480 magnetic tapes, 480 and operating system support, 480-483 performance issues with,
484-488 removable disks, 478-480 master book record (MBR), 464 master file directory (MFD), 388 master file table, 414 master key, 547 master secret (SSL), 586 matchmakers, 112 matrix product, 149 MB (megabyte), 6 MBR (master book record), 464 MCP operating system, 853 mean time to data loss, 469 mean time to failure, 468 mean time to
repair, 469 mechanisms, 56-57 media players, 727 medium access control (MAC) address, 636 904 Index medium-term scheduler, 89 megabyte (MB), 6 memory access, 504 logical, 17, 317 main, see main memory over-allocation of, 327 physical, 17 secondary, 322
semiconductor, 10 shared, 96, 318 unified virtual memory, 433 virtual memory, 433 virtual memory, 756-764 execution and loading of user programs, 762-764 physical memory, 756-759 virtual memory, 759-762 in Windows XP, 834-836 heaps, 835-836 memory
mapping files, 835 thread-local storage, 836 virtual memory, 834-835 memory-mapped I/O, 353, 497 memory-mapped files, 798 memory-mapped files, 835 thread-local storage, 836 virtual memory, 834-835 memory-mapped files, 835 memory-mapped files, 835 memory-mapped files, 835 memory-mapped files, 835 memory-mapped files, 836 virtual memory, 834-835 memory-mapped files, 836 virtual memory-mapped files, 836 vir
memory protection, 285 memory-resident pages, 320 memory-style error-correcting organization, 471 MEMS (micro-electronic mechanical systems), 480 messages: connectionless, 626 in distributed operating systems, 613 messages: connectionless, 626 in distributed operating systems, 626 in distributed operati
message-passing model, 54, 99-102 message switching, 627 methods (Java), 553 metropolitan-area networks (MANs), 28 MFU page-replacement algorithm, 338 micro-electronic mechanical systems (MEMS), 480 microkernels, 61-64 Microsoft Interface Definition
Language, 825 Microsoft Windows, see under Windows,
philosophers solution using, 212-214 implementation of, using semaphores, 214-215 resumption of processes within, 215-217 usage of, 210-212 monitor calls, see system calls monoculture, 571 monotonic, 665 Morris, Robert, 572-574 most-frequently used (MFU) pagereplacement algorithm, 338 mounting, 417 mount points, 395, 821 mount protocol,
440-441 Index mount table, 417, 518 MPEG files, 719 MS-DOS, 811-812 multilevel index, 427 multilevel index, 427 multilevel index, 427 multilevel index, 427 multilevel feedback-queue scheduling algorithm, 168-169 multilevel index, 427 multilevel index, 428 multilev
data, 30, 716-717 multimedia systems, 30, 715 characteristics of, 717-718 CineBlitz example, 728-730 compression in, 725-728 multipartite viruses, 571 multipartite viruses, 571 multiple-coordinator approach (concurrency control), 673
multiple-partition method, 286 multiple universal-naming-convention provider (MUP), 826 multiprocessor scheduling, 169-172 approaches to, 169-170 examples of: Linux, 179-181 Solaris, 173, 175-177 Windows XP, 178-179 and load balancing, 170-171 and processor affinity, 170 symmetric
multithreading, 171-172 multiprocessor systems (parallel systems, tightly coupled systems), 12-13 multiprogramming, 15-17, 88 multitasking, see time sharing multithreading; benefits of, 127-129 cancellation, thread, 139 90S and exed) system call, 138 »• and forkO system call, 138 models of, 129-131 pools, thread, 141-142 and scheduler
activations, 142-143 and signal handling, 139-141 symmetric, 171-172 and thread-specific data, 142 MUP (multiple universal-namingconvention provider), 826 mutex: adaptive, 218-219 in Windows XP, 790 mutex locks, 201, 247-248 mutual exclusion, 247, 666-668 centralized approach to, 666 fully-distributed approach to, 666-668 token-passing
approach to, 668 mutual-exclusion condition (deadlocks), 253 N names: resolution of, 623, 828-829 in Windows XP, 793-794 named pipes, 824 naming, 100-101, 399^100 defined, 643 domain name system, 399 of files, 374 lightweight diretory-access protocol, 400 and network communication, 622-625 national-language-support (NLS) API, 787 NDIS
(network device interface specification), 823 near-line storage, 480 negotiation, 721 NetBEUI (NetBIOSextended user interface), 823 NetBIOS (network device interface)
4,096 pages of 1,024 bytes but only 512 pages of 8,192 bytes. Enough of these sessions can eat up all the network resources of the system, disabling any further legitimate TCP connections. Processes that wish to access a shared-memory segment must attach it to their address space using the shmat () (SHared Memory ATtach) system call. The server
blocks on the accept O method waiting for a client to request a connection. Some viruses modify themselves as they infect other software to avoid the basic pattern-match approach of antivirus programs. The Java thread API allows thread API allows thread the basic pattern-match approach of antivirus programs.
associative memory and that, of those remaining, 10 percent (or 2 percent of the total) cause page faults.:\:...lit?*;:::,.:i..hi:. To ensure orderly access to the memory, a memory controller is provided whose function is to synchronize access to the memory.
loaded in step 3. An application proxy firewall understands the protocols that application programmer. Exercises 369 9.15 What
is the cause of thrashing? The other approach is to allow (or require) the user to specify explicitly how the process should migrate. Without the ability to authorize users and processes, to control their access, and to log their activities, it would be impossible for an operating system to implement security measures or to run securely. Some operating
systems provide facilities for locking an open file (or sections of a file). When a process that owns a mailbox terminates, the mailbox disappears. A complete description of the monitor was given by Hoare [1974]. It can access a segment associated with ring k (k > /). This situation is depicted in Figure 9.5. Notice that marking a page invalid will have
no effect if the process never attempts to access that page. In addition, access privileges can be effectively revoked by the simple technique of changing some of the locks associated with the object (Section 14.7). Obviously, when the copy-onwrite technique is used, only the pages that are modified by either process are copied; all unmodified pages
can be shared by the parent and child processes. In a star network, the failure of a single link results in a network partition, but one of the partitions has only a single site. Bibliographical Notes General discussions concerning security are given by Hsiao et al. The port all ocates a new mailbox and allocates space for its
queue of messages. • Sharing. Since the I/O devices that attach to a computer vary widely, the operating system needs to provide a wide range of functionality to applications to allow them to control all aspects of the devices. For example, if 5 is provided, the first five numbers in the Fibonacci sequence will be output by the child process. Typically, and
operating system provides a rendezvous (also called a matchmaker) daemon on a fixed RPC port. The Win32 thread library available on Windows systems. It is faster because swap space is allocated in much larger blocks, and file lookups and indirect allocation methods are not used (Chapter 12). Once the process is allocated
the CPU and is executing, one of several events could occur: • The process could issue an I/O queue. Such is not the case with a local replacement algorithm. ;.;!.. • To discuss the general structure of distributed operating systems. If we interpret these 8-bit bytes as unsigned integers, the page with the lowest
number is the LRU page, and it can be replaced. 582 Chapter 15 Security • A function V: X - > (Mxyl-> {true, false}). Choose from more than 4,000 titles in approximately 60 languages. The following list includes forms of accidental and malicious security violations. K*ot only can the keys be exchanged in public, but a given user needs only one
```

```
private key, no matter how many other people she wants to communicate with. The client can then send a message one or more times and be assured that it only executes once. For large operating systems (including most general-purpose operating systems like Windows, Mac OS X, and UNIX) or for systems that change frequently, the bootstrap
 loader is stored in firmware, and the operating system is on disk. However, before proceeding, we should mention that some researchers have argued that none of the basic approaches alone is appropriate for the entire spectrum of resource-allocation problems in operating systems. x / i n c l u d e / a s m - i 3 8 6 / u n i s t d. However, when pagee
replacement is called for, these frames can simply be overwritten (because they are never modified), and the pages can be read in from the file system, again if needed. Note that the 578 Chapter 15 Security write message m attacker Figure 15.7 A secure communication over an insecure medium. The lock-key mechanism, as mentioned, is a
compromise between access lists and capability lists. The chapter no longer covers overlays. The solution should exhibit minimal busy waiting. A segment for user data 5. A variant of this scheme employs asymmetry in addressing. Thus, the hardware can distinguish integers, floating-point numbers, pointers, Booleans, characters, instructions,
capabilities, and uninitialized values by their tags. A particular kind of rights amplification is associated with a protected procedure. The protocol also ensures freedom from deadlock, because no transaction ever waits. Swap space is only used as a backing store for pages of anonymous memory, which includes memory allocated for the stack, heap
and uninitialized data of a process. Matters related to secondary and tertiary storage are explained as well. However, to improve performance over two-phase locking, we need either to have additional information about the transactions or to improve performance over two-phase locking, we need either to have additional information about the transactions or to improve performance over two-phase locking, we need either to have additional information about the transactions or to improve performance over two-phase locking, we need either to have additional information about the transactions or to improve performance over two-phase locking, we need either to have additional information about the transactions or to improve performance over two-phase locking.
with large and small complexities and subtleties. The produced in a header file such as the following: /* buffer.h* / typedef i n t buffer.item; #define BUFFER SIZE 5 The buffer will
be manipulated with two functions, insert_item() and remove item(), which are called by the producer and consumer threads, respectively. The result is a powerful and easy-to-use facility—one of the reasons for the huge growth of the World Wide Web. We then explore a key security enabler —cryptography- Finally, we look at mechanisms to guard
against or detect attacks. Facing numerous and possibly conflicting requests for resources, the operating system must decide how to allocate them to specific programs and users so that it can operate the computer system efficiently and fairly. The attack is complete when the attacker gives this constructed binary sequence as input to the process.
That resource can then be allocated to P3, breaking the cycle, in sunimary if a resource-allocation graph does not have a cycle, then the system is not in a deadlocked state. Contrast these two approaches for modeling processes and threads within the kernel. What, then, are the relative merits of-enforcement based solely on a kernel, as opposed to
enforcement provided largely by a compiler? After finishing a request, such tasks may need to send a one-time reply to the task that had requested service; but they must also continue with other service requests, even if the reply mailbox for a client is full. The computer will be slowed down by a factor of 40 because of demand paging! If we want
performance degradation to be less than 10 percent, we need 220 > 200 + 7,999,800 x p, p < 0.0000025. - - - - ... In any case, we are faced with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major components of the page-fault service time: 1. (We encountered a similar situation with three major componen
2 o: 0 0 3 1 0 page frames Figure 9.14 Optimal page-replacement algorithm. Fixed-sized and variable-sized messages 3.6 The Fibonacci sequence is the series of numbers 0,1,1,2,3,5,8 Formally, it can be expressed as: fibo = 0 Jibi = 1 fib,, = fib,, - \ + fib,, - 2 Write a C program using the fork() system call that that generates the Fibonacci sequence in the
child process. It is similar to the RSA encryption algorithm, but the key use is reversed. Repositioning within a file need not involve any actual I/O. The result of this attack program's execution will be a root shell or other privileged command execution. Several versions of UNIX (including Solaris and Linux) also provide a variation of the forkC) system
call—vforkO (for virtual memory fork). The following code is typical: int i, j; int [128][128] data; for (j = 0; j < 128; j++) for (i = 0; i < 128;
components of program state are shared across threads in a multithreaded process? Instead, each processors communicate with one another through communication. In this section, we explore three other
strategies for communication in client-server systems: sockets, remote procedure calls (RPCs), and Java's remote method invocation (RMI). If not, why is it not used by every manufacturer? Get command line arguments a r g v [1], argv[3] */ /* 2. Solaris 10 implements the principle of least privilege via role-based access control, a form of the
access matrix. 3.3.1 Process Creation A process may create several new processes, via a create-process system call, during the course of execution. Normal - communication • sender receiver attacker Man-in-the-middle attacker Figure 15.1 Standard security attacks. The msg_send() call sends a message to a
mailbox. To accomplish this task, we must reduce memory waste, or fragmentation. Polymorphic. 9.4.5.2. The page out process works as follows: The front hand of the clock scans all pages in memory, setting the reference bit to 0. If the page fault occurs on the instruction fetch, we can restart by fetching the instruction again. If we have a user process works as follows:
of twenty pages, we can execute it in ten frames simply by using demand paging and using a replacement algorithm to find a free frame whenever necessary. Once the attached Visual Basic script was opened, the virus propagated by sending itself to the first users in the user's e-mail contact list. Traditionally, f o r k O worked by creating a copy of the
parent's address space for the child, duplicating the pages belonging to the parent. A stack algorithm for which it can be shown that the set of pages in memory with n + 1 frames. 10.1 File Concept 377 When another process executes an openQ call, a new
entry is simply added to the process's open-file table pointing to the appropriate entry in the systemwide table. This feature improves their implementation, maintenance, and portability. Therefore, a more elaborate scheme is needed. Different algorithms exist for solving the critical-section problem, with the assumption that only storage interlock is
available. The string of memory references is called a reference string. Multiuser systems must be less trusting of users. Viruses are a particular problem for users of PCs. UNIX and other multiuser operating system. Several
different strategies can be used to enable a thread to wait for other threads to finish. 10.1 File Concept Computers can store information on various storage media, such as magnetic disks, m
loaded. You talk about "the stack," "the main program," without caring what address Figure 8.18 User's view of a program. In this case, the operating system is designed mostly for ease of use, with some attention paid to performance
and none paid to resource utilization—how various hardware and software resources are shared. This situation results from trying to get the initial locality into memory. It could call a system library to request the load of the contents of a deadlock.
Each of these new processes may in turn create other processes, forming a tree of processes, forming a tree of processes and are not under the operating system's control. 4.2.2 One-to-One Model The one-to-one model (Figure 4.3) maps each user thread to a kernel thread. The logical address is a pair
(selector, offset), where the selector is a 16-bit number: V 13 1 2 in which s designates the segment number, g indicates whether the segment is in the GDT or LDT, and p deals with protection. This type of violation involves unauthorized reading of data (or theft of information). [1989], who continued their work in Anderson et al. The slab allocator
first attempts to satisfy the request with a free object in a partial slab. Another technique is dumpster diving, a general term for attempting to gather information in order to gain unauthorized access to the computer (by looking through trash, finding phone books, or finding notes containing passwords, for example). 14.5.5 Comparison We now
compare the various techniques for implementing an access matrix. The list of possible breaches is almost endless. Note that there is considerable variation in the naming conventions of security holes and that we use the most common or descriptive terms. Output the value of the Fibonacci sequence in the shared-memory segment. When a capability
is created, the current value of the master key is associated with the capability. Full. Reading them is as easy as visiting one of these websites. All the pages of a process still must be in physical memory, however. The setuid mechanism is discussed further in Appendix A. Various synchronization problems (such as the bounded-buffer problem, the
readers-writers problem, and the dining-philosophers problem) are important mainly because they are examples of a large class of concurrency-control problems. Storing the operating system in ROM is suitable for small operating systems, simple supporting hardware, and rugged operation. Conversely, variable-sized messages require a more
complex system-level implementation, but the programming task becomes simpler. A distributed system is a file-service system whose users, servers, and storage devices are dispersed among the sites of a distributed system. Suppose that process P wants to access a file at site A. If it has not been used, these bits will be off. The actual
implementation of someMethod() resides on the server. These goals form the basis for choices among various algorithms and strategies. In fact, this process-creation method was in common use before threads became popular. Users are identified to the system by a unique security ID. While waiting, allocate the CPU to some other user (CPU
scheduling, optional). 9.9.4 Inverted Page Tables Section 8.5.3 introduced the concept of the inverted page table. If it is no longer being used, it will drop from the working set A time units after its last reference. • The client and server use the corresponding port handle to send messages or callbacks and to listen for replies. The most important
determinant of the method used in a particular system is the hardware provided. Slipping the sectors in this way frees up the space of sector 18, so sector 17 can be mapped to it. Indeed, the first edition of Operating Systems Concepts (1983) used 4,096 bytes as the upper bound on page sizes, and this value was the most common page size in 1990.
The slab allocation scheme is thus particularly effective for managing memory where objects are frequently allocated and deallocated, as is often the case with requests from the kernel. The sched process creates several children processes—including pageout and f sf lush. The timestamp-based concurrency-control scheme was provided by Reed
[1983]. Marilyn Turnamian helped generate figures and presentation slides. Prepaging may offer an advantage in some cases. Rather, it can manipulate only an object for which it has a reference. However, beginning with Solaris 9, this system uses the one-to-one model. You think of it as a main program with a set of methods, procedures, or
functions. The free list contains frames that have invalid contents. 16.1.1 Resource Sharing If a number of different sites (with different capabilities) are connected to one another, then a user at one site may be able to use the resources available at another. The virus targeted Microsoft Windows systems and used its own SMTP engine to e-mail itself
to all the addresses found on an infected system. In this instance, the initial value of the semaphore is 1, and its maximum value is 5. Other variants are also possible, but the basic strategy is clear: The user process is allocated any free frame. The wait () system call returns the process identifier of a terminated child so that the parent can tell which of
its possibly many children has terminated. Message passing may be either blocking— also known as synchronous and asynchronous and asynchronous and asynchronous and asynchronous. Most of these devices are standalone units for individual users. Processes may ask for a number of these resources and —once finished—will return them. Assume that the free-frame pool is managed
using the least recently used replacement policy. Kernel processes typically require memory to be allocated using pages that are physically contiguous. •; 22 1 E c CD en 18 execution time Figure 9.19 Locality in a memory-reference pattern. Westall, J. The section is mostly concerned with computer-system organization, so you can skim or skip it if you
already understand the concepts. h > /* required for randQ */ #include void ^producer(void *param) { buffer item rand; while (TRUE) { /* sleep for a random period of time */ sleep(...); /* generate a random number */ rand = rand(); printf ("producer producer produ
*param) { buffer item rand; while (TRUE) { /* sleep for a random period of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("report error condition"); else printf ("consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("consumer consumer consumed of time */ sleep(...); if (remove item(&rand)) fprintf("consumer consumer consu
frames are available, we must select some process and suspend it. The number of producer threads 3. That is, a process can initially request any number of instances of a resource type—say, R,. For instance, messages from two senders may be allowed to map the same file concurrently, to allow sharing
of data. Synchronous signals are delivered to the same process that performed the operation that caused the signal (that is the reason they are considered synchronous). Finally, we have the return address, which specifies where to return control once the function exits. Revocation of capabilities, however, may be inefficient (Section 14.7). Thus, a
part of the final page must be allocated (because pages are the units of allocation.) but will be unused (creating internal fragmentation). We may return to this locality later. Objects may be hardware (such as memory, CPU time, and I/O devices) or software (such as memory, CPU time, and I/O devices) are the units of allocated (because pages are the units of allocation).
program, if you used a system that supports it, run the program using a utility that traces system calls. We can. In this section, we discuss how swap space is managed. Generally, the table of pointers is stored in low memory (the first 100 or so locations). Some transfer data
synchronously, others asynchronously. 1.1.1 User View The user's view of the computer waries according to the interface being used. With no demand paging, user addresses are mapped into physical addresses, so the two sets of addresses can be different. Similarly, a sender can encode its message so that only a computer with a certain key can
decode the message, so that the key becomes the destination. In this section, we describe common methods by which programs cause security breaches. This specification is widely used to determine the security of a facility and to model security solutions, so we explore it here. Then, to replace a page, we can search for the page frame with the
smallest counter. When the CPU is interrupted, it stops what it is doing and immediately transfers execution to a fixed location. Normally, the user program is compiled, and the compiler automatically constructs segments reflecting the input program. Rather than forcing the user to delete the file and then recreate it, this function allows all attribute
to remain unchanged—except for file length—but lets the tile be reset to length zero and its file space released. example:. Zombies make crackers particularly difficult to prosecute because determining the source of the attack and the person that launched it is challenging. Windows XP provides support for multiple operating environments, or
subsystems, with which application programs communicate via a message-passing mechanism. Also, because only one thread can access the kernel at a time, multiple threads are unable to run in parallel on multiprocessors. The Win32 API implements shared memory through memory mapping files. In Figure 9.27, for example, when the kernel
releases the Q. The optimal replacement algorithm wras presented by Belady [1966]. To log in remotely, the user issues the command telnet cs.yale.edu This command results in the formation of a socket connection between the local machine at Westminster College and the "cs.yale.edu" computer. Overflow an input field, command-line argument, or
input buffer—for example, on a network daemon—until it writes into the stack. Revocation replaces the master key with a new value via the set-key operation, invalidating all previous capabilities for this object. One approach to data migration is to transfer the entire file to site A. 368 Chapter 9 Virtual Memory f. This means that the amount of time
between clearing and investigating a bit is often a few seconds. For example, a single Java JVM can run several threads, each in a different protection class. • Each process may be a domain. It takes 28.4 milliseconds to read a single page of 1,024 bytes but 56.4 milliseconds to read the same amount as two pages of 512 bytes each. The greatest
efficiency is obtained wrhen enforcement of protection is supported directly by hardware (or microcode). Processes should be able to switch from one domain to another. A lock is releaseMutex(Mutex); Win32 Semaphores in the Win32 API are also dispatcher
objects and thus use the same signaling mechanism as mutex locks. However, if two sites A and B are not directly connected, messages from one to the other must be routed through a sequence of communication links. However, if two sites A and B are not directly connected, messages from one to the other must be routed through a sequence of communication links. However, if two sites A and B are not directly connected, messages from one to the other must be routed through a sequence of communication links.
15.7 Discuss a means by which managers of systems connected to the Internet could have designed their systems to limit or eliminate the damage done by a worm. Create producer thread(s) */ / * 4. Swapping is discussed in Chapter 8. First, a user may run with more privileges than necessary (for example, as the administrator), allowing programs
that she runs to have more access to the system than is necessary. CHAPTER OBJECTIVES • To provide a high-level overview of distributed systems and the networks that interconnect them. Josh Dees and Rob Reynolds contributed systems and the networks that interconnect them.
waiting. 326 Chapter 9 Virtual Memory physical memory process. The cover was printed by Von Hoffmann, Inc. Mike Shapiro, Bryan Cantrill, and Jim Mauro answered several Solaris-related questions. Determine that the interrupt was a page fault. Global variables 3. W'e can associate with each page frame a counter of the number of pages
associated with that frame. reference string 4 7 0 7 1 0 1 2 1 2 7 1 2 tt 1 2 0 1 { :D a b 4 L stack before a '_J stack after b Figure 9.16 Use of a stack to record the most recent page references. (Modulo arithmetic is used on the indexes, so that P,, is waiting for a resource R,, held by Po-) Then, since process P.+i is holding resource R; while requesting
resource R;+i, we must have F(R,) < F(R,-+i), for all i. The person who wants to send the encrypted message knows no better and so uses the bad key to encrypt the message. Consideration was also given to the feedback provided by the reviewers of the text, as well as comments submitted by readers of earlier editions. Operating systems must
provide a mechanism for parent processes to create new child processes to create new child processes. Access lists correspond directly to the needs of users. They were assisted by Simon Durkin, who managed many details of this project smoothly. The COPS security-scanning package for UNIX was written by Farmer at Purdue University. Formally, we define a one-to-one
function F: R —> N, where N is the set of natural numbers. Whether the high-priority process should be able to replace the low-priority process is a policy decision. Because of all this device variation, the operating system needs to provide a wide range of functionality to applications, to allow them to control all aspects of the devices. The rights held
by a trustworthy procedure are independent of, and may exceed, the rights held by the calling process. The use of higher-level languages for specifying access control was suggested first by Morris [1973], who proposed the use of higher-level languages for specifying access control was suggested first by Morris [1978], Kieburtz and Silberschatz
[1983], and McGraw and Andrews [1979] proposed various 558 Chapter 14 Protection language constructs for dealing with general dynamic-resource-nianagi*ment schemes. However, the terms process scheduling and thread scheduling are often used interchangeably. Virtual memory also allows processes to share files easily and to implement
shared memory. The TSS is used to store the hardware context of each process during context switches. H must be infeasible to find an m' ^ m such that H(m) = H(m'). We discussed this issue briefly in Chapter 6 in connection with semaphores. The number of the sequence will be provided in the command
line. However, objects are created in advance and thus can be quickly allocated from the cache. 4.4.4 Thread Pools In Section 4.1, we mentioned multithreading in a web server. Our Acquisitions Editors, Bill Zobrist and Paul Crockett, provided expert guidance as we prepared this edition. The web page also contains the book's three case-study
appendices and the Distributed Communication appendix. Each of these modules or data elements is referred to by name. Authorizing users must be done carefully to assure that only appropriate users have access to the system. Kessels [1977] proposed an extension to the monitor to allow automatic signaling. The chapter has undergone a major
overhaul, with all sections updated. Encryption is used to provide confidentiality of data being stored or transferred. Among the active debates within the computing system, and/or application software, is increasing the threat of and damage caused by
security intrusions. Kosaraju [1973] followed up on Patil's work to produce a problem that cannot be solved by waitO and signal () operations. Some systems store the operations store the operations are needed, a single request for all of them must be issued.
Solaris 10 advances the protection available in the Sun Microsystems operating systems, such as time-sharing systems, may introduce an additional, intermediate level of scheduling. Because of power, speed, and interface limitations, they
perform relatively few remote operations. One issue of concern with cooperating processes involves synchronization issues. Processes sharing this region consider it part of their virtual address space, yet the actual physical pages to be shared during process
creation with the forkO system call, thus speeding up process creation. 6.17 Suppose the signal () statement in a monitor procedure. Files are mapped by the operating system onto physical devices. A virus signature is a pattern that can be used to identify a virus, typically a series of bytes that make up the virus
code. An application typically is implemented as a separate process with several threads of control. As a result, Microsoft was found guilty of using its operating system monopoly to limit competition. Our example describes a date server that uses connection-oriented TCP sockets. This specific kind of rights amplification corresponds to an
implementation of the s e a l and unseal primitives on capabilities. •; . The use of shared objects that do not require the use of critical sections was discussed in Herlihy [1993], Bershad [1993], and Kopetz and Reisinger [1993]. 16.1.3 Reliability If one site fails in a distributed system, the remaining sites can continue operating, giving the system
better reliability If the system is composed of multiple large autonomous installations (that is, general-purpose computers), the failure of one of them should not affect the rest. The processes are also responsible for ensuring that they are not writing to the same location simultaneously. It simply provides an environment within which other programs
can do useful work. A cache consists of one or more slabs. X :P6rt; P matchmaker replies to client with port P kernel sends RPC From: client To: server Port: P To: client Port: P To: client Port: P matchmaker replies to client with port P daemon listening to port P daemon processes request and processes send output Figure
3.21 Execution of a remote procedure call (RPC). What is the effect when A is set to a very high value? A socket is identified by an IP address concatenated with a port number. New is the coverage of modern storage arrays, including new RAID technology and features such as thin provisioning. Some time later, when the I/O request advances to the
and 2 and have added two new chapters on specialpurpose systems (real-time embedded systems and multimedia systems). Buffers for I/O also consume a significant amount of memory. On the other hand, protection at lower layers in the protocol stack may give insufficient protection to higher-layer protocols. The user may decide to enter some
rights in some entries in column / and other rights in other entries, as needed. Linux is an example: The policy and. Projects To emphasize the concepts presented in the text, we have added several programming exercises and Projects that use the POS1X and Win32 APIsas well as Java. This is illustrated in Figure 12.9
Once the system identifies the boot partition, it reads the first sector from that partition (which is called the boot sector) and continues with the remainder of the boot process, which includes loading the various subsystems and system services. Although datastructure techniques are available for representing sparse matrices, they are not particularly
useful for this application, because of the way in which the protection facility is used. Thus, a computer not holding D(k) cannot decrypt ciphertexts. Associated with each swap area is a swap map—an array of integer counters, each corresponding to a page
slot in the swap area. Assign a specific thread to receive all signals for the process. 3.5 Examples of IPC Systems 3.5.2 An Example: Mach 105? In these actions, Morris exploited the UNIX networking utility rsh for easy remote task execution. As we will see in Chapter 8, advanced memory-management techniques may require extra data to be
switched with each context. In this project, the system call will have limited functionality; it will simply transition back to user mode, print a message that is logged with the kernel messages, and transition back to user mode to kernel mode, print a message that is logged with the kernel messages, and transition back to user mode to kernel mode, print a message that is logged with the kernel messages, and transition back to user mode to kernel mode, print a message that is logged with the kernel messages, and transition back to user mode to kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, print a message that is logged with the kernel mode, and the kernel mode, 
system call). The block of characters to move and the area to which it is to be moved can each also straddle two pages. Indeed, recent trends indicate a move toward software-managed TLBs and operating-system but also consideration of the
 external environment within which the system operates. The process will be restarted only when it can regain its old resources, as well as the new ones that it is requesting. All code and data structures for the library exist in user space. The assembler, in turn, may produce object modules, which are consumed by the loader. A locality is a set of pages
that are actively used together (Figure 9.19). These projects include adding a system call to the Linux kernel, creating a UNIX shell using the fork () system call, a multithreaded matrix application, and the producer-consumer problem using shared memory. If the process does not have the number of frames it needs to support pages in active use, it
will quickly page-fault. We discuss domain switching in greater detail in Section 14.4. Consider the standard dual-mode (monitor-user mode) model of operating system are, what an operating system does for the common features of an operating system operator. In the
past, RAIDs composed of small, cheap disks were viewed as a cost-effective alternative to large, expensive disks; today, RAIDs are used for their higher reliability and higher data-transfer rate, rather than for economic reasons. This violation involves unauthorized destruction of data. This protocol is often applied to resources whose state can be easily
 saved and restored later, such as CPU registers and memory space. Note that a process must be executing in domain D\ to read and write object O\, while only processes in domain D3 may execute object O\. [1999] and Jacob and Mudge [2001] discuss techniques for managing the TLB. The shared-memory method requires communicating processes
to share some variables. Typically, the source code is stored in the / u s r / s r c / l i n u x - 2. When a page must be replaced, LRU chooses the page that has not been used for the longest period of time. Almost all computer resources are scheduled before use. The linear address on the Pentium is 32 bits long and is formed as follows. The star network
 also has a low communication cost, since each site is at most two links away from every other site. ISBN 0-471-69466-5 Printed in the United States of America 10 9 8 7 6 5 4 3 2 1 To my children, Lemot, Sivan, and Aaron Avi Silberschatz To my wife, Carla, and my children, Given Owen and Maddie Peter Baer Calvin In memory of Uncle Sonny, Robert
Jon Heilemcin 1933 — 2004 Greg Gagne Preface Operating systems are an essential part of any computer system. Another common attack is to replay a captured exchange of data. In Section 4.3.2, we describe the WaitForSingleObj ect () function, which is used to wait for a single thread to finish. The details of how the server communicates with the
socket are as follows. Zero-fill-on-demand pages have been zeroed-out before being allocated, thus erasing the previous contents. Selecting a replacement frame, the paging system reads the necessary page into memory as a linear array of bytes, some containing instructions and others containing data?
6.13 Write a bounded-buffer monitor in which the buffers (portions) are embedded within the monitor itself. Under pure demand paging, all 93 frames would initially be put on the free-frame list. • Chapter 22, Influential Operating Systems, has been updated. Internal fragmentation may increase, but this trade-off is acceptable because the life of data
in the swap space generally is much shorter than that of files in the file system. Java programs are composed of classes, each of which is a collection of data fields and functions (called methods) that operate on those fields. To prevent thrashing, we must provide a process with as many frames as it needs. Automatic and explicit buffering c. An optimal
page-replacement algorithm has the lowest page-fault rate of all algorithms and will never suffer from Belady's anomaly. s t r u c t object from its cache. 15 20.2 Compression 718 20.3 Requirements of Multimedia Kernels 720 20.4 CPU Scheduling 722 20.5 Disk Scheduling 723 PART EIGHT CASE STUDIES Chapter 21 The Linux System 21.1 21.2
21.3 21.4 21.5 21.6 21.7 21.8 21.9 21.10 21.11 21.12 Linux History 737 Design Principles 742 Kernel Modules 745 Process Management 748 Scheduling 751 Memory Management 756 FileSvstems 764 Input and Output 770 Interprocess Communication Network Structure 774 Security 777 Summary 779 Exercises 780 Bibliographical Notes 781
Chapter 22 Windows XP 22.1 22.2 22.3 22.4 22.5 History 783 Design Principles 785 System Components 787 Environmental Subsystems File System 814 811 22.6 Networking 822 22.7 Programmer Interface 829 22.8 Summary 836 Exercises 836 Bibliographical Notes 837 773 Contents Chapter 23 23.1 23.2 23.3 23.4 23.5 23.6 Influential Operating
Systems Early Systems 839 Atlas 845 XDS-940 846 THE 847 RC4000 848 CTSS 849 23.7 23.8 23.9 23.10 'MULTICS 849 IBM OS/360 850 Mach 851 Other Systems 853 Exercises 853 Appendix A UNIX BSD (contents online) A.I A.2 A.3 A.4 A.5 A.6 UNIX History A855 Design Principles A860 Programmer Interface A862 User Interface A869 Process
Management A872 Memory Management A876 A.7 A.8 A.9 A.10 File System A886 Interprocess Communication A889 Summary A894 Exercises A895 Bibliographical Notes A896 Appendix B The Mach System Components A900 System A878 I / O System 
Process Management A903 Interprocess Communication A909 Memory Management A914 B.7 Programmer Interface A919 B.8 Summary A920 Exercises A921 Bibliographical Notes A922 Credits A923 Appendix C Windows 2000 (contents online) C.I C.2 C.3 C.4 C.5 History A925 Design Principles A926 System Components A927 Environmental
 Subsystems A943 File System A945 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.6 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.8 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.8 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 887 855 C.8 Networking A952 C.7 Programmer Interface A957 C.8 Summary A964 Exercises A964 Bibliography Credits 885 Index 88
100BaseT Ethernet, 619 aborted transactions, 222 absolute code, 278 absolute path names, 390 abstract data type, 375 access control, in Linux, 778-779 access control list (ACL), 403 access latency, 484 access lists (NFS V4), 656 access matrix, 538-542 and access control, 545-546
defined, 538 implementation of, 542-545 and revocation of access rights, 546-547 access rights, 534, 546-547 acces
fact of life on the Internet. A user must begin by completely reformatting the hard disk, especially the boot sector, which is often targeted for viral attack. Note that many viruses belong to more than one category. There are two simple methods for implementing this scheme: • Use the value of the system clock as the timestamp; that is, a transaction's
timestamp is equal to the value of the clock when the transaction enters the system. • The server creates two private communication ports and returns the handle to one of them to the client. Note the performance penalty inherent in this system.
network. The process then copies the binary sequence from argv [1] to position buffer [0] in the stack frame up to the location of the return address; and
the location of buffer [0], the new return address, is added. Chapter 21 was derived from an unpublished manuscript by Stephen Tweedie. Of course, this privilege is still subject to type verification to ensure that only software capabilities for a specified abstract type are passed to any such procedure. However, this server is single-threaded, meaning
the server cannot respond to concurrent echo clients until the current client exits. This program works by first prompting the user for the name of the source and destination files. It will hold the printer for its entire execution, even though it needs the printer only at the end. The benefits of multithreading can be greatly increased in a multiprocessor
architecture, where threads may be running in parallel on different processors. • Less I/O would be needed to load or swap each user program would run faster. ..-... Hardware-supported protection is also relatively immune to protection violations that might occur as a result of either hardware or system software
malfunction. The amount of time that a client might have to wait for its request to be serviced could be enormous. Further, virtual memory as viewed by the user from physical memory. If the table is in memory, however, user memory accesses can be
degraded substantially. physical memory. 0,430 b. Virtual memory is commonly implemented by demand paging. f. • Between each pair of processes, there exists exactly one link. Thus, the long-term scheduler may need to be invoked only when a process leaves the system. This situation is illustrated in Figure 3.22. With standard procedure calls,
some form of binding takes place during link, load, or execution time (Chapter 8) so that a procedure call. The process may then try to reacquire the capability. Remember, too, that if a user process will result, as the process will
be granted, an entire page frame. This method is more complicated than the first method, but it avoids data copying. There are two options for adding the systems, if a process terminates (either normally), then all its children must also be terminated. The process therefore may have to wait for the disk. Notice that
the number of faults for four frames (ten) is greater than the number of faults for three frames (nine)! This most unexpected result is known as Belady's anomaly: For some page-replacement algorithms, the page-fault rate may increase as the number of faults for four frames (nine)! This most unexpected result is known as Belady's anomaly: For some page-replacement algorithms, the page-fault rate may increase as the number of faults for four frames (nine)! This most unexpected result is known as Belady's anomaly: For some page-replacement algorithms, the page-fault rate may increase as the number of faults for four frames (nine)! This most unexpected result is known as Belady's anomaly: For some page-replacement algorithms, the page-fault rate may increase as the number of faults for four frames (nine)! This most unexpected result is known as Belady's anomaly: For some page-replacement algorithms, the page-fault rate may increase as the number of faults for faults fa
threats to be monitored. Hence, this write operation is rejected, and T, is rolled back. This amplification may be necessary to allow P the right to access the storage segment representing A so as to implement the operation that P defines on the abstract data type. The details of memory management hardware have been modernized. 3.4.2.2
Synchronization Communication between processes takes place through calls to sendO and receive () primitives. Once a signal has been generated by the occurrence of a certain event (e.g., division by zero, illegal memory access, user entering, etc.), the signal is delivered to a process where it must be handled. For instance, we would want to have
complex protection system on a computer used by a university to process students for classwork. The code in the boot BOM instructs the disk controller to read the boot blocks into memory (no device drivers are loaded at this point) and then starts executing that code. With multiple processes competing for frames
we can classify page-replacement algorithms into two broad categories: global replacement and local replacemen
consumer process. : . For instance, it might be desirable to allow users to access a network without letting for Threads to Complete Once all worker threads have completed, the main thread will output the product contained in matrix C. To ensure that
deadlocks never occur, the system can use either a deadlockprevention or a dea
the following, say whether it will (or is likely to) improve CPU utilization. Encryption of messages is an ancient practice, of course, and there have been many encryption algorithms, dating back to before Caesar. For example, C and C++ use pointers frequently, and pointers tend to randomize access to memory, thereby potentially diminishing a
process's locality. However, if one printer is on the ninth floor and the other is in the basement, then people on the ninth floor may not see both printers as equivalent, and separate resource classes may need to be defined for each printer is on the ninth floor may not see both printers as equivalent, and separate resource classes may need to be defined for each printer.
 especially if hardware support for atomic operations is available. For example, in Figure 14.5(a), a process executing in domain D2 can copy the read operation into any entry associated with file F2. To reduce these types of overhead, we introduce the concept of checkpoints. All system-call executions can be logged for analysis of program behavior
(or misbehavior). A program written for the .NET Framework need not worry about the specifics of the hardware or the operating system on which it will run. This scheme has two variants: 1. We therefore require that, prior to execution of a write(X) operation, the log records corresponding to X be written onto stable storage. A capability-creating
program would be able to execute a primitive operation that would seal a data structure, rendering the latter's contents inaccessible to any program components that did not hold either the seal or the unseal privilege. This assumption is not always correct, however, because of hardware or software errors. The SSL protocol is initiated by a client c to
 communicate securely with a server. For instance, systems that implement swapping may use swap space to hold an entire process image, including that datum until it is retrieved at a later time. Data capabilities are interpreted by
microcode in the CAP machine. [1991], and Black [1990], Zabatta and Young [1998] compare Windows NT and Solaris threads on a symmetric multiprocess does not modify the address space of the parent, vf ork() is intended to be used when the child process calls execO
immediately after creation. Chapters 10 through 13 describe how the file system, mass storage, and I/O are handled in a modern computer system. 9.7 Memory-Mapped Files 351 to shared memory. User space kernel space Figure 9.4 Transfer of a
paged memory to contiguous disk space. There are two main types of encryption algorithms: symmetric and asymmetric and asymmet
that the page has been modified. This program is composed of two functions: main() and setup (). The default signal handler for SIGINT is to terminate the program. Essentially, the attack exploits a bug in a program. Each of these pieces should be a well delineated portion of the system, with carefully defined inputs, outputs, and functions. The major
difficulty arises when one instruction may modify several different locations. Instead, she must learn the principles and techniques of protection, since the system provides her with no library of procedures. In this discussion, we use SSL to mean both SSL and TLS. 4.1 Overview A thread is a basic unit of CPU utilization; it comprises a thread ID, a
program counter, a register set, and a stack. In cases where the data are extremely important and fast failure recovery is necessary, the price is worth the functionality. To create an operation, we must perform system for a particular machine configuration, we must perform system for a particular machine configuration, we must perform system for a particular machine configuration, we must perform system for a particular machine configuration, we must perform system for a particular machine configuration, we must perform system for a particular machine configuration for the price is worth the functionality.
clock algorithm discussed in Section 9.4.5.2. On Alpha and, multiprocessor x86 systems, clearing the entry in the translation look-aside buffer on other processors. • Access rights. This user has started the Netscape browser (pid of 7785) and the emacs editor (pid of 8105). Memory-access time is 100
 nanoseconds. Scheduling of this kind is a fundamental operating-system function. When the file is closed, the file-table entry is deleted. 15.2.4 Stack and Buffer Overflow The stack- or buffer-overflow attack is the most common way for an attacker outside the system.
For instance, consider the following: • Programs often have code to handle unusual error conditions. Communication speeds range from 1 megabit per second, for networks such as AppleTalk, infrared, and the new Bluetooth local radio network, to 1 gigabit per second for gigabit Ethernet. All forms of ROM are also known as firmware, since their
characteristics fall somewhere between those of hardware and those of software. In key-based schemes, the operations of defining keys, inserting them into lists, and deleting them from lists should not be available to all users. For example, programmers and systems managers need to fully understand the algorithms and technologies they are
deploying. The URL is: New to this edition is a print supplement called the Student Solutions Manual. The Linux operating system typically uses utilities such as lilo and grub to maintain a list of bootable kernels, from which the user can choose during machine boot-up. A process, when it is not executing, is placed in some waiting queue. Schemes
that implement revocation for capabilities include the following: • Reacquisition. A process is executed until it must wait, typically for the completion of some I/O request. Many of these features are not enabled by default, however, which may be one reason for the myriad security breaches on Windows XP systems. The messages are then routed to
other nearby systems and in this way either are propagated to all hosts on the network (public messages) or are transferred to their destination (private messages). A client communicates with the server by creating a socket and connecting to the port on which the server is listening. If the CPU does not poll the control bit, but instead receives an
interrupt when the device is ready for the next byte, the data transfer is said to be interrupt driven. A list of pointers is maintained with each object, pointing to all capabilities associated with that object. They can be read-only or read-write. It also provides computation by removing the matching key from the table.
An edge from node A to node B corresponds to a direct communication link between the two sites. r i s f; ::-.;; | ; :-. A privilege is the right to execute a system call or to use an option within that system resource, such as storage objects.
Software preference. Anyone with rudimentary computer skills and access to the exploit—a so-called script kiddie—can then try to launch the attack at target systems. Once this information is determined, it can be used in several ways. The routers control the path each message takes through the net. Extending Kernel Source You can now
a variety of protection policies to be implemented. This method appears to be a good compromise and is used in several systems, including Solaris and BSD UNIX. The operating system shifts the reference bit for each page into the high-order bit. Such a system also
provides the user with a distributed file system, which is a file-service system whose users, servers, and storage devices are dispersed among the sites of a distributed system. Tluis, a logical address consists of a two tuple: < segment-number, offset > . 3.7 Summary 115 5 client remote object val = server.someMethod(A,B) boolean someMeihod
(Object x, Object y) implementation of someMethod II stub skeleton A, B, someMethod boolean return value Figure 3.23 Marshalling parameters. The type of the objects specified in the message is important, since objects defined by the operating system—such as ownership or receive access rights, task states, and memory segments—may be sent in
messages. Tt clears all the reference bits before selecting the next page for replacement. The failure of a site must be detected by the system, and appropriate action may be needed to recover from the failure. It should then be easy to see how other, similar operations, such as renaming a file, can be implemented. All the resources of the process—
including physical and virtual memory, open files, and I/O buffers—are deallocated by the operating system. A declarative notation is natural because access privileges are closely related to the linguistic concept of data type. Therefore, in some cases, an asynchronous signal may be delivered only to those threads that are not blocking it. • A link may
be associated with more than two processes. The times must also be maintained when page tables are changed (due to CPU scheduling). Thus, ky is the public key and ks is the private key. Several processes are kept in memory at one time. Reference bits are associated with each entry in the page table. » Size. • Chapter 4, Threads, is the old Chapte
5. They work by searching all the programs on a system for the specific pattern of instructions known to make up the virus. Much computer data in modern systems travels over private leased lines, shared lines like the Internet, wireless connections, or dial-up lines. In this way, we always have the "time" of the last reference to each page. Thus
process i needs WSSj frames. Output all modified data residing in volatile storage to the stable storage to the stable storage to the stable storage to the stable but runs at 100 megabits per second and is becoming common. However, if parameters are passed that refer to segments in a lower ring (that is, segments not accessible to the called procedure)
then these segments must be copied into an area that can be accessed by the called procedure. For example, if a firewall rule allows a connection from a host and identifies that host by its IP address, then another host could send packets using that same address and be allowed through the firewall. Unfortunately, it does not take great programmers
to launch security attacks. 9,6 Thrashing If the number of frames allocated to a low-priority process's execution. 2, 3. The long-term scheduler controls the degree of multiprogramming (the number of processes in memory). At least one resource
must be held in a nonsharable mode; that is, only one process at a time can use the resource. This technique frees programmers from the concerns of memory-storage limitations. A cracker could launch a port seamier to try to connect to, say, port 25 of a particular system or a range of systems. We can illustrate the swapping idea by considering
again schedule 2 of Figure 6.23. • Process management. If a queue of processes is waiting for the device (other processes that have caused page faults), we have to add device-queuing time as we wait for the paging device to be free to service our request, increasing even more the time to swap. The first three references cause faults that fill the
 three empty frames. Instead of swapping in a whole process, the pager brings only those necessary pages into memory. Thrashing has occurred, and system throughput plunges. h and limix/kernel. The number of kernel threads. »
                                ntation is not an issue because each unique kernel data structure has an associated cache, and each cache is comprised of one or more slabs that are divided into chunks the size of the objects being represented. A name is usually a string of characters, such as example.c. Some systems differentiate between uppercase and
lowercase characters in names, whereas other systems do not. For example, there are books, alphabet books, alp
service routine for the interrupting device. For example, when a function is called, it defines a new locality. Over longer distances, the cost of using high-quality cable is enormous, and the exclusive use of the cable tends to be prohibitive. It is perhaps the most commonly used cryptographic protocol on the Internet today, since it is the standard
protocol by which web browsers communicate securely with web servers. We invoke the ZeroMemoryO function to allocate memory for each of these structures before proceeding with CreateProcess (). Overestimation wastes disk space that could otherwise be used for files, but it does no other harm. The location of directories and index blocks is also
important. These chapters cover methods for process scheduling, interprocess communication, process synchronization, and deadlock handling. 6.18 Consider a system consisting of processes Pi, Pi,..., P,,, each of which has a unique priority number. * 4. As an alternative to sector sparing, some controllers can be instructed to replace a bad block by
sector slipping. Instead of returning to the main routine it was in before Morris's call, the finger daemon was routed to a procedure within the invading 536-byte string now residing on the stack. [1988], Kramer [1988], and Garfinkel et al. Moreover, we have substantially updated and expanded the coverage of security. remote service, 650-651 and
consistency, 649-650 replication of files in, 652-653 stateful vs. The most common ones are locking protocols and timestamp ordering schemes. Finally, the Mult icastSocket class is a subclass of the DatagramSocket class is a subclass of the DatagramSocket class. 3.4.2 Message-Passing Systems In Section 3.4.1, we showed how cooperating processes can communicate in a shared-memory
environment. stack stack •'. 1 shared Hbrary shared library 1 heap data code code Figure 9.3 Shared library using virtual memory. It initializes all aspects of the system, from CPU registers to device 1.2 Computer-System Organization mouse keyboard printer 7 monitor disks!: disk; ; controller CPU USB COhtrolfer: ^adapter memory.
Figure 1.2 A modern computer system. The cost in time and money to send a message from site A to site B 16.4 Network Topology 621 • Availability. Each of these hops could go over a secure or insecure network. At a low level, messages are passed between systems, much as messages are passed between processes in the single-computer message
system discussed in Section 3.4. Given message passing, all the higher-level functionality found in standalone systems can be expanded to encompass the distributed system. Thus, we see that localities are defined by the program structure and its data structures. I/O is often implemented by a separate I/O processor. A mailbox can be viewed
abstractly as an object into which messages can be placed by processes and from which messages can be removed. The sending process or by the mailbox. Some systems—such as cellular phones, PDAs, and game consoles—store the entire operating system in ROM. Caching the
directories and index blocks in main memory can also help to reduce the disk-arm movement, particularly for read requests. Here, we describe one such algorithm, known as RSA after the names of its inventors (Rivest, Shamir and Adleman.) The RSA cipher is a block-cipher public-key algorithm and is the most widely used asymmetrical algorithm.
For example, the cache representing semaphores objects, etc. Events reported to an administrator include any monitored file or directory whose signature differs from that in the database (a changed file), any file or directory in a
monitored directory for which a signature does hot exist in the database (an added file), and any signature in .the.database.for. Next, we elaborate briefly on each of the three methods for handling deadlocks. Preface Chapter 5, CPU Scheduling, is the old Chapter 6. We will further explore these—and other—benefits of virtual memory later in this
chapter. local allocation, 342-343 proportional allocation, 342-343 proportional allocation, 343-356 in Linux, 759-762 and memory mapping, 348-353 basic mechanism, 348-353 basic mechanism, 348-353 basic mechanism, 348-350 I/O, memory-mapped, 353 in Win32 API, 350-353 network, 647 page replacement for conserving, 327-339 and application performance, 339 basic
mechanism, 328-331 counting-based page replacement, 338 FIFO page replacement, 331-333 LRU-approximation page replacement, 336-338 LRU page replacement, 336-338 LRU page replacement, 331-335 LRU-approximation page replacement, 336-338 LRU page replacement, 338-339 separation of logical memory from physical memory by, 317 size of, 316 in Solaris, 363-365 and
thrashing, 343-348 cause, 343-345 page-fault-frequency strategy, 347-348 working-set model, 345-347 unified, 433 in Windows XP, 363 virtual memory fork, 327 virtual memory fork, 328 virtual memory
VM manager, see virtual memory manager VMS operating system, 853 VMware, 67 vnode, 418 vnode number (NFS V4), 656 volume stable of volume stab
contents, 386 von Neumann architecture, 8 VPNs, see virtual private networks vulnerability scans, 592-593 VxWorks, 710-712 W WAFL file system, 444-446 wait-die scheme, 677-678 waiting thread state (Windows XP), 789 waiting time, 157 wait queue, 773 WANs, see virtual private networks Web-based computing, 34 web clipping, 31
Web distributed authoring and versioning (WebDAV), 824 wide-area networks (WANs), 15, 28, 619-620 Win32 API, 350-353, 783-784 Windows XP, 783-836 application compatibility of, 785-786 design principles for, 785-787 desktop versions of
784 environmental subsystems for,1 811-814 16-bit Windows, 812 32-bit Windows, 812 32-bit Windows, 812 32-bit Windows, 812 1-813 logon, 814 Win32, 813 extensibility of, 786-787 file systems, 814-822 change journal, 821 compression and encryption, 821 mount points, 821 NTFS B+ tree, 816 NTFS internal layout, 814-816 NTFS metadata,
816 recovery, 816-817 security, 817-818 volume management and fault tolerance, 818-821 volume shadow copies, 821-829 history of, 783-785 interprocess communication example, 106-108 networking, 822-829 Active Directory, 828 distributed-processing mechanisms, 824-826 domains, 827-828 interfaces, 822 name resolution, 828-829 protocols,
822-824 redirectors and servers, 826-827 performance of, 786 portability of, 785 Part One Overview An operating system acts as
an intermediary between the user of a computer and the computer hardware. Authentication failures can tell us quite a lot about break-in attempts. 1,10 c. However, such a procedure must not be regarded as universally trustworthy (the procedure is not allowed to act on other types, for instance), and the trustworthiness
must not be extended to any other procedures or program segments that might be executed by a process. Each of these pieces should be a well-delineated portion of the system, with carefully defined inputs, outputs, and functions. • Allocation. The information about all files is kept in the directory structure, which also resides on secondary storage.
The bug can be a simple case of poor programming, in which the program was expecting. Mutual exclusion. c. is holding the DVD and process P; is holding the printer. The chapter offers a significantly updated discussion of scheduling
issues for multiprocessor systems, including processor affinity and load-balancing algorithms. If the number of free pages falls below lotsfree, a process known as the pageout starts up. The Win32 API provides several functions related to thread pools. The kernel sends notification of event occurrences to the Notify port. Operating systems for
handheld computers are designed to provide an environment in which a user can easily interface with the computer to execute programs. If we pass a value of NULL, the operating system selects the location on the user's behalf. It is similar to the standard RPC mechanism that is widely used, but it is optimized for and specific to Windows XP. The
number of bits of history can be varied, of course, and is selected (depending on the hardware available) to make the updating as fast as possible. In addition, if these copies are modified, the various copies will be inconsistent. Discuss the importance of obtaining such a statistical profile. Alternatively, an operating system may provide several
different page sizes. [1976] in connection with their work on concurrency control for System R. In many ways, the sharing of memory-mapped files is similar to shared memory as described in Section 3.4.1. Not all systems use the same mechanism for both; on UNIX and Linux systems, for example, memory mapping is accomplished with the mmap ()
system call, whereas shared memory is achieved with the POSJX-compliant shmgetO and shmatO systems calls (Section 3.5.1). 4. 16.3 Network Structure 16.2.2.3 617 Process Migration A logical extension of computation migration is process migration.
constraints on the service order for requests. Furthermore, each transaction may be assigned a unique identifier. The child process will then write the Fibonacci sequence to shared memory and finally will detach the segment. What we are about to see is a complex dance in which asymmetric cryptography is used so that a client and server can
establish a secure session key that can be used 586 Chapter 15 Security for symmetric encryption of the session between the two—all of this* while avoiding man-in-the-middle and replay attacks. One of these buddies is further divided into two 64-KB buddies—B; and B«. Appendix C was derived from an unpublished manuscript by Cliff Martin. For
example, entering the command ps - e l will list complete information for all processes currently active in the system. With a larger page size, we must allocate and transfer not only what is needed but also anything else that happens to be in the page, whether it is needed or not. The basic protection system will not allow an unverified, user-defined,
protected procedure access to any storage segments (or capabilities) that do not belong to the protection environment in which it resides. Neither system is widely used, but they are interesting proving grounds for protection theories. Address I • mi: . What is the maximum acceptable page-fault rate for an effective access time
of no more than 200 nanoseconds? The sum total of all protection systems within a computer system (hardware, software, firmware) that correctly enforce a security policy is known as a trusted computer base (TCB). The server first establishes a Print Writer to object that it will use to communicate with the client. To illustrate a deadlock state,
consider a system with three CD RVV drives. If the pageout processes, thereby freeing all pages allocated to swapped processes.
resources available in the system. The circles represent the resources that serve the queues, and the arrows indicate the flow of processes in the system. Revocation of access rights in a dynamic protection model is typically easier to implement with an access-list scheme than with a capability list. Booting begins in a Windows 2000 system by running
code that is resident in the system's ROM memory. Because the memory is shared, any changes the child makes to the shared memory will be reflected in the parent process as well. Requests for disk service can be greatly influenced by the file-allocation method. A timeout duration (or INFINITE) For example, if THandles is an array of thread
HANDLE objects of size N, the parent thread can wait for all its child threads to complete with the statement: WaitForMultipleDbjectsCN, THandles, TRUE, INFINITE); A simple strategy for waiting on several threads using the Pthreads using the Pthreads using the Pthreads join() or Java's join threads using the Pthreads using the Pthread
message"Caught Control C" and then invokes the exit () function to terminate the program. However, we are wasting the effort spent to bring in the page for the low-priority process. The delivery of the symmetric key is a huge challenge. For example, a variable can be defined as private or the low-priority process. The delivery of the symmetric key is a huge challenge.
t e c t e d so that it can be accessed only by the class that contains it, subclasses of that class, or classes in the same package. Initial access to the file proceeds through ordinary demand paging, resulting in a page fault. Consider the following scenario, which is based on the actual behavior of early paging systems. Another option is to demand pages
from the file system initially but to write the pages to swap space as they are replaced. RMI and RPCs differ in two fundamental ways. If a file is opened for reading, then a capability for read access is placed in the file-table entry. Consider the representation of 32-bit integers. As an alternative example, we next consider process creation in Windows.
Most versions of UNIX are Cl class. is added to the graph (Figure 7.3). However, because we provide a value of NULL, we do not name the mutex. This is shown in Figure 8.22. ;;;rs...;;.;;...; : domain; n ^ ; : :: :; \\ ii: ;i-i -· ;i. A language implementation might provide standard protected procedures to interpret software capabilities that would
realize the protection policies that could be specified in the language. Fortunately, the level of abstraction that RMI provides makes the stubs and skeletons transparent, allowing Java developers to write programs that invoke distributed methods just as they would invoke local methods. 15.6 The UNIX program COPS scans a given system for possible
security holes and alerts the user to possible problems. When a page must be replaced, the oldest page is chosen. Exercises 241 Mutex locks are acquired by invoking the WaitForSingleDbject 0 function, passing the function the HANDLE to the lock and a flag indicating how long to wait. This trap is the result of the operating system's failure to bring
the desired page into memory. number of frames Figure 9.21 Page-fault frequency. For example, if the lock ordering in the Pthread program shown in Figure 7.1 was F(first mutex) = 5 then threacLtwo could not request the locks out of order. 1. The value of the counter indicates the number of mappings to the swapped page; for
example, a value of 3 indicates that the swapped page is mapped to three different processes (which can occur if the swapped page is storing a region of memory shared by three processes). • To describe various CPU-scheduling algorithms, • To discuss evaluation criteria for selecting a CPU-scheduling algorithm for a particular system. I.;!.. •
Reading a file. Notice that the numbers are not guaranteed to be unique, however. WThen we switch a process from one domain to another, we are executing an operation (switch) on an object (the domain). When a process from one domain to another, we are executing an operation (switch) on an object (the domain).
fast as they are fixed. Answer the following questions: a. We can keep an 8-bit byte for each page in a table in memory. As indicated by its name, an APC is roughly equivalent to an asynchronous signal in UNIX. Incoming messages that have a timestamp already in the history are ignored. This execution can also be produced by the two-phase locking
protocol. Of course, a firewall itself must be secure and attack-proof; otherwise, its ability to secure connections can be compromised. That is, to keep the slowdown due to paging at a reasonable level, we can allow fewer than one memory access out of 399,990 to page-fault. A compiler can separate references for which it can certify that no
```

protection violation could occur from those for which a violation might be possible, and it can treat them differently. As operation of To with the

```
write(A) operation of T\. Two physical writes are required for every logical write requested. Chapter 9, Virtual Memory, is the old Chapter 10. The next time the system is rebooted, a special, command is run to tell the SCSI controller to replace the bad sector with a spare. A process must request a resource before using it and must release the
resource after using it. This code segment is then compiled so that the assembly language instructions can be modified. Operations on objects are defined procedurally. vf ork() operates differently from f ork() with copy-on-write. This link can be implemented in a variety of ways. Inverted page tables were discussed in an article about the IBM RT
storage manager by Chang and Mergen [1988]. The term capability was introduced by Dennis and Horn [1966]. 16.1 Motivation A distributed system is a collection of loosely coupled processors interconnected by a communication network. Encryption is a means for constraining the possible receivers of a message. :: B^; For instance, if a web-page
form expects a user name to be entered into a field, the attacker could send the user name, plus extra characters to overflow the buffer and reach the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto the stack, plus a new return address to load onto
file's permissions. Read the desired page into the newly freed frame; change the page and frame tables. Otherwise, the calling thread blocks indefinitely—as we are specifying INFINITE—until the semaphore becomes signaled. Clearly, the hit ratio is related 9.9 Other Considerations 359 to the number of entries in the TLB, and the way to increase the
hit ratio is by increasing the number of entries in the TLB. The second case involves disrupting the network of the facility. The set of pages in the most 346 Chapter 9 Virtual Memory recent A page references is the working set (Figure 9.20). If the bit is set, we know that the page has been modified since it was read in from the disk. For example, we
can keep a counter of the number of references that have been made to each page and develop the following two schemes. Similarly, the resource type printer may have a file extension of either .EXE or .DLL. Such pages cannot be
modified; thus, they may be discarded when desired. The trusted party receives proof of identification from some entity and certifies that the mapped view is the entire file. When users invoke this service program, they take the risk that the program
will malfunction and will either damage the given data or retain some access right to the data to be used (without authority) later. This method is necessary because the early versions of VAX did not implement the reference bit correctly. We contrast the main differences in operating-system design between these systems and centralized systems. */
void setup(char inputBuffer [], char *args[],int *background) { /** full source code available online */ int background = 0; printf(
COMMAND-> "); /* setup() calls exitO when Control-D is entered */ setup(inputBuffer, args, fcbackground); /** the steps are: (1) fork a child process using fork() (2) the child process will invoke the setup 0 function again. Exercises 231 A transaction is a program unit that
must be executed atomically; that is, either all the operations associated with it are executed to completion, or none are performed. The problem is one of authentication—what we need is proof of who (or what) owns a public key. DEADLOCK WITH MUTEX LOCKS Let's see how deadlock can :occur in a multithreaded Pthread program using mutex
locks. The readers-writers problem was suggested by Courtois et al. The stub unmarshals this return value and passes it to the client. On UNIX, a listing of processes can be obtained using the ps command. The verification algorithm is then V\{kv\}\{m, a\} = (ak < mod\ N \sim H(m)), where kv satisfies kvks mod \{p - l\}(q - 1) - 1. The protection domain to
which the class is assigned depends on the URL from which the class was loaded and any digital signatures on the class file. A TLB can reduce the performance degradation to an acceptable level. The section on Linux scheduling has been revised to cover the scheduler used in the 2.6 kernel. In contrast, a mailbox that is owned by the operating
system has an existence of its own. Also discuss under what circumstance the opposite holds. Scott Graham, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Holliday, Ahmed Kamel, Richard Guy, Max Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hillyer, Mark Hailperin, Rebecca Hartman, Wayne Hathaway, Christopher Haynes, Bruce Hathaway
Gary Lippman, Carolyn Miller, Preface xv Michael Molloy, Yoichi Muraoka, Jim M. 12.4.6 Selection of a Disk-Scheduling Algorithm Given so many disk-scheduling Algorith
approach to system design?:::::'•: '•: '• The device controller is responsible for moving the data between the peripheral devices that it controls and its local buffer storage. As in the previous edition, the appendices are provided online. The following variables reside in a region of memory shared by the producer and consumer processes:
#define BUFFER_SIZE 10 typedef s t r u c t { }item; item buffer [BUFFER_SIZE]; i n t in = 0; in t out = 0; The shared buffer is implemented as a circular array with two logical pointers: in and out. A linked or indexed file, in contrast, may include blocks that are widely scattered on the disk, resulting in greater head movement. 4.4.3 Signal Handling
A signal is used in UNIX systems to notify a process that a particular event has occurred. After copying the disk file to the printer, it releases these two resources and terminates. The regional networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks, such as NSFnet in the northeast United States, are interlinked with routers (Section 16.5.2) to form the worldwide networks (Section 16.5.2) to form the worldwide netwo
discussed in Kurose and Ross [2005]. Sharable resources, in contrast, do not require mutually exclusive access and thus cannot be involved in a deadlock. If all processes are I/O bound, the ready queue will almost always be empty, and the short-term scheduler will have little to do. The unbounded buffer places no practical limit on the size of the
buffer. This approach has several significant advantages: 14.9 Language-Based Protection 551 1. • A function E: K->• (M - • C). The third parameter of 0, we allow both reads and writes to the shared region. Every operating
system probably has its own replacement scheme. We would appreciate hearing from you about any textual errors or omissions that you identify. Division D includes only one class and is used for systems 15.8 Computer-Security Classifications 601 that have failed to meet the requirements of any of the other security classes. To accommodate such
requirements, an operating system may choose to do its own disk scheduling and to spoon-feed the requests to the disk controller, one by one, for some types of F/O. A device controller maintains some local buffer storage and a set of special-purpose registers. Objects are considered remote if they reside in a different Java virtual machine (JVM). It
can also limit connections based on source or destination address, source or destination port, or direction of the connection. Some companies now enforce this as policy by removing all incoming attachments to e-mail messages. If the JVM is implemented in software, the Java interpreter interpreter interprets the bytecode operations one at a time. If there is a
page fault, all the old values are written back into memory before the trap occurs. Managing the TLB in software and not hardware comes at a cost in performance issues were discussed by Anderson et al. For example, if the
user enters I s -1 at the COMMAND-> prompt, args [0] becomes equal to the string I s and a r g s [1] is set to the string to -1.9.6.6 I/O Interlock When demand paging is used, we sometimes need to allow some of the pages to be locked in memory.
translation? To implement this scheme, we associate with each data item Q two timestamp values: • W-timestamp (Q) denotes the largest timestamp of any transaction that successfully executed write(Q). The chapter presents an enhanced discussion of thread libraries, including the POSIX, Win32 API, and Java thread libraries. If a page fault occurs
and if the page does not exist in the freeframe pool, how is free space generated for the newly requested page? Because these programs run under the user's own account, the macros can run largely unconstrained (for example, deleting user files at will). Both Linux and FreeBSD are readily available to computer-science departments, so many
students have access to these systems. A right is copied from access(/,/), the stack, as the value of the stack, as the value of the stack pointer allows relative
access to parameters and automatic variables. On such a system, the new process may get two open files, img.jpg and the terminal device, and may simply transfer the datum between the two. 15.11 What commonly used computer programs are prone to man-in-themiddle attacks? 12.7 RAID Structure Disk drives have continued to get smaller and
cheaper, so it is now economically feasible to attach .many disks to a computer system. To ensure that this condition does not hold, we can use the following protocol. The issues of lowering the overhead associated with protection costs and enabling user-level access to networking devices were discussed in McCanne and Jacobson [1993] and Basu et
al. The date server shown in Figure 3.19 uses the Java, io .BufferedReader class. Authentication, when combined with hashing, can prove that data have not been changed. Commonly, files represent programs (both source and object forms) and data. Once the transaction releases a lock, it enters the shrinking phase, and no more lock requests can be
issued. To illustrate the difference between these two protocols, we consider a process that copies data from a DVD drive to a file on disk, sorts the file, and then prints the results to a printer. A global page-replacement algorithm is used; it replaces pages without regard to the process to which they belong. This separation allows maximum flexibility
if policy decisions are to be changed later. If A is too small, it will not encompass the entire locality; if A is too large, it may overlap several localities. For the simple systems, we need only compare or add to the logical address—operations that are fast. To access data item Q, transaction 7} must first lock Q in the appropriate mode. But many
electronic-disk devices contain a hidden magnetic hard disk and a battery for backup power. Whereas the minimum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture, the maximum number of frames per process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the architecture are not all the process is defined by the arch
financially. • Chapter 3, Processes, is the old Chapter 4. When external power is restored, the controller copies the data back into the RAM. Operating systems, we now cover these topics earlier in the text. Such an algorithm
does exist and has been called OPT or MIK. The following example illustrates the use of shmget (): segment id = shmget(IPCJPRIVATE, s i z e , SJRUSR | SJVVUSR); This first parameter specifies the key (or identifier) of the shared-memory segment. In fact, RC4 itself has vulnerabilities. Furthermore, firewalls do not prevent attacks that tunnel, or
travel within protocols or connections that the firewall allows. The processors in a distributed system vary in size and function. If we cannot change the content of a domain, we can provide the same effect by creating a new domain with the changed content and switching to that new domain when we want to change the domain content. • File-open
count. When a connection is received, the server returns the date and time to the client. Deliver the signal applies. If the link is full, the sender must block until space is available in the queue. Other users are accessing
the same computer through other terminals. 10.1 File Concept 375 • Time, date, and user identifying the specific thread. System 360/370 MVC (move character) instruction., which can move up to 256 bytes from one location to
another (possibly overlapping) location. A virus is a fragment of code embedded in a legitimate program. With a local replacement strategy, the number of frames allocated to a process does not change. • To explain the fundamentals of encryption, authentication, and hashing. We can either replace (swap out) all pages with the smallest value or use
the FIFO method to choose among them. The worm then searched for rsh data files in these newly broken accounts on remote systems. Discuss these solutions. In addition, the KTHREAD includes the kernel stack (used when the thread is running in kernel mode) and a pointer to
the TEB. Use, The process can operate on the resource (for example, if the resource is a printer, the process can print on the printer). If a page that has been modified is to be replaced, its contents are copied to the disk. Wait in a gueue for this device until the read request is serviced. If accesses to any types of data were random rather than
patterned, caching would be useless. Commands may come from files during batch-mode execution or directly from a terminal when in an interactive or time-shared mode. If we were to implement the system calls of a typical operating system and store them in a segment associated with ring 0, what should be the values stored in the ring field of the
segment descriptor? i: '•••'•:: "•:::,;;;;•::••:••:•-i'.ii!:iii..ii3iii iii "•'": '-."-•-. • Blocking send. Note in Figure 9.2 that we allow for the heap to grow upward hi memory as it is used for dynamic memory allocation. The worm searched these special files for site names that would allow remote execution without a
password. The Kernel mailbox is used by the kernel to communicate with the task. One message can be given to the operating system to keep, even though the mailbox to which it is being sent is full. The processes need to know only each other's identity to communicate. 16.3.2 j ] i J \ • j 5 *• : • 3 Wide-Area Networks Wide-area networks emerged in
the late 1960s, mainly as an academic research project to provide efficient community of visers. The equivalent of this in Win32 is WaitForSingleObj ect (), which is passed a handle of the child process—pi . This certificate is a
structure containing the following: • Various attributes attrs of the server, such as its unique distinguished name and its common (DNS) name • The identity of a public encryption algorithm E () for the server • A validity interval interval interval during which the certificate should be considered valid • A digital signature a on
the above information by the CA—that is, a = S(kCA)({ attrs, E(ke), interval >) In addition, prior to the protocol's use, the client is presumed to have obtained the public verification algorithm V(1A)—that is, the probabilities that an alarm indicates an intrusion and that no alarm indicates no intrusion. The valid-invalid bit scheme described in Section
8.5 can be used for this purpose. 14.10 Drotection domain: ; : ; ::apie! t iii il \ ; socket |; rS; |: S .? The worm executed a buffer-overflow attack on f inger. u t il. Now, if H(m) — H(m'), we know that the message has not been modified. It can scan a range of systems, determine the services running on those systems, and
attempt to attack all appropriate bugs. Here is an example: Suppose that logical block 17 becomes defective and the first available spare follows sector 202. If a process has been allocated more pages than its working-set minimum, the virtual memory manager removes pages until the process reaches its working-set minimum. Yet another kind of
attack is the man-in-the-middle attack, in which an attacker sits in the data flow of a communication, masquerading as the sender to the receiver, and vice versa. This property, called serializability, can be maintained by simply executing each transaction within 226 Chapter 6 Process Synchronization a critical section. It is important that the goals of
the system be well defined before the design begins. It is especially concerned with the operation and control of I/O devices. An operating system is similar to a government. 540 Chapter 14 Protection; i object; (a) N-l_^ -. On simple disks, such as some disks with [DE controllers, bad blocks are handled manually. Otherwise, access is denied, and an
exception condition occurs. This setup allows the JVM to bide the implementation details of the underlying operating system and to provide a consistent, abstract environment that allows Java programs to operate on any platform that supports- a JVM. For example, H(m) can be sent along with a message; but if H is known, then someone could modify
m and recompute H(m), and the message modification would not be detected. ability to share code across processes 8.6 On a system with paging, a process cannot access memory that it does not own. Flash memory is slower than DRAM but needs no power to retain its contents. The hardware—the central processing unit (CPU), the memory, and the
input/output (I/O) devices—provides the basic computing resources for the system. A process can cause the terminate process via an appropriate system call (for example, Terminate process via an appropriate system call (for example, Terminate process via an appropriate system.) In a multiprogramming environment, several process via an appropriate system call (for example, Terminate process via an appropriate system.)
typed object A, for instance, this capability may include an auxiliary right to invoke some operation P but would not include any of the so-called kernel rights, such as read, write, or execute, on the segment that represents A. The connection will consist of a pair of sockets: (146.86.5.20:1625) on host X and (161.25.19.8:80) on the web server. User
threads are supported above the kernel and are managed without kernel support, whereas kernel threads are supported and managed directly by the operating system. In this case, the disk head has to move the entire width of the disk. We can establish upper and lower bounds on the desired page-fault rate (Figure 9.21). Intuitively, whether a
request to open a file should be allowed will generally depend on which class has requested the open. In the following section, we discuss how the paging unit turns this linear address into a physical address. That is, K n=\ For example, if A were a 3-by-2 matrix and B were a 2-by-3 matrix, element Cxi would be the sum of Axi x £>i,i and A>,2 x
B2.iFor this project, calculate each element C,-,y in a separate worker thread. Using Figure 9.27 as a guide, draw the tree illustrating how the following memory requests are allocated: • request 120 bytes 
that either paging or segmentation be used, to provide small packets of information (pages or segments) that can be shared. From there, of course, the cracker could install Trojan horses, back-door programs, and so on. Belady's optimal algorithm is for a fixed allocation; Prieve and Fabry [1976] presented an optimal algorithm for situations in which
the allocation can vary. The antivirus software analyzes the behavior of the code in the sandbox before letting it run unmonitored. In the shared-memory model, a region of memory that is shared by cooperating processes is established. It also installed a daemon to allow unlimited remote access by an intruder and another that allowed an intruder to
route spam through the infected desktop computer. Thus, the working set is an approximation of the program's locality. The data structure for a sector typically consists of a header, a data area (usually 512 bytes in size), and a trailer. Specifying the order in which a particular process may invoke the various operations of a resource (for example, a
file must be opened before it can be read): It should be possible to give two processes different restrictions on the address space of the current process must be preserved as the space of the next task is prepared for use. Such systems may include small
handheld or real-time devices, personal computers, workstations, and large mainframe computer systems. The CPU and the device controllers can execute concurrently, competing for memory cycles. As we have seen, some factors (internal fragmentation, locality) argue for a large page for a large page for a large page.
size. For example, consider a machine in which all memory-reference instructions have only one memory address. This book is printed on acid free paper. Copy-on-write is a common technique used by several operating systems, including Windows XP, Linux, and Solaris. The debugging option was useful to system administrators and was often left on
For example, consider a system with one printer and one DVD d rive. As before, a deadlock exists in the system if and only if the wait-for graph contains a cycle. The host computer systems, a small piece of code known as the bootstrap
program or bootstrap loader locates the kernel, loads it into main memory, and starts its execution. Another important issue involves the semantics of a call. That is, when the right R* is copied from access(/t,/), only the right R (not R") is created. The rings are numbered from 0 to 7. The buffer-overflow attack is especially pernicious
because it can be run between systems and can travel over allowed communication channels. The openO call can also accept accessmode information—create, read-only, read—write, append-only, and so on. The chapter features expanded coverage of motivating virtual memory as well as coverage of memory-mapped files, including a programming
example illustrating shared memory (via memory-mapped files) using the Win32 API. A system beyond class Al might be designed and developed in a trusted facility by trusted personnel. the boolean value returned from someMethod () and sends this value back to the client. When a page has been selected, however, we inspect its reference 9.4 Page
Replacement reference bits 337 pages i 0 V next victim circular queue of pages (a) (b) Figure 9.17 Second-chance (clock) page-replacement algorithm. 348 Chapter 9 Virtual Memory T ^ rafcife ifewtrfeHgiire •SJGji f •• tiros; • as .refeifgiifieg M: daja^aMt Cocife;;sKciioii§ r:e -{lie % fapft Is at:fe' [fafls. a.
The function is then executed as requested, and any output is sent back to the requester in a separate message. Generically, we perform a state restore to resume operations. If the stored and calculated numbers are different, this mismatch indicates that the data area
of the sector has become corrupted and that the disk sector may be bad (Section 12.5.3). This method requires the extra overhead of the initial request but is more flexible than the first approach. In many ways, they are also the slowest major component of the computer. The chapter provides an overview of real-time computer systems and describes
how operating systems must be constructed to meet the stringent timing deadlines of these systems. One popular variation on the many-to-many model still multiplexes many user-level threads to a smaller or equal number of kernel threads but also allows a user-level thread to be bound to a kernel thread. This method is appropriate for devices that
have fast response times, such as video controllers. This mechanism allows the parent process to communicate easily with its child process. In Figure 3.26 we show a C program that uses the function handle. SIGINT gine that uses the function handle. Signal. Viruses are usually borne via email, with spam the most common vector. (Hint: Restrict the generality
of B; see Kessels [1977].) 6.22 Write a monitor that implements an alarm clock that enables a calling program to delay itself for a specified number of time units (ticks). In particular, it would be reasonable to allow only the owner of an object to set the keys for that object. Rather, a program can access an object only via the methods defined on that
object by its class. The code body of P may be allowed to read or to write to the segment of A directly, even though the calling process cannot. This requirement results in a higher communication cost. Therefore, if the copy of the page on the disk has not been overwritten (by some other page, for example), then we need not write the memory page to
the disk: It is already there. In a system using the working-set model, for example, we keep with each process a list of the pages in its working set. In such an environment, each computer maintains its own local file system. Let's look more closely at how the bounded buffer can be used to enable processes to share memory. These two schemes are not
mutually exclusive and can be used simultaneously within a single operating system. Providing enough frames to each process to avoid thrashing may require process to avoid thrashing may require process swapping and scheduling. Pthreads Semaphores—named and unnamed. Signals are defined in the include file / u s r / i n c l u d e / s y s / s i g
n a l. Consider both the system level and the programmer level. • : . Users should not be aware that their processes are running on a paged system—paging behavior of that process but also on the paging behavior of other processes.
other. The operating system would be designed to change the user ID of any program run from this directory, either to the equivalent of root or to the user ID of the owner of the directory. Modems are devices that accept digital data from the computer side and convert it to the analog signals that the telephone system uses. Perform necessary error
checking to ensure that a nonnegative number is passed on the command line. The parent may have to partition its resources (such as memory or files) among several of its children. The searching process is time consuming. 14.6 Access In Section 10.6.2, we described how access controls
can be used on files within a file system. Thus, if we had forty frames, we could run eight processes, rather than the four that could run if each required ten frames (five of which were never used). When three keys are used, the effective key length is 168 bits. Once instructions have been converted to native code, they are kept and will continue to run
as native code for the CPU. The fixed location usually contains the starting address where the service routine for the interrupt is located. Periodically, or each time a program is run, the operating system recomputes the signature and compares it with the signature on the original list; any differences serve as a warning of possible infection. In general,
with enough redundancy (in both hardware and data), the system can continue operation, even if some of its sites have failed. For instance, the MS-DOS format command performs logical formatting and, as a part of the process, scans the disk to find bad blocks. Output all log records currently residing in volatile storage (usually main memory) onto
stable storage. It is similar in many respects to the IPC mechanism described in Section 3.4, and it is usually built on top of such a system. For instance, one user might create the file example.c, and another user might create the file example.c, and another user might edit that file by specifying its name. 14.5 Implementation of Access Matrix How can the access matrix be implemented effectively? If
a system crash occurs, the information in the log is used in restoring the state of the updated data items, which is accomplished by use of the undo and redo operations. Thread cancellation is the task of terminating a thread before it has completed. The following program segment is used to manage a finite number of instances of an available
resource. However, whereas f ork () has the child process inheriting the address space of the Linux operating system reflecting the most recent version of the kernel—
Version 2.6 —at the time this book was written. These locations hold the addresses of the interrupt service routines for the various devices. A multiprogramming. But what happens if the process tries to access a page that was not brought into memory? If you
choose to add this system call to an existing file in the source directory, all that is necessary is to add the sys helloworld () function to the file you choose, asmlinkage is a remnant from the days when Linux used both C++ and C code and is used to indicate that the code is written in C. The paging hardware, in translating the address through the page
table, will notice that the invalid bit is set, causing a trap to the operating system. One concern is the size of the page table. GO Copyright © 2005 John Wiley & Sons, Inc. In both equal and proportional allocation, of course, the allocation may vary according to the multiprogramming level. Furthermore, when the kernel has finished with an object and
releases it, it is marked as free and returned to its cache, thus making it immediately available for subsequent requests from the kernel.
```