**IT241 Final Exam Study Guide**

1. A bit of history here. Originally, operating systems for mainframes were designed primarily to maximize resource utilization. It is the most important core program that runs on a computer. Every computer, except dummy terminals, will have to have an operating system in order to run any other programs.
2. A debugger or debugging tool is a computer program on its own that is used to test and debug other programs. If a program terminates abnormally, a dump of memory may be examined by a debugger to determine the cause of the problem. Debugger is a powerful tool that can be used to detect and replicate the original problem as well as trace the running program step by step.
3. Early in the history of computer, each computer ran one process at a time. This was not an efficient practice because when a process is waiting for another service, the CPU stayed idle. To increase CPU productivity, multiprogramming approach was introduced to reduce idle time and maximize CPU time. **The number of processes in memory is called degree of multiprogramming. Processes running in such an environment are called concurrent processes.**
4. An “**asynchronous procedure call**” or APC, is a function that executes asynchronously in the context of a particular thread. When an APC is queued to a thread, the system issues a software interrupt. Next time when the thread is scheduled, it will run the APC function. Signals can be emulated in windows through asynchronous procedure calls.
5. Shortest-job-first or SJF, is a scheduling algorithm in which scheduling is approximated by predicting the next CPU burst with an exponential average of the measured lengths of previous CPU bursts. SJF gives the least average waiting time for a set of processes. The difficulty of using SJF is knowing the length of the next CPU request. In practice, SJF cannot be implemented as the optimal algorithm because we don’t know the length of the next CPU burst.
6. In operating systems, a semaphore is a variable or an abstract data type that is used to control access by multiple processes in a parallel programming or a multi-user computing environment. There are different types of semaphores. A counting semaphore is essentially an integer variable that allows a resource count. A binary semaphore is a semaphore that is restricted to values 0 and 1 or locked and unlocked, for example.
7. Preemption occurs in computing environment. For example, a CPU may be preempted from a process, a process may be preempted by a scheduler.
8. Memory access and management are very important in modern computing operations. Instructions and data have to be fetched from memory before tasks can be executed. Address binding is an important part in this process because the symbolic names used in user programs must be mapped or bound to physical memory addresses. During compile time, if it is known where the program resides in physical memory, absolute code can be generated for compile-time binding. If it is unknown during compile time, the program will be recompiled.
9. Virtual memory is a memory management approach that is used to optimize memory usage, free applications from having to manage shared memory spaces, and even create more memory logically than it actually has available physically. **In systems that support virtual memory,** **physical memory is separated from logical memory.**
10. A source file or source code is essentially a file or a program that a software developer writes to execute a task or job. Source file or source code is a sequence of functions or sometimes called procedures.
11. A hard disk drive or HDD, is a data storage device for data storage and retrieval. **Data is stored and retrieved in** **blocks**. Transfers between memory and disk are performed one block at a time.
12. Shortest-seek-time-first or SSTF scheduling algorithm is a direct improvement upon the first-come-first-serve (FIFO) algorithm. SSTF services each request with the minimum seek time. SSTF has the benefits of shorter average response time and simplicity.
13. Low-level formatting is a hard disk operation and differs from high-level formatting in which an operation is performed directly against disk sectors without going through the file system layer. Low-level formatting divides a disk into sections that the disk controller can read and write.
14. Swap space management is a low-level task in the operating system. The main goal in the design and implementation of swap space is to provide the best throughput for the virtual memory system. Virtual memory uses disk space as n extension of the main memory. Since disk access is much slower than memory access, swap space method can significantly improve system performance.
15. RAID is a data storage technology that uses multiple disks to provide fault tolerance, thus improve overall performance and increase storage capacity. Using RAID, data is copied or mirrored on one or more disks in the same array. If one disk fails, the data is still saved and preserved. A RAID structure is primarily used to ensure higher data reliability.
16. Disk head scheduling algorithms takes the following into account of the current position of the disk head: FCFS, SCAN and LOOK.
17. A Master Boot Record or MBR, is a special type of boot sector at the very beginning of partitioned computer mass storage devices like removable drives or fixed disks for use with PC-compatible systems. The location where Windows places its boot code is the Master Boot Record (MBR).
18. Hard disk drive performance is measured by access time and data transfer time. The access time or response time measures the time it takes before a drive actually transfers the data. The two components of access or positioning time are, seek time and rotational latency.
19. The control register of an I/O port can be written by the host to issue a command or to change the setting or mode of a device.
20. An interrupt priority scheme can be used to allow the most urgent work to be finished first and make it possible for high-priority interrupts to preempt the execution of a low priority interrupt. In addition, an interrupt priority scheme can be used to defer the handling of low-priority interrupt without masking off all interrupts.
21. Direct Memory Access or DMA, is a function that allows certain hardware subsystems within a system to access system memory independently of the CPU. With DMA, CPU only needs to initiate the transfer without having to perform the task. This frees the CPU to execute other tasks while transfer is in progress. Note, DMA controllers can steal memory access cycles from the main CPU.
22. A block device reads and writes data in fixed size blocks. A character-stream device reads and writes data in byte or bytes at a time.
23. A block device is a computer data storage device that supports reading and writing of the data in fixed-size blocks, sectors, or clusters. Raw I/O accesses a block device as a simple array of blocks. Examples of block devices are, hard drives, NAND flash memory cards, or mask ROM.
24. Domain is a group of network resources that are assigned to a group of users and are managed a common set of rules and procedures. In the UNIX operating system, a domain is associated with the user.
25. Multics or Multiplexed Information and Computing Service, was an important time-sharing operating system in the early days. In MULTICS, the protection domains are organized in a ring structure.
26. Access Control Matrix or Access Matrix, provides very detailed control for particular processes and operations. Anything that a system needs to access such as a file, a process, is regarded as an object. In an access matrix, the control right allows a process to change the entries in a row.
27. Tables are foundations of all databases. Methods and formats for accessing tables in different system vary. The global table implementation of an access table consists of sets of ordered triples.
28. One way to partition the matrix is by rows and these are stored in data structure called Capability List. In capability list, each object has a tag to denote its type. When a process tries to gain access to an object, the operating system can check the appropriate capability list.
29. Access matrix provides a mechanism for protection without imposing a particular protection policy on the system or its users. Global table is the simplest approach. Among all the implementations of the access matrix, lock-key is a compromise between two other implementations.
30. **In computer security, the most common method used by attackers to breach security is masquerading. Masquerading is an attack that uses fake identities such as network identity or stolen passwords.**
31. In computer systems, a **Trojan** **horse** is a program or a code segment in which malicious or harmful codes are contained inside harmless program or data. It can obtain controls and do its intended damage such as destroying file allocation table on the hard drive.
32. Computer worms use the **spawn** **mechanism** to ravage system performance and can continue to grow as the Internet expands. In addition, worms can shut down an entire network.
33. A **denial of service attack or DoS**, is aimed at disrupting legitimate use of a system. It can temporarily or indefinitely interrupt or suspend services of a host in a network.
34. Different types of password system has been used such as access control based ssh or single sign-on. In a **paired**-**password** system, the computer supplies one part of a password and the user enters the other part which makes it more secure.
35. A **polymorphic** virus changes each time it is installed to avoid detection by antivirus software while keeping the original algorithm intact. This technique is used by computer viruses, shellcodes and computer worms.
36. **What are the four levels of security measures that are necessary for system protection?**

To protect a system, security measures must take places at four levels: physical (machine rooms, terminals, and workstations); human (user authorization, avoidance of social engineering); operating system (protection against accidental and purposeful security breaches); and network (leased, Internet, and wireless connections).

1. What is a trap door? Why is it problematic?

A trap door is an intentional hole left in software by the designer of a program or system. It can allow circumvention of security features for those who know about the hole. Trap doors pose a difficult problem because, to detect them, we have to analyze all the source code for all components of a system.

1. How does a virus differ from a worm?

A worm is structured as a complete, standalone program whereas a virus is a fragment of code embedded in a legitimate program.

1. What is the most common way for an attacker outside of the system to gain unauthorized access to the target system?

The stack- or buffer-overflow attack is the most common way for an attacker outside the system to gain unauthorized access to a system. This attack exploits a bug in the software in order to overflow some portion of the program and cause the execution of unauthorized code.

1. A process is said to operate within a protection domain which specifies the resources that the process may access. List the ways that a domain can be realized.

A domain may be realized where each user, process, or procedure may be a domain. In the first case, the set of objects that can be accessed depends on the identity of the user. In the second case, the set of objects that can be accessed depends upon the identity of the process. Finally, the third case specifies that the set of objects that can be accessed depends on the local variables defined with the procedure.

1. What is an access matrix and how can it be implemented?

An access matrix is an abstract model of protection where the rows represent domains and the columns represent objects. Each entry in the matrix consists of a set of access rights. Access matrices are typically implemented using a global table, an access list for objects, a capability list for domains, or a lock-key mechanism.

1. What was the main disadvantage to the structure used to organize protection domains in the MULTICS system?

The ring structure had the disadvantage in that it did not allow the enforcement of a need-to-know principle. For example, if an object needed to be accessible in one domain, but not in another, then the domain that required the privileged information needed to be located such that it was in a ring closer to the center than the other domain. This also forced every object in the outer domain to be accessible by the inner domain which is not necessarily desired.

1. Why is a global table implementation of an access matrix not typically implemented?

The global table implementation suffers from a couple of drawbacks that keep it from being a popular implementation type. The first drawback is that the table is usually large and cannot be stored in main memory. If the table cannot be stored in main memory, extra I/O must be used to access this table. In addition, a global table makes it difficult to take advantage of special groupings of objects or domains.

1. Explain the concept of polling between a host and a controller.

When a host tries to access the controller, it constantly reads the status of a "busy register" and waits for the register to clear. This repetitive checking is termed polling.

1. What is interrupt chaining?

Interrupt chaining is a technique in which each element in the interrupt vector points to the head of a list of interrupt handlers. When an interrupt is raised, the handlers on the corresponding list are called one by one, until one is found that can service the request. This is a compromise between the overhead of a huge interrupt table and the inefficiency of dispatching to a single interrupt handler.

1. Why is DMA used for devices that execute large transfers?

Without DMA, programmed I/O must be used. This involves using the CPU to watch status bits and feed data into a controller register one byte at a time. Therefore, DMA was developed to lessen the burden on the CPU. DMA uses a special-purpose processor called a DMA controller and copies data in chunks.

1. What is the purpose of a programmable interval timer?

The programmable interval timer is hardware used to measure elapsed time and to trigger operations. The scheduler uses this mechanism to generate an interrupt that will preempt a process at the end of its time slice.

1. What is a storage-area network?

A storage-area network (SAN) is a private network (using storage protocols rather than networking protocols) connecting servers and storage units. The power of a SAN lies in its flexibility. Multiple hosts and multiple storage arrays can attach to the same SAN, and storage can be dynamically allocated to hosts.

1. What is a disadvantage of the SSTF scheduling algorithm?

Although the SSTF algorithm is a substantial improvement over the FCFS algorithm, it is not optimal. SSTF may cause starvation of some requests. If a continual stream of requests arrives near one another, a request of a cylinder far away from the head position has to wait indefinitely.

1. What is the advantage of LOOK over SCAN disk head scheduling?

The LOOK algorithm is a type of SCAN algorithm. The difference is that, instead of forcing the disk head to fully traverse the disk, as is done in the SCAN algorithm, the disk head moves only as far as the final request in each direction.