Toby Chappell

CPSC 380

Homework #5

Part V – I/O & Security Management

1. What are the advantages and disadvantages of supporting memory-mapped I/O to device-control registers? (4 pts)

Advantages: Eliminates the need for special I/O instructions from instruction set, does not require enforcement of protection rules that prevent user from executing those instructions

Disadvantages: Memory translation units need to make sure that the memory addresses associated with the device control registers are not accessible by user programs

1. In most multi-programmed systems, user programs access memory through virtual addresses, while the operating system uses raw physical addresses to access memory. What are the implications of this design on the initiation of I/O operations by the user program and their execution by the operating system? (5 pts)

When the user performs I/O operations, they need to create a buffer (specified by a virtual address) from which to perform these actions. The kernel then needs to issue the I/O operation and needs to translate the virtual addresses into physical addresses from the user’s buffer into its own buffer. Since translation is performed in software, there is a lot of overhead involved.

1. What are the various kinds of performance overheads associated with servicing an interrupt? (4 pts)

The cost of saving and restoring process state and the cost of flushing the instruction pipeline and restoring the instructions into the pipeline when the process is restarted.

1. What is blocking I/O and under what circumstance should it be used? What is non-blocking I/O and under what circumstance should it be used? (6 pts)

Blocking: Control does not return to the application until the I/O is complete. Should be used when the process will be waiting for one specific event (i.e. a keyboard read by an application program)

Non-blocking: Control returns immediately without waiting for the I/O to complete. Should be used when I/O can come from more than one source and the order of the I/O arrival is not predetermined (i.e. program that accepts both keyboard and mouse input).

1. 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. Suggest a scheme for implementing this policy efficiently. (5 pts)

This can be dealt with by setting up a dynamic protection structure that changes the set of resources available with respect to the time allotted for each type of user. This is due to the fact that as the day progresses, the users allowed to play games changes. When the time comes that a user’s eligibility is over, the user must be revoked from the system. Revocation could be immediate, selective (since the computer staff may access it at any hour), total, and temporary (since rights to access will be given back later in the day).

1. What is the need-to-know principle? Why is it important for a protection system to adhere to this principle? (4 pts)

A process may access at any time those resources that it has been authorized to access and are required currently to complete its task. It is important in that it limits the amount of damage a faulty process can cause in a system

1. How are the access-matrix facility and the role-based access-control facility similar? How do they differ? (6 pts)

The roles in a role-based access control facility are similar to the domain in the access-matrix facility. Just as a domain is granted access to certain resources, a role is also granted access to the appropriate resources. The two approaches differ in the amount of flexibility and the kind of access privileges that are granted to the entities. Certain access-control facilities allow modules to perform a switch operation that allows them to assume the privileges of a different module, and this operation can be performed in a transparent manner.

1. Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions. (5 pts)

One form of hardware support that guarantees that a buffer overflow attack does not take place is to prevent the execution of code that is located in the stack segment of a process’s address space. Another approach is to program in languages that checks the bounds of a buffer (such as Java).

1. A password may become known to other users in a variety of ways. Is there a simple method for detecting that such an event has occurred? (3 pts)

An easy way to detect if a password has become known is to print the last time the user logged on the system whenever the user logs in.

1. The list of all passwords is kept within the operating system. Thus, if a user manages to read this list, password protection is no longer provided. Suggest a scheme that will avoid this problem. (3 pts)

Passwords could be encrypted internally so that they can only be accessed in coded form. The only person with access or knowledge of decoding should be the system operator.