**Student name:** Federico Watkins

**CSIS 3810:** Operating Systems

**Chapter:** 14-15 Protection and Security

**Assignment:** 10

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. 🡪 14.13 | 1. 🡪 14.20 | 1. 🡪 14.21 | 1. 🡪 15.6 | 1. 🡪 15.7 | 1. 🡪 15.15 |

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.

I would use a dynamic protection structure that would change the set of resources available for each of the three categories of users based on the time allotted. The domain of users that are able to play the computer games would change as time change. A revocation process happen at the time that a user’s eligibility is over. The revocation may be total, immediate, selective for the computer staff, or temporary for rights to be returned.

1. Discuss which of the following systems allow module designers to enforce the need-to-know principle.
   1. The MULTICS ring protection scheme

The ring protection scheme in MULTICS doesn’t necessarily enforce the need-to-know principle. If an object must be accessible in a domain at ring level j but not accessible in a domain at ring level i, then j must be less then i. But such requirement means that every object accessible in level i must also be accessible in level j.

* 1. Hydra’s capabilities

In Hydra, the rights-amplification mechanism makes sure that only the privileged code has access privileges to protected objects, and if such code invokes code in other modules, the objects could be exported to the other modules after lowering the access privileges to the exported objects. Hence, such mechanism provides extremely detailed control over access rights and helps to guarantee that the need-to-know principle is satisfied.

* 1. JVM’s stack-inspection scheme

With the JVM’s stack inspection scheme, when a sequence of calls is made within a doPrivileged code block, then all of the code fragments in the called procedure have the same access privileges as the original code block that performed the doPrivileged operation, thus violating the need-to-know principle.

1. Describe how the Java protection model would be sacrificed if a Java program were allowed to directly alter the annotations of its stack frame.

A doPrivileged() block receives an access request from a thread, the stack frame of the calling thread is annotated based on the calling thread’s protection domain. The thread with an annotated stack frame is able to make any ensuing method calls that require certain privileges. Hence, the annotation serves to mark a calling thread as being privileged. A program could possibly perform an operation for which it doesn’t have the needed permission by letting a Java program directly alter the annotations of a stack frame. Therefore violating the security model of Java.

1. The UNIX program COPS scans a given system for possible security holes and alerts the user to possible problems. What are two potential hazards of using such a system for security? How can these problems be limited or eliminated?

* An intruder could modify the program disabling some of its features or even taking advantage of its features to create new security flaws.
* It’s possible for an intruder to get a copy of COPS, study it, and locate security breaches which COPS does not detect. Then that intruder could abuse systems in which the management depends on COPS for security, thinking it is providing security, when all COPS is providing is management complacency.
* Although not fool proof solutions, the program could be placed on a read-only medium or file system to keep it from been modified. Access to the program could be provided only to trusted systems managers to prevent it from falling into malicious hands.

1. 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. What are the drawbacks of making the change that you suggest?

* Managers of system can use a firewall between the system and the Internet. Such system filter the packets moving from one side to the other, making sure that only valid packets owned by authorized users are allowed to access the protect systems.
* Firewalls are widely considered to make use of the systems less convenient, and network connections less efficient.

1. Consider a system that generates 10million 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. If the intrusion-detection system has a true-alarm rate of 0.6 and a false-alarm rate of 0.0005, what percentage of alarms generated by the system correspond to real intrusions?

Probability of occurrence of intrusive records:

Probability that an alarm corresponds to a real intrusion:

References:

1. Operating System Concepts, Ninth Edition, Abraham Silberschartz, Peter bear Galvin, Greg Gagne. Entire Chapter 14-15 for each question in its respective section.
2. Dr. Szabo Tutorials Chapter 14-15 (all pertaining files).

I learned that protection refers to a mechanism for controlling the access of programs, processes, or users to the resources defined by a computer system. To distinguish between protection and security, which is a measure of confidence that the integrity of a system and its data will be preserved. The chapter focused on protection and discussed the goals and principles of protection in a modern computer system. I’m better prepared to explain how protection domains, combined with an access matrix, are used to specify the resources a process may access. To examine capability-based and language-based protection systems. We examined ways in which resources may be accidentally or purposely misused. We then looked at mechanisms to guard against or detect attacks. Also discussed security threats and attacks in greater details. Learned about the fundamentals of encryption, authentication, and hashing. Examined the uses of cryptography in computing and described various countermeasures to security attacks.