**System Protection**

1. In a ring-protection system, level 0 has the greatest access to objects, and level n (where n > 0) has fewer access rights. The access rights of a program at a particular level in the ring structure are considered a set of capabilities. What is the relationship between the capabilities ofa domain at level j and a domain at level i to an object (for j >i)?
   * Domain "j" is a smaller set inside of Domain "i".
2. What protection problems may arise if a shared stack is used forparameter passing?

* Add a counter and have it increase for that object after it is accessed. Before accessing an object check the counter.

1. If all the access rights to an object are deleted, the object can no longer be accessed. At this point, the object should also be deleted, and the space it occupies should be returned to the system. Suggest an efficient implementation of this scheme.
   * Reference counts
2. Why is it difficult to protect a system in which users are allowed to do their own I/O?

* Any time we give control over to users we run the risk of them messing something up. As far as using hardware and processes for I/O operations there is a lot of management that needs to be done to make sure that each process and hardware piece is being used properly. If users have free use of I/O operations then we run the risk of tasks not being completed in the order that they should be, and also the integrity of the entire system being compromised.
* In earlier chapters we identified a distinction between kernel and usermode where kernel mode is used for carrying out privileged operationssuch as I/O. One reason why I/O must be performed in kernel modeis that I/O requires accessing the hardware and proper access to thehardware is necessary for system integrity. If we allow users to performtheir own I/O, we cannot guarantee system integrity

1. Consider a computing environment where a process is given the privilege of accessing an object only n times. Suggest a scheme forimplementing this policy.

* Add an integer counter with the capability

**System Security**

1. What are the four levels where security measures must be taken?

Security must occur at four levels to be effective:

Physical

Human

Avoid social engineering, phishing, dumpster diving

Operating System

Network

1. What is the most common technique for security attacks?

Masquerading - one participant in a communication pretends to be someone else (another host or person).

1. Provide examples of at least three program threats.

1. Trojan Horse

2. Trap Door

3. Logic Bomb

4. Stack and Buffer Overflow

5. Viruses

1. Provide examples of at least two system and network threats.

1. Worms

2. Port Scanning

3. DOS

1. Make a list of six security concerns for a bank’s computer system. For each item on your list, state whether this concern relates to physical, human, or operating-system security.

The system should be located in a safe location - Physical

The location of the system should be wellguarded - Human

All operations should be recorded in a logsystem - Operating System, Human

Backup the system frequency - Human

The backup medias need to be protected - Human

The operating system needs to be updatedfrequency for fixing the bugs - Operating system, Human

Other security concerns related to bank computer system are:

1. Data Breach:This is the most dangerous and most common security concern.Data can be leaked out by internal intruders or some external factors. This is basically related to physical security.

2. DDOS: Distributes Denial Of Service is the attack when computers are made unreachable on internet by keeping them busy handling fake server requests. suppose a hacker can easily make server busy handling fake requests.