**Operating System - Assignment - 6**

***Q.1 Suppose the following disk request sequence (track numbers) for a disk with 100 tracks is given: 45, 20, 90, 10, 50, 60, 80, 25, 70. Assume that the initial position of the R/W head is on track 50. What is the distance that will be traversed by the R/W head when***

***a. the Shortest Seek Time First (SSTF) algorithm is used***

***b. the SCAN (Elevator) algorithm (assuming that SCAN algorithm moves towards 100 when it starts execution).***

**Answer:**

1. Given a disk with 100 tracks And Sequence 45, 20, 90, 10, 50, 60, 80, 25, 70.

Initial position of the R/W head is on track 50.

In SSTF, requests are served as following

|  |  |
| --- | --- |
| **Next Served** | **Distance Traveled** |
| 50 | 0 |
| 45 | 5 |
| 60 | 15 |
| 70 | 10 |
| 80 | 10 |
| 90 | 10 |
| 25 | 65 |
| 20 | 5 |
| 10 | 10 |

Total Distance = 130

1. If Simple SCAN is used, requests are served as following

|  |  |
| --- | --- |
| **Next Served** | **Distance Traveled** |
| 50 | 0 |
| 60 | 10 |
| 70 | 10 |
| 80 | 10 |
| 90 | 10 |
| 45 | 65 |
| 25 | 20 |
| 20 | 5 |
| 10 | 10 |

Total Distance = 140

***Q.2 What are the main differences between capability lists and access lists?***

**Answer:**

An access list is a list for each object consisting of the domains with a nonempty set of access rights for that object. A capability list is a list of objects and the operations allowed on those objects for each domain.

***Ques 3: (a) Discuss the strengths and weaknesses of implementing an access matrix using access lists that are associated with objects.***

**Answer:** The strength of storing an access list with each object is the control that comes from storing the access privileges along with each object, thereby allowing the object to revoke or expand the access privileges in a localized manner. The weakness with associating access lists is the overhead of checking whether the requesting domain appears on the access list. This check would be expensive and needs to be performed every time the object is accessed.

***(b)Discuss the strengths and weaknesses of implementing an access matrix using capabilities that are associated with domains.***

**Answer:** Capabilities associated with domains provide substantial flexibility and faster access to objects. When a domain presents a capability, the system just needs to check the authenticity of the capability and that could be performed efficiently. Capabilities could also be passed around from one domain to another domain with great ease allowing for a system with a great amount of flexibility.

However, the flexibility comes at the cost of a lack of control; revoking capabilities and restricting the flow of capabilities is a difficult task.

***Ques 4: Explain following concepts clearly:***

***(a) Trojan Horses***

***(b)Polymorphic Viruses***

***(c) Denial of Service Attacks***

**Answer:**

1. A Trojan Horse is a program that secretly performs some maliciousness in addition to its visible actions. Some Trojan horses are deliberately written as such, and others are the result of legitimate programs that have become infected with viruses. Spyware is a version of a Trojan Horse that is often included in "free" software downloaded off the Internet. Spyware programs generate pop-up browser windows, and may also accumulate information about the user and deliver it to some central site
2. A polymorphic virus is a complicated computer virus that affects data types and functions. It is a self-encrypted virus designed to avoid detection by a scanner. Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.

Polymorphism, in computing terms, means that a single definition can be used with varying amounts of data. In order for scanners to detect this type of virus, brute-force programs must be written to combat and detect the polymorphic virus with novel variant configurations.

1. A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.