OPERATING SYSTEM ASSIGNMENT

Submitted by:

(102116122) ANSH MIDHA

BE Second Year (CS12)

Submitted to: Dr. Tanu

Computer Science and Engineering Department

Thapar Institute of Engineering and Technology

November 2022

1. **Define various aspects of Security of/in an OS and list various security Attacks / Program Threats.**

A- The term OS Security refers to measures that ensure confidentiality, integrity and availability (i.e., CIA) of the CPU, memory, disk, software programs and most importantly the information stored on the computer from various threats.

A system is said to secure, if under all circumstances, its resources are used as intended and no unauthorized usage of the system is carried out. But no OS can guarantee absolute safety from these threats.

The security of an OS is considered compromised on any of the following accounts:

- Breach of confidentiality
- Breach of integrity
- Breach of availability
- Theft of service
- Denial of service

Security measures taken by the OS to ensure safety from threats/attacks:

i. Authentication:

Authentication refers to identification of each user of the system and associating the programs they are allowed to execute with them, i.e., matching an existing user with the programs they're allowed to use.

A few of the techniques used to authenticate users at the OS level are:

- Username/password combos
- Security card/keys
- Biometric Signatures- fingerprint, retina, signature scanning
- Multi-factor authentication- Combination of what a user knows (password), and something they own (biometric)

ii. Using OTPs (One Time Passwords):

OTPs add an additional security layer over the pre-existing authentication system, wherein the user has to enter a short randomly generated password every time the try to login to the system. An OTP cannot be reused, hence the name.

OTPs can be implemented using any of the following measures:

- Network passwords- OTP sent over the network, to a registered contact number or a registered email address.
- Random keys- The users are handed out a hardware device (mostly a card) with random key value mappings (letters-numbers). The OS asks the user to enter the numbers corresponding to a random set of letters generated at the time of login.
- Secret keys- The user receives a secret key that is not to be shared. The OS asks for this key when a login attempt is made and matches it with user credentials to whom the key has been allotted.

iii. Virtualization:

Virtualization enables us to abstract software from hardware, ultimately separating the two, resulting in high level of flexibility and efficiency. There exist many types of virtualizations including desktop, application, network, server, storage and OS virtualization.

OS virtualization allows us to use various isolated user environments using the same OS kernel. This is enabled which the help of a tool called “hypervisor” which effectively separates the actual device from the virtual environments.

There are several types of VMs (Virtual Machines) that can run alongside each other. Here are the three major categories:

- Fully locked down VM: provide access to sensitive content
- Unlocked VM: provide access to unrestricted content
- Semi locked down VM: provide access to standard applications and resources

Types of Program threats:

i. Virus – The most infamous threat, it can replicate itself on the computer system. Highly dangerous, they can modify/delete user files, crash systems.

ii. Trojan Horse – Trojan horses are programs that trap user credentials like the username and password, which are later sent to a malicious user who can then log into the system and access resources.

iii. Trap Door – When a legitimate program has a security hole in its code and performs illegal action without the knowledge of the user, it is called as a trap door.

iv. Logic Bomb – A modified trap door, a logic bomb misbehaves only when certain prerequisites are met. Otherwise, it behaves as a genuine program, thus making it harder to detect.

v. Worm – A type of malware that replicates itself and infects other computers while remaining active on the host computer too. Frequently overlooked until their replication depletes system resources, slowing/stopping other activities.

Types of System threats:

i. Worm – Explained above

ii. Port Scanning – A hacker detects system vulnerabilities in order to make an attack on the system with this technique.

iii. Denial of Service – DoS attacks usually prevent the user from making legitimate use of the system resources.

2. Explain various categories of viruses (related to Operating systems).

A- A computer virus is a program embedded inside another, created with the ability to self-replicate, infecting other programs in the process. It is developed to spread from one host to another and there are numerous ways on how your computer is affected. It can be through email attachments, file downloads, software installations, or unsecured links.

Cybercriminals are getting better at stealing our confidential data, developing every virus better than the previous one. Every virus has a payload that performs an action. These actions range from innocuous pranks that don't do any harm, to causing damage to the system and its data.

The major types of computer viruses are:

- File Virus – This type of virus attaches itself to an executable program. It is parasitic virus, which infects files with .exe or .com extensions. It resembles a parasite, where it leaves no file intact but keeps the host functional. It works by appending itself to the end of the e=file and changing the start of the program so that the control jumps to it as soon as execution begins. After the execution of its code, the control return to the main code.
- Boot Sector Virus – This type of virus affects the MBR of the computer, executed every time the system is booted and OS is loaded. It enables malicious control over the computer. One of the easier viruses to avoid, it hides out in a file on a USB or email attachment.
- Macro Virus – Unlike most viruses written in low-level programming languages (C or assembly), macro viruses are written in high-level programming languages (Visual Basic). Macro viruses deliver a payload when the file is opened, and the macro is run.
- Source Code Virus – This virus looks for the source of the program, and modifies it to include virus and to help spread it.
- Polymorphic Virus – Most antiviruses recognise viruses based on their virus signatures. Thus, to avoid recognition and detection, a polymorphic virus changes its virus signature each time it is installed, but the functionality remains the same.
- Encrypted Virus – To avoid detection by antivirus, this virus exists in encrypted form. Its code includes the decryption algorithm, so it first decrypts itself and then executes.

- Stealth Virus – It is a smart virus which changes the code that can be used to detect it. For example, it changes the read system call so that the original file is shown rather than the infected one.
- Tunnelling Virus – To bypass detection by antivirus, this virus loads itself in the interrupt handler chain. Thus, the interception programs which remain in the background of an OS and catch viruses, become disabled.
- Multipartite Virus – This is a very infectious virus which can affect multiple parts of the system including boot sector, memory, files, etc. This makes it difficult to contain.
- Armoured Virus – This kind of virus is made of code difficult for the antivirus to unravel and understand. It uses a variety of techniques like using a fake location, or using compression to complicate itself.
- Resident Virus – Resident viruses install onto the RAM and meddle together with the device operations. They're so sneaky that they can even attach to the antivirus software files. It stays dormant until a certain time, or until the user performs a certain task.
- Direct action – When a seemingly safe file is executed, a direct-action virus delivers a payload immediately. They can also lay dormant until a specific action is carried out or a certain timeframe passes. It targets a special file type, commonly .exe files by replicating and infecting files. Due to its targeted nature, this virus type is easier to detect and get rid of.

3. Describe various Security Defences including Firewalling systems to Protect Systems and Networks.

A- Network security includes all steps taken to protect the confidentiality, integrity and availability of the computer network and the data within it. It is important since it safeguards sensitive data from cyber-attacks and keeps the network usable and ensures the safety of the network.

Network security is critical because it keeps cyber criminals from accessing our resources and data, because if they do get a hold of it, a variety of problems can be caused.

- Operational risks – An enterprise without the necessary network security measures risks being disrupted by its own operations, since these networks depend on devices and software that malfunction when compromised by viruses, or malware.
- Financial risks for Personally Identifiable Information – As evident, data breaches are expensive, both for the individual and the organisation. Thus, organizations that handle sensitive personal information should be well equipped with network security measures. Data breaches can ruin a company's reputation and expose it to lawsuits.
- Financial risk for compromised intellectual property – Like personal information, organizations can even have their own intellectual property, which not only costly but also results in loss of a company's ideas, inventions and products which ultimately leads to loss of competitive advantage.
- Regulatory issues – Many governments require an established organization to lie under some prerequisite security protocols which include network security protocols. For example, organizations in the European Union that deal with citizens' data must follow the General Data Protection Regulation (GDPR). Violations of these regulations can lead to fines.

Network security is enforced using a combination of hardware and software tools, wherein the main goal is to prevent unauthorized or malicious access into or over parts of the network. An appointed security official determines the strategies necessary for keeping an organization's network safe. Everyone who has access to this network is required to follow these protocols. The choice of these policies and protocols varies between networks and

change over time. Strong protection usually involves usage of multiple approaches, commonly known as layered security, or defence-in-depth.

- Access control – Limiting the access to network applications and systems to specific user or group of users.
- Antivirus and Antimalware – Software designed to detect, remove and prevent malicious virus or malware attacks.
- Application security – Monitor and protect applications that organizations use to run their business.
- Behavioural analytics – Analyse network behaviour and detect any abnormal activities.
- Cloud security – Cloud service often comes bundled with cloud security tools, where the cloud provider itself manages the security of its infrastructure.
- Data loss prevention – These tools monitor data in use, in motion and at rest to detect and prevent data breaches.
- Email Security – Email is one of the most insecure methods of sending files and sensitive data that employees unwittingly engage in.
- Firewall - Software or firmware inspects incoming and outgoing traffic to prevent unauthorized network access. Firewalls are some of the most widely used security tools. They are positioned in multiple areas on the network. Next-generation firewalls offer increased protection against application-layer attacks and advanced malware defence with inline deep packet inspection.
- Intrusion Detection Systems – An IDS detects unauthorized access attempts and flags them as potentially dangerous.
- Intrusion Prevention Systems – An IPS prevents intrusions by detecting and blocking unauthorized attempts to access the network.
- Mobile device security – Monitoring and controlling which mobile devices have access to the network and what they do once connected is crucial for modern network security.
- Multifactor authentication – Two or more factors to authenticate a user’s identity.

- Network segmentation – Breakage of a large network into small, easy-to-manage segments.
- Sandboxing – Scan for malicious software by opening a file in an isolated environment before giving it access to the network.
- Security information and event management – This technique logs data from applications and networks and monitors for suspicious behaviour.
- Software-defined perimeter – An SDP sits at top of the network and conceals it from attackers and unauthorized users.
- Virtual Private Network – A VPN secures the connection from an endpoint to a company's network. It uses tunnelling protocols to encrypt information sent and received over the network.
- Web security - This practice controls employee web use on an organization's network and devices, including blocking certain threats and websites.

Benefits of network security include:

- Functionality
- Privacy and security
- Intellectual property protection
- Compliance

4. Discuss strategies for Implementing the Access Matrix.

A- Various strategies for implementing the access matrix in the operating system are as follows:

- Global Table – It is the most basic access matrix representation. In this method a set of ordered triplet in the form of < domain, object, rights-set > is maintained in a file. When an operation Q has been performed on an object O and domain D, the table will search for a triplet < D, O, rights-set >. The operation will only proceed if this triplet is found/located, otherwise an exception or error condition will arrive.
- Access Lists for objects – Every access matrix column may be used as a single object's access list. It is possible to delete the blank entries. For each object, the resulting list contains an ordered pair in the form of that define all domains for that object and a non-empty set of access rights. We may start by checking the default set and then find the access list. If the item is found, we enable the action otherwise we verify the default set. If A is the default set, we grant access, otherwise access is denied, and an extraordinary scenario arises. This method refers to column-wise decomposition of access matrix.
- Capability Lists for Domains – A domains capability list is a collection of objects and the actions that can be done on them. A capacity is a name or address that is used to define an object. If you want to perform operation Q1 on object O1, the process will run Q1 while specifying the capability for O1. If the capability is found in possession, then this implies that access is allowed.
- Lock-Key Mechanism – It is a Comparison between the capability list and access list. Each domain has a set of keys that are special bit patterns. On the other hand, each object has a list of locks, which are also special bit patterns. Thus, giving it the name of Lock-Key Mechanism. If a domain has a key that stratifies one of the locks on the object, then only a domain-based could access an object. The process isn't allowed to modify its keys. It is a hybrid of Access Lists and Capabilities. It is represented in the form of tuple as (object o, key k). It indicates that the subject can access the object o using key k. Objects has an access control list in the form of tuple (l, A), it is called a lock entry indicating lock l that can be accessed by modes in the set A. In this method, the system looks for the tuple in the capability list of the subject and if the tuple is not found then

the access will not be permitted. Otherwise, access is only permitted if there exists a lock entry.

- Capabilities: - This method refers to row wise decomposition of the access matrix. The subject is assigned with a tuple in the form of (object a, Manner M [s, object a]) for all the objects a that are allowed to access. These tuples are called the capabilities. If a subject possesses the capability of form (object o, Manner M [s, object o]) then it is allowed to an object o in the manner M [s, object o]. There is no limit to accessing the objects until and unless the subject holds the capacity to access the object. Capabilities contains two fields namely,

  a) Object Descriptor: - It may contain the address of the objects. Since it contains address, it may be used as an addressing mechanism, i.e., it may be used to find objects.

  b) Access Rights: - Access rights contain the rights that the subject has on object such as read, write and execute.

5. Explain different techniques for Free-Space Management under Disk management.

A- There exists a system software in OS, called file management system, which is the one that manipulates and keeps track of free spaces for allocation and de-allocation of memory blocks to files. The record of free available blocks is called free space list. Whenever a new file is created, it searches the free space list for required space, to the contrary, when a file is deleted, its allotted space is freed and is added to the free space list.

Since the memory is a complex component of the system, it is not easy for the OS to allocate and de-allocate memory blocks freely. Thus, it uses various techniques, methods, and structures for adding and freeing up the space, implemented into the free space list itself.

- Bitmap or Bit Vector – It is one of the most frequently used methods to implement the free space list. A bitmap or bit vector corresponds to a series of bits where each bit represents a disk block. The bits as usual can take two values: 1, meaning a free block, and 0, meaning an occupied block.

  PROs:

  - Simple and easy to understand
  - Consumes less memory
  - It is efficient to find free space

  CONs:

  - The OS goes through all the blocks until it finds a free block.
  - It is not efficient when the disk size is large

- Linked List – This is another approach of implementing the free space list. Here this approach suggests keeping all the free blocks in the memory linked together in a linked list with the stored head pointer corresponding to the first free block. Whenever a block is allocated, its head pointer is shifted to the next block similarly a new block is appended to the list when an occupied block is freed.

PROs:

- Available space is used efficiently
- New free space can be added easily

CONs:

- The overhead of maintaining the head pointer
- not efficient when we need to reach every block of memory

- Counting – In this approach, an entry in the free space includes two parameters- “address of first free disk block (in the form of a pointer)” and “a number n which correspond to the number of free contiguous disk blocks that follow the first one”.

  PROs:

  - A bunch of free blocks take place very fast
  - The list is smaller in size

  CONs:

  - The first free block requires more space

- Grouping – A modification of linked list approach, in this technique, the addresses of the free blocks is stored in the first free block. Here, the first block stores addresses of n blocks out of which n-1 blocks are actually free and the last block stores the addresses of next free n blocks.

  PROs:

  - Addresses of large number of free blocks can be located easily and quickly.

  CONs:

  - The entire list is to be changed if one block is occupied.

REFERENCES:

[1]- www.tutorialspoint.com

[2]- www.hysolate.com

[3]- www.geeksforgeeks.com

[4]- www.uniserveit.com

[5]- www.hightouchtechnologies.com

[6]- www.proofpoint.com

[7]- www.imperva.com

[8]- www.us.norton.com

[9]- www.techtarget.com

[10]- www.javatpoint.com

[11]- www.scaler.com