Confidentiality Policies

UNIT - 2

Confidentiality Policies

- A confidentiality policy is a security policy dealing only with confidentiality.
- Confidentiality is one of the factors of privacy, an issue recognized in the laws of many government entities.
- It put constraint on what information can legally be obtained from individuals. Also it place constraints on the disclosure and use of that information.
- Unauthorized disclosure can result in penalties that include jail or fines.
- Confidentiality policies place no trust in objects.
- The policy statement dictates whether that object can be disclosed. It says nothing about whether the object should be believed

Goal

- To maintain an outline for the management and administration of network.
- To protect an organisation's computing resources
- To eliminate legal liabilities arising from workers or third parties.
- To prevent wastage of company's computing resources
- To prevent unauthorised modifications of the data .

Discretionary Access Control (DAC)

- Discretionary access control (DAC) is a type of security access Control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects.
- DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password.
- In DAC, each system object has an owner, and each initial object Owner is the subject that causes its creation.
- DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

Mandatory Access Control (MAC).

1. Mandatory Access Control (MAC) is a type of access control by which the operating system constraints the ability of a subject to access or perform some sort of operation on an object.
2. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.
3. Mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret.
4. Each user and device on the system is assigned a similar classification and clearance level.
5. When a person or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted.

The advantage and disadvantages of DAC and MAC ?

Advantages of Discretionary Access Control (DAC):

a. Intuitive

b. Easy to implement

Disadvantages of Discretionary Access Control (DAC) :

a. Inherent vulnerability

b. Maintenance of ACL (Access Control List) of capability lists

c. Maintenance of Grant/Revoke.

Advantages of Mandatory Access Control (MAC):

a. Ensure a high degree of protection; prevent any illegal flow of information.

b. Suitable for military and high security types of applications.

Disadvantages of Mandatory Access Control (MAC) :

a. Require strict classification of subjects and objects

b. Applicable to few environments.

Confinement principle

1. The confinement principle is the principle of preventing a server from leaking information that the user of the service considers confidential.

2. The confinement principle deals with preventing a process from taking disallowed actions.

3. Consider a client/server situation: the client sends a data request to the server; the server uses the data, performs some function, and sends the results (data) back to the client.

4. In confinement principle, access control affects the function of the server in two ways:

- a. Goal of service provider : The server must ensure that the resources it accesses on behalf of the client include only those resources that the client is authorized to access.
- b. Goal of the service user: The server must ensure that it does not reveal the client's data to any other entity which is not authorized to see the client's data.

Error 404 digital hacking in India part 2 chase

- In error 404 digital hacking in India part 2 chase experts discuss about some attack related to cyber attack and the attacker can control the overall system if proper security is not provided to the system.
- Israel's power grid hit by a big hack attack. It is one of the worst cyber attacks ever.
- In 2014 a hydropower plant in upstate New York got hacked.
- Iran's infrastructure including its main nuclear power plant is being targeted by a new and dangerous powerful cyber worm.
- Bangladesh best group hacked into nearly 20,000 Indian website including the Indian Border Security Force.
- First virus that could crash power grid or destroy pipeline is available online for anyone to download and tinker with.
- India's biggest data breach when the SBI debit card branch happens. When this happened bank where initially in a state of denial but subsequently they had to own up cyber security breach that took place in Indian history.

Rootkit

- **A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence.**
- **Rootkit is a collection of tools that enabled administrator-level access to a computer or network.**
- **Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tools**
- **Rootkits are generally associated with malware such as Trojans, worms viruses that conceal their existence and actions from users and other system processes.**
- **A rootkit allows us to maintain command and control overa computer without the computer user/owner knowing about it.**

- **Purpose of rootkits:**
- The purpose of a rootkit is for a malware to give its owner, a (often) permanent, hidden remote access to our computer.
- To avoid detection, they tamper with the system to conceal the presence of the malware (for example, hide files) and its activities (for example running processes).
- **Examples of rootkits:**
- NT Rootkit: One of the first malicious rootkits targeted at Windows OS.
- Hacker Defender: This early Trojan altered/augmented the OS at a very low level of functions calls. Machiavelli: The first rootkit targeting Mac OSX. This rootkit creates hidden system calls and kernel threads. Greek wiretapping: This rootkit targeted Ericsson's AXE PBX.

Types

1. Application rootkits:

- Application rootkits replace legitimate files with infected rootkit files on our computer.
- These rootkits infect stand ard programs like Microsoft Office, Notepad, or Paint.
- Attackers can get access to our computer every time we run those programs.
- Antivirus programs can easily detect them since they both operate on the application layer.

2. Kernel rootkits:

- Attackers use these rootkits to change the functionality of an operating system by inserting malicious code into it.
- This gives them the opportunity to easily steal personal information.

3. Bootloader rootkits

- The bootloader mechanism is responsible for loading the operating system on a computer.
- These rootkits replace the original bootloader with an infected one. This means that bootloader rootkits are active even before the operating system is fully loaded.

4. Hardware and firmware rootkits:

- This kind of rootkit can get access to a computer's BIOS system or hard drives as well as routers, memory chips, and network cards.

5. Virtualized rootkits

- Virtualized rootkits take advantage of virtual machines in order to control operating systems.
- These rootkits create a virtual machine before the operating system loads, and then simply take over control of our computer.
- Virtualized rootkits operate at a higher level than operating systems, which makes them almost undetectable.
- **How can we prevent rootkits ?**

1. Avoid opening suspicious emails.
2. Avoid downloading cracked software.
3. Install software updates:
4. Anti-malware software prevents varieties of malware.

Detour used in Unix user ids and process ids.

- 1 Detour is defined as few words about Unix user IDs and IDs associated with Unix processes.
- 2. Every user in Unix like operating system is identified by different integer number, this unique number is called as UserID.
- 3.There are three types of UID defined for a process, which can be dynamically changed as per the privilege of task.
- **The three different types of UIDs defined are**
- **Real UserID**: It is account of owner of this process. It defines which files that this process has access to.
- **Effective UserID** : It is normally same as real User ID, but sometimes it is changed to enable a non-privileged user to accese files that can only be accessed by root
- **Saved UserID**: It is used when a process is running with elevated privileges (generally root) needs to do some under-privileged work, this can be achieved by temporarily switching to non-privileged account.

Intrusion Detection System (IDS) ?

- An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
- Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms

Security Hard

- **Today in computers and on the internet attack is easier than defense There are many reasons for this, but the most important is the complexity of these systems.**
- **Complexity is the worst enemy of security. The more complex a system is, the less secure it is**
- **A hacker typically targets the "attack surface" of a system. The attack surface of a system contains all the possible points that a hacker might target.**
- **A complex system means a large attack surface, and that means a huge advantage for the hacker.**

Access control list

- An access-control list is a list of permissions attached to an object.
- An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
- Each entry in a typical ACL specifies a subject and an operation.

Access control technology includes:

1. Access Technology Architectures
2. Communications technologies
3. Authentication technologies
4. Infrastructure technologies

Software Fault Isolation (SFI)

- **Goal and solution**
- Software Fault Isolation (SFD is an alternative for unsafe languages, example C, where memory safety is not granted but needs to be enforced at runtime by program instrumentatioon.
- SFI is a program transformation which confines a software component to a memory sandbox. This is done by pre-fixing every memory access with a carefully designed code sequence which efficiently ensures that the memory access occurs within the sandbox.
- **SFI approach:**
- Traditionally, the SFI transformation is performed at the binary level and is followed by an a posteriori verification by a trusted SFI verifier.
- Because the verifier can assume that the code has undergone the SFI transformation, it can be kept simple, thereby reducing both verification time and the Trusted Computing Base.
- This approach is a simple instance of Proof Carrying Code where the complier is untrusted and the binary verifier is either trusted or verified.
- Traditional SFI is well suited for executing binary code from an untrusted origin.

VM Based Isolation

- A VM is an isolated environment with access to a subset of physical resources of the computer system.
- Each VM appears to be running on the bare hardware, giving the appearance of multiple instances of the same computer, though all are supported by a single physical system.
- A process VM is a virtual platform created for an individual process and destroyed once the process terminates.
- Virtually all operating systems provide a process VM for each one of the applications running, but the more interesting process VMs are those which support binaries compiled on a different instruction set.
- A system VM supports an OS together with many user processes. When the VM runs under the control of a normal OS and provides a platform- independent host for a single application we have an application VM, for example, Java Virtual Machine (JVM).

- Made By : - AKTU WALA (Satyam Sahu)