Unit-8

Security Management

Introduction

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.

OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Creating secure accounts with required privileges only (i.e., user management)

Security problems

Security must consider external environment of the system and protect the system resources. Crackers attempt to break security. Threat is potential security violation. Attack can be accidental or malicious. Easier to protect against accidental than malicious misuse. There are various security problems in operating system out of them major security problems are listed below:

- User authentication
- Program threats
- System threats

User authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic.

a. Passwords

The most common approach to authenticating a user identity is the use of passwords. When the user identifies herself by user ID or account name, she is asked for a password. If the user-supplied password matches the password stored in the system, the system assumes that the account is being accessed by the owner of that account. Passwords are often used to protect objects in the computer system, in the absence of more complete protection schemes.

They can be considered a special case of either keys or capabilities. For instance, a password could be associated with each resource (such as a file). Whenever a request is made to use the resource, the password must be given. If the password is correct, access is granted. Different passwords may be associated with different access rights.

For example, different passwords may be used for reading files, appending files, and updating files. In practice, most systems require only one password for a user to gain full rights. Although more passwords theoretically would be more secure, such systems tend not to be implemented due to the classic trade-off between security and convenience. If security makes something inconvenient, then the security is frequently bypassed or otherwise circumvented.

b. Password Vulnerabilites

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Strong protection starts with strong passwords. Use a variety of lowercase and uppercase letters, numbers, characters and symbols; the more jumbled the better. And, be sure to change them every few months. Never use combinations that include personal information or are easy to guess, like the website name, your name, birthday, or social security number. Don't use the same password for more than one account. It seems like the easy choice, but it comes with risks. If a hacker does get into one of your accounts, then they will be able to access all the other ones with the same login.

c. Encrypted Password

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Using one-way encryption formats, user passwords may be encrypted and stored the directory, which prevents clear passwords from being accessed by any users including the system administrators. Using two-way encryption formats, passwords are encrypted while stored in the database, and decrypted when returned to an authorized client. Use of two-way encryption protects the password stored in the database.

d. One Time Password and Biometrics Password

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

e. User Authorizations

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources.

During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

a. Trojan Horse

Trojan horse is a program downloaded and installed on a computer that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.

Typically, the Trojan horse is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware that is hidden inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

The easiest way to protect a system from a Trojan horse is by never opening or downloading emails or attachments from unknown sources. Deleting these messages before opening will delete the Trojan horse threat

b. Trap Door

Trapdoor- is a method of gaining access to some part of a system other than by the normal procedure (e.g. gaining access without having to supply a password). Hackers who successfully penetrate a system may insert trapdoors to allow them entry at a later date, even if the vulnerability that they originally exploited is closed. There have also been instances of system developers leaving debug trapdoors in software, which are then discovered and exploited by hackers.

c. Stack and buffer overflow

A buffer is a temporary area for data storage. When more data (than was originally allocated to be stored) gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.

In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information. Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user’s input. There are two types of buffer overflows: stack based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack: memory space used to store user input.

d. Logic Bomb

A logic bomb is a piece of code inserted into an operating system or software application that implements a malicious function after a certain amount of time, or specific conditions are met. For example a programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company. Logic bombs are often used with viruses, worms, and trojan horses to time them to do maximum damage before being noticed.

System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

a. Worms

A **worm** is a malicious, self-replicating program that can spread throughout a network without human assistance. Worms cause damage similar to viruses, exploiting holes in security software and potentially stealing sensitive information, corrupting files and installing a back door for remote access to the system, among other issues. Worms often utilize large amounts of memory and bandwidth, so affected servers, networks and individual systems are often overloaded and stop responding. But worms are not viruses. Viruses need a host computer or operating system. The worm program operates alone. The worm is often transmitted via file-sharing networks, information-transport features, email attachments or by clicking links to malicious websites. Once downloaded, the worm takes advantage of a weakness in its target system or tricks a user into executing it. Some worms have a phishing component that entices users to run the malicious code.

b. Viruses

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

Different types of viruses are:

1. Boot sector virus
This type of virus can take control when you start — or boot — your computer. One way it can spread is by plugging an infected USB drive into your computer.

2. Web scripting virus
This type of virus exploits the code of web browsers and web pages. If you access such a web page, the virus can infect your computer.

3. Browser hijacker
This type of virus "hijacks" certain web browser functions, and you may be automatically directed to an unintended website.

4. Resident virus
This is a general term for any virus that inserts itself in a computer system's memory. A resident virus can execute anytime when an operating system loads.

5. Direct action virus
This type of virus comes into action when you execute a file containing a virus. Otherwise, it remains dormant.

6. Polymorphic virus
A polymorphic virus changes its code each time an infected file is executed. It does this to evade antivirus programs.

7. File infector virus
This common virus inserts malicious code into executable files — files used to perform certain functions or operations on a system.

8. Multipartite virus
This kind of virus infects and spreads in multiple ways. It can infect both program files and system sectors.

9. Macro virus
Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through email attachments.

A computer virus attack can produce a variety of symptoms. Here are some of them:

- **Frequent pop-up windows.** Pop-ups might encourage you to visit unusual sites. Or they might prod you to download antivirus or other software programs.
- **Changes to your homepage.** Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.
- **Mass emails being sent from your email account.** A criminal may take control of your account or send emails in your name from another infected computer.
- **Frequent crashes.** A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on.
- **Unusually slow computer performance.** A sudden change of processing speed could signal that your computer has a virus.
- **Unknown programs that start up when you turn on your computer.** You may become aware of the unfamiliar program when you start your computer. Or you might notice it by checking your computer's list of active applications.
- **Unusual activities like password changes.** This could prevent you from logging into your computer.

How to protect against computer viruses?

- Use a trusted antivirus product.
- Avoid clicking on any pop-up advertisements.
- Always scan your email attachments before opening them.
- Always scan the files that you download using file sharing programs.
- Update your operating system regularly.
- Increase your browser security settings.
- Don’t open messages from unknown senders.

e. Denial of Services

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.