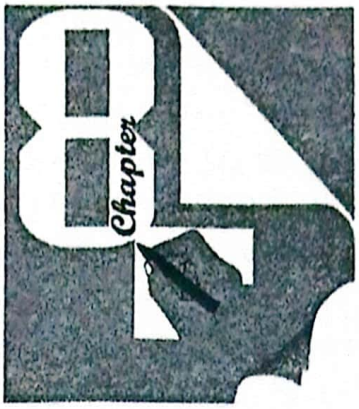

SECURITY MANAGEMENT

CHAPTER OUTLINE

After comprehensive study of this chapter, you will be able to:

- Introduction, Security Problems, User Authentication: Passwords, Password Vulnerabilities, Encrypted Password, One Time Password and Biometrics Password
- User Authorizations, Program Threats: Trojan Horse, Trap Door, Stack and Buffer Overflow
- System Threats: Worms Viruses, Denial of Services.

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 etc.

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

User need to enter a registered username and password with Operating system to login into the system.

b. Password Vulnerabilities

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'll 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 in 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 passwords 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 the function of specifying access rights/privileges to resources, which is related to information security and computer security in general and to access control in particular.

Authorization is also interested in who the user is, but is used to determine what functions, actions, data, or other parts of an application the user has access. Authorization answers the question 'what can you do?' It's not a requirement for a user that's been authenticated to also be authorized. An unauthenticated user may have some access to an application, although usually in a very limited capacity.

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 examples 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.

- Trojan Horse
- Trap Door
- Stack and buffer overflow
- Logic Bombetc.

a. **Trojan horse**

A 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.

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.

In brief a trap door is a secret entry point into a program that allows someone to gain access without normal methods of access authentication.

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 intentionally inserted into a software system that will set off a malicious function when specified 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.

System Threats

A system threat 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 create such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- Worm
- Viruses
- Port Scanning
- Denial of Service etc.

a. **Worms**

A computer worm is a malicious, self-replicating software program (popularly termed as malware) which affects the functions of software and hardware programs.

Worms don't need a host program in order for them to run, self-replicate and propagate. Once a worm has made its way onto our system, usually via a network connection or as a downloaded file, it can then make multiple copies of itself and spread via the network or internet connection infecting any inadequately-protected computers and servers on the network. Because each subsequent copy of a network worm can also self-replicate, infections can spread very rapidly via the internet and computer networks.

b. **Viruses**

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.

What are the symptoms of a computer virus?

The computer may be infected if we recognize any of these malware symptoms:

- Slow computer performance
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

How to protect against computer viruses?

When you arm yourself with information and resources, you're wiser about computer security threats and less vulnerable to threat tactics. Take these steps to safeguard your PC with the best computer virus protection:

- Use antivirus protection and a firewall
- Get antispyware software
- Always keep your antivirus protection and antispyware software up-to-date
- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Web sites
- Only download software from sites you trust.
- Carefully evaluate free software and file-sharing applications before downloading them.
- Don't open messages from unknown senders
- Immediately delete messages you suspect to be spam

c. **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.

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

EXERCISE

Multiple Choice Questions

What is not an important part of security protection?

a) Large amount of RAM to support antivirus
b) Strong passwords
c) Audit log periodically
d) Scan for unauthorized programs in system directories

2. What is used to protect network from outside internet access?
   a) A trusted antivirus
   b) 24 hours scanning for virus
   c) Firewall to separate trusted and un-trusted network
   d) Deny users access to websites which can potentially cause security leak

3. How do viruses avoid basic pattern match of antivirus?
   a) They are encrypted
   b) they act with special permissions
   c) They modify themselves
   d) none of the mentioned

4. How does an antivirus of today identify viruses?
   a) Previously known patterns
   b) It can detect unknown patterns
   c) It can take high priority to increase scanning speed
   d) None of the mentioned

5. What is are two safe computing practices?
   a) Not to open software from unknown vendors
   b) Open and execute programs in admin level/root
   c) Open and execute programs in presence of antivirus
   d) None of the mentioned

6. What are the common security threats?
   a) File Shredding
   b) File sharing and permission
   c) File corrupting
   d) File integrity

7. Which of the following is the least secure method of authentication?
   a) Key card
   b) fingerprint
   c) Retina pattern
   d) Password

8. Why is one time password safe?
   a) It is easy to generated
   b) it cannot be shared
   c) It is different for every access
   d) it is a complex encrypted password

9. Which happens first authorization or authentication?
   a) Authorization
   b) Authentication
   c) Authorization & Authentication are same
   d) none of the mentioned

10. What is not a best practice for password policy?
   a) Deciding maximum age of password
   b) Restriction on password reuse and history
   c) Password encryption
   d) Having change password every 2 years

Subjective Questions

1. How to secure operating system? Explain.
2. Define security problems in Os with suitable example.
3. What do you mean by user Authentication? Explain various user authentication methods with example.
4. What is Password Vulnerabilities? Explain.
5. How can you Encrypted Password? Explain.
6. What is one Time Password? Explain their advantages.
7. What is Biometrics Password? Explain.
8. What is User Authorizations? How it is differ from user authentication?
9. What is Program Threats? Explain various program threats in brief.
10. Define Trojan horse and Trap Door with their advantages.
11. What do you mean by Buffer Overflow? Explain.
12. What is System Threats? Explain various system threats with example.
13. Compare Worms and Viruses.
14. What do you mean by denial of Services in OS?
15. How to secure your system? Explain.
16. What is virus? Explain their properties.
17. Define Trap door with suitable example.
18. Define Trojan horse in detail.
19. What is the use of anti-virus? Explain.
20. Explain in detailed about buffer overflow.

ANSWERS KEY

1. (a)	2. (c)	3. (c)	4. (a)	5. (a)	6. (b)	7. (d)	8. (c)	9. (a)	10. (d)

❑❑❑