BCA
Fourth Semester
“ Operating System“

Security Management

- 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 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.

Security Problem

- The operating system can allow users to protect their resources. We say that a system is secure if its resources are used and accessed as intended under all circumstances.
- Unfortunately, it is not generally possible to achieve total security.
- Security violations of the system can be categorized as being either intentional(malicious) or accidental.
- Among the forms of malicious access are the following:

Unauthorized reading of data (theft of information).

- Unauthorized modification of data.
- Unauthorized destruction of data.

Security Problem Contd…

- To protect the system, we must take security measures at various levels:

Physical – The site containing the computer system must be physically secured against the suspicious entry. E.g. protection of Data centers, servers, connected terminals.

Human – Proper user authorization, Avoid social engineering, phishing, dumpster diving. E.g a legimate looking e-mail, web page, finding phone books, finding hints of passwords etc.

Operating System – Protect from accidental or purposeful security breaches, protection mechanisms, debugging, updating etc. (finding possible breaches is endless)

Network – Most data today travels over the shared lines like internet, wireless, lease lines etc.

Password Vulnerabilities

Encryption Password

Encryption password is one common method of protecting information transmitted over unreliable links.

The basic mechanism works as follows.

1. The information (text) is encrypted (encoded) from its initial readable

form (called clear text), to an internal form (called cipher text). This internal text form, although readable, does not make any sense.

2. The cipher text can be stored in a readable file, or transmitted over unprotected channels.

3. To make sense of the cipher text, the receiver must decrypt (decode) it back into clear text.

Even if the encrypted information is accessed by an unauthorized person or program, it will be useless unless it can be decoded.

- Encryption algorithm consists of

Set of K keys.

Set of M Messages.

Set of C cipher texts (encrypted messages).

Encryption Password Contd…

- A function E : K → (M→C). That is, for each k € K, E(k) is a function for generating cipher texts from messages.
- Both E and E(k) for any k should be efficiently computable functions.
- A function D : K → (C → M). That is, for each k € K, D(k) is a function for generating messages from cipher texts.
- Both D and D(k) for any k should be efficiently computable functions.
- An encryption algorithm must provide this essential property: Given a

  Cipher text c € C, a computer can compute m such that E(k)(m) = c only if it possesses D(k).
- Thus, a computer holding D(k) can decrypt cipher texts to the plain texts used to produce them, but a computer not holding D(k) cannot decrypt cipher texts.
- Since cipher texts are generally exposed (for example, sent on the network), it is important that it be infeasible to derive D(k) from the cipher texts.

Authentication

Authentication refers to identifying the 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. Operating Systems generally identifies/authenticates users using following three ways:

- **Username / Password** - User need to enter a registered username and password with Operating system to login into the system.
- **User card/key** - User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- **User attribute - fingerprint/ eye retina pattern/ signature** - User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords

One time passwords provides 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 password to user on registered mobile/ email which is required to be entered prior to login.

Biometric Password

User Authorization

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** - Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- **Trap Door** - If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- **Logic Bomb** - Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- **Virus** - Virus as name suggests can replicate them on computer system .They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

- **Program Threats:**

Stack and Buffer Overflow

System Threats

System threats refer 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 mis-used. Following is the list of some well-known system threats.

- **Worm** -Worm is a process which can choke down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worm processes can even shut down an entire network.

- **Port Scanning** - Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.

- **Denial of Service** - Denial of service attacks normally prevents user to make legitimate use of the system. For example user may not be able to use internet if denial of service attacks browser's content settings.

END