CSC 223 Principles of OS

OS Security and Protection

- Security is keeping unauthorized entities from doing things you don’t want them to do.
- In computing Security refers to providing a protection to computer system resources such as:
- CPU
- memory
- disk
- software programs
- Most importantly data/information stored in the computer system.

- Unauthorized users may cause severe damage to computer or data stored in it.
- Therefore, computer system must be protected against;
  - unauthorized access
- malicious access to system memory
  - viruses
  - worms

Components of Security

- *Authentication*
- *Prevention*
- *Detection*
- *Correction*
- *Identification*
- *Program Threats*
- *System Threats*
- *Computer Security Classifications*

1. Authentication

- Authentication refers to identifying the each user of the system and associating them with executing programs.
- Alternatively, it is the proof of the identity of a user logging on to some network.
- The Operating System creates 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:

1. **User knowledge**

This can be a **Username and Password** - User need to enter a registered username and password with Operating system to login into the system.

2. **User possession(physical authentication)** – this can be a **User card or key, the** User needs to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

3. **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.
- Valid for only one log in session or transaction – avoids short comings associated with traditional passwords.
- 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.

2. **Prevention**

- The most desirable outcome of the operating system for preventing intruders from successfully penetrating into the system security.
- Preventive measures include:

Preventive measures include:

- Limiting new passwords to those that pass a quality checks.
- check a password length
- diversity of characters
- Passwords to be changed at periodic intervals. Example Equity 24/7 passwords
- Encrypting data, either when transmitted or stored.

- Turing off unused or duplicated services. Reducing the number of system entry points that will intern reduce the probability of finding an entry point. Achieved through logging out.
- Implementing an internal firewall example configure programs to denied network access.
- Monitor security advisories, updating software and configuration of information as needed. OS provides information on security vulnerabilities and how to fix them.

3. Detection

- Effective detection may discourage intrusion attempts. The ability to check, identify and reduce intrusion effects Constant monitoring provides the best hope for fast discovery.
-

Methods of detection:

- The OS provides auditing systems that record information about system events.
- For instance the time and user involved in each system login can be logged. Monitoring of system activities can detect unusual activities.
- OS provides virus checkers to search the contents of the files and boot programs for the presence of known abnormalities.

- The existence of a long- running process in a list of currently executing processes may indicate suspicious activity.
- The current state of the system can be checked against the previous state(comparing the two states).

4. Correction

- It is necessary to take a corrective action after a system has been penetrated.
- This can be achieved through the following ways:
- Perform periodic(interval) backups to enable to roll back into the previous state
- Allows system to reload/restore/refresh incase the back-up does not exist.

- Is necessary to change all resident security information. I.e. all users to change their password.
- Vulnerability that allows the system to be penetrated should be fixed. I.e. deactivating a service, installing a bug fix or modifying the system configuration.

5. Identification

- It is required to identify the source of an attack to discourage intruders.
- This can be achieved through:
- Use of audit trails which can provide useful information. Provides the record of logged in events.

- Systems accessed through modems can keep track of the sources of incoming calls using caller-rid.
- System accessed through a network can record the address of the connection computer. Attacks related through a series of computers must be traced to their origin.
- All services can be configured to require users authentication

6. Encryption

- Is one common method of protection information transmitted over unreliable links. The basic mechanism work as follows.

1. The information (text) is encrypted from its initial readable form to an internal form
2. The internal form can be stored in a readable file, or transmitted over unprotected channel

3. To make sense of internal form, the receiver must decrypt it back into clear text.

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

7. 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.

- **Trap Door (back door)** –A secret entry point into a program that allow someone who is aware of the back door to gain access without going through the usual security access procedures.
- 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 program inserted into a software by in intruder. It lies dormant until a predefined condition(s) is met; The program then triggers an authorized act.
- Examples-presence of absence of certain files, a particular day of the week/time or a particular user running the application.

- **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.
- **Virus** - Virus as name suggests can replicate itself on a computer system, when it succeeds the code is said to be infected and when the infected code is executed the virus also executes. It’s highly dangerous and can modify/delete user files, crash systems.

8. 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 misused.

Following is the list of some well-known system threats.

- **Worm** –It’s a program that can replicate itself and send copies from computer to computer across network connections.

- **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.

Computer Security Classifications

- As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D.
- This is widely used specifications to determine and model the security of systems and of security solutions