

Security management

Introduction

- Security refers to providing a protection system to computer resources such as CPU, memory, Disk, software program and most importantly data/ information stored in the computer system.
- It must be required to protect the computer system from unauthorized access and run computer program.
- Os security encompasses many different techniques and methods which ensure safety from threats and attacks.
- Os allow different applications and program to perform required tasks and stop unauthorized interference.

Introduction

- Os security may be approached in many ways, including
 - Performing regular OS patch update.
 - Installing updated antivirus engines and software
 - Uses of firewall
 - Creating secure accounts with required privileges only(i.e user management)

Security problem

- Security must consider external environment of the system and protect the system resources.
- Cracker attempt to break security. Threat is potential security violation.
- Attacker can be accidental or malicious.
- Easier to protect against accidental than malicious.
- Major security problem are:
 - User authentication
 - Program threat
 - System threat

User authentication

- Identifying each user of the system and associating the executing programs with those user.
- Responsibility of OS to create a protection system which ensures that a user who is running a particular program is authentic.
- **Password**: need to enter a registered username and password with operating system to login into the system.
- **Password vulnerability**
- **Encrypted password**
- **One time password and biometric password**
- **User authorization**

Program Threats

- If a user program made a process to do malicious task, 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. Some of the well known program threats are:
 - 1) Trojan Horse
 - 2) Trap door
 - 3) Stack and buffer overflow
 - 4) Logic Bomb etc.

System Threat

- A system threat refers to misuse of the system services and network connections to put user in trouble.
- System threat create such an environment that operating system resources/ user files are misused. Some of the well-known system threat are:
 - 1) Worm
 - 2) Viruses
 - 3) Port scanning
 - 4) DOS(denial of service)