AMIRAJ

COLLEGE OF ENGINEERING & TECHNOLOGY

CHAPTER-8
SECURITY & PROTECTION

Subject:- OS **Code:-3140702**	**Prepared by:** **Asst.Prof.Foram Patel** **(Computer Department,ACET)**	AMIRAJ COLLEGE OF ENGINEERING & TECHNOLOGY

SECURITY IN OS

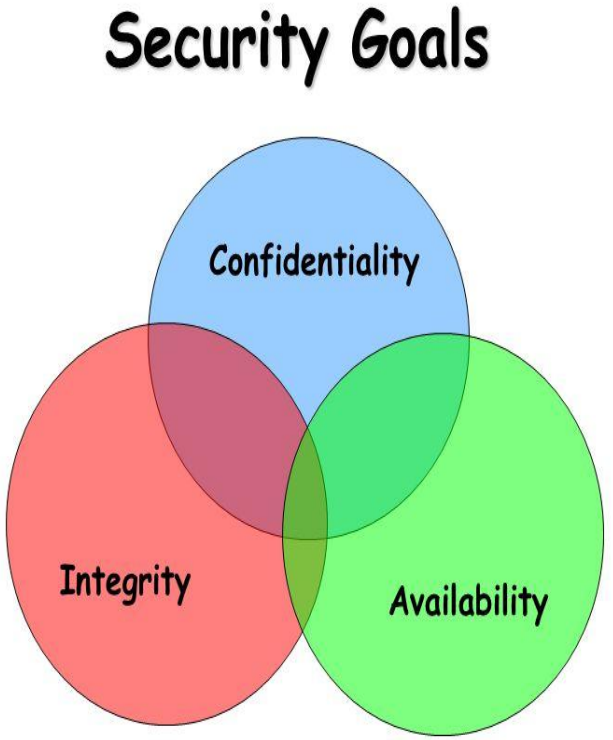
- Interference in resource utilization is a very serious threat in an OS.
- OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.
- Security refers to providing a protection system to computer system resources such 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.
- OS use two sets of techniques to counter threats to information namely: Protection , Security.

PROTECTION AND SECURITY

- Protection and security requires that computer resources such as CPU, softwares, memory etc. are protected.
- This can be done by ensuring integrity, confidentiality and availability in the operating system
- It involves guarding a user's data and programs against interference by other authorized users of the system.
- Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system.
- **Need of Protection:**
- To prevent the access of unauthorized users
- To improve reliability by detecting errors.

SECURITY GOALS

•**Confidentiality:**
•Preventing the disclosure of information to unauthorized users.
• To protect personal privacy and proprietary information.
•**Data integrity:**
•Ensuring the accuracy and authenticity of data.
•The requirement that a computer system's resources can be modified only by authorised parties.
•**Availability:**
• The requirement that a computer system be accessible at required times by authorised parties.



AUTHENTICATION

- Authentication is the process of recognizing a user's identity.
- Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be.
- Authentication means verifying the identity of someone (a user, device, or an entity) who wants to access data, resources, or applications.

ONE TIME PASSWORDS

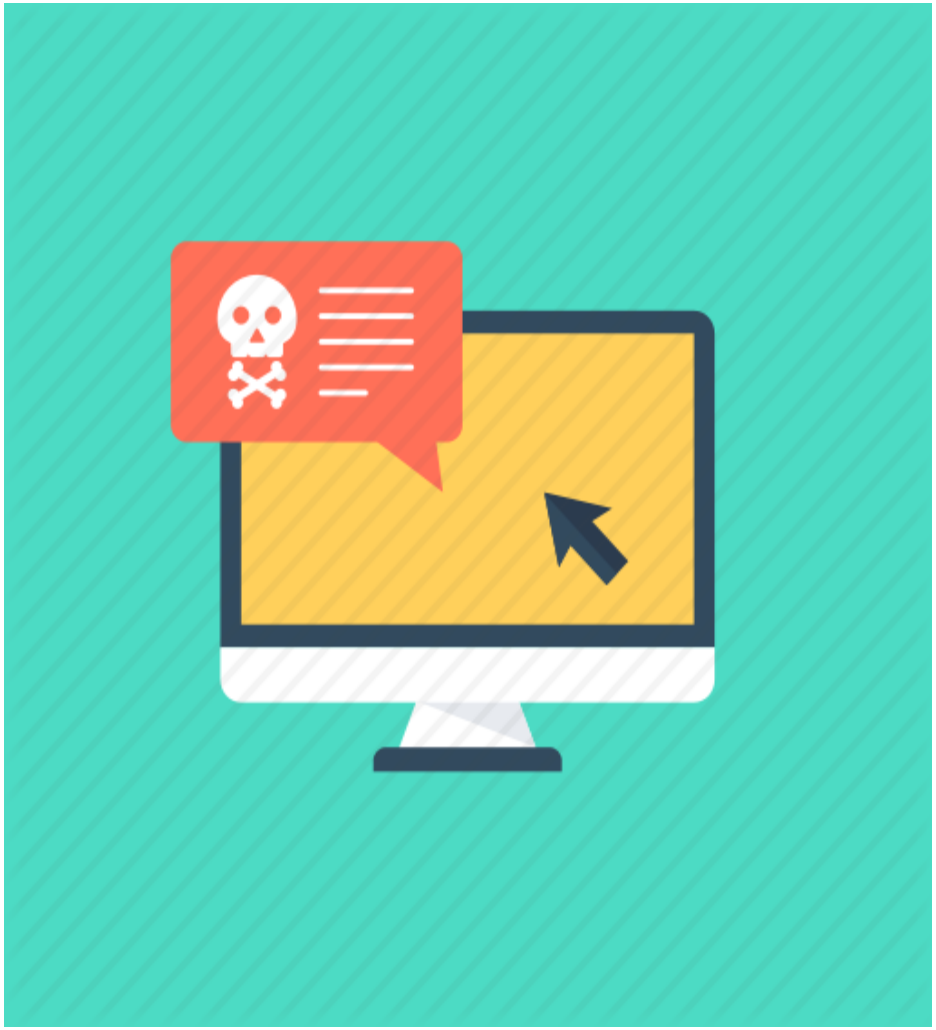
- One time passwords provides additional security along with normal authentication.
- In One-Time Password system, a unique password is required every time user tries to login into the system.
- Once a one-time password is used then it can not be used again.
- **One time password are implemented in various ways.** –
- Random numbers
- Secret key
- Network password

PROGRAM THREATS

- **Trojan horse:**
- Code that misuses its environment
- A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- **Worms:**
- worm is self-replicating malware that duplicates itself to spread to uninfected computers.
- **Virus:**
- Virus are self-replicating and are designed to infect other programs.
- **Trap door:**
- **Logic bomb:**

PROGRAM THREATS

- **Trap door:**
- A computer trapdoor, also known as a back door.
- **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.
- A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.



DESIGN PRINCIPLES OF SECURITY

- Principle of Least Privilege
- Principle of Fail-Safe Defaults
- Principle of Economy of Mechanism
- Principle of Complete Mediation
- Principle of Open Design
- Principle of Separation of Privilege
- Principle of Least Common Mechanism

ACCESS CONTROL LIST

•An access control system determines what rights a particular entity has for a set of objects.

•It answers the question

E.g., do you have the right to read /etc/passwd

•Subjects are the active entities that do things

E.g., you, Alice, students, Dr. Jaeger

• Objects are passive things that things are done to

E.g., /etc/passwd, CSE website, project data, grades

• Operations are actions that are taken

E.g., read, view, share, change

ACCESS MATRIX

•An access control matrix is a table that defines access permissions between specific subjects and objects.

•View protection as a matrix (access matrix) „Rows represent domains „ Columns represent objects „Access(i, j) is the set of operations that a process executing in Domain i can invoke on Objectj.

object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	