OPERATING SYSTEM

PROTECTION & SECURITY

Protection and security require that the computer resources such as CPU, softwares, memory etc. are protected. This extends to the operating system as well as the data in the system. This can be done by ensuring integrity, confidentiality and availability in the operating system. The system must be protected against unauthorized access, viruses, worms etc.

What is the difference between protection and security in operating system?

The main difference between protection and security is that the protection focuses on internal threats in a computer system while security focuses on external threats to a computer system. An operating system provides a mechanism to prevent interference with logical and physical resources.

Comparison Chart

Features	Security	Protection
Basic	Provides the system access to the legitimate users only.	Controls the access to the system resources.
Handles	More complex concerns.	Quite simple queries.
Policy	Describes which person is allowed to use the system.	Specifies what files can be accessed by a particular user.
Type of threat involved	External	Internal
Mechanism	Authentication and encryption are performed.	Set or alter the authorization information.

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)

THREATS TO PROTECTION AND SECURITY

A threat is a program that is malicious in nature and leads to harmful effects for the system. Some of the common threats that occur in a system are:

VIRUS

Viruses are generally small snippets of code embedded in a system. They are very dangerous and can corrupt files, destroy data, crash systems etc. They can also spread further by replicating themselves as required.

Prof. Srijoni Maitra, Bethune College

TROJAN HORSE

A trojan horse can secretly access the login details of a system. Then a malicious user can use these to enter the system as a harmless being and wreak havoc.

TRAP DOOR

A trap door is a security breach that may be present in a system without the knowledge of the users. It can be exploited to harm the data or files in a system by malicious people.

WORM

A worm can destroy a system by using its resources to extreme levels. It can generate multiple copies which claim all the resources and don't allow any other processes to access them. A worm can shut down a whole network in this way.

DENIAL OF SERVICE

These types of attacks do not allow the legitimate users to access a system. It overwhelms the system with requests so it is overwhelmed and cannot work properly for other users.

PROTECTION AND SECURITY METHODS

The different methods that may provide protect and security for different computer systems are:

AUTHENTICATION

This deals with identifying each user in the system and making sure they are who they claim to be. The operating system makes sure that all the users are authenticated before they access the system. The different ways to make sure that the users are authentic are:

- **Username/ Password**

  Each user has a distinct username and password combination and they need to enter it correctly before they can access the system.

- **User Key/ User Card**

  The users need to punch a card into the card slot or use they individual key on a keypad to access the system.

- **User Attribute Identification**

Different user attribute identifications that can be used are fingerprint, eye retina etc. These are unique for each user and are compared with the existing samples in the database. The user can only access the system if there is a match.

ONE TIME PASSWORD

These passwords provide a lot of security for authentication purposes. A one-time password can be generated exclusively for a login every time a user wants to enter the system. It cannot be used more than once. The various ways a one-time password can be implemented are:

- **Random Numbers**

  The system can ask for numbers that correspond to alphabets that are pre-arranged. This combination can be changed each time a login is required.

- **Secret Key**

  A hardware device can create a secret key related to the user id for login. This key can change each time.