CS-3103 : Operating Systems : Sec-A (NB) :
Protection & Security…..

Protection → What is protection in the context of OS ?

- The processes in an operating system must be protected from one another's activities.
- To provide such protection, we can use various mechanisms to ensure that only processes that have gained proper authorization from the operating system can operate on the files, memory segments, CPU, and other resources of a system.
- Protection refers to a mechanism for controlling the access of programs, processes, or users to the resources defined by a computer system.
- This mechanism must provide a means for specifying the controls to be imposed, together with a means of enforcement.
- We distinguish between protection and security, which is a measure of confidence that the integrity of a system and its data will be preserved.

Goals of Protection

- Obviously to prevent malicious misuse of the system by users or programs.
- To ensure that each shared resource is used only in accordance with system policies, which may be set either by system designers or by system administrators.
- To ensure that errant programs cause the minimal amount of damage possible.
- Note that protection systems only provide the mechanisms for enforcing policies and ensuring reliable systems. It is up to administrators and users to implement those mechanisms effectively.

What does Operating System Security (OS Security) mean?

- What is operating system security?
- How do operating systems contribute to system security?
- Alternatively, if we're trying to develop a secure system, what do we demand from the OS?

- Operating system security is the process of ensuring OS integrity, confidentiality and availability.

  OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

The Security Problem

- The Security Problem
- Authentication
- Program Threats
- System Threats
- Threat Monitoring
- Encryption

- Security must consider external environment of the system, and protect it from:
  - unauthorized access.
  - malicious modification or destruction
  - accidental introduction of inconsistency.
- Easier to protect against accidental than malicious misuse.

System Vulnerabilities and Application Security

- Since operating system provides an environment for application programs to execute and access resources, the OS becomes vulnerable to attacks on its security.
- Attacks may be intended or unintended.
- **Phishing**: Information is a very costly resource. The attacker poses as a known friend or organization and sends an email to an unsuspecting receiver, who, in his simplicity, parts with his confidential information.
- **Pretexting**: The attacker impersonates a co-worker or an officer on the phone and asks for confidential information from an unsuspecting receiver. Eg., Credit card information or OTP may be asked over phone. Or, SMS can allure us by stating 'You have won million dollar lottery, please send name, address…..'
- This type of gathering of information by unfair means is called **social engineering**.

Malicious Code

- Malware (malicious software) compromises the security of the system for the following purposes:
  - Command and control: The purpose may be to control the activities of the system and deny its resources and services to its legitimate users. In extreme case, the malware may destroy the resources of the system. E.g., some malware corrupt the boot sector of the hard disk after which the hard disk becomes non-available for use.
  - Stealth: The malicious code hides itself in order to escape the protection mechanism of the operating system.
  - Data collection : The malicious software may extract confidential information from files and databases of the system. It may collect information by sniffing (hacking) into the communication channel between various nodes of the company network.
  - Covert communication: Act of social engineering.

Popular Malicious Codes

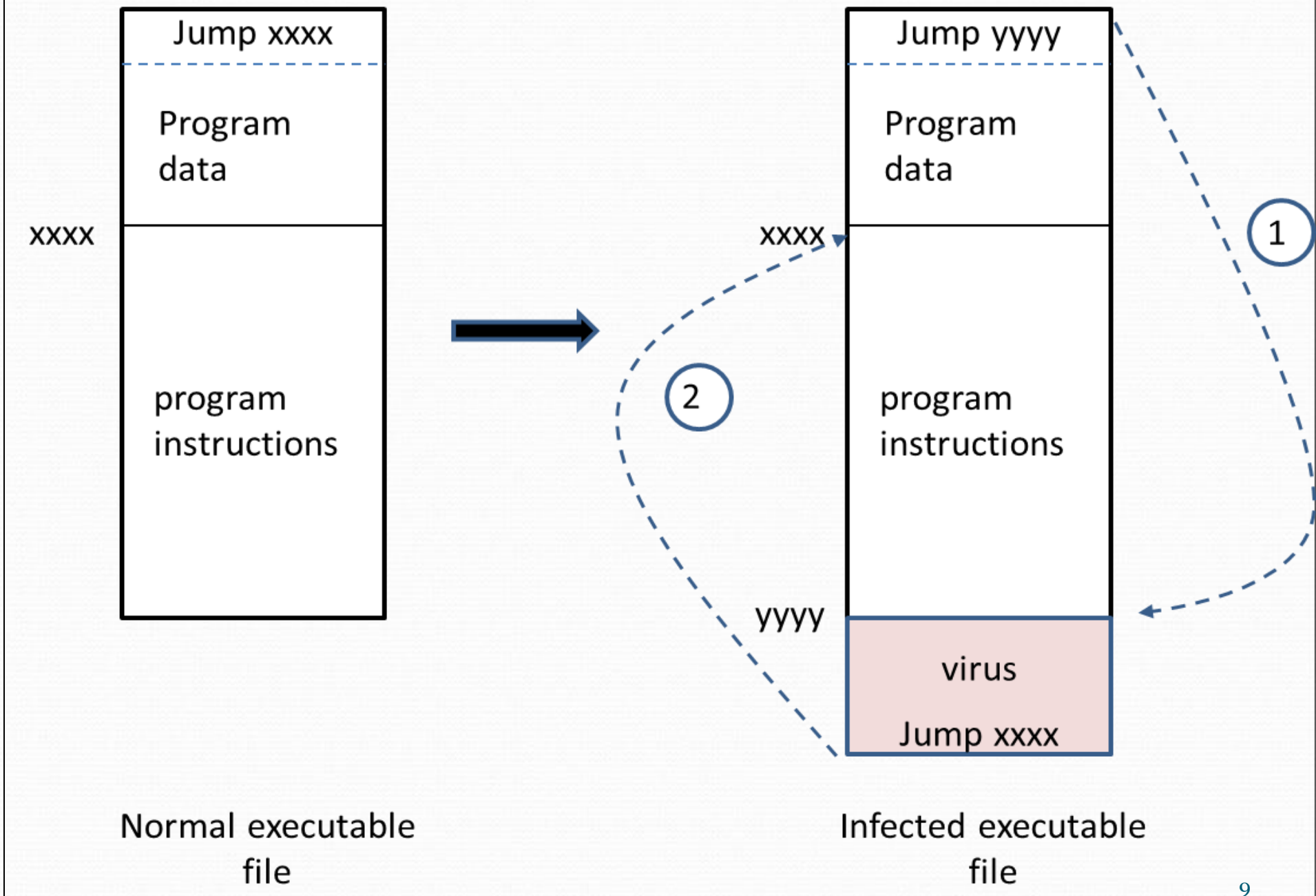
- *Computer virus*
- *File virus*
- *Boot sector virus*
- Replication module
- Payload module
- Trojan horse
- Worm
- Logical bomb

The computer virus is a program code. It infects a computer system by replicating itself on a visited computer system or device.

File virus: This virus attaches itself to a file called a carrier file, that is executable in nature. Goal is to take control to the executable part of the program.

Boot sector virus displaces the code of the boot sector of a disk to some other sector and marks it bad. E.g., brain virus

File Virus Attack



- Trojan Horse
  - Code segment that misuses its environment.
  - Exploits mechanisms for allowing programs written by users to be executed by other users.
  - Malicious software. It is self-standing, non-replicating code. It has a mischievous goal disguised behind a 'attractive stated goal'. Generally, the Trosan Horses are sent as attachments with e-mails or are embedded into games.
  - **Destructive Trosans**: deletes files from system.
  - **Proxy Trosan**: Its steals important data such as passwords, credit card information etc. for its creator.
  - **Remote access Trojan**: It takes control of the system on behalf of a remote hacker.
  - **Denial of service (DOS) Trojan**: It makes the resources unavailable on the computer system or the computer network. E.g., flooding the network with useless tasks.
- **Trap Door** : Specific user identifier or password that circumvents normal security procedures. Could be included in a compiler.

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 example 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 suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly 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

System Threats

- Worms – use spawn mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs in *finger* and *sendmail* programs.
  - Grappling hook program uploaded main worm program.
- Viruses – fragment of code embedded in a legitimate program.
  - Mainly effect microcomputer systems.
  - Downloading viral programs from public bulletin boards or exchanging floppy disks containing an infection.
  - *Safe computing*.

System Threats

System threats refers 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 creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- **Worm** – Worm is a process which can choked 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. Worms 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, a user may not be able to use internet if denial of service attacks browser's content settings.

Something You Know: Passwords

- Very common
- Very easily guessed
- Originally stored in plaintext, but that's a very bad idea
- Today, passwords are usually stored hashed
- However — some network authentication schemes, such as challenge/response, require plaintext (or equivalent)

One Time passwords

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

Virus Detection and Prevention

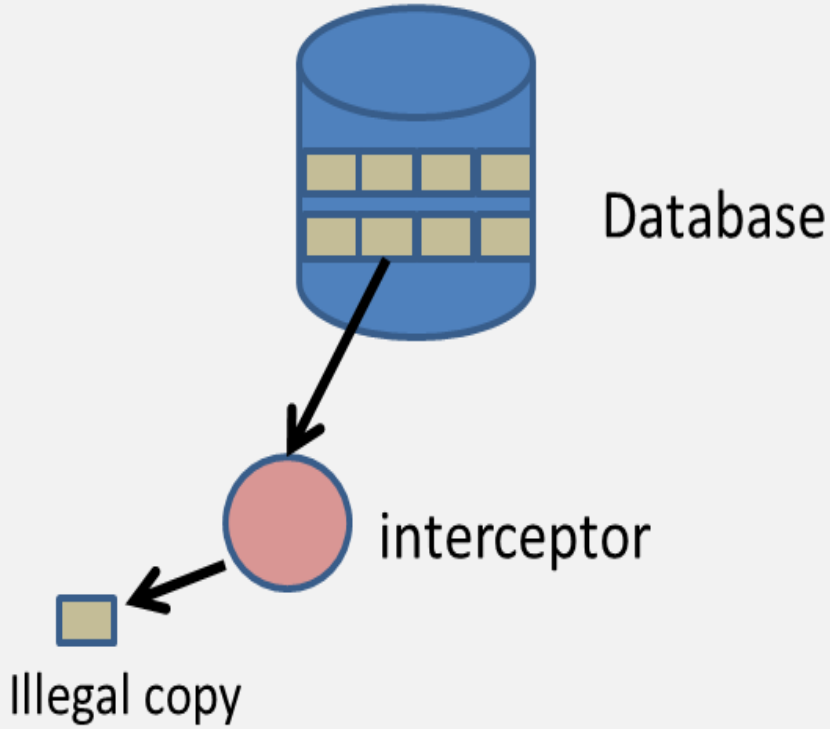
- The virus detection system can be categorised into two types:
  - Signature detection
  - Anomaly detection
- The signature detection systems use pre-generated signatures to check the integrity of files or disks.
- The anomaly detection system checks for abnormal behaviour of an executing program.

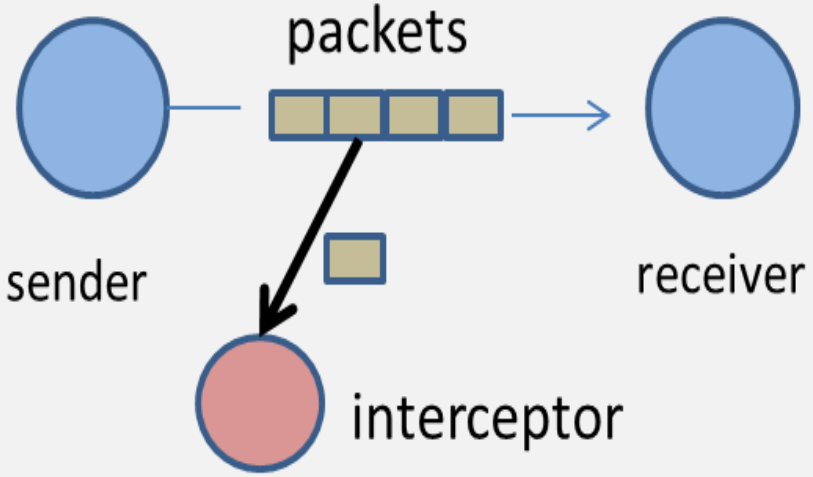
Security

- The following security issues need to be addressed for designing a secure computer and network system:
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity

Types of Threats

- **Interception**: When an unauthorized subject gains access to a confidential object such file or data base.

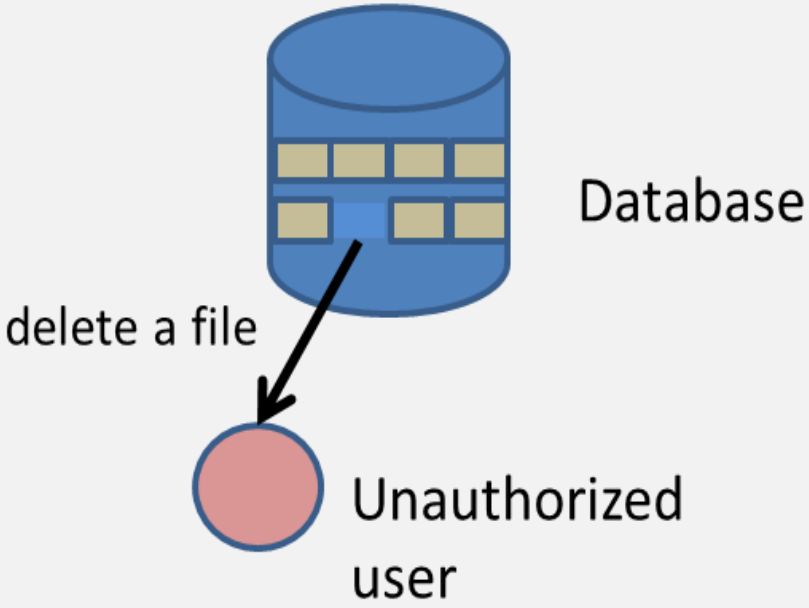


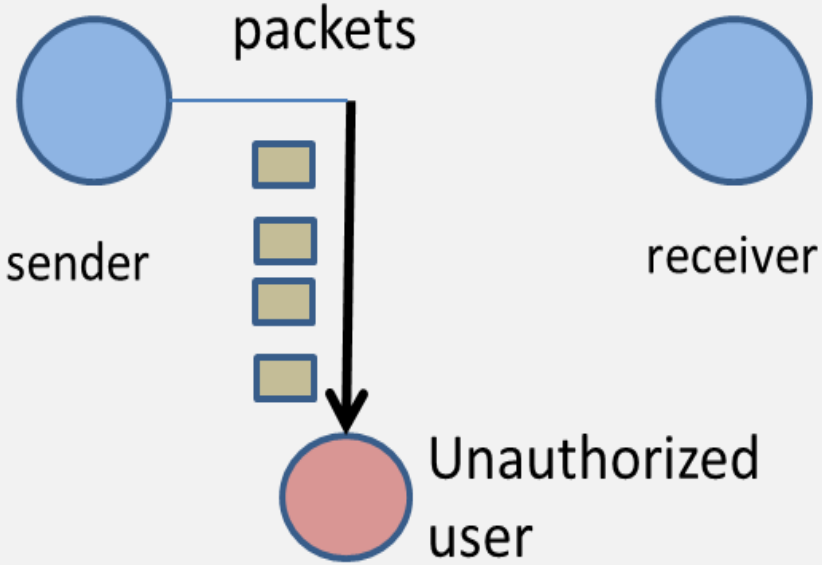


Interception

Interruption

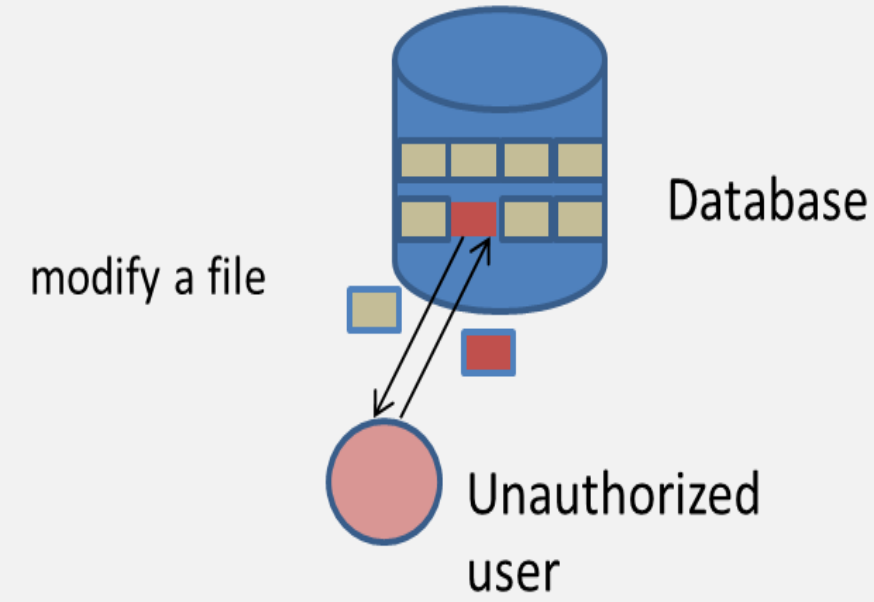
- It is a destructive attack on the system that makes resources unavailable.
- Interruption is an attack on the **availability** of resources.

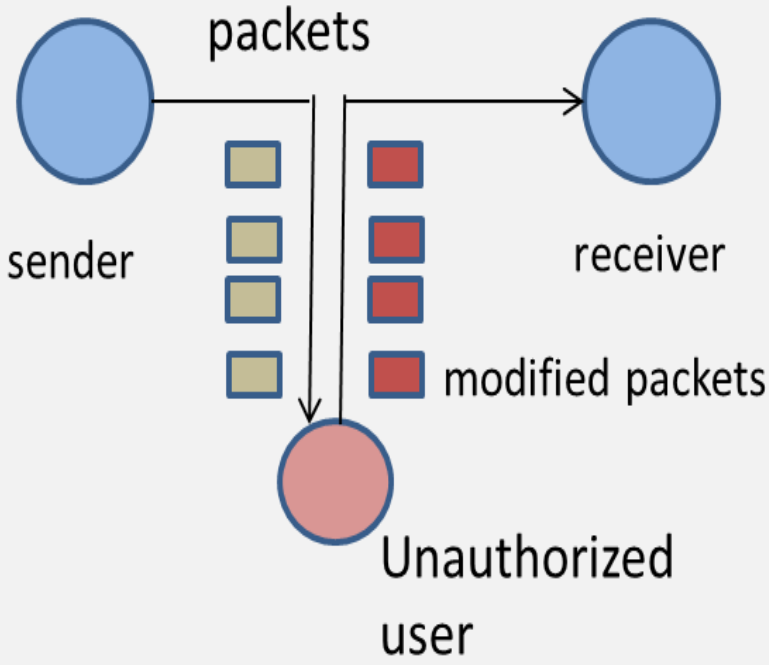




Modification

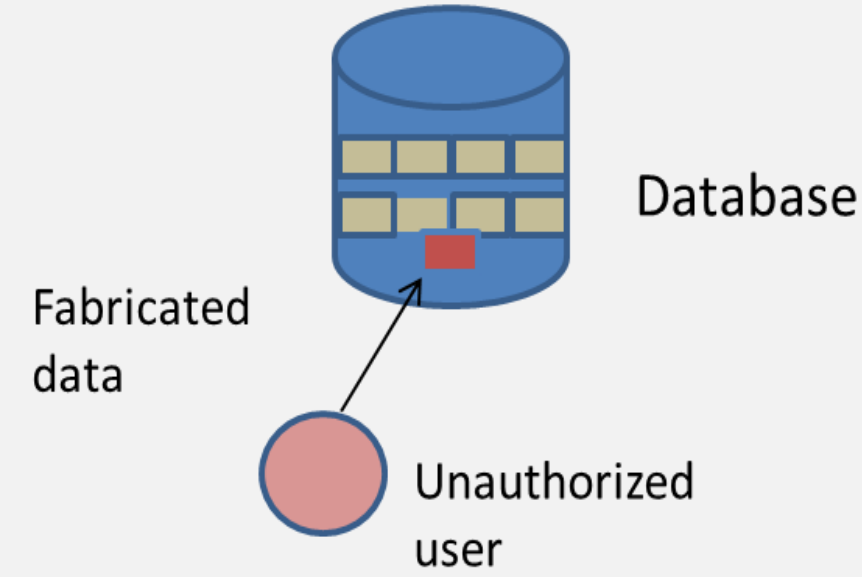
- The unauthorized user may modify the contents of a file or data packet after gaining access to it.
- It is a threat to the **integrity** of resources.

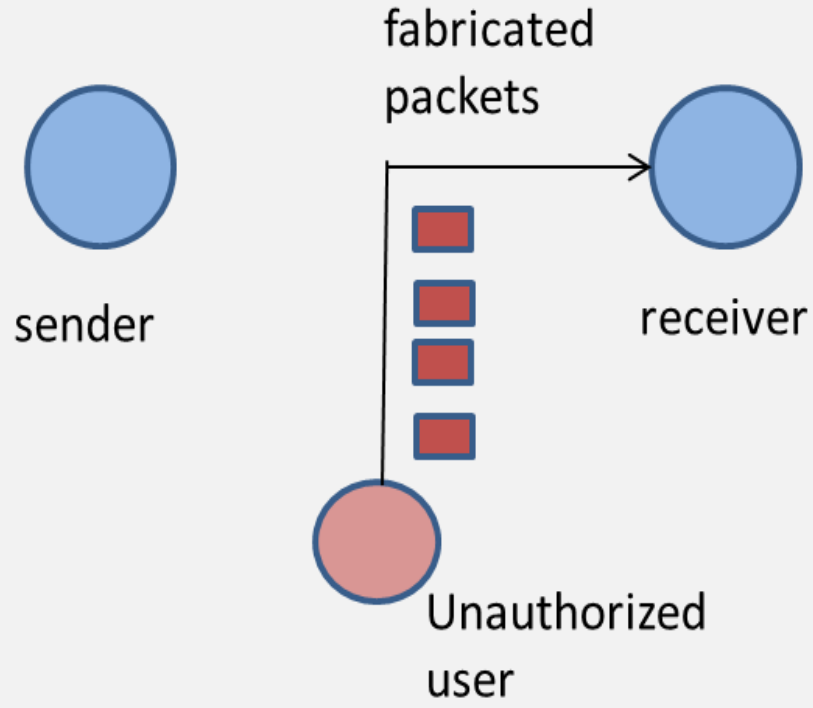




Fabrication

- It is a threat to the authenticity of resources.
- An unauthorized user may fabricate messages and broadcast them across the network.





Protection

- Systems are made secure by mechanisms that defend or guard against possible attacks, such as eavesdropping, masquerading, infiltration, etc.
- When the operating system opens a process, it defines the protection domain for the process.
- The protection domain comprises the set of resources that the process can access with stated rights such as read, write, append, etc.

- In 1975, Saltzer and Schroeder suggested the following principles for designing a secure information system:
  - Economy of mechanism
  - No protection
  - Complete mediation
  - Easy to use
  - Separation of privileges
  - Open design

Protection Mechanisms

- The following security mechanisms are used for computer and network security:
  - Authentication
  - Authorization
  - Auditing
  - Encryption

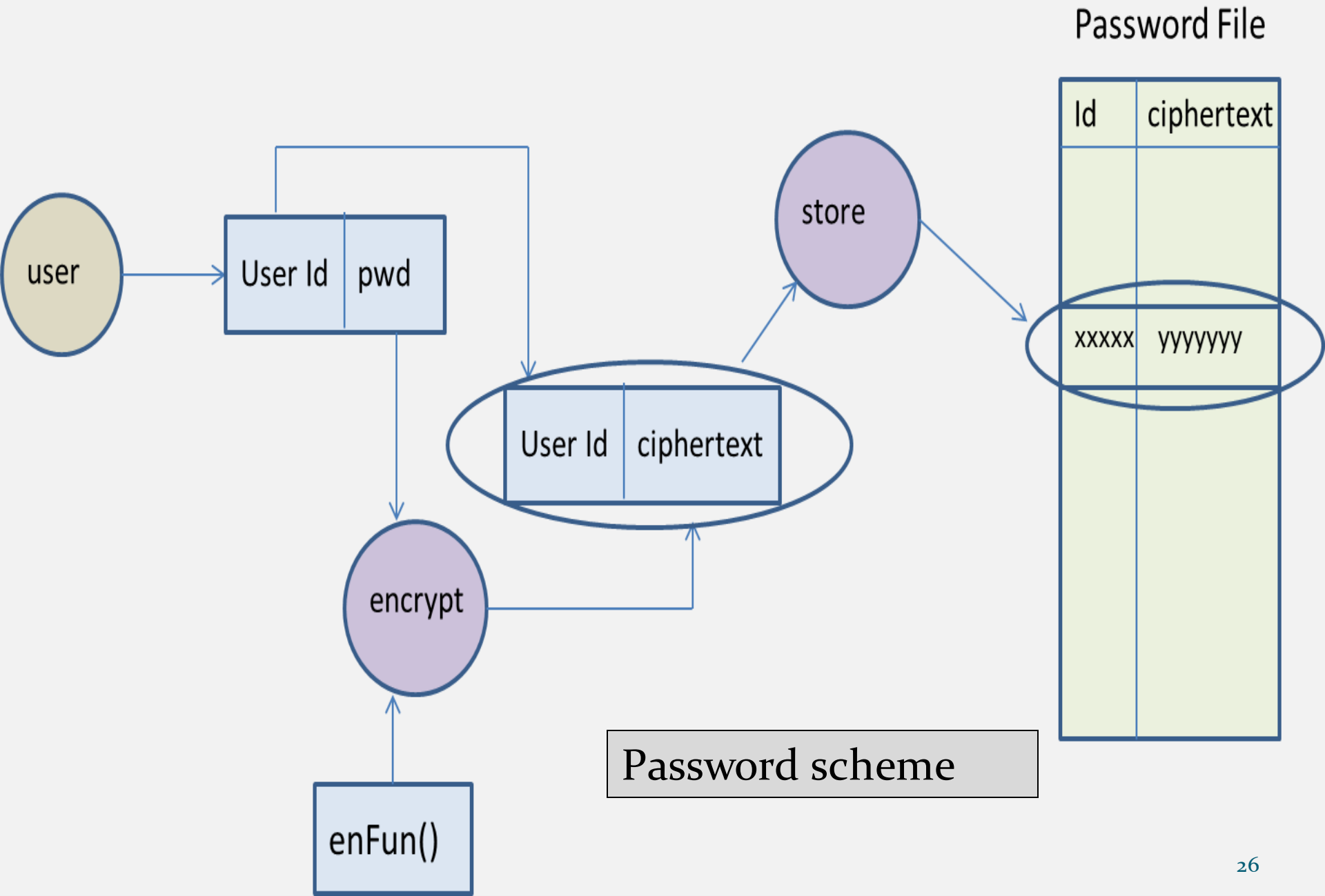
Authentication

- This is an act of verifying the identity of a subject who intends to access system resources.
- The system uses either of the following authentication mechanisms to verify the identity of the user:
  - Password
  - Biometric authentication
- **Password**: This is the most common method of verifying the identity of a user of the computer system.

Password file

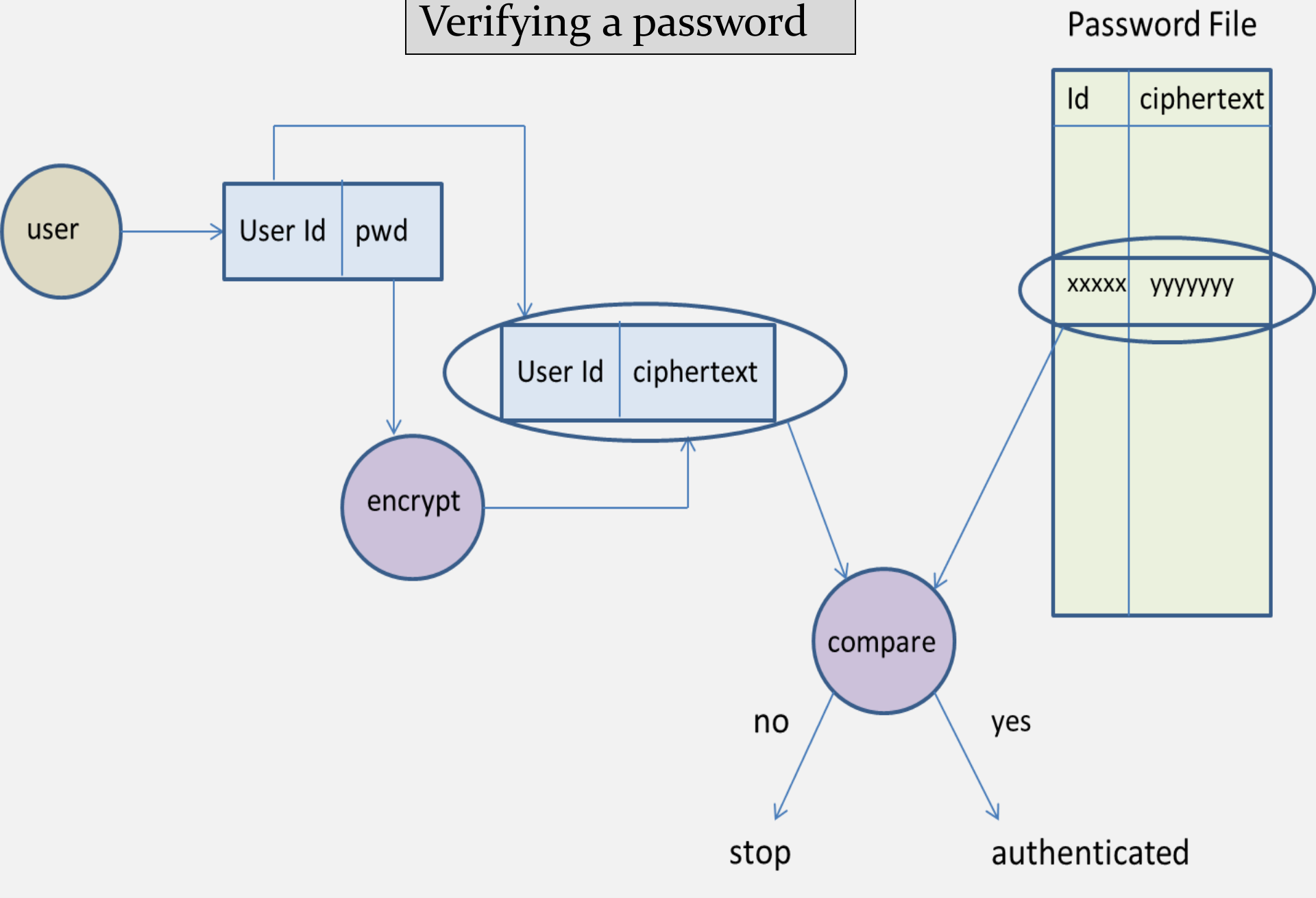
User Id	ciphertext
xxxx	yyyyyyyyy

Authentication



Authentication

Verifying a password



Authentication

- **Biometric authentication**: This type of identification is based on biological identification.
- The most common method is to use the fingerprints of the user to authenticate his identity.
- The other method uses the user's iris as the biological entity for user authentication.

Authorization

- The act of determining which actions an authenticated person is allowed to perform on the computer system or network.
- Some of the popular protection mechanisms are discussed below:
  - Role-based access control (RBAC)
  - Access control matrix
  - Bell–LaPadula model

Possible Questions & Answers

Differentiate between threat and attack.

"A threat is a category of objects, persons, or other entities that represents a constant danger to an asset".
"An attack is an act or event that exploits vulnerability".
Main difference between threat and attack is a threat can be either intentional or unintentional where as an attack is intentional. Threat is a circumstance that has potential to cause loss or damage whereas attack is attempted to cause damage. Threat to the information system doesn't mean information was altered or damaged but attack on the information system means there might be chance to alter, damage, or obtain information when attack was successful.

What do you mean by theft of service and denial of service?

Theft of service: 1) Application Level Attack; 2) Attacker Gains Increased Access To Restricted or Limited Resources; 3) Opportunistic Attack; 4) Typically does not result in system administration access. **TOS** means a violation that involves unauthorized use of resources. For example, an intruder (or intrusion program) may install a daemon on a system that acts as a file server.

Denial of Service: A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.

Possible Questions & Answers

- Explain the term “breach of confidentiality” and “breach of availability”.

“Breach of confidentiality”: This type of violation involves unauthorized reading of data (or theft of information). Typically, a breach of confidentiality is the goal of an intruder. Capturing secret data from a system or a data stream, such as credit-card information or identity information for identity theft, can result directly in money for the intruder.

“Breach of availability”: This violation involves unauthorized destruction of data. Some crackers would rather wreak havoc and gain status or bragging rights than gain financially. Website defacement is a common example of this type of security breach.

Explain masquerading and replay attack.

Masquerading and Replay attack: Attackers use several standard methods in their attempts to breach security. The most common is **masquerading**, in which one participant in a communication pretends to be someone else (another host or another person). By masquerading, attackers breach **authentication**, the correctness of identification; they can then gain access that they would not normally be allowed or escalate their privileges—obtain privileges to which they would not normally be entitled. Another common attack is to replay a captured exchange of data. A **replay attack** consists of the malicious or fraudulent repeat of a valid data transmission. Sometimes the replay comprises the entire attack—for example, in a repeat of a request to transfer money. But frequently it is done along with **message modification**, again to escalate privileges. Consider the damage that could be done if a request for authentication had a legitimate user’s information replaced with an unauthorized user’s.

Possible Questions & Answers

Discuss how one-time password scheme is implemented

To avoid the problems of password sniffing and shoulder surfing, a system can use a set of paired passwords. When a session begins, the system randomly selects and presents one part of a password pair; the user must supply the other part. In this system, the user is challenged and must respond with the correct answer to that challenge.

This approach can be generalized to the use of an algorithm as a password. Such algorithmic passwords are not susceptible to reuse. That is, a user can type in a password, and no entity intercepting that password will be able to reuse it. In this scheme, the system and the user share a symmetric password. The password pw is never transmitted over a medium that allows exposure. Rather, the password is used as input to the function, along with a challenge ch presented by the system. The user then computes the function $H(pw, ch)$. The result of this function is transmitted as the authenticator to the computer. Because the computer also knows pw and ch, it can perform the same computation. If the results match, the user is authenticated. The next time the user needs to be authenticated, another ch is generated, and the same steps ensue. This time, the authenticator is different. This one-time password system is one of only a few ways to prevent improper authentication due to password exposure.

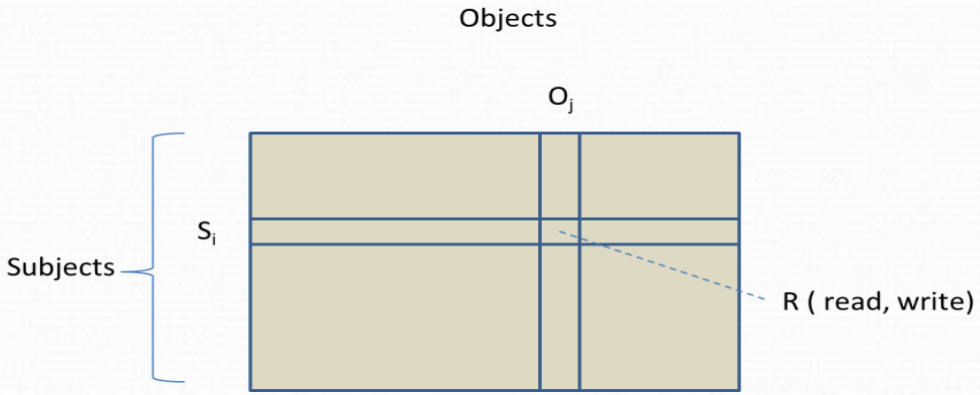
One-time password scheme

One-time password systems are implemented in various ways. Commercial implementations use hardware calculators with a display or a display and numeric keypad. These calculators generally take the shape of a credit card, a key-chain dongle, or a USB device. Software running on computers or smartphones provides the user with $H(pw, ch)$; pw can be input by the user or generated by the calculator in synchronization with the computer. Sometimes, pw is just a personal identification number (PIN). The output of any of these systems shows the one-time password. A one-time password generator that requires input by the user involves two-factor authentication. Two different types of components are needed in this case—for example, a one-time password generator that generates the correct response only if the PIN is valid. Two-factor authentication offers far better authentication protection than single-factor authentication because it requires "something you have" as well as "something you know."

Another variation on one-time passwords uses a code book, or one-time pad, which is a list of single-use passwords. Each password on the list is used once and then is crossed out or erased. The commonly used S/Key system uses either a software calculator or a code book based on these calculations as a source of one-time passwords. Of course, the user must protect his code book, and it is helpful if the code book does not identify the system to which the codes are authenticators.

Access Control Matrix

- In order to control the access by a subject to an object, in 1971, Lampson, Graham and Denning proposed a matrix called the **access matrix,** wherein rows represent subjects and columns represent objects.
- Each cell of the matrix represents a set R of rights of the subject S_i to the corresponding object O_j.



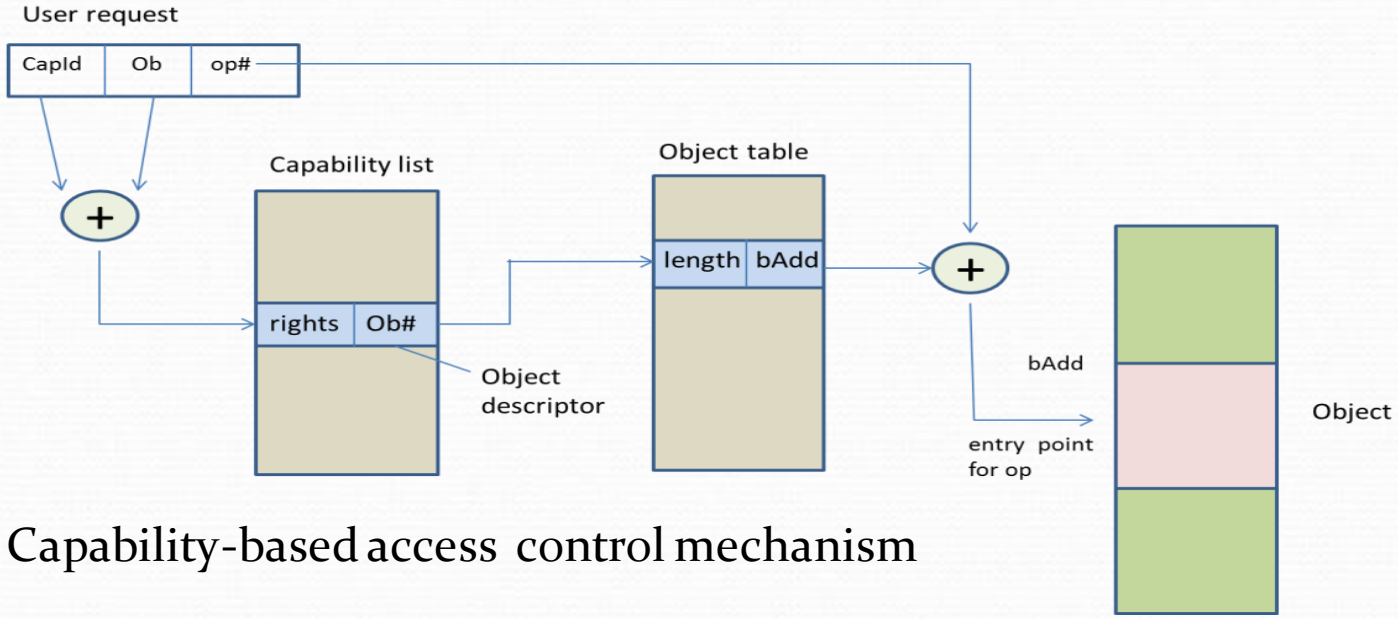
The access matrix

Implementation of Access Control Matrix

- The matrix can be implemented in two ways:
  - Subject-centric
  - Object-centric
- The subject-centric approach creates a **capability list** for every subject. On the other hand, the object-centric approach creates an **access control list** for every object.

Capability List

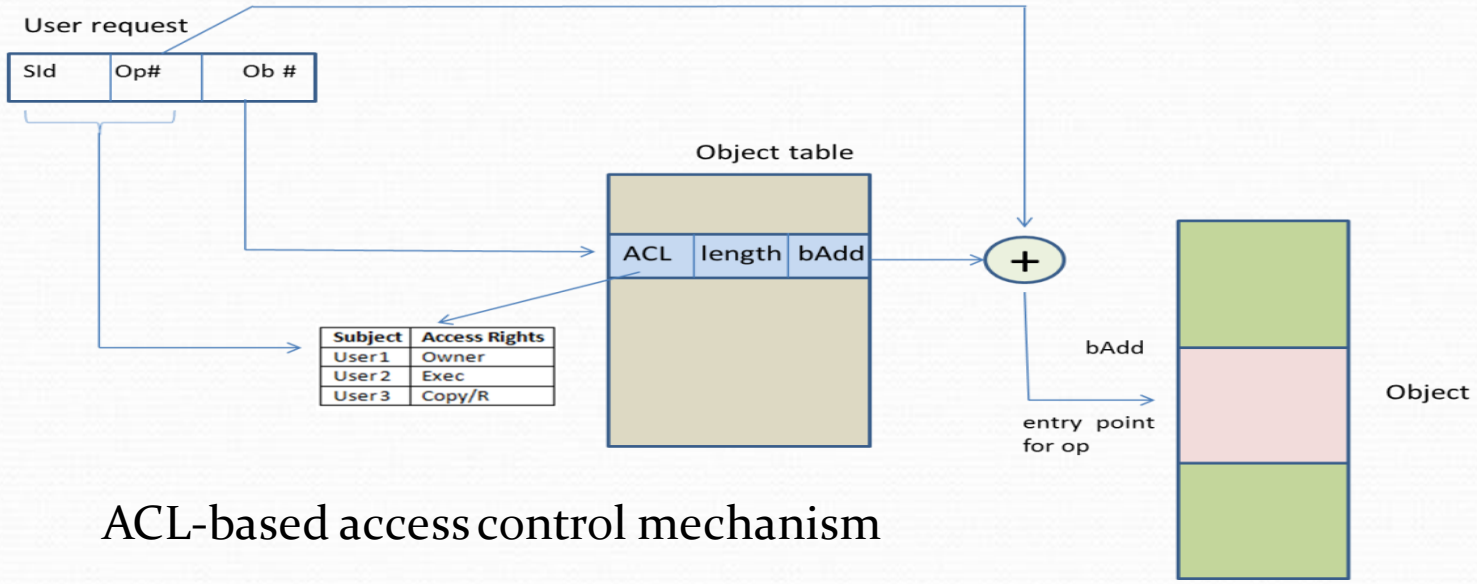
- This is a subject-centric approach, wherein for every subject, a list of capabilities is created.
- Each capability is a pair (o, c) where o is an object and c is the set of rights that the subject S has for object o.



Capability-based access control mechanism

Access Control List

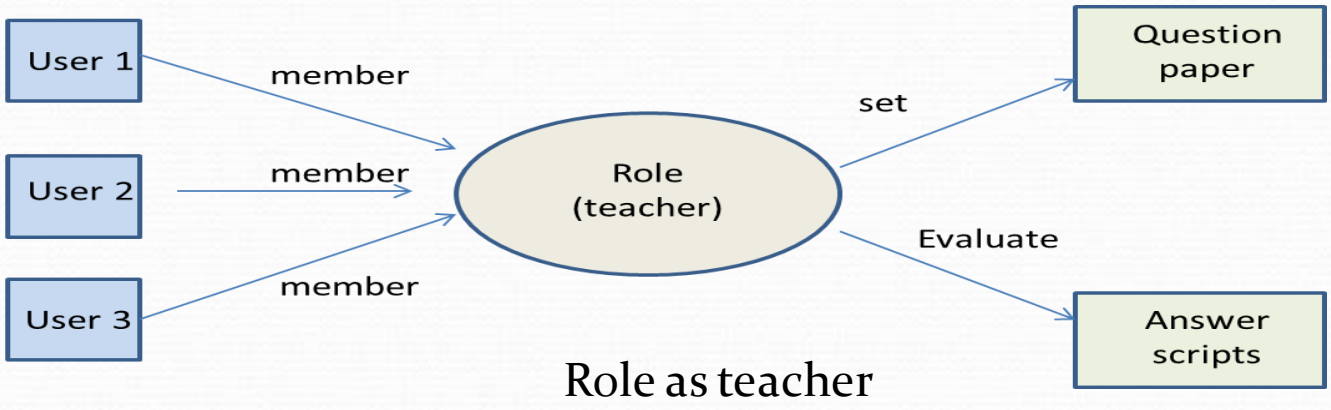
- This is an object-centric approach, wherein for every object O, an access control list (ACL) is created.
- Each ACL is a list of pairs (s, c) where s is a subject and c is the set of rights that the subject has for object o.



ACL-based access control mechanism

Role-based Access Control (RBAC)

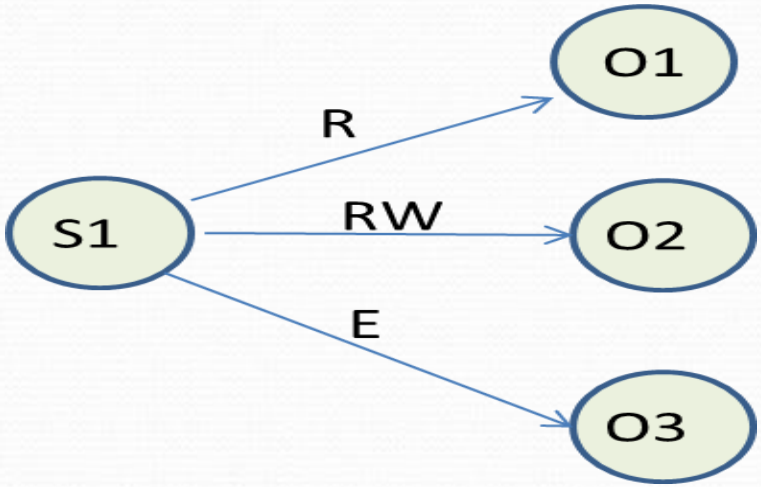
- A 'role' is a set of transactions that a user or set of users can perform.
- The transactions are assigned to a role by the system administrator.



Role as teacher

The Take–Grant Model

- This is method of protecting objects from unauthorised access.
- It is useful in a system where there are a large number of subjects with access rights for an equally large number of objects.



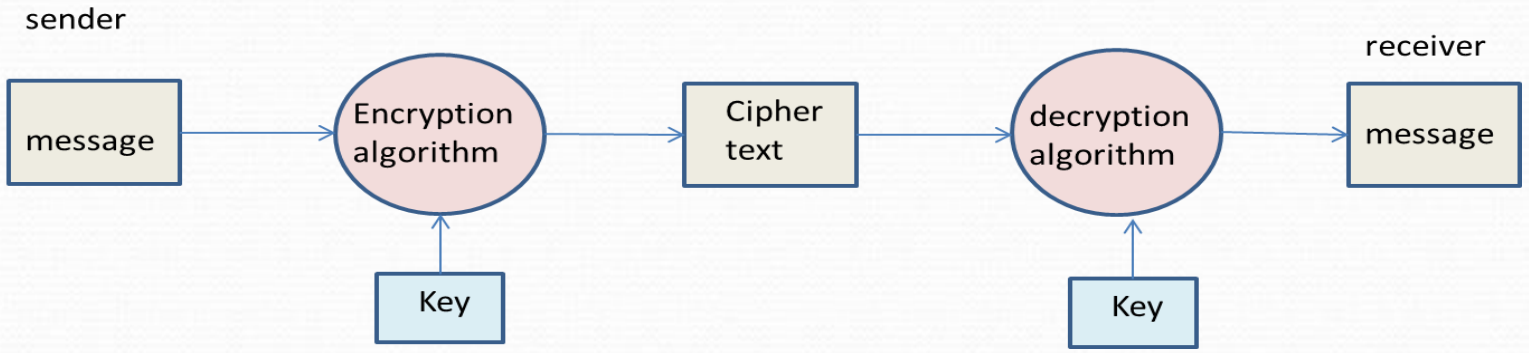
A directed graph

Bell–LaPadula Model

- It guarantees the confidentiality of classified information stored on a computer system, such as mainframe systems.
- The security system is modelled as a state transition system with the following components:
  - Set of subjects
  - Set of objects
  - Access matrix
  - Set of state transition rules

Data Encryption

- The computer network can be protected from unauthorised users by encrypting the data into a form which is not understandable to unauthorised users.



Cryptography model

Linux Security System

- Linux uses password authentication to authenticate the users of the system.
- At the first level, Linux authenticates the user through his/her username and password.
- Thereafter, it determines which resources the user is authorised to access and in what mode.

Permission symbol	Remarks
'r'	The user can read
'w'	The user can write
'x'	The user can execute
'-'	Access is denied

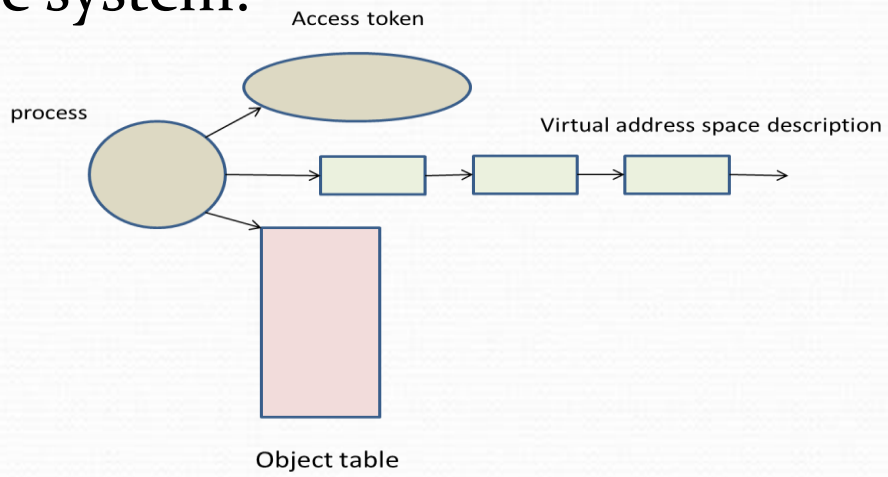
Permissions allowed on files/directories/applications

User	Remarks
Owner	The owner of the file or application
Group	Member of the group that own the file or application
Everyone	All users with access to the system.

User categories

Windows Security Systems

- Windows uses two security tools:
  - Access token
  - Security descriptor
- Access control, wherein it assigns an access token to every process and security descriptor to every object present in the system.



Access token is assigned to a process