UNIT-5

Authentication

Easy and small chapter so almost everything is imp. 5 to 7.5 marks asked in exam from this chapter.

⊛ Authentication:

Authentication is the process of validating the identity of someone or something. Authentication process consists of two steps:

i) Identification: Presenting an identifier to the security system.

ii) Verification: Binding entity (person) and identifier.

There are four general means of authenticating a user's identity:

i) Something the individual knows:
→ Password, a person identification number (PIN).

ii) Something the individual possesses:
→ Cryptographic keys, smart cards, physical keys.

iii) Something the individual is:
→ Recognition by fingerprint, retina and face.

iv) Something the individual does:
→ Recognition by voice pattern, handwriting characteristics.

⊛ Authentication System: [Imp]

Authentication systems are security measures put in place to secure data and systems by requiring additional input beyond username and password for users to access a system.

Authentication system consists of five components that are required for overall authentication process and they are as follows:

i) Authentication information (A) → information that provides identity.

ii) Complementary information (C) → information stored on computer and used to validate authentication information.

iii) Complementation Function (F) → Function that generates the complementary information from the authentication information.

iv) Authentication Function (L) → Function that provides identity.

v) Selection Function (S) → Function enabling entity to create or alter information A or C.

⊛. Password Based Authentication:

A password is an information associated with an entity (usually person) that confirms the entity's identity. A password is a string of alphabets, numbers and special characters, which is supposed to be known only to the entity that is being authenticated.

Password based authentication involves authenticating a user by using name and password. These are the oldest and easiest methods to implement. In password based authentication following sequence of processes occur:

→ The user requests a resource controlled by server.

→ The server requires client authentication before permitting access to the requested source.

→ In response client first gets dialog box for username and password required by server.

→ The client sends name and password.

→ The server looks up the name and password in its local database and if they match, accepts the user and displays requested resource else denys.

⊛. Dictionary Attack: [Imp]

Dictionary attack is the guessing of password by repeated trial and error. It attempts to defeat an authentication mechanism by trying each word in a dictionary as password. A dictionary attack can be performed both online and offline.

Online Dictionary Attack: In online dictionary attack, the attacker tries to guess the correct password by interacting with the login server. The attacker repeatedly tries to log in or gain

access like any other user. This type of attack works better if a hacker has list of likely passwords. If the attack takes too long, it might get noticed by a system administrator. Online attack can be very slow because the speed of attack depends on speed of internet connection and the speed of target server. Defense: disconnection, disabaling, jailing etc.

Offline Dictionary Attack: In offline dictionary attack, the attacker first collects message between the users and servers or finds a copy of the password file. Then the attacker tries to guess correct password by matching the passwords in his dictionary with the collected information without requiring any feedback from the login server. Attackers need to get their hands on the password storage file from the system they want to access, so it's more complicated than the online attack. But once they will be able to log in without anyone noticing.

Defense: Append the password with a random string and hash the result.

⑧. Challenge Response System: [Imp]

Challenge response is a handshake authentication process in which the authenticator issues a challenge to the user seeking authentication. The user must provide a correct response in order to be authenticated. The challenge may take many forms depending on the system. In some systems, it may be a password request or number of questions that were answered by user during first time authentication. The person seeking authentication must respond to the system challenge. When the server receives the user response, it checks to be sure the password or answers to questions are correct. If so, the user is authenticated. If not the user is denied.

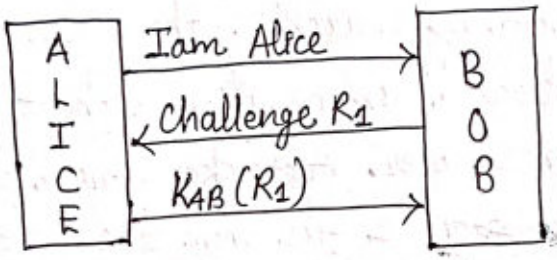
⑧ One Way Authentication:

One way authentication involves a single transfer of information from one user (A) to another (B), and establishes the following:

i) The identity of A and that the message was generated by A.
ii) That the message was intended for B.
iii) The integrity and originality of the message.

Only the identity of the initiating entity is verified in this process, not that of the responding entity.

Example:



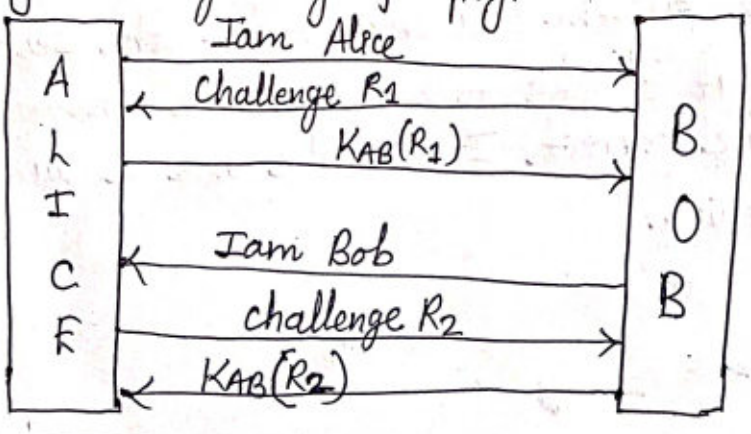
Assume that Alice and Bob share a secret key K_{AB}.

⑨ Mutual Authentication:

In one-way authentication, only one party verifies the identity of the other party. But in mutual authentication, both communicating parties verify each other's identity. Mutual authentication establishes the following elements:

i) The identity of A and that the message generated by A.
ii) That the message was intended for B.
iii) The integrity and originality of the message
} these three points similar to above
iv) The identity of B and that the reply message generated by B.
v) That the message was intended for A.
vi) The integrity and originality of reply.

Example:



⊛ Biometric System:

Biometrics refers to metrics related to human characteristics. Biometric authentication is a user identity verification process that involves biological input, or the scanning or analysis of some part of the body.

Process:

→ The user database contains a sample of user's biometric characteristics.
→ During authentication process, the user need to provide a new sample of user's biometric characteristic.
→ This is matched with the one in the database, and if the two samples are same, the user is considered to be a valid one.
→ The samples produced during every authentication process can vary slightly (e.g, cuts on the finger).
→ An approximate match can be accepted.

or types of biometrics

Common Physical Characteristics: Fingerprint, Face, Retina, Iris, Vein pattern, Hand and finger geometry etc.

Behavioural Characteristics: Voice, Gait, Signature dynamics etc.

⊛ Needham-Schroeder Scheme:

Needham-Schroeder is a shared key authentication protocol designed to generate and propagate a session key. It includes the symmetric key protocol and asymmetric key protocol.

→ Symmetric key protocol establishes a session key to protect further communication.
→ Asymmetric key protocol provides mutual authentication between two parties communicating on a network.

⊛. Kerberos Protocol: [Imp]

Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos was designed to authenticate user requests for network resources. It is based on the concept of a trusted third party that performs secure verification of users and services. This trusted third party is called the key distribution center (KDC).

Ticket → A ticket is something a clients present to an application server to demonstrate the authenticity of its identity.

Components of Kerberos:

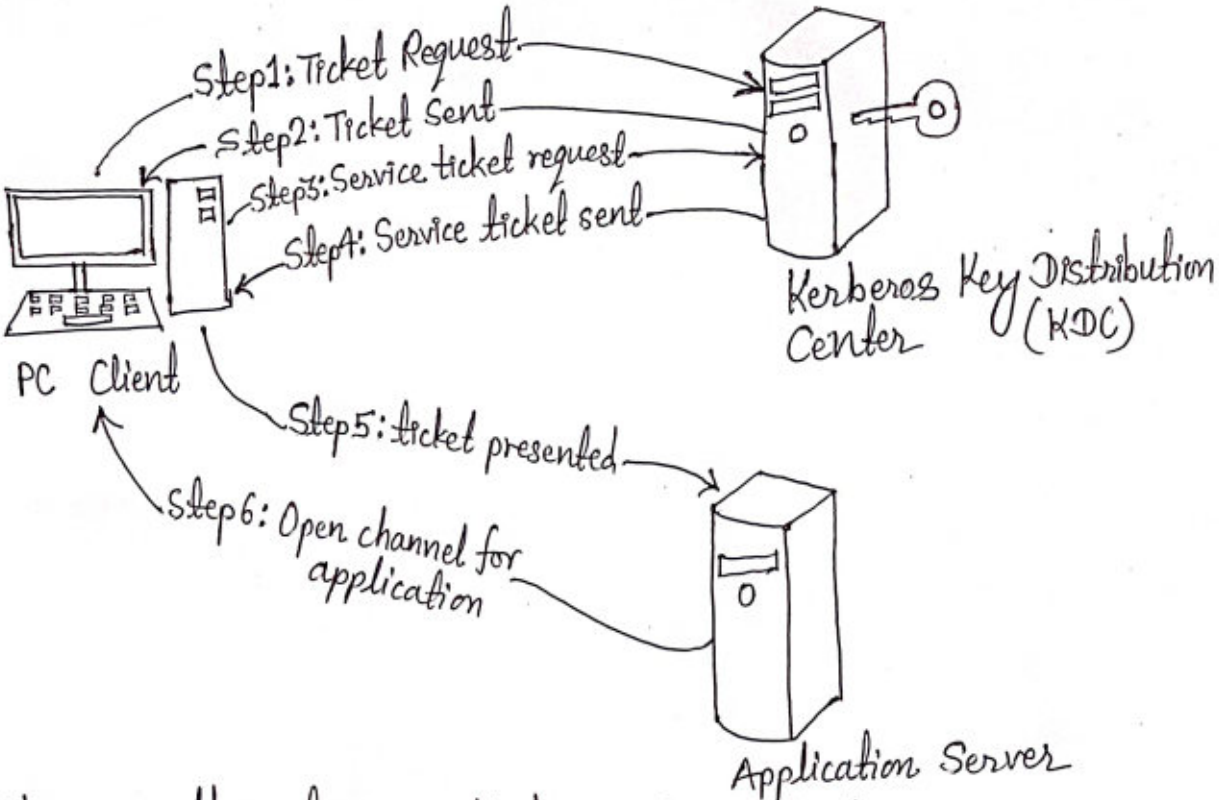
i) Client → Clients are applications acting on behalf of user who need access to a resource or service.

ii) Key distribution center (KDC) → It is the authentication server in a Keberos environment. It consists of database, authentication server and ticket granting server (TGS).

iii) Host/Application server → It's the server user want to connect with or the app user want to use in the server.

Working of Kerberos:

When authenticating, Kerberos uses symmetric encryption and a trusted third party which is called KDC. Kerberos stores ticket for a session on the user's machine and any Kerberos aware service will look for this ticket instead of prompting the user to authenticate through a password.



Following are the steps in Kerberos Authentication:

1. PC client sends a ticket request to a Kerberos KDC.
2. The Kerberos KDC returns a ticket and a session key to PC client.
3. A ticket request for application server is sent to Kerberos KDC by a PC client.
4. The Kerberos KDC returns a ticket for application server to PC client.
5. The ticket is sent to application server by PC client.
6. Application server opens the channel for application for PC client.

*Kerberos Version 5: The minor differences between version 4 and version 5 are as follows:

→ Version 5 has longer ticket lifetime.
→ Version 5 allows tickets to be renewed
→ Version 5 can accept any symmetric-key algorithm.
→ Version 4 uses a different protocol for describing data types.
→ Version 5 has more overhead than version 4.