RGPVNOTES.IN

Program : **B.E**

Subject Name: **Information Security**

Subject Code: **IT-8001**

Semester: **8th**

Unit-III Authentication

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server.

- If the credentials match, the process is completed, and the user is granted authorization for access. The permissions and folders returned define both the environment the user sees and the way he can interact with it, including hours of access and other rights such as the amount of allocated storage space.
- The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization.
- The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server.

Password-based authentication

- In private and public computer networks (including the Internet), authentication is commonly done through the use of login IDs (usernames) and passwords. Knowledge of the login credentials is assumed to guarantee that the user is authentic.
- Each user registers initially (or is registered by someone else, such as a systems administrator), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password.
- However, password-based authentication is not considered to provide adequately strong security for any system that contains sensitive data.

Certificate-Based Authentication

Certificate-based authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc.

- In the case of user authentication, it is often deployed in coordination with traditional methods such as username and password.
- One differentiator of certificate-based authentication is that unlike some solutions that only work for users, such as biometrics and one-time passwords (OTP), the same solution can be used for all endpoints – users, machine, devices and even the growing Internet of Things (IoT).

Mutual authentication

Mutual authentication, also called two-way authentication, is a technology in which both entities in a communications link authenticate each other.

- In a network environment, the client authenticates the server and vice-versa. In this way, network users can be assured that they are doing business exclusively with legal entities and servers can be certain that all would-be users are attempting to gain access for legitimate purposes.
- Mutual authentication is gaining acceptance as a tool that can minimize the risk of online fraud in e-commerce.

Shared secret-based authentication

Shared key authentication (SKA) is a verification method in which a computer or terminal uses the Wired Equivalent Privacy (WEP) protocol to access a wireless network.

- It pre-establishes that a requesting system knows a shared secret key required for authentication.
- The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard assumes that the key is delivered to wireless clients using a secured channel that is independent of the standard. In practice, the user types in the password for the Wi-Fi network to gain access.
- Shared key authentication (SKA) is not considered a secure method of granting network access because it uses conventional unsecured channels, like writing and verbal exchange, to share a security key for granting access.
- Although the dissemination of the key is a large security issue, the authentication itself is secured using 64 or 128-bit encryption. It is difficult for an intruder to gain access without knowledge of the key.

Asymmetric based authentication

Key-based authentication is a kind of authentication that may be used as an alternative to password authentication. Instead of requiring a user's password, it is possible to confirm the client's identity by using asymmetric cryptography algorithms, with public and private keys.

- Nowadays, password authentication is more popular than public key authentication. It does not require much preparation (at least, from the client's point of view), and perhaps is generally more intuitive. To log into a server, users must provide their secret passwords, which are verified by the server.
- A disadvantage of this method is that, when a server is publicly available, it may be targeted by various types of brute force and dictionary attacks, and the password may eventually be broken and revealed. Moreover, this method requires the users to remember their (ideally difficult and complex) passwords.
- Public key authentication offers a solution to these problems. The idea is to assign a pair of asymmetric keys to every user. Users would store their public keys in each system they want to use, while at some time their private keys would be kept secure on the computers, the users want to use to connect with those secured systems.
- During establishing the connection, the server would use the public key to authenticate the client, for example by encrypting some number and asking the client to decrypt it, by using his corresponding private key.

Authentication and key agreement

Key exchange protocols enable two or more parties to establish a shared encryption key that they can use to encrypt or sign data that they plan to exchange. Key exchange protocols typically employ cryptography to achieve this goal.

- Different cryptographic techniques can be used to achieve this goal. For two parties to communicate confidentially, they must first exchange the secret key that will be used to encrypt and decrypt messages.
- This initial exchange the encryption key is called the key exchange. Key exchange protocols are designed to solve the problem of confidentially when establishing a secret key between two or more parties without letting an unauthorized party somehow intercept, infer or otherwise obtain the key.
- A simple example for a key exchange protocol is for one party to write down a secret key, place it in a tamper-evident envelope and send it to the receiver. If the envelope is intact, then the secret key can be used by both parties to encrypt and decrypt messages.

Centralized Authentication

The Central Authentication Service (CAS) is a single sign-on protocol for the web. Its purpose is to permit a user to access multiple applications while providing their credentials (such as user id and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password.

- The name CAS also refers to a software package that implements this protocol. The CAS protocol involves at least three parties: a client web browser, the web application requesting authentication, and the CAS server.
- It may also involve a back-end service, such as a database server, that does not have its HTTP interface but communicates with a web application.
- When the client visits an application requiring authentication, the application redirects it to CAS. CAS validates the client's authenticity, usually by checking a username and password against a database (such as Kerberos, LDAP or Active Directory).
- If the authentication succeeds, CAS returns the client to the application, passing along a service ticket. The application then validates the ticket by contacting CAS over a secure connection and providing its service identifier and the ticket. CAS then gives the application trusted information about whether a user has successfully authenticated.
- CAS allows multi-tier authentication via proxy address. A cooperating back-end service, like a database or mail server, can participate in CAS, validating the authenticity of users via information

it receives from web applications. Thus, a webmail client and a webmail server can all implement CAS.

Eavesdropping

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission. The term eavesdrop derives from the practice of standing under the eaves of a house, listening to conversations inside.

VoIP systems that don't use encryption make it relatively easy for an intruder to intercept calls. Explanation:

- Eavesdropping is easier to perform with IP-based calls than TDM-based calls. Any protocol analyzer can pick and record the calls without being observed by the callers. There are software packages for PCs that will convert digitized voice from standard CODECs into WAV files.
- The speakerphone function can be turned on remotely, with the caller on mute so that there is no sound coming from the phone. This has happened with some IP phones in executives' offices. Their offices can be listened to without their knowledge.
- PCs and laptops that have microphones attached or integrated into them can be enabled as listening devices without the user's knowledge. There is a rootkit available for this purpose

Kerberos

Kerberos is a network protocol that uses secret-key cryptography to authenticate client-server applications. Kerberos requests an encrypted ticket via an authenticated server sequence to use services. The protocol gets its name from the three-headed dog (Kerberos, or Cerberus) that guarded the gates of Hades in Greek mythology.

- Kerberos was developed by Project Athena - a joint project between the Massachusetts Institute of Technology (MIT), Digital Equipment Corporation and IBM that ran between 1983 and 1991.
- An authentication server uses a Kerberos ticket to grant server access and then creates a session key based on the requester's password and another randomized value.
- The ticket-granting ticket (TGT) is sent to the ticket-granting server (TGS), which is required to use the same authentication server.
- The requester receives an encrypted TGS key with a time stamp and service ticket, which is returned to the requester and decrypted.
- The requester sends the TGS this information and forwards the encrypted key to the server to obtain the desired service.
- If all actions are handled correctly, the server accepts the ticket and performs the desired user service, which must decrypt the key, verify the timestamp and contact the distribution centre to obtain session keys.
- This session key is sent to the requester, which decrypts the ticket. If the keys and timestamp are valid, client-server communication continues.
- The TGS ticket is time stamped, which allows concurrent requests within the allotted time frame.

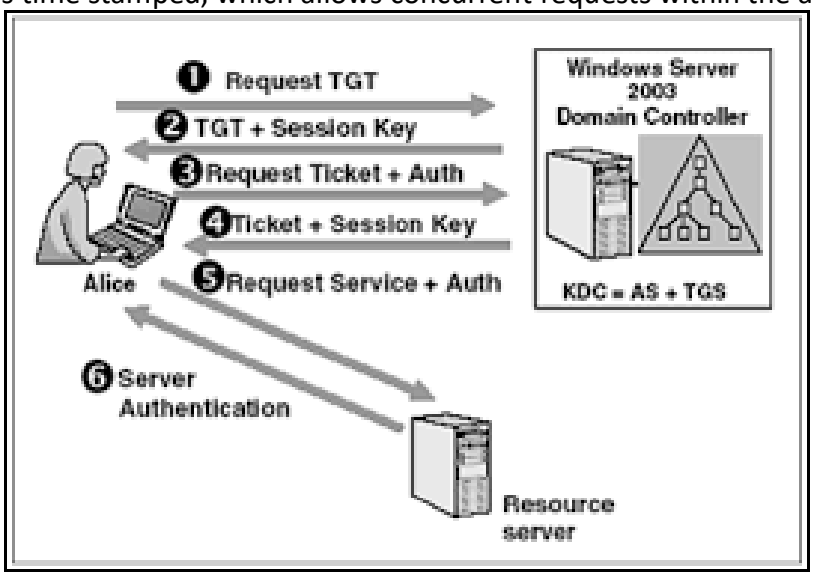

Figure 3.1 Kerberos

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec)is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session.

- IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).
- Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
- IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.
- IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Transport Layer (TLS) and the Application layer (SSH).
- IPsec can automatically secure applications at the IP layer.

Security association & Encapsulating security payload

- The IP security architecture uses the concept of a security association as the basis for building security functions into IP.
- A security association is simply the bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a flow in one direction.
- Therefore, in normal bi-directional traffic, the flows are secured by a pair of security associations.
- Security associations are established using the Internet Security Association and Key Management Protocol (ISAKMP).
- ISAKMP is implemented by manual configuration with pre-shared secrets, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), and the use of IPSECKEY DNS records. defines Better-Than-Nothing Security (BTNS) as an unauthenticated mode of IPsec using an extended IKE protocol.

Encapsulating Security Payload: Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite.

- In IPsec, it provides origin authenticity, integrity, and confidentiality protection of packets.
- ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.
- Unlike Authentication Header (AH), ESP in transport mode does not provide integrity and authentication for the entire IP packet.
- However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header (including any outer IPv4 options or IPv6 extension headers) remains unprotected.
- ESP operates directly on top of IP, using IP protocol number 50.

Tunnel and Transfer modes

Modes of Operation: IPsec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

Transport mode

- In transport mode, only the payload of the IP packet is usually encrypted or authenticated.
- The routing is intact since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be modified by network address translation, as this always invalidates the hash value.
- The transport and application layers are always secured by a hash, so they cannot be modified in any way, for example by translating the port numbers.

- A means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

Tunnel mode

- In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.
- Tunnel mode is used to create virtual private networks for network-to-network communications (e.g., between routers to link sites), host-to-network communications (e.g., remote user access) and host-to-host communications (e.g., private chat).

Internet key exchange protocol

The Internet Key Exchange (IKE) is an IPsec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access. Specified in IETF Request for Comments (RFC) 2409, IKE defines an automatic means of negotiation and authentication for IPsec security associations (SA).

- Security associations are security policies defined for communication between two or more entities; the relationship between the entities is represented by a key.
- The IKE protocol ensures security for SA communication without the pre-configuration that would otherwise be required.
- A hybrid protocol, IKE implements two previous security protocols, Oakley and SKEME, within an ISAKMP (Internet Security Association and Key Management Protocol) TCP/IP-based framework. ISAKMP specifies the structure for key exchange and authentication; the Oakley protocol specifies a sequence of key exchanges and describes their services (such as identity protection and authentication), and SKEME specifies the actual method of key exchange.
- Although IKE is not required for IPsec configuration, it offers many benefits, including automatic negotiation and authentication; anti-replay services (see anti-replay protocol); certification authority (CA) support; and the ability to change encryption keys during an IPsec session.

Secure Socket Layer (SSL)

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

- SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.
- The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.
- SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.
- TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled, and specific Web pages can be identified as requiring SSL access.
- Any Web server can be enabled by using Netscape's SSL Ref program library which can be downloaded for non-commercial use or licensed for commercial use. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

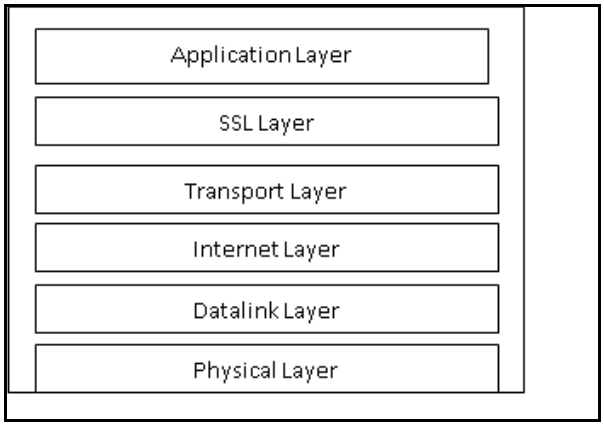

Figure 3.2 SSL Layer

SSL Sub-Protocols

- Handshake Protocol
- Record Protocol
- Alert Protocol

SSL Handshake Message Format

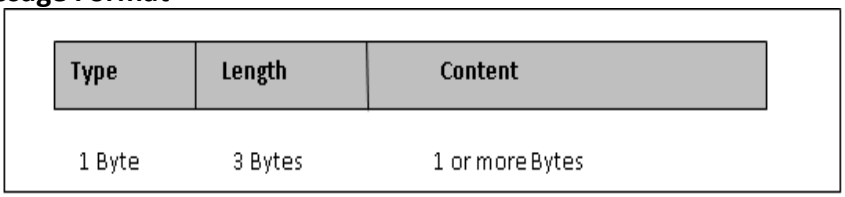

Figure 3.3 SSL Handshake Message

SSL Handshake Process

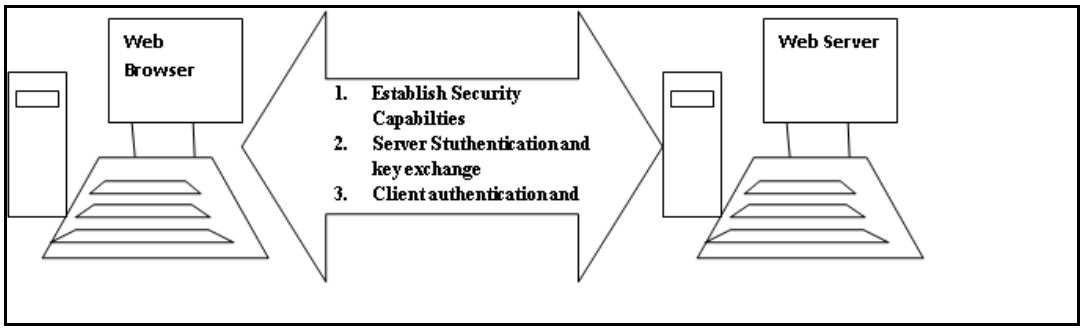

Figure 3.4 SSL Handshake process

Transport layer security

- (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet.
- It enables privacy, integrity, and protection for the data that's transmitted between different nodes on the Internet. TLS is a successor to the secure socket layer (SSL) protocol.
- TLS primarily enables secure Web browsing, applications access, data transfer, and most Internet-based communication.
- It prevents the transmitted/transported data from being eavesdropped or tampered. TLS is used to secure Web browsers, Web servers, VPNs, database servers and more.

TLS protocol consists of two different layers of sub-protocols:

- TLS Handshake Protocol: Enables the client and server to authenticate each other and select an encryption algorithm before sending the data
- TLS Record Protocol: It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in