N|DE
Network Defense Essentials

Module 03

# Network Security Protocols


# Module Objectives

1. Understanding the Different Network Security Protocols
2. Examples of Network Security Protocol: 1. **RADIUS**
3. Examples of Network Security Protocol: 2. **TACACS+**
4. Examples of Network Security Protocol: 3. **Kerberos**
5. Examples of Network Security Protocol: 4. **PGP**
6. Examples of Network Security Protocol: 5. **S/MIME**

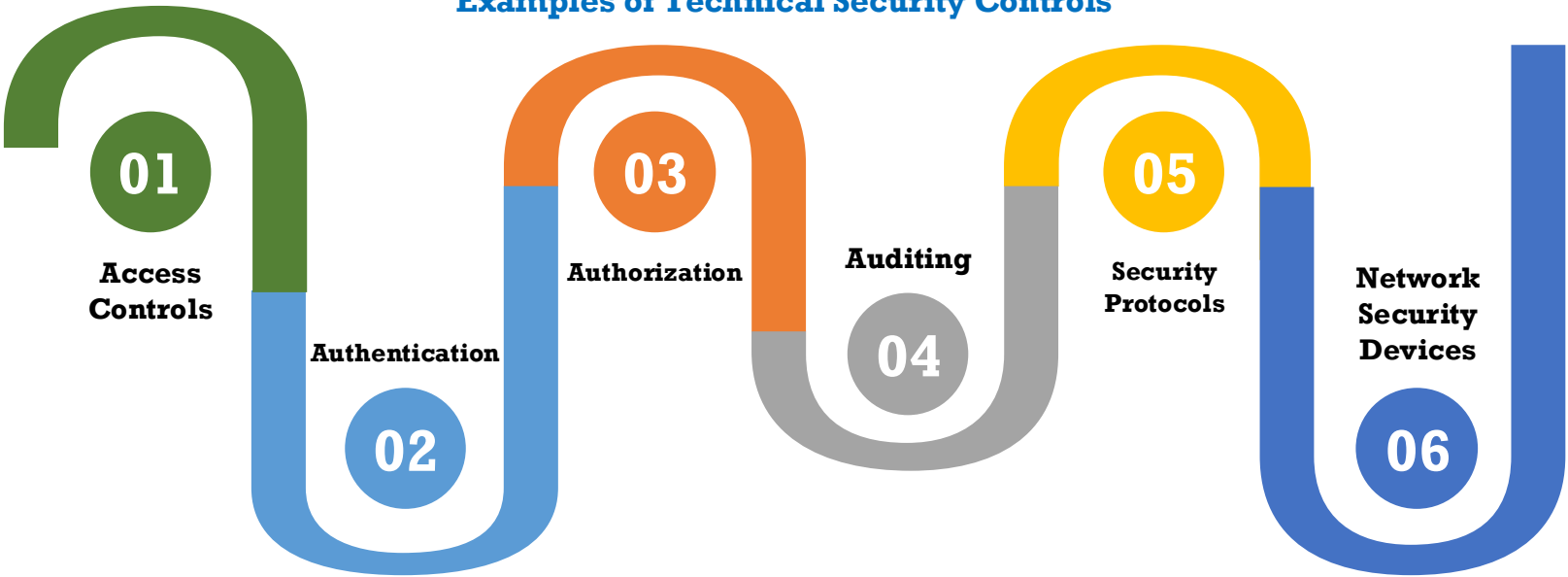
# Module Flow

01 Understanding Network Security Protocols

# Network Security Controls: Technical Security Controls

- This is a set of security measures taken to protect data and systems from unauthorized personnel

## Examples of Technical Security Controls



# Network Security Protocols

- RADIUS
- TACACS +
- Kerberos
- PGP
- S/MIME

- Secure HTTP
- HTTPS
- TLS
- SSL
- IPsec

# Network Security Protocols

- There are various security protocols that works at the network, transport and application layers. These protocols help organizations to enhance the security of their data and communication against different types of attacks.

## Security protocols that work at Application Layer are as follows:

1) **RADIUS:** The RADIUS protocol provides security to remote access server to communicate with a central server.
2) **TACACS+:** The TACACS+ provides security using a client server model.
3) **Kerberos:** The Kerberos provides security using a client-server model.
4) **PGP protocol:** The PGP protocol provides security to the data through the method of encryption and decryption.
5) **S/MIME protocol:** Commonly known as Secure/Multi-Purpose Internet Mail Extension. The S/MIME protocol provides security to e-mails.
6) **Secure HTTP:** Secure HTTP provides secuirty to the data traversing through the world wide web.
7) **HTTPS:** The HTTPS ensures security of the data in a network.

# Network Security Protocols

- There are various security protocols that works at the network, transport and application layers. These protocols help organizations to enhance the security of their data and communication against different types of attacks.

## Security protocols that work at Transport layer:

1) **Transport Layer Security (TLS):** The TLS protocol provides security and dependability of data between two communicating parties.
2) **Secure Sockets Layer (SSL):** The SSL protocol provides security to the communication between a client and a server.

## Security protocols that work at Network layer:

1) **Internet Protocol Security (IPsec):** The IP sec protocol authenticates the packets during the transmission of data.

# Remote Authentication Dial-in User Service (RADIUS)

- Remote authentication dial-in user service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting (AAA) for remote access servers to communicate with a central server. RADIS has a client-server model, which works on the application layer of OSI model by using UDP or TCP as a transport protocol. [RFC2865 and RFC 2866

Provides Authen Author Accoun

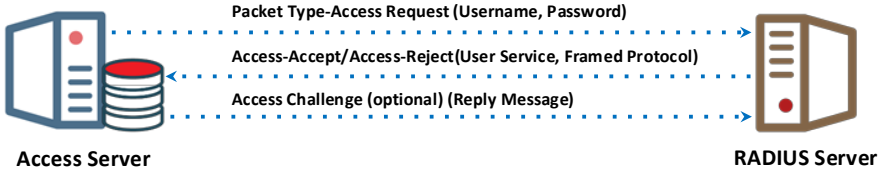
## Authentication Steps in RADIUS

1) A client initiates a connection by sending the **access-request packet** to the server

2) The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **access-accept message** along with the **access-challenge** to the client for additional authentication, else it sends back an **accept-reject** message

Username + Password

3) Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted

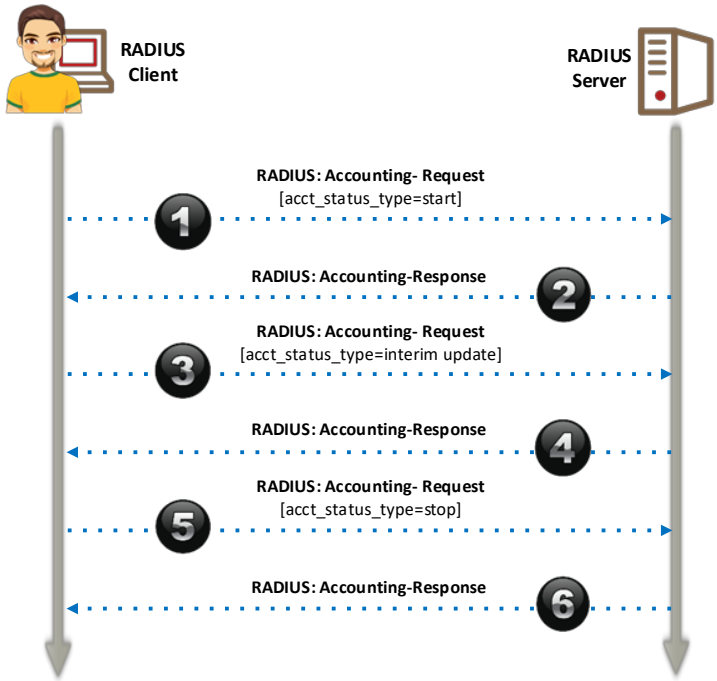


# Remote Authentication Dial-in User Service (RADIUS) (Cont'd)

## Radius Accounting Steps

- Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted

- The server receives this message and sends back the **accounting-response message** which states the successful establishment of the network



# Remote Authentication Dial-in User Service (RADIUS) (Cont'd)

## Radius AAA Protocol for mobile and local networks

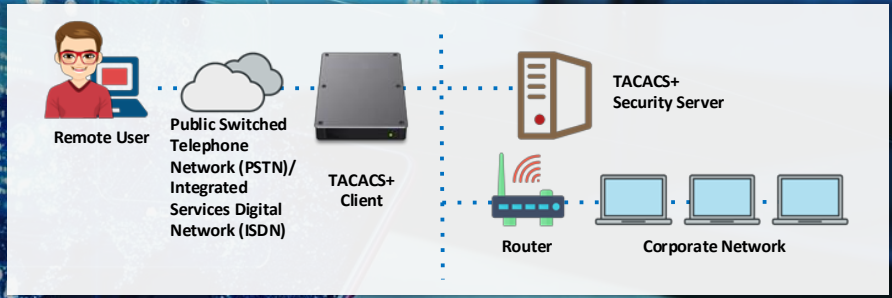
- Its uses the password authentication protocol(PAP), the challenge handshake authentication protocol(CHAP) or extensible authentication protocol (EAP) in order to authenticate the users communicating with servers.
- The components of a RADIUS AAA protocol are:
  - Access clients
  - Accesss server
  - RADIUS proxies
  - RADIUS servers
  - User account databases

Radius messages are sent as UDP messages and allow one RADIUS message in the UDP payload section of the RADIUS packet. RADIUS messages consist of a RADIUS header and other RADIUS attributes.

تعمولك جاء عليه سؤال

# Terminal Access Controller Access Control System Plus (TACACS+)

- The terminal access controller access control system plus (TACACS+) is a **network security protocol** used for AAA of network devices such as switches, routers, and firewalls through one or more **centralized servers**
- TACACS+ **encrypts** the entire communication between the client and the server including the user's password which protects it from sniffing attacks
- It is a **client-server model** approach where the client (user or network device) requests for connection to a server, the server authenticates the user by examining their credentials




**Authentication of TACACS+**

Consider the following example of authentication where a laptop user is connecting to a network-attached storage (NAS, router). The TACACS+ authentication involves the following steps:

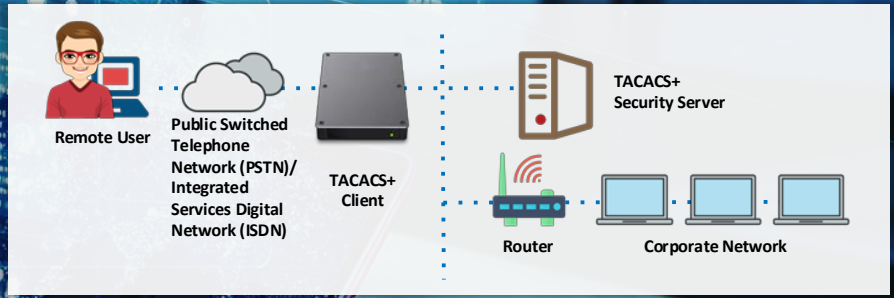
- **Step 1**: A user initiates the connection for authentication
- **Step 2**: The router and the user exchange authentication parameters
- **Step 3**: The router sends the parameters to the server for authentication
- **Step 4**: The server responds with the REPLY message based on the provided information

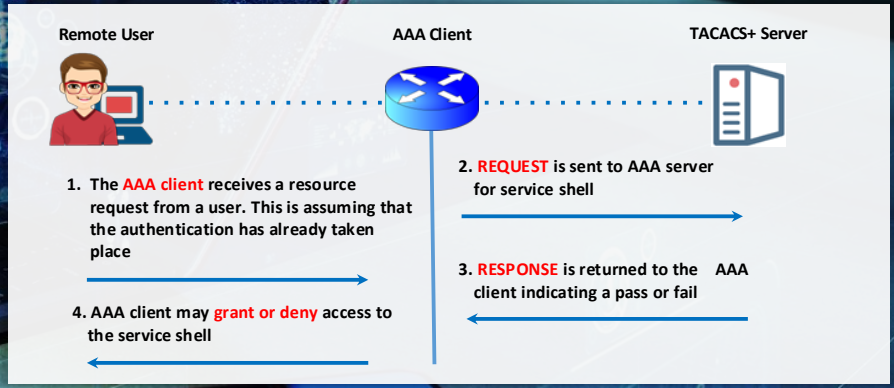
# Terminal Access Controller Access Control System Plus (TACACS+)

**Authentication of TACACS+**

Consider the following example of authentication where a laptop user is connecting to a network-attached storage (NAS, router). The TACACS+ authentication involves the following steps:

- **Step 1**: A user initiates the connection for authentication
- **Step 2**: The router and the user exchange authentication parameters
- **Step 3**: The router sends the parameters to the server for authentication
- **Step 4**: The server responds with the REPLY message based on the provided information



# RADIUS vs TACACS+

**Difference between RADIUS and TACACS+**

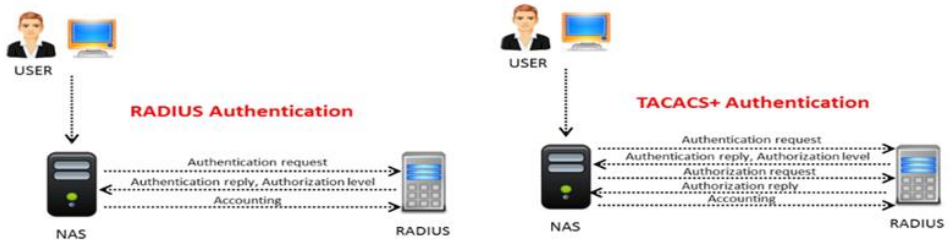



FIGURE 3.48: Schematic Showing the Different Between RADIUS and TACACS+ Protocols

| RADIUS | TACACS+ |
|---|---|
| Combines authentication and authorization | Separates all three elements of AAA, thus making it more flexible |
| Encrypts only the password | Encrypts the username and password كل شي |
| Requires each network device to contain authorization configuration | Central management for authorization configuration |
| UDP- Connectionless UDP ports 1645/1646, 1812/1813 | TCP- Connection oriented TCP port 49 |

TABLE 3.2: Difference between RADIUS and TACACS+

# Kerberos

- Kerberos is a network **authentication protocol** that is implemented for authenticating requests in computer networks.

## Kerberos authentication protocol (KAP)

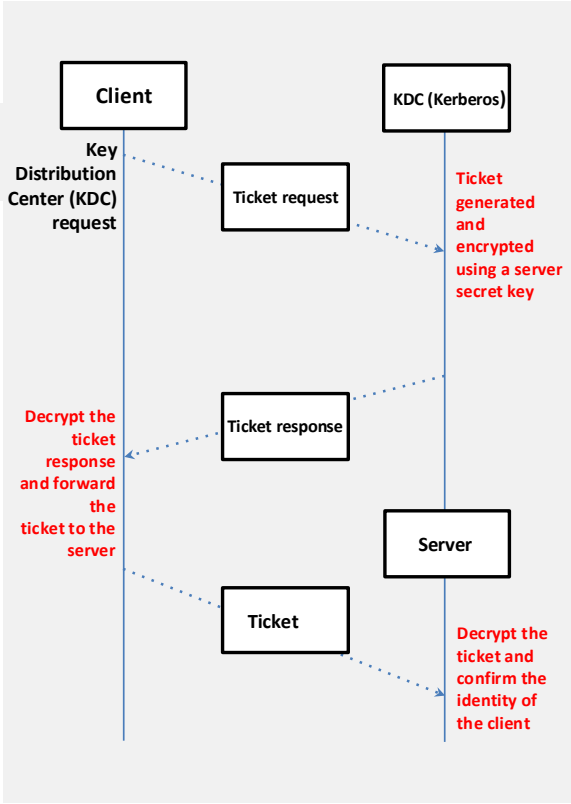
**01** A user sends his/her credentials to an **authentication server** (**AS**)

**02** The AS hashes the password of the user and verifies their credentials in the active directory database. If the credential matches, then AS (consisting of the ticket granting service, TGS) sends back the TGS session key and ticket granting ticket (TGT) to the user to create a session

**03** Once users are authenticated, they send the TGT to request a service ticket to the server or TGS for accessing the services

**04** The TGS authenticates the TGT and grants a **service ticket** to the user. The service ticket consists of the ticket and a session key

**05** The client sends the service ticket to the server. The server uses its key to **decrypt** the information from the TGS and the client is authenticated to the server



سیناریو : این افضل پروتوکله

# Pretty Good Privacy (PGP)

- Pretty good privacy (PGP) is an application layer protocol which provides **cryptographic privacy** and authentication for network communication

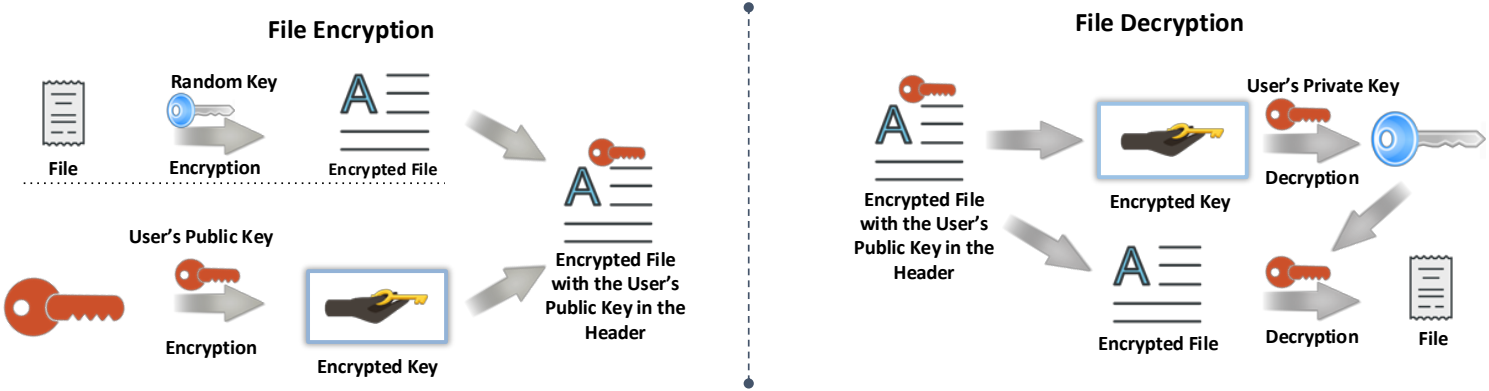
- It encrypts and decrypts email communication as well as authenticates messages with **digital signatures** and encrypts stored files

**How Does PGP Work?**

Every user has a public encryption key and a private key. Messages are sent to another user after encrypting them using the public key. The receiver decrypts the message using their private key. PGP compresses the message, resulting in an increase in the security of the message in the network. PGP creates a session key which is used only once. It encrypts the message using the session key along with the encryption algorithm. The session key is encrypted by the recipient's public key. The public key encrypted session key is sent to the recipient along with the encrypted message.

A recipient uses their private key to decrypt the session key and to decrypt the entire message.

# Pretty Good Privacy (PGP)




There are two versions of PGP:

- RSA Algorithm
- Diffie-Hellman Algorithm

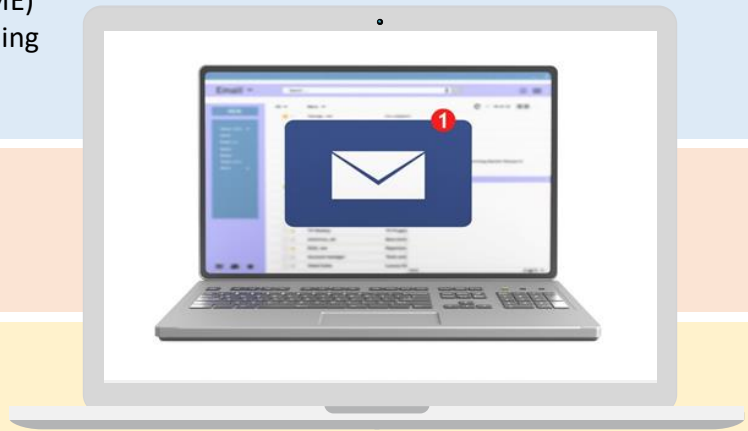
PGP creates a hash code from the user's name and signature to encrypt the sender's private key. The receiver uses the sender's public key to decrypt the hash code.

# Secure/Multipurpose Internet Mail Extensions (S/MIME)

**01** Secure/multipurpose internet mail extensions (S/MIME) is an application layer protocol which is used for sending **digitally signed** and **encrypted email messages**

**02** It uses the **RSA** system for email encryption

**03** Network defenders need to **enable** S/MIME-based security for mailboxes in their organizations

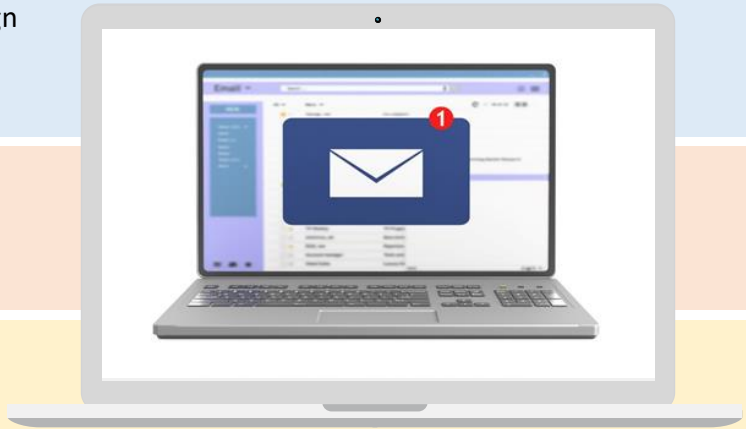


# Secure/Multipurpose Internet Mail Extensions (S/MIME)

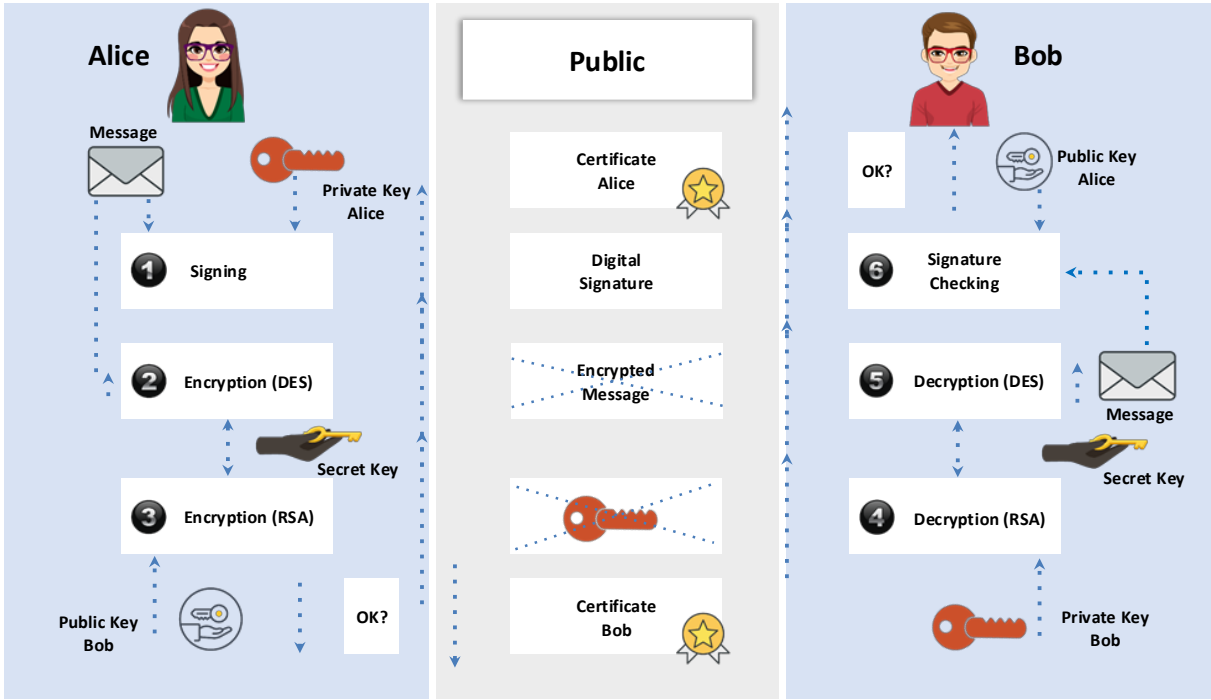
**04** Secure/multipurpose internet mail extensions (S/MIME) allows you to encrypt email messages and digitally sign them to ensure confidentiality, integrity and non-repudiation for messages.

**05** It provides cryptographic security services such as: Authentication, Message integrity, Non-repudiation, Privacy, Data Security

**06** An S/MIME protocol needs to ensure that it gains a certificate from the CA or from a public CA. The protocol uses different private keys for signature and for encryption.

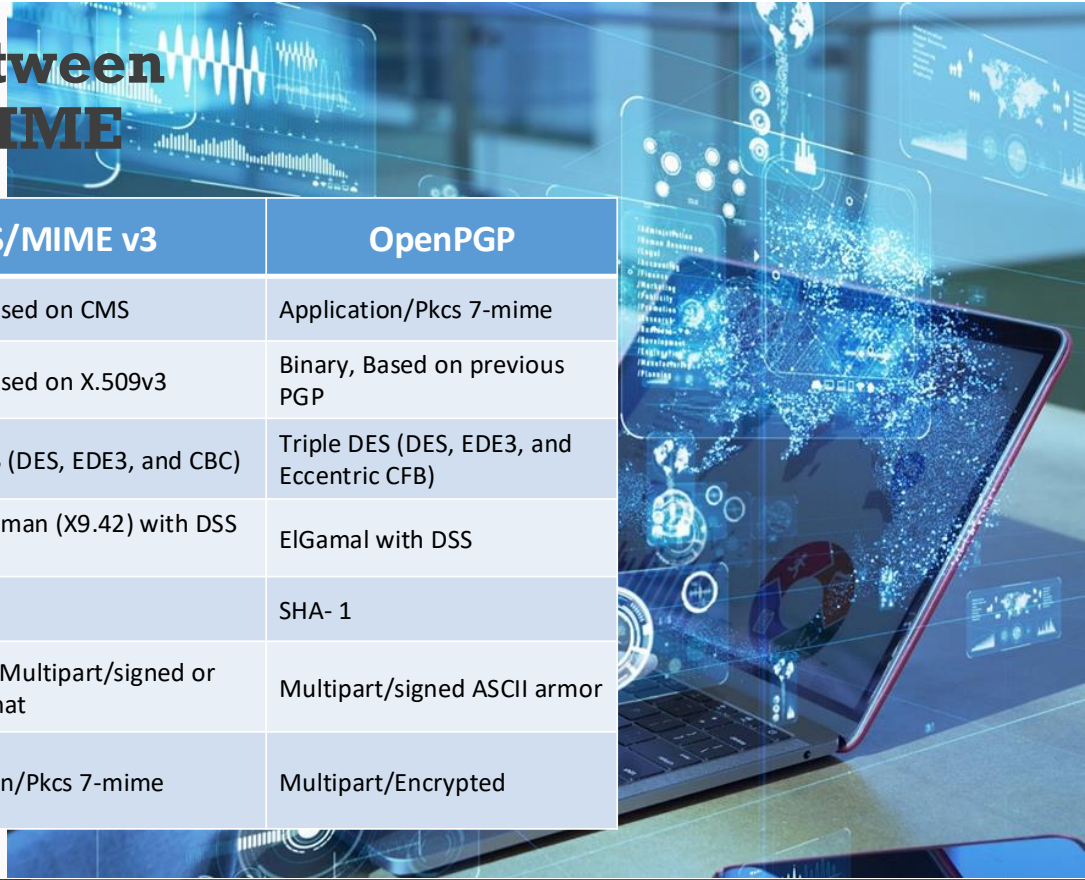


# Secure/Multipurpose Internet Mail Extensions (S/MIME) (Cont'd)



# Differences between PGP and S/MIME

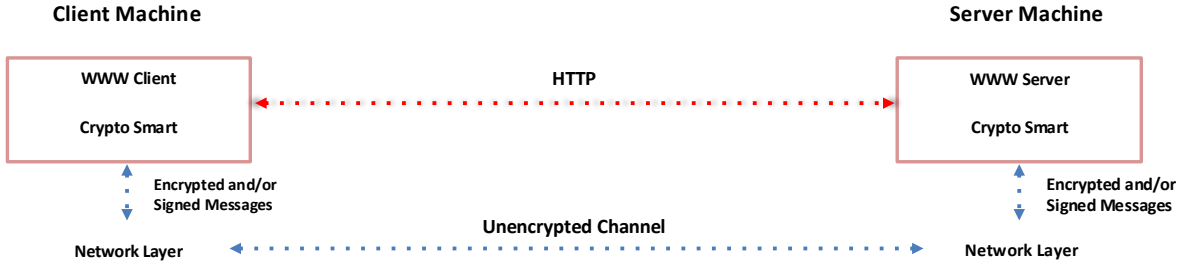
| Mandatory Features | S/MIME v3 | OpenPGP |
|---|---|---|
| Message Format | Binary, Based on CMS | Application/Pkcs 7-mime |
| Certificate Format | Binary, Based on X.509v3 | Binary, Based on previous PGP |
| Symmetric Encryption Algorithm | Triple DES (DES, EDE3, and CBC) | Triple DES (DES, EDE3, and Eccentric CFB) |
| Signature Algorithm | Diffie-Hellman (X9.42) with DSS or RSA | ElGamal with DSS |
| Hash Algorithm | SHA- 1 | SHA- 1 |
| MIME Encapsulation of Signed Data | Choice of Multipart/signed or CMS Format | Multipart/signed ASCII armor |
| MIME Encapsulation of Encrypted Data | Application/Pkcs 7-mime | Multipart/Encrypted |



# Secure Hypertext Transfer Protocol (S-HTTP)

- Secure hypertext transfer protocol (S-HTTP) is an application layer protocol that is used to **encrypt web communications** carried over HTTP
- It is an alternative for the **HTTPS** (SSL) protocol
- It ensures **secure data transmission** of individual messages, while SSL establishes a secure connection between two entities thus ensuring security of the entire communication

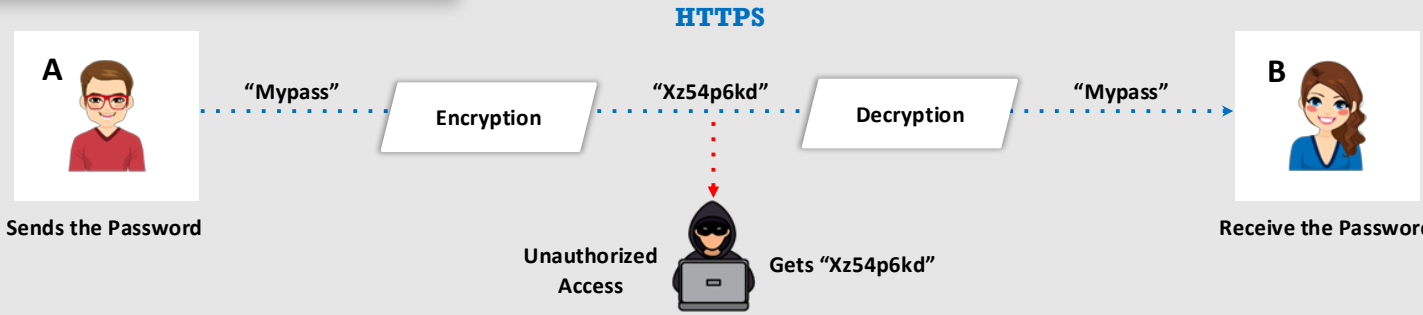

**S-HTTP Application- Level Security**




**Note**: Not all Web browsers and servers support S-HTTP

# Hypertext Transfer Protocol Secure (HTTPS)


- Hypertext transfer protocol secure (HTTPS) ensures **secure communication** between two computers over HTTP
- The connection is **encrypted** using a transport layer security (TLS) or SSL protocol
- It is often used in **confidential online transactions**
- It protects against **man-in-the-middle attacks** since the data are transmitted over an encrypted channel



# Hypertext Transfer Protocol Secure (HTTPS)


HTTPS mainly uses SSL in order to protect any website, thus making it easier for users to access the website. SSL has the following advantages:

- It encrypts the confidential information during exchange of data.
- It maintains a record of the details of the certificate owner.
- A CA checks the owner of the certificate while issuing it.
- It is often used in confidential online transactions.

# Transport Layer Security (TLS)

- Transport layer security (TLS) ensures a **secure communication** between client-server applications over the internet by ensuring the confidentiality and reliability during communication using symmetric cryptography.
- It authenticates communication applications using public key cryptography.
- It **prevents** the network communication from being eavesdropped or tampered

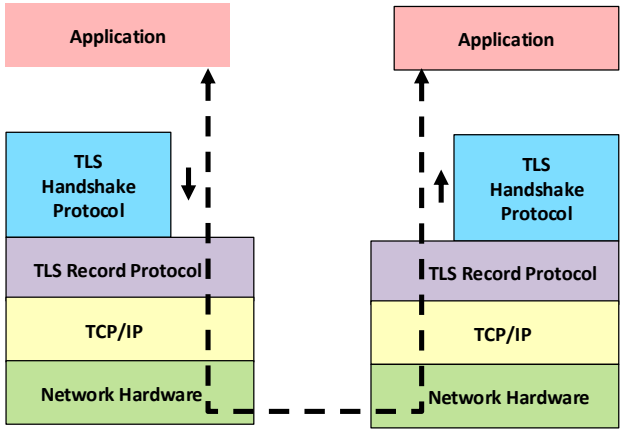
## Layers of TLS Protocol

**TLS Record Protocol**

- It ensures **connection security** with encryption

**TLS Handshake Protocol**

- It ensures server and client **authentication**




# Secure Sockets Layer (SSL)

- Secure sockets layer (SSL) was developed by Netscape for **managing the security** of a message transmission on the internet
- It uses the **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections

The secure sockets layer (SSL) is a protocol used for providing a secure authentication mechanism between two communicating applications such as a client and a server. SSL requires ca reliable transport protocol, such as TCP, for data transmission and reception.

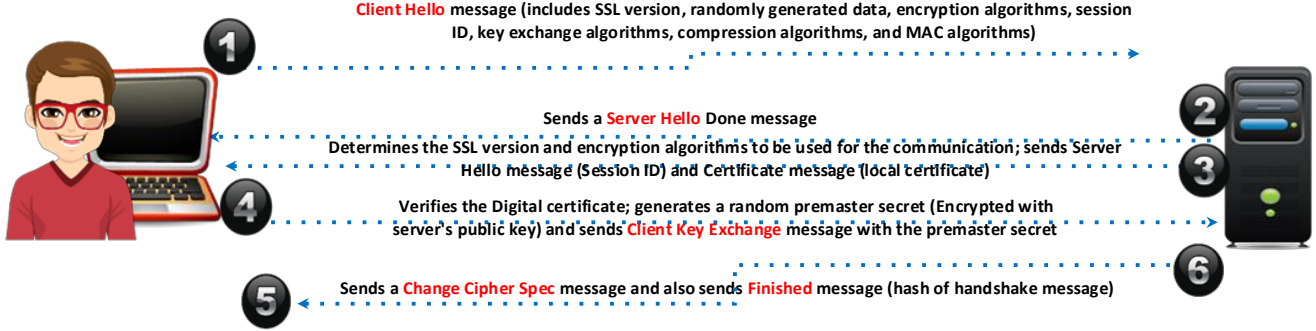
Any application-layer protocol that is higher than SSL, such as HTTP, FTP, and telnet, can form a transparent layer over the SSL. SSL acts as an arbitrator between the encryption algorithm and session key. It also verifies the destination server prior to the transmission and reception of data. SSL encrypts the complete data of the application protocol to ensure security.

The SSL protocol also offers "**channel security**" via three basic properties:

- **Private channel**: All the messages are encrypted after a simple handshake is used to define a secret key.
- **Authenticated channel:** The server endpoint of the conversation is always encrypted, whereas the client endpoint is optionally authenticated.
- **Reliable channel:** Message transfer undergoes an integrity check.

SSL uses both asymmetric and symmetric authentication mechanisms. Public key encryption verifies the identities of the server, the client, or both. Once the authentication is completed, the client and the server can create symmetric keys allowing them to communicate and transfer data rapidly. An SSL session is responsible for carrying out the SSL handshake protocol for organizing the states of the server and clients, thus ensuring the consistency of the protocol.

# Secure Sockets Layer (SSL)



# Internet Protocol Security (IPsec)

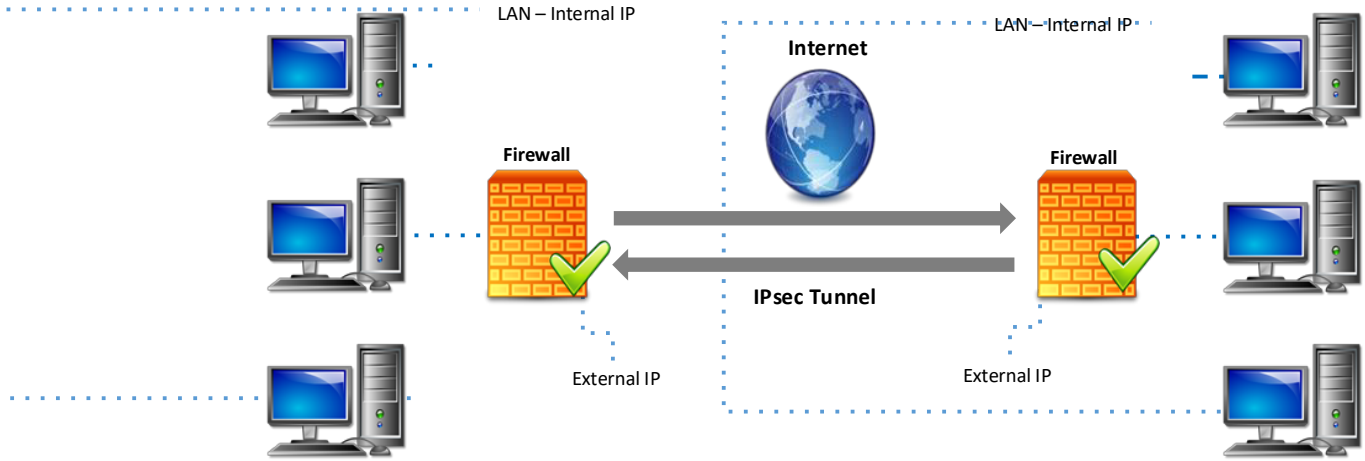
- Internet protocol security (IPsec) is a network layer protocol that ensures a **secure** IP level communication
- It provides **end-to-end security** at the internet layer of the internet protocol suite

- It **encrypts** and **authenticates** each IP packet in the communication
- It **supports** network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection

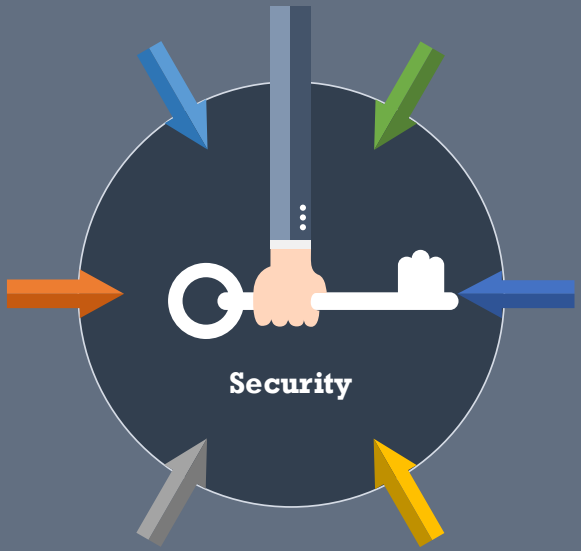
The internet protocol security (IPsec) protocol ensures secure communications over the IP network. It works at the application layer of the communication model. It makes use of the cryptographic security services to ensure a secure communication. It allows authentication of the IP packets during communication of data. IPsec is applied in virtual private networks and remote user access. It is used between a pair of hosts, a pair of security gateways, or between a security gateway and a host. It consists of two security services, namely, an authentication header (AH) and an encapsulating security payload (ESP). The AH allows authentication of the sender, whereas the ESP allows authentication of the sender as well as encryption of the data.

It provides secure communication for network-level peer authentication, data origin authentication and ensures data integrity, data confidentiality (encryption), and replay protection.

# Internet Protocol Security (IPsec)



# Module Summary




This module has discussed the essentials of network security, goal of network defense, and the information assurance (IA) principles

It has discussed benefits and challenges of network defense

It also discussed different types of network defense approaches and types of network security controls

Finally, this module ended with a detailed discussion of various network security protocols

In the next module, we will discuss in detail on identification, authentication, and authorization concepts