19z701 - Cryptography

NETWORK AND INTERNET SECURITY PROTOCOLS

22z211-Aravind Krishnan P
22z213-Arulmozhi B
22z217-Elakkiya G
22z218-Gayathri K S
22z226-Iniyaa N
23z433-Naveen P

Introduction & Fundamentals – Basics of Network Security

Definition of Network Security

- Network security involves protecting computer networks from unauthorized access, misuse, malfunction, modification, or destruction.
- It ensures that data is transmitted safely between devices over a network.

Goals of Network Security (CIA Triad)

1. **Confidentiality** – Ensuring that information is accessible only to authorized users.
    - Example: Encryption of messages so only intended users can read them.
2. **Integrity** – Maintaining the accuracy and consistency of data during transmission.
    - Example: Hashing or checksums to detect any modification in data.
3. **Availability** – Ensuring reliable access to network services and data when needed.
    - Example: Using redundancy and backup systems to prevent downtime.

Common Threats and Attacks

1. **Denial of Service (DoS) Attack:**
   Overloads a system or network, making it unavailable to legitimate users.
   - Example: Flooding a website with fake traffic.
2. **Man-in-the-Middle (MitM) Attack:**
   The attacker intercepts communication between two parties to steal or alter data.
   - Example: Eavesdropping on public Wi-Fi connections.
3. **Spoofing:**
   Impersonating a trusted device or user to gain unauthorized access.
   - Example: IP spoofing or email spoofing.
4. **Phishing:**
   Tricking users into revealing sensitive information using fake emails or websites.
5. **Malware:**
   Malicious software such as viruses, worms, ransomware that harm or steal data.

Security Services and Mechanisms

Security Service	Purpose	Example Mechanism
Authentication	Verifies the identity of a user or device	Passwords, Digital Certificates
Access Control	Restricts unauthorized access	Firewalls, ACLs
Data Confidentiality	Protects data from unauthorized disclosure	Encryption
Data Integrity	Ensures data is not altered	Hash Functions, Checksums
Non-repudiation	Prevents denial of message origin	Digital Signatures
Availability	Keeps services running continuously	Backups, Redundancy

Concept of Cryptography in Network Security

- **Cryptography** is the science of securing data using mathematical techniques.
- It converts plaintext into unreadable ciphertext and vice versa using keys.

Types of Cryptography:

1. **Symmetric Key Cryptography** – Same key for encryption & decryption (e.g., AES, DES).
2. **Asymmetric Key Cryptography** – Uses public & private key pairs (e.g., RSA, ECC).

Applications:

- Secure communication (HTTPS, VPNs)
- Digital signatures & certificates
- Data encryption in storage and transmission

Protocols for Secure Communication – SSL/TLS and HTTPS

Aravindhkrishnan P
22z211

SSL and TLS

SSL (Secure Sockets Layer)

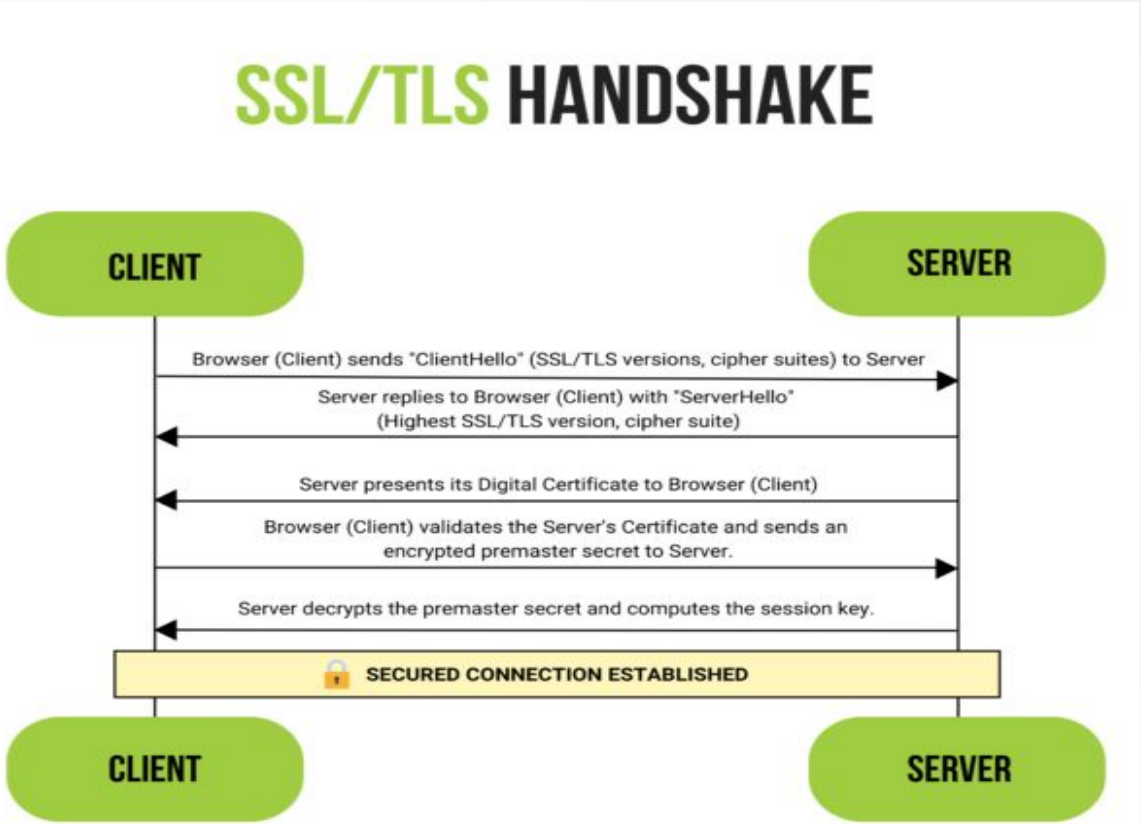
SSL is a protocol that secures the connection between a **user's browser and a web server** by encrypting data, ensuring privacy and protection from attackers. It provides confidentiality, authentication, and data integrity during online communication.

TLS (Transport Layer Security)

TLS is the **advanced and more secure version of SSL** that enhances encryption strength and performance. It is the standard protocol used today to protect internet communications, with TLS 1.3 offering the highest level of security.

What SSL/TLS Does

Encryption – Converts data into unreadable form to protect it from attackers.
Authentication – Verifies the website's identity using digital certificates.
Data Integrity – Ensures data isn't modified or corrupted during transmission.



1)ClientHello

2)ServerHello

3)Server Certificate

4)Verification and Key Exchange

5)Secure Connection Established

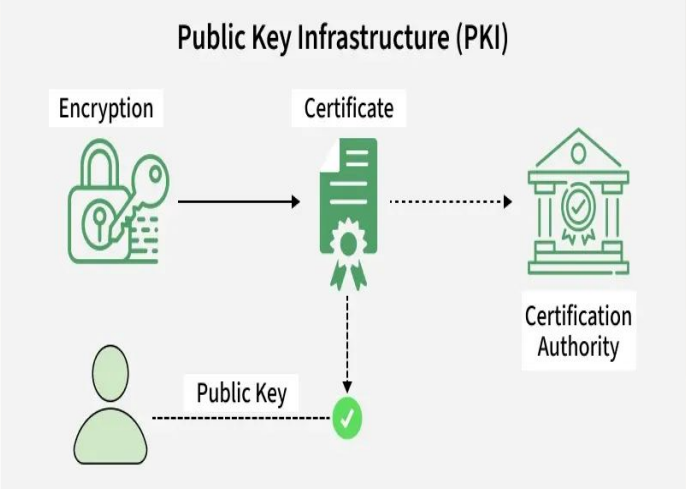
Public key Infrastructure

1. PKI and Encryption
PKI uses cryptographic methods to secure communication by linking public keys with verified identities. It prevents man-in-the-middle attacks using trusted digital certificates.

2. Digital Certificates
Digital certificates (X.509) uniquely identify users or systems and bind their public key to verified identity details. They ensure that communication happens with the intended entity.

3. Certification Authority (CA)
A CA is a trusted body that issues, verifies, and manages digital certificates. It validates identity, digitally signs certificates, and ensures trust in online transactions.

4. Revocation and Verification
If a certificate becomes invalid or compromised, the CA can revoke it. Verification of certificates using the CA's public key confirms authenticity and secure access.



How HTTPS Secures Web Traffic

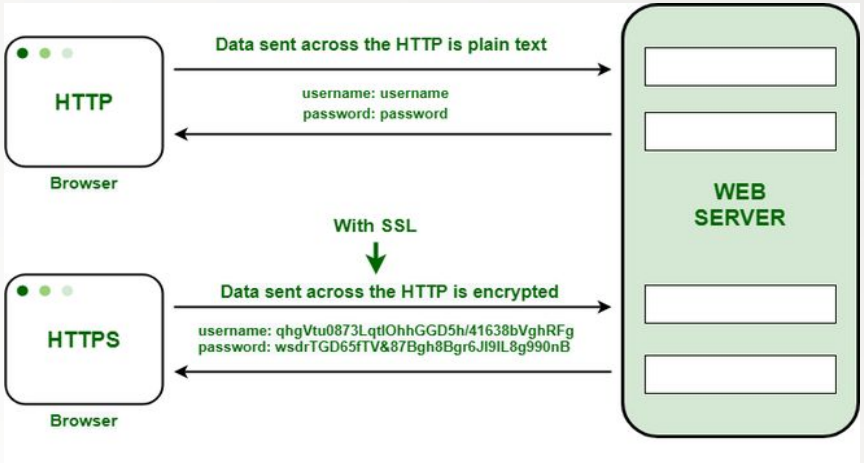
HTTPS = HTTP + SSL/TLS – adds encryption and authentication to HTTP. Uses **port 443** for secure data transmission.

Encrypts data between browser and server to prevent interception.

Authenticates the website to ensure it's genuine.

Maintains data integrity – prevents tampering during transfer.

Displays a **padlock** 🔒 **icon** in the browser to indicate a secure connection.



Email and Data Protection Protocols

Naveen P
23z433

Intro

Email and data protection are essential in today's interconnected digital environment. Sensitive information like **financial data, corporate documents, and personal communications** often travel across unsecured networks, making them vulnerable to interception or manipulation.

To maintain secure communication, several protocols are used: **Pretty Good Privacy (PGP)**, **Secure/Multipurpose Internet Mail Extensions (S/MIME)**, and secure file transfer methods such as **SFTP** and **FTPS**.

Pretty Good Privacy (PGP)

Overview:

- Created by *Phil Zimmermann (1991)* for secure email communication.
- Uses **hybrid encryption**:
  - **Symmetric** encryption for message content.
  - **Asymmetric** (public/private keys) for exchanging session keys.

Features:

- Digital signatures ensure authenticity and integrity.
- Uses a **Web of Trust** model for key verification.

How PGP Works

1. Sender encrypts message with a **session (symmetric) key**.
2. Session key is encrypted using recipient's **public key**.
3. Recipient decrypts the session key with their **private key**.
4. Message is then decrypted using that session key.

S/MIME (Secure/Multipurpose Internet Mail Extensions)

Overview:

- Built into enterprise email systems (e.g., Outlook, Gmail for Business).
- Based on **X.509 certificates** issued by trusted **(CAs).**

Functions:

- Encrypts messages for confidentiality.
- Digital signatures for authenticity and integrity.
- Automatic key management via certificates.

Secure File Transfer Protocols

SFTP (SSH File Transfer Protocol):

- Operates over **SSH (Port 22)**.
- Encrypts both authentication and data.
- Common in server-to-server and cloud file transfers.

FTPS (File Transfer Protocol Secure):

- Extension of **FTP** using **SSL/TLS (Port 990)**.
- Adds encryption and server authentication.
- Compatible with older FTP systems.

IPSec - Internet Protocol Security

Arulmozhi B - 22z213

IPSec - Internet Protocol Security

IP security (IPsec) is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.

Features of IPSec:

Authentication: IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
Confidentiality: IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
Integrity: IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
Key management: IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.

IPSec-Protocols

AH - Authentication Header

The authentication mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit.

ESP - Encapsulating Security Payload

The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.

IKE -Internet Key Exchange

Manages key generation, exchange, and negotiation of security parameters.

IPSec Architecture

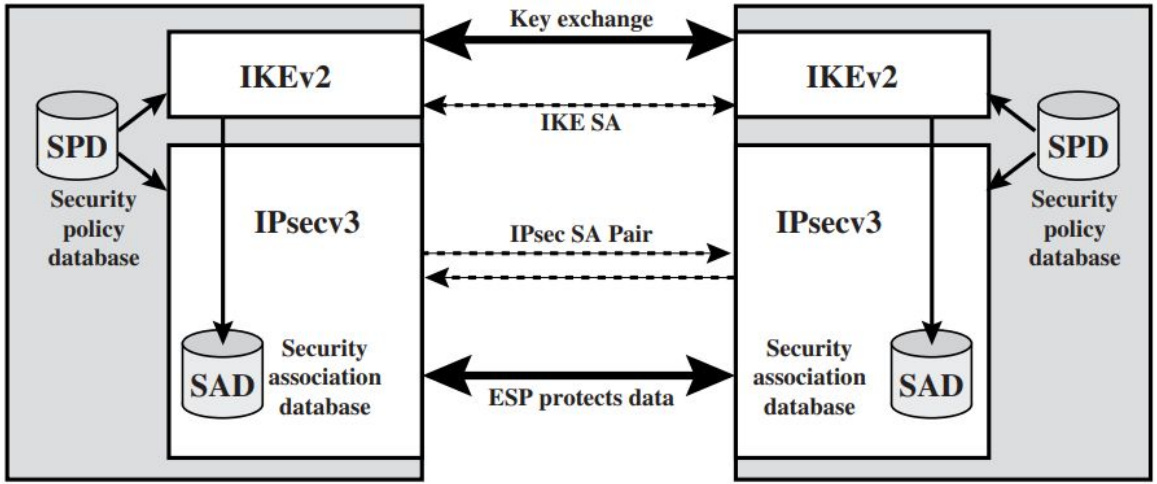
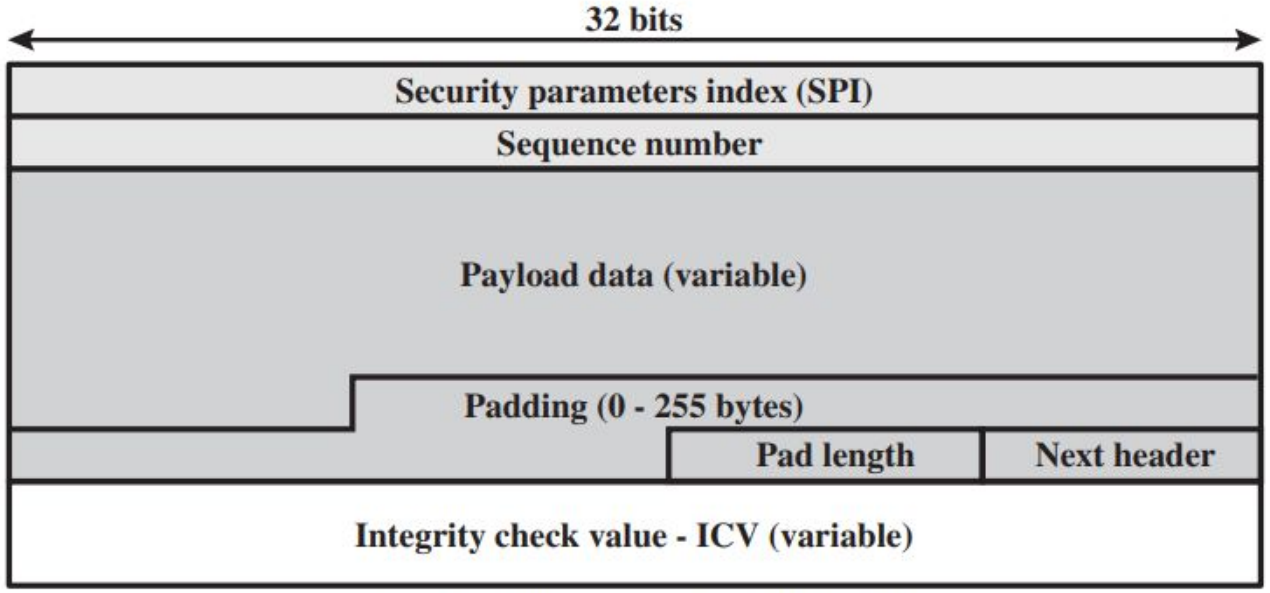


Figure 19.2 IPsec Architecture

ESP-Encapsulating Security Payload



(a) Top-level format of an ESP Packet

ESP Packet Format

Security Parameters Index (32 bits): Identifies a security association.
Sequence Number (32 bits): A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
Payload Data (variable): This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
Pad Length (8 bits): Indicates the number of pad bytes immediately preceding this field.
Next Header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
Integrity Check Value (variable): A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

Modes of ESP

Transport mode ESP: Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.

Tunnel mode ESP: Authentication applies to the entire IP packet delivered to the outer IP destination address (e.g., a firewall), and authentication is performed at that destination. The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination

1. Which of the following provides both authentication and confidentiality in IPSec?
A) AH (Authentication Header)
B) ESP (Encapsulating Security Payload)
C) IKE (Internet Key Exchange)

2)In which mode do you think IPSec is commonly used for VPNs : Transport Mode or Tunnel Mode?

Network Access & Authentication Protocols

GAYATHRI K S
22Z218

Network Access & Authentication Protocols

Network Access and Authentication Protocols ensure that only **authorized users** and **devices** can access network resources.

These protocols help maintain **security, confidentiality, integrity, and accountability** in communication.

Common authentication protocols include:

Kerberos: Ticket-based authentication system.

RADIUS: Centralized Authentication, Authorization, and Accounting (AAA) protocol.

EAP: Framework that supports multiple authentication methods.

Used in enterprise systems, wireless networks, and secure login mechanisms.

KERBEROS AUTHENTICATION PROTOCOL

Kerberos is a **network authentication protocol** developed at **MIT**.

It provides **secure authentication** using **symmetric key cryptography** and **trusted third-party servers**.

Eliminates the need to send passwords over the network.

Works based on the **“ticket” system** for verified and time-limited access.

Commonly used in **Windows domains**, **enterprise environments**, and **university networks**.

Main Components of Kerberos

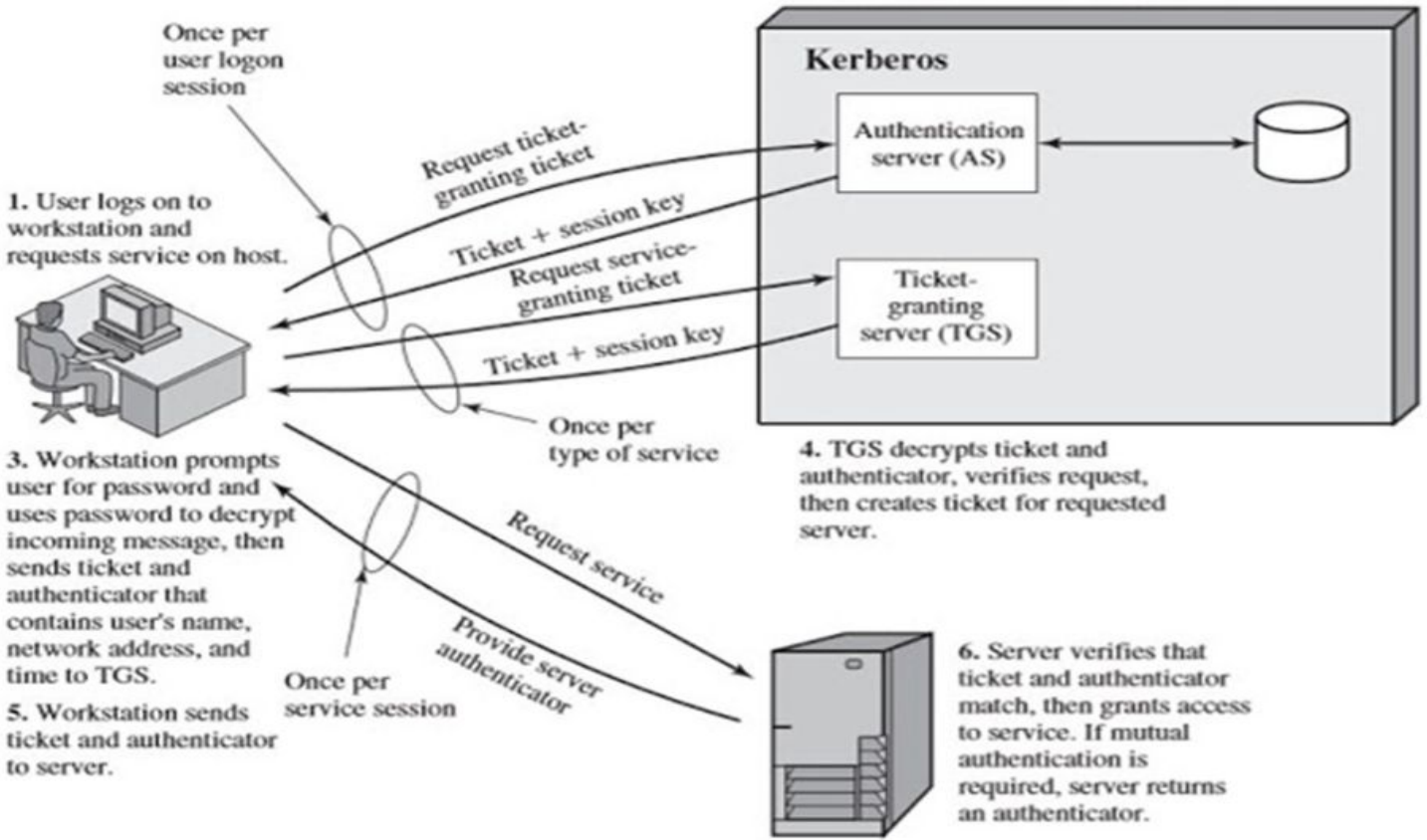
Client: The client is one who initiates communication for a service request.

Server: It contains the service that the user wants to access.

Authentication Server: It verifies the user's details, if the authentication happens successfully then it generates TGT (Ticket Granting Ticket) that provides a time span for a limited time or fixed time.

Ticket Granting Server: TGS issues a service ticket as a service that verifies a user to the server and grants access to the user.

Service Server (Application server): The actual server providing the requested service.


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Once per user logon session
Kerberos
Authentication server (AS)
Request ticket-granting ticket
Ticket + session key
1. User logs on to workstation and requests service on host.
Request service-granting ticket
Ticket-granting server (TGS)
Ticket + session key
Once per type of service
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
Request service
Provide server authenticator
Once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

RADIUS SERVER AUTHENTICATION PROTOCOL

RADIUS (Remote Authentication Dial-In User Service) is a **client-server protocol** used for **centralized authentication, authorization, and accounting (AAA)**.

Developed by **Livingston Enterprises**, standardized by **IETF**.

Widely used by **Internet Service Providers**, **corporate networks**, and **Wi-Fi systems**.

Operates over **UDP ports 1812 (Authentication)** and **1813 (Accounting)**.

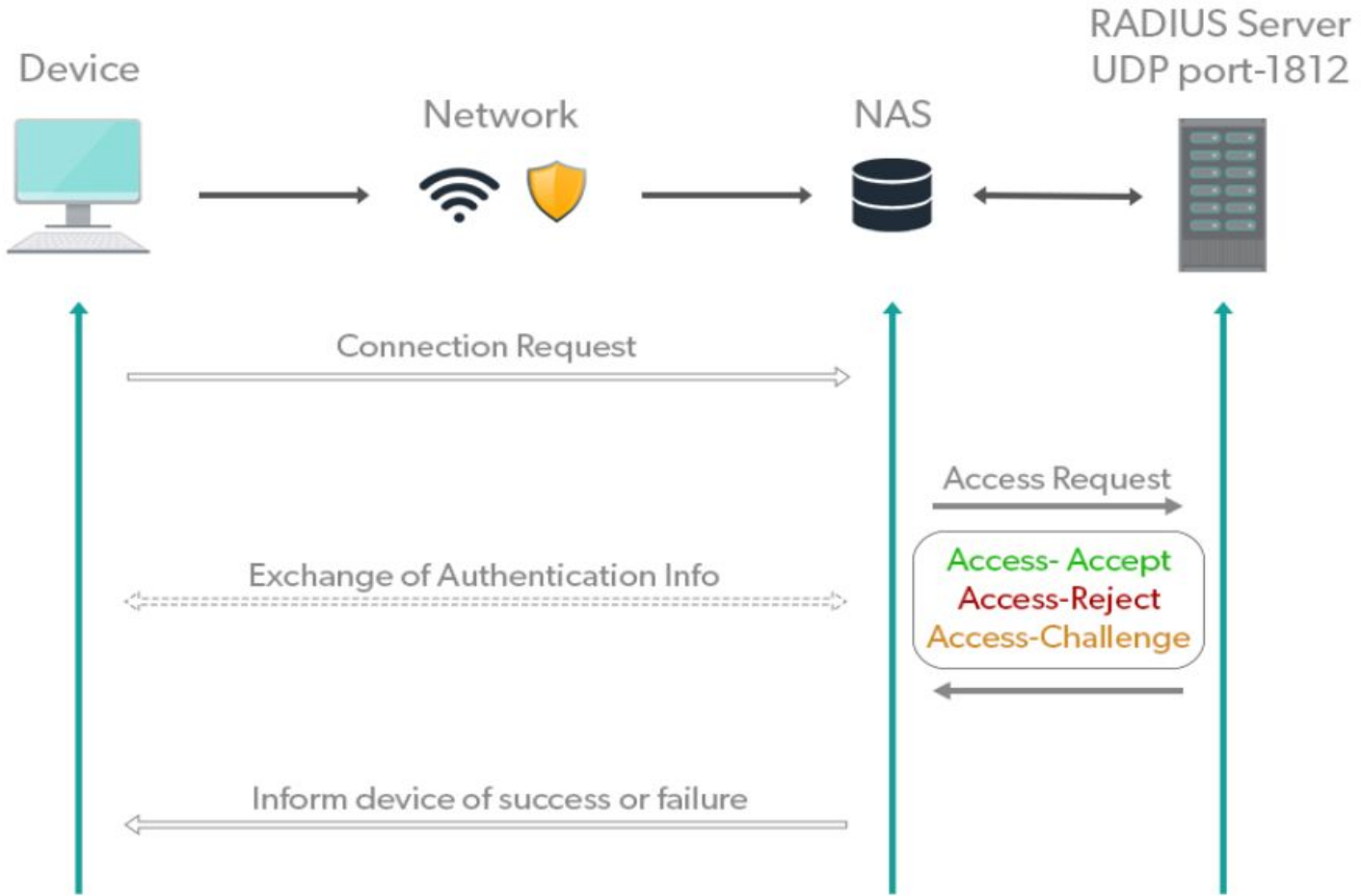
Ensures centralized control over who can access the network and tracks their usage.

RADIUS Components

RADIUS uses a client-server model, and its three primary components include the:

1. **Client/Supplicant:** The device/user seeking access to a network.
2. **Network Access Server (NAS):** The gateway between a user and a network.
3. **RADIUS Server:** Authentication server that ensures the user is allowed to access the network with the proper permission levels. This server can also provide accounting functions for the purposes of billing, time tracking, and device/connection details.

RADIUS Authentication Process



Other Common Network Authentication Protocols

TACACS+ (Terminal Access Controller Access Control System Plus)

- Used mainly by **Cisco network devices**
- Separates **Authentication, Authorization, and Accounting (AAA)**
- Uses **TCP Port 49** and **encrypts entire packets** (more secure than RADIUS)

LDAP (Lightweight Directory Access Protocol)

- Used to **access and manage directory services** (e.g., Active Directory)
- Often integrated with **Kerberos or RADIUS** for centralized authentication

OAuth 2.0 / OpenID Connect

- Common in **web and cloud logins**
- Uses **token-based authentication** instead of passwords
- Example: “**Sign in with Google**” or “**Sign in with Facebook**”

EAP (Extensible Authentication Protocol)

- Used in **Wi-Fi (802.1X) enterprise networks**
- Works with **RADIUS** to support methods like **EAP-TLS**, **PEAP**, etc.

In the Kerberos authentication process, what is the main purpose of the Ticket-Granting Ticket (TGT)?

A) To encrypt the user's password before sending it to the server
B) To request service tickets without re-entering the password
C) To establish a direct connection with the service server
D) To store user credentials permanently

RADIUS mainly operates using which transport protocol and port for authentication?

A) TCP Port 49

B) UDP Port 88

C) UDP Port 1812

D) TCP Port 1813

Modern & Emerging Security Protocols

INIYAA-22Z226

DNSSEC (Domain Name System Security Extensions)

Domain Name System Security Extensions(DNSSEC) is a DNS extension protocol and are used for securing DNS records by employing digital signatures and cryptographic keys(public and private) for encryption and decryption.

Why It's Needed ?

Traditional DNS is vulnerable to attacks like:

- DNS Spoofing / Cache Poisoning – attackers fake DNS responses to redirect users to malicious sites.

- Man-in-the-Middle (MITM) – intercepting DNS requests to change the response.

How DNSSEC Works

1. DNS Query Request

User enters a domain ,The local DNS (ISP) checks its cache; if not found, it forwards the request up the DNS chain.

2.Root DNS Server

- If the local DNS cannot resolve the query, it contacts a Root DNS Server.
- The root server does not have the exact IP address but directs the query to the correct Top-Level Domain (TLD) server (e.g., .com, .org, .net).

3.TLD DNS Server

- The TLD server receives the request from the root server.
- It also doesn’t store the full IP address but provides the address of the Authoritative Name Server responsible for that specific domain.

4.Authoritative Name Server

- The Authoritative DNS Server holds the actual DNS records
- With DNSSEC enabled, it signs the DNS response using its private key, creating a digital signature that proves authenticity.

5. DNS Response Verification

- The resolver verifies the digital signature using the public key.
- If valid → data is trusted; if not → the response is rejected.

6. User Access

The verified IP address is returned, allowing the user's browser to connect securely to the website.

HSTS (HTTP Strict Transport Security)

HSTS is a web security policy that ensures browsers connect to a website exclusively via HTTPS, never through HTTP. It protects users by preventing SSL stripping and man-in-the-middle (MITM) attacks.

When a user visits a website via HTTPS for the first time, the server sends a special HTTP response header:

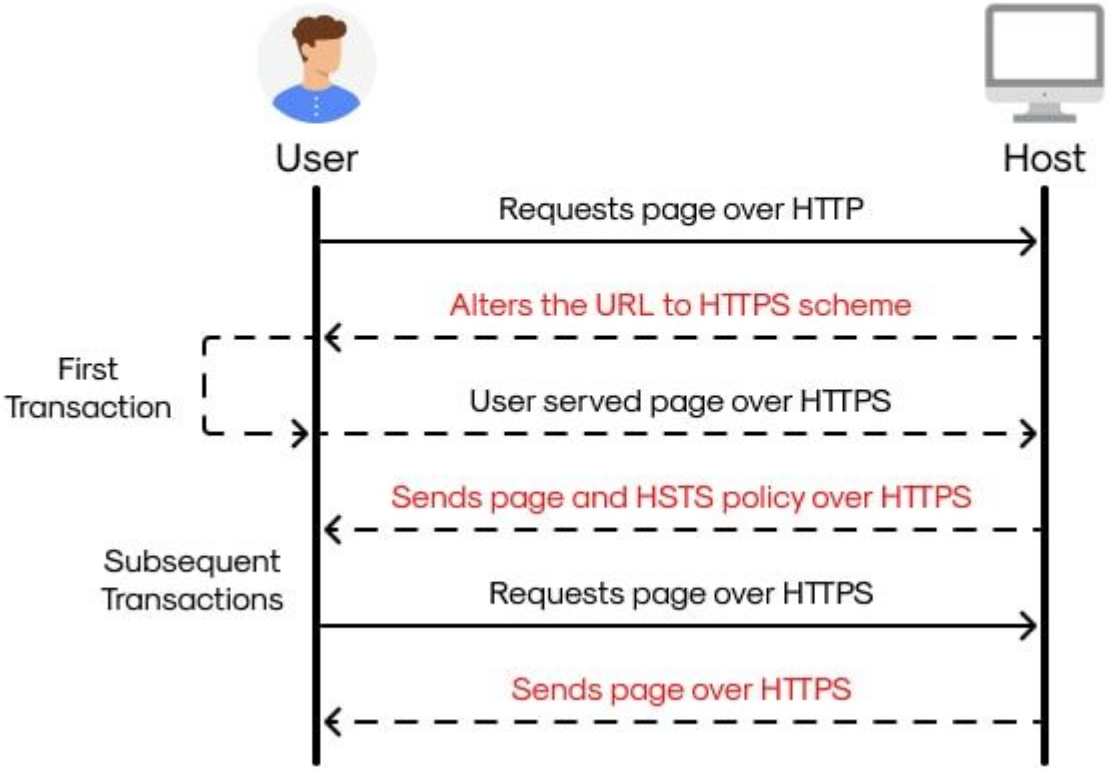
syntax:

Strict-Transport-Security: max-age=<expire-time>; includeSubDomains; preload

max-age=<expire-time>:Defines how long the browser should remember to use HTTPS
includeSubDomains: Applies the HSTS rule not just to the main domain, but also to all its subdomains.
Preload: Once a domain is on the preload list, browsers like Chrome or Safari will automatically enforce HTTPS for it .even on a user's first visit.

wallarm

How HSTS Works in Browsers?

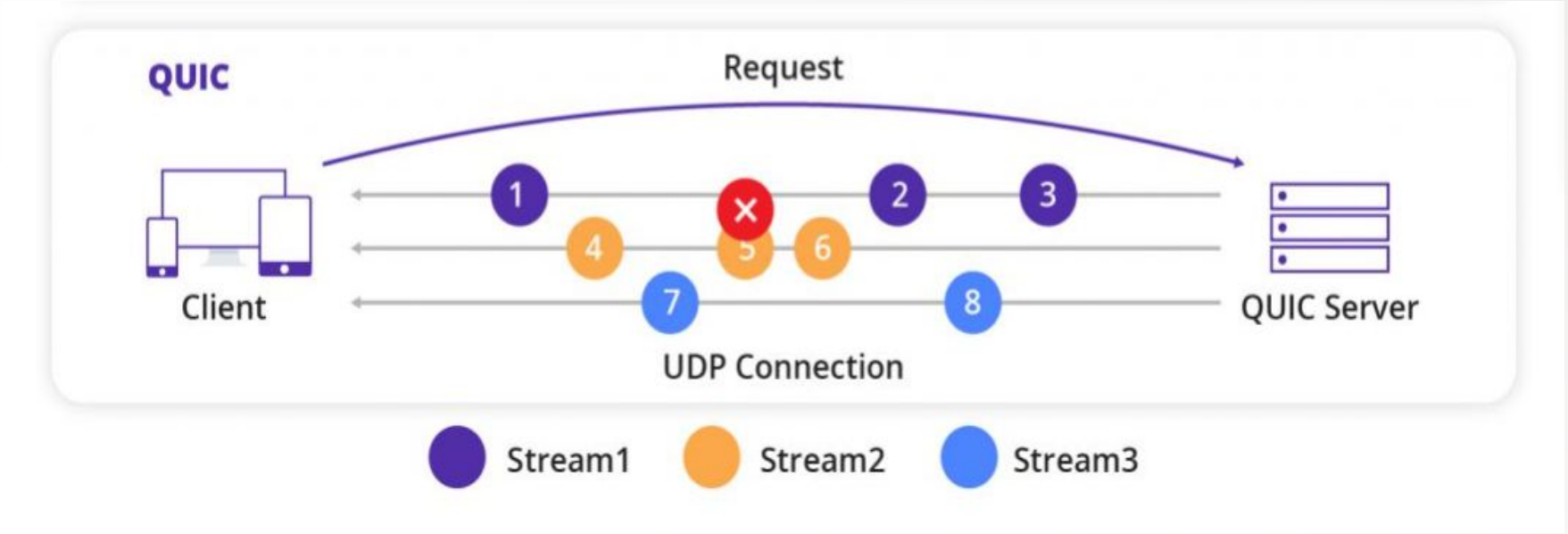


QUIC (Quick UDP Internet Connections)

QUIC is a transport layer network protocol developed by Google that aims to make internet connections faster and more secure than traditional TCP (used by HTTP/HTTPS).

Key Features:

- Uses UDP instead of TCP
- Faster connection setup
- Built-in encryption
- Improved performance


QUIC
Request
1
2
3
4
5
6
7
8
Client
QUIC Server
UDP Connection
Stream1
Stream2
Stream3

THANK YOU!