

Network & Internet Security Protocols

Prithvin K C
Sandeep K
Vigneshwaran P
Krishanu Dey
Mukesh E
Sudharsan S

Introduction

22z271
Vigneshwaran P




What is Network Security?

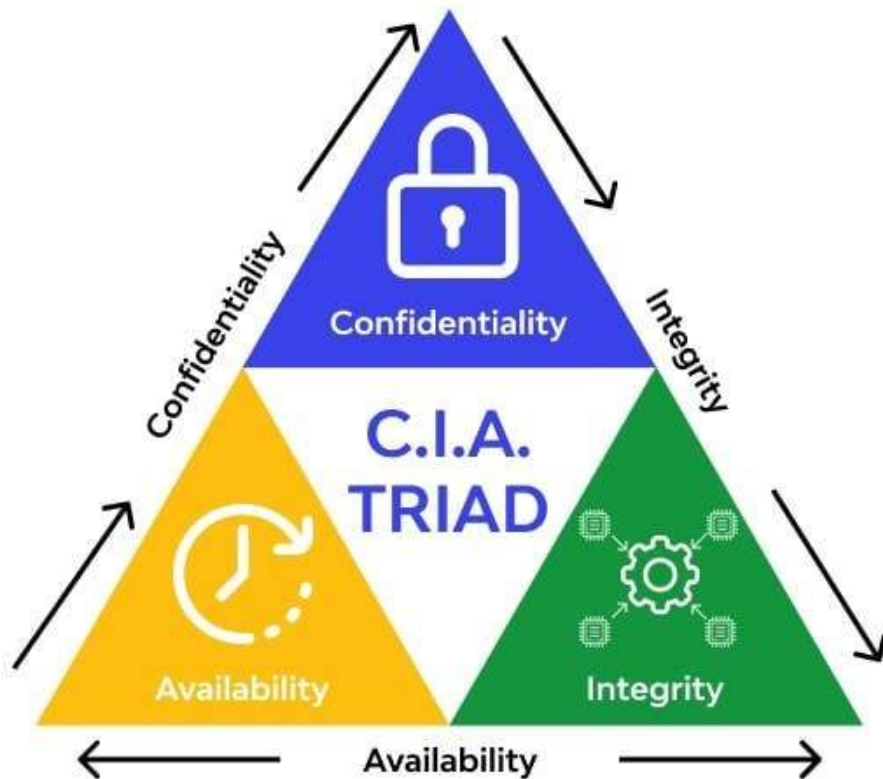
- Network Security refers to protecting **data transmission** and **networked systems** from unauthorized access or misuse.
- Involves **cryptography, authentication, and secure protocols** to maintain trust.
- Goal: ensure **safe communication** across wired & wireless networks.
- Cryptography is the **foundation** that enables secure data exchange in networks.

Why Do We Need Network Security?

- Cyber threats target **data confidentiality**, **system integrity**, and **service availability**.
- Increasing risks:
 - Phishing
 - Ransomware
 - Data leaks
 - Man-in-the-middle attacks.
- Network security uses **encryption (cryptography)** and **protocols** like SSL/TLS, IPsec to protect against these.

CIA Triad (Core Security Principles)

Principle	Description	Cryptographic Mechanism / Example
 Confidentiality	Ensures that sensitive information is accessible only to authorized users. Prevents data disclosure	Encryption algorithms – AES, RSA, DES Protocols – SSL/TLS, IPsec (ESP)
 Integrity	Guarantees that data is not altered or tampered with during transfer or storage, Any unauthorized modification can be detected.	Hashing algorithms – SHA-256, MD5 Digital Signatures, Message Authentication Codes (MAC)
 Availability	Ensures that systems and data are available to legitimate users whenever needed, even during attacks or failures.	Redundancy, Backups, Firewalls Load Balancing, DDoS Mitigation






Major Security Threats

- **Eavesdropping:** Intercepting unencrypted data → solved using **encryption**.
- **Data Modification:** Altering transmitted packets → prevented by **integrity checks** (hashing).
- **Identity Spoofing:** Pretending to be another → prevented using **authentication** (digital signatures).
- **Denial of Service:** Overwhelming network resources → handled by network-level defenses.

Need for Security Protocols

Security protocols define **how cryptography is applied** to protect communication.

They ensure:

-  **Confidentiality:** Encryption of transmitted data.
-  **Integrity:** Hashing and signatures.
-  **Authentication:** Certificates, keys, tokens.

Examples: **SSL/TLS, IPsec, PGP, SSH, Kerberos.**

Cryptography Basics

Krishanu Dey

22z277

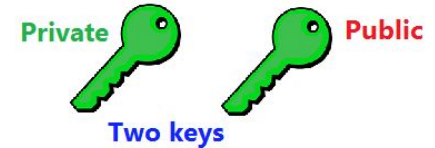
Symmetric vs Asymmetric Encryption

Feature	Symmetric	Asymmetric
Keys Used	Same key for encryption & decryption	Public key for encryption, private key for decryption
Speed	Faster	Slower
Security	Less secure (key sharing risk)	More secure (no need to share private key)
Example	AES, DES	RSA, ECC

Symmetric Encryption



Asymmetric Encryption



What is Hashing?

- Converts data into a fixed-length hash value.
- It's a one-way function – cannot be reversed.
- Used to verify data integrity.
- Small input changes produce completely different outputs (avalanche effect).

Examples:

SHA-256, MD5, SHA-1



Digital Signatures

- Provide authentication, integrity, and non-repudiation.
- Created using private key and verified using public key.
- Ensures the message hasn't been tampered with.

Process:

1. Sender hashes the message.
2. Encrypts the hash with their private key → Digital Signature.
3. Receiver decrypts using sender's public key and verifies hash.

Public Key Infrastructure (PKI)

- Framework for managing digital keys and certificates.
- Includes:
 - **Certificate Authority (CA):** Issues certificates.
 - **Registration Authority (RA):** Verifies user identity.
 - **Certificate Repository:** Stores valid/revoked certificates.
- Ensures secure key distribution and trust between parties.

Digital Certificates

- Electronic document issued by a Certificate Authority (CA).
- Binds a public key to an entity's identity.
- Common standard: X.509
- Used in HTTPS, email security, and code signing.

Example:

Website's SSL/TLS certificate proves it's legitimate.

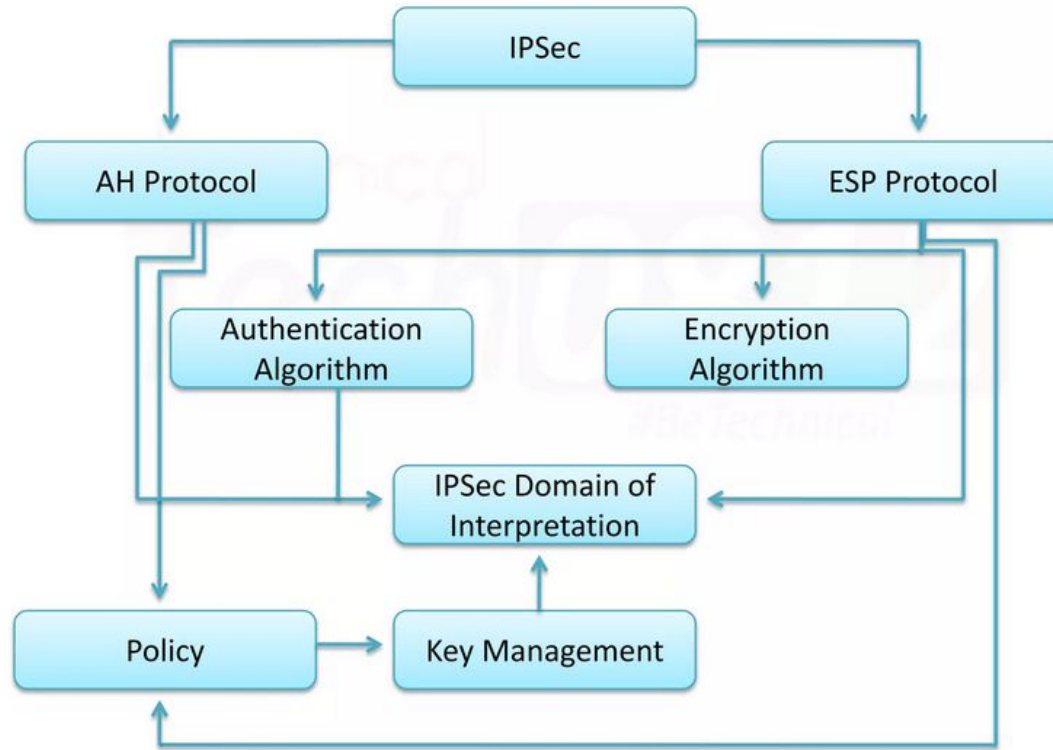
Network Layer Security

Mukesh E - 22z278

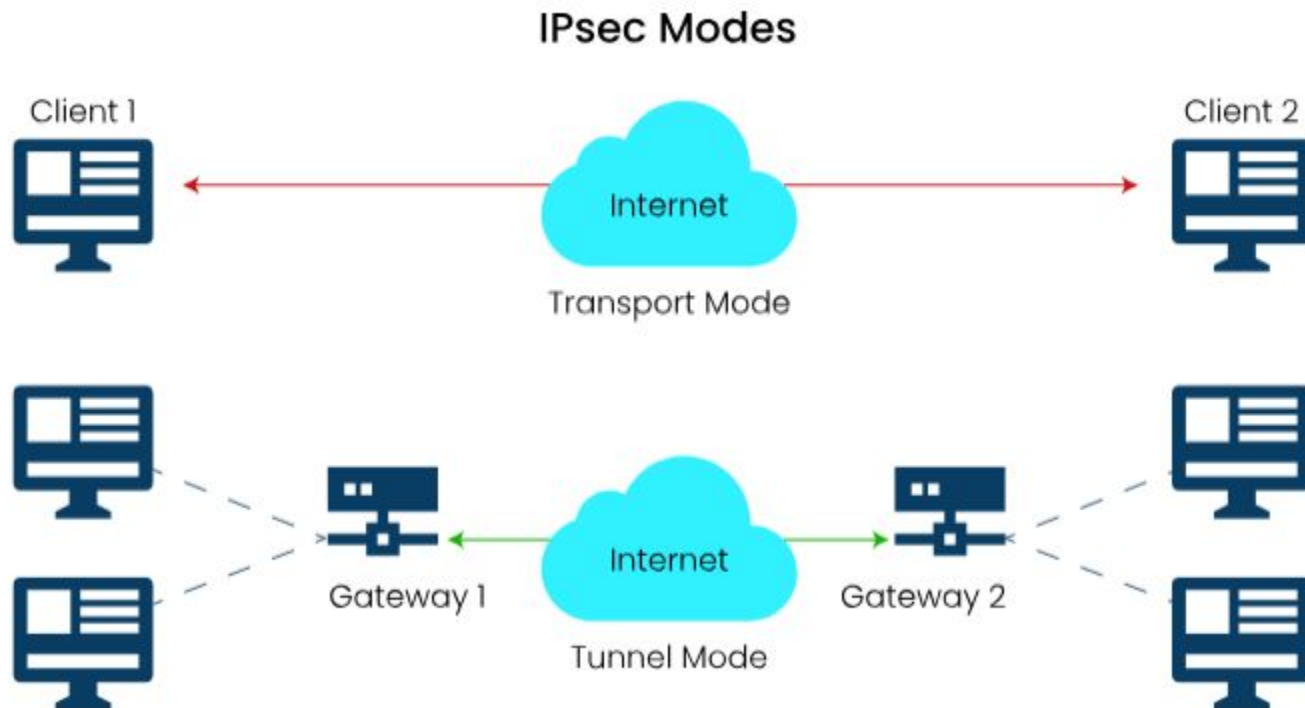
What is IPsec?

- ❑ IPsec – Internet Protocol Security
- ❑ Operates at the Network Layer (Layer 3).
- ❑ Provides Confidentiality, Integrity, and Authentication using cryptography.
- ❑ Works for both IPv4 and IPv6.

IPsec Architecture



Modes Of IPsec



IPsec Workflow



1. Host A sends interesting traffic to Host B.

2. Routers A and B negotiate an IKE phase one session.



3. Routers A and B negotiate an IKE phase two session.



4. Information is exchanged via IPsec tunnel.



5. IPsec tunnel is terminated.

Web & Transport Security

Sandeep K-22z257

SSL/TLS Handshake Process

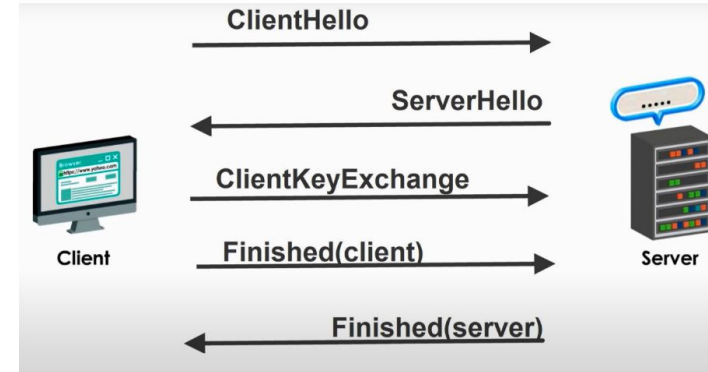
Goal: Establish a secure, encrypted connection between client and server.

Purpose:

- Enables **confidentiality** (via encryption)
- Ensures **authentication** (via certificates)
- Maintains **data integrity**

SSL/TLS Handshake Steps

- **Client Hello:**
Client sends supported TLS versions, cipher suites, and a random number.
- **Server Hello:**
Server responds with chosen protocol, cipher suite, and its digital certificate (public key).
- **Key Exchange:**
Client verifies the certificate → creates a session key → encrypts and sends it using the server's public key.
- **Session Key Established:**
Both generate the same session key for symmetric encryption.
- **Handshake Complete:**
Secure channel established — encrypted communication begins.



HTTPS Overview

HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP that uses **SSL/TLS encryption** to protect communication between a web browser and a server.

How It Works:

- Combines **HTTP + SSL/TLS** for secure data transfer.
- Establishes an **encrypted channel** through a TLS handshake.
- Uses **port 443** instead of 80.

HTTPS Provides:

Encryption

Authentication

Integrity

SSL vs TLS – Key Differences

FEATURE	SSL (SECURE SOCKETS LAYER)	TLS (TRANSPORT LAYER SECURITY)
Developed By	Netscape (1990s)	IETF (as successor to SSL)
Versions	SSL 2.0, 3.0 (now deprecated)	TLS 1.0 → 1.3 (current standard)
Security	Vulnerable to attacks	Stronger encryption algorithms
Handshake	Slower, less efficient	Faster, supports modern ciphers
Usage Today	Obsolete	Actively used globally

Authentication & Email Security

PRITHVIN K C
22Z249

Email Security: PGP & S/MIME

- **PGP (Pretty Good Privacy)**
 - Uses **public key cryptography** and **digital signatures** to encrypt messages.
 - Ensures that only the intended recipient can read the email.
 - Provides **confidentiality, integrity, and authenticity**.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**
 - Uses **X.509 digital certificates** from trusted authorities.
 - Commonly built into corporate email systems like Outlook and Gmail.
 - Helps verify sender identity and protect against **spoofing and tampering**.

Network Authentication Protocols

- **Kerberos:**
 - A trusted third-party system using a **Key Distribution Center (KDC)**.
 - Provides **mutual authentication** through time-based *tickets*.
 - Used in enterprise networks (e.g., Windows Active Directory).
- **RADIUS (Remote Authentication Dial-In User Service):**
 - Centralized protocol for **user authentication and accounting**.
 - Common in **Wi-Fi, VPNs, and ISP networks**.
- **TACACS+ (Terminal Access Controller Access Control System):**
 - Used for **network device administration**.
 - Separates authentication, authorization, and accounting for more control.

Wi-Fi Security Protocols

- **WEP (Wired Equivalent Privacy):** First Wi-Fi security standard; now outdated due to weak encryption.
- **WPA (Wi-Fi Protected Access):** Introduced TKIP to strengthen security.
- **WPA2:** Replaced TKIP with **AES encryption**, becoming the industry standard.
- **WPA3:** Latest version with **individual data encryption**, **stronger passwords**, and protection against brute-force attacks.

Emerging Protocols & Trends

Sudharsan s
23z435

DNSSEC (Domain Name System Security Extensions)

- DNSSEC secures the DNS system by digitally signing DNS data to prevent spoofing and redirection attacks.
- It ensures users always reach the authentic website they intended to visit.
- By using public-key cryptography, DNSSEC maintains data integrity and authenticity in domain name lookups.

SSH (Secure Shell)

- SSH provides a **secure channel** for remote login and file transfers over unsecured networks.
- It encrypts data, verifies user identity, and ensures message integrity.
- System administrators use SSH instead of insecure tools like Telnet or FTP to manage servers safely.

TLS/SSL Attacks

Even strong security protocols can have flaws — like **Heartbleed**, which leaked sensitive data, and **POODLE**, which exploited SSL 3.0.

- These attacks revealed weaknesses in outdated versions of SSL/TLS.
- They remind us why **patching and upgrading security protocols** regularly is essential.

Zero Trust Security Model

Zero Trust means “**never trust, always verify.**”

- Every user and device must be continuously authenticated before accessing resources.
- It minimizes insider threats and enhances cloud security through **strict access controls** and **real-time verification**.

Quantum-Safe Encryption

Quantum computers could break today’s cryptographic algorithms like RSA or ECC.

- Quantum-safe encryption introduces **new algorithms** that can resist quantum attacks.
- This is a key trend for the future of cybersecurity, ensuring **long-term data protection**.

Thank You