Application Layer Protocols & Network Security

1. Key Networking Protocols

Protocol	Port	Description	Security Consideration
HTTP	80	Unsecured web communication (plaintext)	Vulnerable to eavesdropping
HTTPS	443	HTTP + SSL/TLS encryption	Secure against sniffing
FTP	20 (data), 21 (control)	File transfer protocol (unencrypted)	Use **SFTP (22)** or **FTPS** instead
DNS	53	Translates domain names to IPs	Vulnerable to **DNS spoofing**
DHCP	67 (server), 68 (client)	Assigns IP addresses dynamically	**DHCP spoofing** possible
SMTP	25 (unencrypted), 587 (TLS)	Sends emails	Use **SMTPS (465)** for security

1. HTTP (Hypertext Transfer Protocol)

Port: 80 (Unencrypted)
Function: Transfers web pages in plaintext between clients (browsers) and servers.

Key Features:

- **Stateless protocol** (no memory of previous requests).
- Uses **GET, POST, PUT, and DELETE** methods.
- Vulnerable to **eavesdropping, MITM attacks**.

2. HTTPS (HTTP Secure)

Port: 443 (Encrypted via SSL/TLS)
Function: Secure version of HTTP with data encryption.

Key Features:

- Uses **TLS/SSL certificates** (issued by CAs like DigiCert, Let's Encrypt).
- Encrypts data with **AES, ChaCha20** (symmetric) + **RSA/ECC** (asymmetric).
- Prevents **MITM, tampering, and snooping**.

Security Advantages:

✓ **Data Integrity** (Hashing with SHA-256).
✓ **Authentication** (Prevents phishing via cert checks).

3. FTP (File Transfer Protocol)

Port: 20 (Data), 21 (Control)
Function: Transfers files between client and server.

Modes:

- **Active FTP** → Server connects back to client (issues with firewalls).
- **Passive FTP** → Client initiates both connections (better for firewalls).

Security Risks:

- **No encryption** → Credentials sent in plaintext.
- **Brute-force attacks** on FTP logins.

Secure Alternatives:

- **SFTP (SSH FTP, Port 22)** → Encrypted over SSH.
- **FTPS (FTP + SSL, Port 989/990)** → FTP with TLS.

4. DNS (Domain Name System)

Port: 53 (UDP/TCP)
Function: Translates domain names (e.g., google.com) to IPs (e.g., 8.8.8.8).

DNS Record Types:

Record	Purpose	Example
A	IPv4 Address	example.com → 192.0.2.1
AAAA	IPv6 Address	example.com → 2001:db8::1
CNAME	Alias	www.example.com → example.com
MX	Mail Server	example.com → mail.example.com
TXT	SPF/DKIM Records	"v=spf1 include:_spf.google.com ~all"

DNS Security Risks:

- **DNS Spoofing** (Fake DNS responses).
- **DNS Amplification Attacks** (DDoS using open resolvers).

Protections:

- **DNSSEC** (Digitally signs DNS records).
- **DoH (DNS over HTTPS)** / **DoT (DNS over TLS)**.

5. DHCP (Dynamic Host Configuration Protocol)

Port: 67 (Server), 68 (Client)
Function: Automatically assigns IP addresses to devices on a network.

DHCP Process (DORA):

1. **Discover** → Client broadcasts "DHCP Discover".
2. **Offer** → Server responds with "DHCP Offer" (IP lease).
3. **Request** → Client accepts with "DHCP Request".
4. **Acknowledge** → Server confirms with "DHCP Ack".

Security Risks:

- **DHCP Spoofing** → Rogue server gives malicious IPs.
- **Exhaustion Attacks** → Flooding DHCP requests.

Protections:

- **DHCP Snooping** (Network switches filter rogue DHCP).
- **Static IP Reservations** for critical devices.

6. SMTP (Simple Mail Transfer Protocol)

Port: 25 (Unencrypted), 587 (TLS), 465 (SMTPS)
Function: Sends emails between servers.

SMTP Commands:

- HELO → Initiates connection.
- MAIL FROM → Sender's email.
- RCPT TO → Recipient's email.
- DATA → Email body.
- QUIT → Ends session.

Security Risks:

- **Open Relays** → Spammers abuse unsecured SMTP servers.
- **Email Spoofing** → Fake "From" addresses.

Protections:

- **SPF, DKIM, DMARC** (Email authentication protocols).
- **Force TLS** (Encrypts email transit).

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Purpose:

Encrypts data transmitted over networks (e.g., web traffic, emails) to prevent eavesdropping and tampering.

- **SSL** (Deprecated, insecure) → Replaced by **TLS** (v1.2, v1.3 are secure).
- Works via **asymmetric + symmetric encryption**:
  - **Asymmetric** (RSA/ECC): Handshake/key exchange.
  - **Symmetric** (AES/ChaCha20): Encrypts actual data.

Security Risks & Fixes:

Risk	Solution
Expired Certificates	Auto-renew with **ACME** (e.g., Certbot).
Weak Ciphers (e.g., DES)	Enforce **TLS 1.2+**, disable SSL.
MITM Attacks	Use **HSTS** (HTTP Strict Transport Security).

Firewalls

Purpose:

Filters network traffic to block unauthorized access while allowing legitimate communication.

Types of Firewalls:

Type	How It Works	Use Case
Packet-Filtering	Blocks traffic by IP/port.	Basic network security.
Stateful Inspection	Tracks active connections (state).	Enterprise networks.
Proxy Firewall	Acts as an intermediary (analyzes content).	Web filtering.
Next-Gen (NGFW)	Deep packet inspection (DPI), IDS/IPS.	Advanced threat prevention.

Quick Comparison

Feature	SSL/TLS	Firewall
Purpose	Encrypts data in transit.	Filters network traffic.
Layer	Transport Layer (OSI Layer 4).	Network/Layer 3 or Application/Layer 7.
Attack Prevention	MITM, sniffing.	Unauthorized access, DDoS.

Digital Signature

Digital signatures provide **authentication**, **integrity**, and **non-repudiation** for digital documents/messages.

Common Algorithms

Algorithm	Usage	Key Size (Bits)
RSA	Widely used (SSL, PGP)	2048, 4096
ECDSA	Efficient (Bitcoin, TLS)	256, 384
DSA	Older systems (FIPS)	1024, 2048
EdDSA	Modern (Ed25519)	256

Digital Signature Process

Signing:

1. **Hash** the message (SHA-256, SHA-3).
2. **Encrypt** the hash with the sender's **private key**.
3. **Attach** the signature to the message.

Verification:

1. **Decrypt** the signature with the sender's **public key,** → reveals the hash.
2. **Hash** the received message.
3. **Compare** the two hashes:
    - **Match** → Valid signature.
    - **Mismatch** → Tampered or forged.