UNIT IV · LESSON 09

Application Layer & Network Security

client–server & P2P · DNS · HTTP · email · FTP · SNMP · Telnet/SSH · multimedia · security basics

30
questions in Unit IV
OS · Networks · Cloud

ARCHITECTURES PARADIGMS

- **Client–server**: always-on server with fixed IP (web, mail)
- **Peer-to-peer**: peers act as both (BitTorrent); self-scalable
- Application needs: data loss tolerance, throughput, timing, security → choose TCP or UDP

WEB HTTP

- Stateless, request–response over TCP **80** (HTTPS **443** with TLS)
- **Non-persistent** (HTTP/1.0: new TCP connection per object, 2 RTT each) vs **persistent** (HTTP/1.1 default, keep-alive; pipelining)
- HTTP/2: binary framing, multiplexing, header compression, server push; HTTP/3 runs over **QUIC (UDP)**

Method	Purpose
GET	retrieve (data in URL)
POST	submit data in body
PUT	replace/upload resource
DELETE	remove resource
HEAD	headers only
OPTIONS / PATCH	capabilities / partial update

NAMES → IP DNS

- Distributed **hierarchical** database: root (13 logical root servers) → **TLD** (.com, .in) → **authoritative** servers; **local** resolver
- **Recursive** query (resolver does the work) vs **iterative** query (server returns referral)
- Caching with **TTL** reduces load

Record	Holds
A	IPv4 address
AAAA	IPv6 address
CNAME	alias → canonical name
MX	mail server for domain
NS	authoritative name server
PTR	reverse lookup (IP → name)
SOA	start of authority (zone info)
TXT	text (SPF, verification)

- Port **53** (UDP; TCP for zone transfer)

WEB HTTP (CONTD.)

Code	Meaning
1xx	informational
200 OK, 201 Created	success
301 / 302 / 304	moved permanently / found / not modified

WEB HTTP (CONTD.)

Code	Meaning
400 / 401 / 403 / 404	bad request / unauthorised / forbidden / not found
500 / 503	server error / service unavailable

- **Cookies** add state; **web cache (proxy)**, conditional GET (If-Modified-Since)
- URL = protocol://host:port/path?query#fragment

FTP · TELNET · SSH FILE TRANSFER & REMOTE LOGIN

- **FTP**: two TCP connections — **control 21** (persistent, out-of-band) and **data 20** (per file); active vs passive mode; ASCII / binary
- **TFTP**: UDP 69, no authentication, simple (booting diskless hosts)
- **SFTP / SCP** over SSH
- **Telnet** (23): plain-text remote terminal; **SSH** (22): encrypted remote login, tunnelling
- **NVT** (network virtual terminal) in Telnet

STREAMING MULTIMEDIA

- Streaming stored audio/video (HTTP/DASH, buffering), live streaming, interactive real-time (VoIP)
- **RTP** (sequence numbers, timestamps) over UDP; **RTCP** for feedback
- **SIP** sets up calls; **H.323** ITU suite
- Jitter removed by **playout buffer**; FEC and interleaving for losses
- Compression: **MPEG** (video), MP3/AAC (audio), JPEG (images)

SMTP · POP · IMAP EMAIL

Protocol	Role	Port
SMTP	push mail: client → server → server	25 (587 submission)
POP3	download (usually delete from server)	110 (995 TLS)
IMAP	manage mail **on server**, folders, sync	143 (993 TLS)

- **MIME**: non-ASCII content, attachments (base64), Content-Type
- Components: user agent, **MTA** (message transfer agent), MDA, mail access agent
- Webmail uses HTTP between browser and server

SNMP NETWORK MANAGEMENT

- **Manager**, **agent**, **MIB** (management information base), **SMI** (naming/encoding with ASN.1)
- PDUs: GetRequest, GetNextRequest, GetBulk, SetRequest, Response, **Trap** (agent → manager)
- UDP **161** (agent), **162** (traps); v3 adds security
- Other: **NTP** (123) time sync, **DHCP** configuration, **LDAP** directories (389)

CIA SECURITY GOALS

- **Confidentiality**, **Integrity**, **Availability** (+ authentication, non-repudiation)
- Attacks: passive (eavesdropping, traffic analysis) vs active (masquerade, replay, modification, **DoS/DDoS**)

CIA SECURITY GOALS (CONTD.)

- Malware: virus, worm (self-propagating), trojan, ransomware, spyware; **phishing**, MITM, SQL injection

WHERE SECURITY PROTOCOLS

Layer	Protocol
Application	PGP / S/MIME (email), HTTPS
Transport	**SSL / TLS** (handshake, record protocol)
Network	**IPsec**: AH (authentication), ESP (encryption); transport / tunnel modes; VPNs
Link	WPA2 / WPA3 (Wi-Fi, AES-CCMP), 802.1X

- **Firewall**: packet filter (stateless), stateful inspection, application gateway (proxy), circuit-level gateway
- **IDS** (detects) vs **IPS** (blocks); signature- vs anomaly-based
- **DMZ** for public servers; **VPN** for secure tunnels

Q → A RAPID RECALL

DNS record for mail server	MX
DNS record for IPv6	AAAA
HTTP status for "Not Found"	404
Persistent connections by default from	HTTP/1.1
Protocol pushing mail between servers	SMTP

KEYS CRYPTOGRAPHY

Symmetric (secret key)	Asymmetric (public key)
one shared key	key pair: public + private
fast	slow
DES (56-bit key), 3DES, AES (128/192/256), RC4, Blowfish	**RSA**, Diffie–Hellman, ECC, ElGamal
key distribution problem	digital signatures, key exchange

- n users: symmetric needs **n(n−1)/2** keys; asymmetric needs **2n**
- **RSA**: $n = pq$, $\varphi = (p-1)(q-1)$, $e \cdot d \equiv 1 \pmod{\varphi}$; $C = M^e \bmod n$, $M = C^d \bmod n$
- Example $p = 3$, $q = 11 \rightarrow n = 33$, $\varphi = 20$, $e = 3 \rightarrow d = \mathbf{7}$; $M = 4 \rightarrow C = 4^3 \bmod 33 = \mathbf{31}$
- **Hash**: MD5 (128-bit), **SHA-1 (160)**, SHA-256; message digest for integrity
- **Digital signature**: sign hash with sender's **private** key, verify with public key
- **Digital certificate** (X.509) issued by a **CA** binds a public key to an identity (PKI)

Q → A RAPID RECALL (CONTD.)

Keeps mail on the server with folders	IMAP
FTP control connection port	21
SNMP agent → manager alert	trap
Encrypted remote login	SSH (22)

Q → A RAPID RECALL (CONTD.)

Keys for 10 users, symmetric	45
Signature created with	sender's private key
Security at the network layer	IPsec

TRAP EXAM TRAPS

- FTP sends control information **out-of-band** (separate connection)
- HTTP is stateless even though cookies add sessions
- POP3 is a pull protocol; SMTP is push
- Encrypt with receiver's **public** key for confidentiality; sign with own **private** key
- DES key is 56 bits (64 with parity)