Network & Application Layer Security - Exam Notes

IPSec Overview:

- IPSec = set of security algorithms + framework for secure communication
- Applications: Secure remote access, branch office VPNs, intranet/extranet connections, e-commerce security
- Benefits: Transparent to apps (below transport layer), assures routing messages and updates are authentic

IPSec Modes:

- Tunnel Mode: Protects the entire IP datagram, used between gateways
- Transport Mode: Protects payload only, used end-to-end

Security Associations (SAs):

- Defines how two entities secure their communication
- SA is unidirectional (need two for bidirectional traffic)
- Identified by: SPI, destination IP, protocol (AH/ESP)
- SPD: Maps traffic to policies; SAD: Stores active SAs and keys

IPSec Protocols:

- AH: Provides authentication and integrity
- ESP: Provides confidentiality + optional authentication
- IKE: Exchanges cryptographic keys before communication

SSL/TLS:

- SSL (Secure Socket Layer) evolved into TLS (Transport Layer Security)
- Provides encryption/authentication above TCP layer
- HTTPS = HTTP over SSL (uses port 443)
- Steps: Server sends public key, client encrypts session info, session key is used

Transport Layer Security:

- TCP SYNC attacks: Exploits predictability of Initial Sequence Numbers (ISNs)

- ISNs should be random and increment every 4 ms (RFC)
- Predictable ISNs allow impersonation attacks

Application Layer Threats:
- DNS Spoofing: Redirects traffic via forged DNS responses
- Cache Poisoning: Injects false data into DNS cache
- Browser Vulnerabilities: Malicious code in helper apps, mobile code exploits (Java applets, ActiveX)
- Cookies: Track user activity and violate privacy
- Forms & Scripts: Exploits like buffer overflows
- Email: Insecure by default; transit visible, SMTP has flaws

Securing Applications:
- PGP, S/MIME: Secure email communication
- Security-enhanced protocols:
  * FTP to FTPS
  * HTTP to HTTPS
  * SMTP to SMTPS
  * DNS to DNSSEC
- SSL/TLS: Can be app-embedded or protocol-level (used by browsers)
- Application-Specific: SET (on HTTP), S-MIME (on SMTP)