Lecture 2 – Network Security Fundamentals

Networks and System Security

Core Security Principles (CIA Triad)

Confidentiality - Preserving authorized restrictions on information access and disclosure, protecting personal privacy and proprietary information. Loss = unauthorized disclosure.

Integrity - Guarding against improper information modification or destruction, ensuring nonrepudiation and authenticity. Loss = unauthorized modification or destruction.

Availability - Ensuring timely and reliable access to information. Loss = disruption of access to information or systems.

Network Stack & TCP/IP Model

Network layering breaks message sending into separate components, each handling different parts of communication (TCP/IP model).

Application Layer - Encodes/decodes messages in a form understood by sender and recipient.

Transport Layer - Breaks messages into packets with packet numbers and total count. Recipient uses this to reassemble in correct order and detect missing packets.

Network Layer - Adds sender's and recipient's addresses so the network knows where to send messages and where they came from.

Link Layer - Enables packet transfer between nodes on a network and between different networks.

IP Addressing

Original Scheme - Class-based system (Classes A, B, C, etc.)

CIDR (Classless Inter-Domain Routing) - Modern scheme using notation like 192.168.60.5/24 where /24 indicates first 24 bits are network ID.

Lecture 2 – Network Security Fundamentals

Special Addresses:

- Private: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Loopback: 127.0.0.0/8 (commonly 127.0.0.1)

DHCP - Dynamic Host Configuration Protocol automatically assigns IP addresses.

Security at Different Layers

Application Layer (PGP, S/MIME) - Security embedded in the application itself.

Transport Layer (SSL/TLS) - Application-agnostic, adds security features to TCP packets.

Network Layer (IPSec) - Covers all applications; removes security management from application developers; customization for specific applications is difficult.

Core Security Mechanisms

Authentication & Integrity - Provided by public-key cryptography and secure transmission of message digests (digitally signed hash values). Uses paired public/private keys for operations like encryption and digital signing.

Confidentiality - Provided by symmetric key cryptography. Same secret key used for both encryption and decryption.

PGP (Pretty Good Privacy)

Developed by Phil Zimmermann as hybrid cryptosystem combining conventional and public key cryptography.

Key Features:

- Provides strong encryption accessible to everyone
- Email encryption system using state-of-art algorithms
- "Closest you're likely to get to military-grade encryption" - Bruce Schneier
- Successfully resisted government decryption attempts (Red Brigade 2003, Boucher case 2006)

Lecture 2 – Network Security Fundamentals

Five Services:

1. Authentication Service
2. Confidentiality Service
3. Compression Service
4. E-mail Compatibility Service
5. Segmentation Service

Authentication - Uses public-key cryptography (RSA/SHA or DSS/SHA). Creates 160-bit SHA message digest, encrypts with sender's private key (digital signature), prepends to message. Receiver uses sender's public key to decrypt and compare.

Confidentiality - Uses symmetric-key encryption (CAST-128 default, IDEA, or 3DES in CFB mode). Randomly generated 128-bit session key encrypts message. Session key itself encrypted using receiver's public key (RSA or ElGamal). Both concatenated and transmitted.

Compression - Uses ZIP algorithm after signature but before encryption. Makes storage efficient, decouples encryption from verification, reduces patterns that aid cryptanalysis.

E-mail Compatibility - Uses Base64 encoding to represent binary data as ASCII strings for character-oriented transmission.

Segmentation - Breaks down large messages (limit can be as low as 50,000 octets). Process: Compression → Encryption → ASCII Conversion (radix-64) → Segmentation. Digital signature and session key appear only once, typically in first segment.

Key Management:

- Uses short key identifiers (key ID) - least significant 64 bits of public key (8 bytes)
- Private Key Ring: Stores paired private/public keys (private keys encrypted using hash of passphrase)
- Public Key Ring: Stores public keys for correspondents

Web of Trust - Unique bottom-up authentication approach. User's public key can be signed by any other user. If you fully trust User A, and A signs B's public key, you may

subsequently trust B fully. Key Legitimacy field automatically derived by PGP from trust values.

IPSec (IP Security)

Group of protocols for securing connections between devices, often used for VPNs. Adds encryption and authentication to IP routing process.

Key Features:

- Provides authentication, confidentiality, and key management at Network Layer
- Built into IPv6, can be used with IPv4
- Covers all applications running over network
- Largest application: Virtual Private Networks (VPNs)

Components:

Authentication Header (AH) - Protocol 51, provides IP-level authentication (source verification and integrity protection). Contains:

- 32-bit Security Parameter Index (SPI) - establishes Security Association
- Sequence Number - prevents replay attacks
- Authentication Data - MAC calculated using SHA-1 or HMAC

Encapsulating Security Payload (ESP) - Protocol 50, provides IP-level confidentiality through encryption. Can also provide authentication.

Modes of Operation:

Transport Mode - Regular mode for source-to-destination travel. Endpoints carry out own security checks. AH/ESP header inserted after original IP header. ESP encrypts TCP segment (header + data). Used for end-to-end communication between two hosts.

Tunnel Mode - Used when endpoints cannot carry out security checks. Packets routed to designated locations for security insertion/verification. Original IP packet encapsulated inside new IP header (IP-in-IP protocol). ESP encrypts entire inner IP packet. Used when one or both ends are security gateways.

Security Association (SA):

Lecture 2 – Network Security Fundamentals

- One-way logical connection providing security services
- Uniquely identified by three parameters: Security Protocol Identifier (AH or ESP), IP Destination Address, Security Parameters Index (SPI - 32-bit unsigned integer)

Security Association Database (SAD) - Defines parameters for each SA including: SPI, sequence number counter, anti-replay window, AH/ESP information, lifetime, IPsec protocol mode, Path MTU.

Security Policy Database (SPD) - Relates IP traffic to specific SAs. Contains entries defining IP traffic subsets mapped to SAs. Uses selectors (Remote IP, Local IP, Next layer protocol, Name, Local/remote ports) to filter outgoing traffic.

Internet Key Exchange (IKE) - Establishes SA and exchanges keys before AH/ESP use. Declares specific authentication and encryption algorithms. Combines three protocols:

- ISAKMP (Internet Security Association and Key Management Protocol)
- Oakley Key-Exchange Protocol (Diffie-Hellman based for packet encryption key)
- SKEME protocol (re-keying feature)
- Oakley Cookie Exchange prevents Diffie-Hellman clogging attacks

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

History: Originally developed by Netscape in 1995. IETF standardized SSL v3 as TLS v1 (RFC 2246). Combined acronym SSL/TLS common due to OpenSSL library popularity.

Purpose: Provides Transport Layer Security (sits immediately above TCP). Critical for secure web commerce (HTTPS) and secures various application traffic (email, chat, SSH). Security relies on certificates issued by Certificate Authorities (CA).

Authentication Types:

- Server-Only: Client verifies server's certificate, encrypts client-generated secret key with server's public key, sends to server
- Server-Client: Client also sends its certificate to server for authentication

Protocol Stack (Two Layers):

Upper Layer:

- SSL Handshake Protocol - Authenticates clients and servers

Lecture 2 – Network Security Fundamentals

- SSL Cipher Change Protocol - Minor role
- SSL Alert Protocol - Conveys SSL-related alerts

Lower Layer:

- SSL Record Protocol - Transmits data confidentially

Connection vs Session:

- Connection: One-time, transient peer-to-peer information transport (associated with a session)
- Session: Enduring association between client and server with set of security parameters (e.g., 48-byte Master Secret). Can consist of multiple connections.

SSL Record Protocol - Sits directly above TCP, provides confidentiality and message integrity.

Five-step operation:

1. Fragmentation - Message fragmented into blocks ≤ 2^{14} (16,384) bytes
2. Compression (Optional) - Lossless compression (SSLv3 doesn't specify)
3. Adding MAC - Message Authentication Code computed and appended
4. Encryption - Compressed message and MAC encrypted using symmetric-key encryption (3DES, RC4-128)
5. Append SSL Record Header - Declares content type, version, length

SSL Handshake Protocol Phases:

- Phase 1: Establish Capabilities - Client and server agree on security capabilities
- Phase 2: Server Authentication/Key Exchange - Server validates identity
- Phase 3: Client Key Exchange/Authentication - Client sends required keys and potentially certificate
- Phase 4: Finish Setup - Finalize secure connection state

Heartbeat Extension:

- Purpose: Keep SSL/TLS session alive during temporary lulls, avoiding overhead of renegotiating security parameters

Lecture 2 – Network Security Fundamentals

- Sits on top of SSL/TLS Record Protocol
- Key messages: HeartbeatRequest and HeartbeatResponse
- Uses retransmit timer; terminates session if response not received
- Request includes arbitrary payload and length; receiver must return unchanged as replay attack protection

Heartbleed Bug (April 7, 2014):

- Exploited Heartbeat Extension
- Receiver didn't check that declared payload_length matched actual content size
- Attacker could request large payload length (up to 2^{16} bytes) while sending minimal content
- Caused receiver to allocate memory based on requested length and return unverified memory contents
- Could expose private keys, passwords, etc.

Applications & Real-World Examples

"A Day in the Life" Scenario:

- Mobile client connects to network
- Uses DHCP to get IP address, first-hop router address, DNS server address
- Uses ARP to get MAC address of router interface
- DNS query to resolve www.google.com
- TCP 3-way handshake (SYN, SYNACK) establishes connection
- HTTP request sent and reply received
- Each step involves encapsulation/decapsulation through protocol layers

IPSec Applications:

- Secure branch office connectivity over Internet
- Secure remote access over Internet
- Establishing extranet/intranet connectivity with partners

Lecture 2 – Network Security Fundamentals

- Enhancing e-commerce security
- Can encrypt/authenticate all traffic at IP level, securing all distributed applications