Internet Layer Security & IPSec - Comprehensive Exam Notes

1. Internet Protocols Foundation

1.1 Background & Concepts

- **IP Address Purpose**: Numerical labels (e.g., 192.168.32.170) assigned to devices for network communication
- **Two Main Functions**:
  - Network interface identification
  - Location addressing
- **Analogy**: Like student numbers at university - helps manage records efficiently and facilitate quick information retrieval

1.2 IPv4 Protocol Structure

IPv4 Header Fields (Critical for Exams)

1. **Version (4 bits)**: Always 4 for IPv4
2. **Header Length (4 bits)**: Length in 32-bit words (minimum 5 = 20 bytes)
3. **Total Length (16 bits)**: Entire packet size (header + data) in bytes (max 65,535)
4. **Identification (16 bits)**: Unique identifier for packet fragments (same data = same ID)
5. **Fragment Offset (13 bits)**: Position of fragment in original packet
6. **Time to Live (8 bits)**: Hop limit, decrements at each router (starts at 64/128)
7. **Protocol (8 bits)**: Transport layer protocol (TCP=6, UDP=17)
8. **Header Checksum (16 bits)**: Error-checking for header integrity
9. **Source Address (32 bits)**: Sender's IP address
10. **Destination Address (32 bits)**: Receiver's IP address
11. **IP Options (variable)**: Optional control information (multiple of 32 bits)

IPv4 Vulnerabilities

- **Address Spoofing**: No authentication on source IP address
- **Impact**: Enables DoS attacks, impersonation of trusted sources
- **Attack Process**:
  1. Craft packets with forged source IP addresses

2. Flood target server with spoofed packets
3. Server overwhelmed trying to respond to fake addresses

1.3 IPv6 Protocol

Key Improvements over IPv4

- **Address Space**: 128-bit addresses vs 32-bit (vastly expanded capacity)
- **Simplified Header**: Reduced from 14 to 8 fields
- **Extension Headers**: Optional fields handled only when needed
- **Better Performance**: Faster processing and streamlined routing

IPv6 Adoption Challenges

- **Compatibility Issues**: Not directly compatible with IPv4
- **Infrastructure Costs**: Requires hardware/software upgrades
- **Limited Immediate Benefits**: NAT workarounds reduce urgency

2. Supporting Protocols

2.1 DHCP (Dynamic Host Configuration Protocol)

DHCP Process (4-Step Handshake)

1. **DHCP Discover**: Client broadcasts to find DHCP servers
2. **DHCP Offer**: Server responds with available IP and configuration
3. **DHCP Request**: Client accepts the offer
4. **DHCP Acknowledgment**: Server confirms IP assignment

DHCP Vulnerabilities

- **DHCP Spoofing**: Rogue DHCP server provides malicious configuration
- **Consequences**: DoS, network interception, traffic redirection

2.2 ICMP (Internet Control Message Protocol)

Functions

- **Error Reporting**: Unreachable destinations, time exceeded
- **Network Diagnostics**: Ping utility for reachability testing
- **Performance Monitoring**: Round-trip time measurement

ICMP Vulnerabilities

- **ICMP Flooding**: High volume of ping packets overwhelm target
- **Ping of Death**: Oversized ICMP packets cause system crashes

2.3 Routing Protocols

RIP (Routing Information Protocol)

- **Purpose**: Dynamic routing within smaller networks
- **Mechanism**: Routers exchange routing tables with hop counts
- **Vulnerabilities**:
  - **RIP Spoofing**: Fake route advertisements redirect traffic
  - **Route Poisoning**: Marking legitimate routes as unreachable (hop count 16)

BGP (Border Gateway Protocol)

- **Purpose**: Inter-domain routing between Autonomous Systems
- **Difference from RIP**: Path-vector mechanism for larger networks
- **Vulnerability**: Session hijacking through route advertisement manipulation

3. IPSec Protocol Suite

3.1 IPSec Overview

- **Purpose**: Secure IP communications at network layer
- **Development**: Standardized in 1998, widespread adoption in late 1990s
- **Key Advantage**: Protects all applications with single configuration

3.2 IPSec Communication Modes

Transport Mode

- **Scope**: Only payload encrypted/authenticated
- **Header**: Original IP header unchanged
- **Use Case**: End-to-end communication between hosts

Tunnel Mode

- **Scope**: Entire original packet encapsulated
- **Header**: New IP header added for routing

- **Use Case**: VPNs, site-to-site connections

3.3 IPSec Security Protocols

Authentication Header (AH)

- **Provides**: Integrity and authentication
- **Does NOT provide**: Confidentiality (no encryption)
- **Coverage**: IP header + AH header + payload

Encapsulating Security Payload (ESP)

- **Provides**: Confidentiality + optional integrity and authentication
- **Use Case**: Secure, private communication
- **Coverage**: Variable (depends on configuration)

3.4 AH Header Structure (Transport Mode)

```
[IP Header][AH Header][TCP/UDP Header][Payload]
```

AH Header Fields

1. **Next Header (8 bits)**: Protocol type following AH (TCP, UDP)
2. **Payload Length (8 bits)**: AH header length in 32-bit words
3. **Reserved (16 bits)**: Always zero, reserved for future use
4. **Security Parameters Index (SPI) (32 bits)**: Points to Security Association
5. **Sequence Number (32 bits)**: Replay protection counter
6. **Authentication Data (variable)**: Integrity verification for entire packet

3.5 ESP Header Structure (Tunnel Mode)

```
[New IP Header][ESP Header][Original IP Header][TCP/UDP Header][Payload][ESP Trailer][ESP Auth]
```

ESP Header Fields

1. **SPI (32 bits)**: Identifies Security Association
2. **Sequence Number (32 bits)**: Replay protection counter
3. **Payload Data**: Encrypted original packet
4. **Padding**: Aligns data to encryption block size

5. **Pad Length**: Number of padding bytes
6. **Next Header (8 bits)**: Protocol type within payload
7. **Authentication Data (optional)**: Integrity check for immutable fields

3.6 Security Associations (SA)

SA Components

- **SPI**: Unique identifier for the SA
- **Cryptographic Algorithms**: Encryption (AES) and authentication (SHA-256)
- **Keys**: Generated through IKE protocol
- **Lifetime**: SA validity period before rekeying

IPSec Policy Actions

1. **Discard**: Block non-compliant traffic
2. **Protect**: Apply IPSec security (encryption/authentication)
3. **Bypass**: Allow trusted traffic without IPSec

3.7 Internet Key Exchange (IKE)

IKE Purpose

- Establish and negotiate SA parameters
- Select cryptographic algorithms
- Generate shared keys securely
- Manage key lifetimes and renewal

IKE Phase 1: Secure Channel Establishment

Main Mode (6 messages):

- Identity protection from eavesdroppers
- Mutual authentication
- Session key establishment

Aggressive Mode (3 messages):

- Faster but no identity protection
- Mutual authentication and key establishment

IKE Phase 2: IPSec SA Negotiation

- Conducted through secure Phase 1 channel
- Negotiate encryption algorithms (AES, 3DES)
- Negotiate integrity algorithms (HMAC-SHA1, HMAC-MD5)
- Set SA lifetime
- Optional Perfect Forward Secrecy via new DH exchange

4. Security Mechanisms & Anti-Replay

4.1 Anti-Replay Protection

- **Method**: Non-repeating sequence numbers in packets
- **Challenge**: IP is connectionless - packets may arrive out of order
- **Solution**: Sliding window mechanism to handle late arrivals

4.2 Mutable but Predictable Fields

- **Definition**: Fields that change during transmission but final values are predictable
- **AH Inclusion**: Can be included in integrity checks because sender can predict receiver's values
- **Examples**: TTL field (predictably decremented at each hop)

5. Attack Scenarios & Vulnerabilities

5.1 Reflection Attack

- **Target**: Symmetric key authentication schemes
- **Method**: Adversary replays authentication tag from original sender
- **Process**: Use challenge from first session as response in second session

5.2 Network Layer Attacks

SYN Flooding

- **Type**: DoS attack with reconnaissance elements
- **Method**: Send TCP SYN packets to server from random IPs
- **Impact**: Overwhelm server resources, identify open ports

IP Spoofing

- **Method**: Use IP address of trusted host

- **Requirement**: Modify packet headers consistently
- **Impact**: Bypass IP-based access controls

IP Hijacking Methods

1. **Hijack Unused Address**: Take over dormant IP (use DoS to shut down legitimate device)
2. **Redirect Hijacking**: Use ICMP redirect messages
3. **Promiscuous Hijacking**: Man-in-the-middle on network path

6. Key Exam Concepts

6.1 Critical Understanding Points

- **IPSec operates at network layer** - protects all applications automatically
- **ESP provides confidentiality**, AH provides only integrity/authentication
- **Transport mode** for end-to-end, **Tunnel mode** for VPNs
- **Sequence numbers prevent replay attacks**
- **IKE establishes SAs** through two-phase process

6.2 Common Misconceptions

- IPSec doesn't eliminate need for application-layer security
- Not all network environments support IPSec
- User identification often still needed at application layer
- IPv6 adoption faces practical challenges despite technical advantages

6.3 Protocol Interactions

- **DHCP vulnerability** enables network-level attacks
- **ICMP required for diagnostics** but creates DoS vectors
- **Routing protocol attacks** can redirect traffic for interception
- **IPSec provides comprehensive solution** but requires proper implementation

7. Practical Implementation Notes

7.1 ESP Encryption Coverage

- **Encrypted**: Original IP header, transport header, payload
- **Authenticated**: New IP header, ESP header, encrypted payload, ESP trailer

7.2 AH Authentication Coverage

- **Authenticated**: IP header (mutable fields zeroed), AH header, payload
- **Not Encrypted**: All fields remain in plaintext

7.3 SA Management

- **Unidirectional**: Separate SAs needed for each direction
- **Policy-Driven**: Administrator defines protection requirements
- **Automatic**: IKE handles SA establishment and renewal