Link Layer Security - Comprehensive Notes

Overview

Link Layer Security encompasses protocols and mechanisms that secure data transmission at the data link layer (Layer 2) of the OSI model. This layer is responsible for node-to-node delivery of data frames within a local network segment.

Wired Protocols

1. Ethernet Protocol

Foundation: Standardized in 1983 under IEEE 802.3, Ethernet is the fundamental protocol for wired Local Area Networks (LANs).

Ethernet Frame Structure

- **Preamble**: Synchronization signals for receiver clocks (identical values across all frames)
- **Destination Address**: Receiver's MAC address (48 bits, 12 hexadecimal digits)
- **Source Address**: Sender's MAC address (e.g., 00:1A:2B:3C:4D:5E)
  - First 24 bits: Device manufacturer identifier
  - Last 24 bits: Device-specific identifier
- **Type**: Indicates the network layer protocol payload
- **Data**: Actual payload with optional padding
- **Frame Check Sequence (FCS)**: CRC-32 error detection; corrupted frames are discarded

Security Vulnerabilities

MAC Address Spoofing: MAC addresses are easily forgeable due to lack of authentication mechanisms.

Attack Scenarios:

1. **Router Accepts Duplicate MAC Addresses**: Adversary forges device A's MAC address → Router forwards data to both legitimate device and attacker → Data interception
2. **Router Rejects Duplicate MAC Addresses**: Adversary forges device A's MAC address → Router detects conflict → Both devices disconnected → Denial of Service

2. Address Resolution Protocol (ARP)

Purpose: Maps IP addresses to MAC addresses within local area networks.

ARP Operation Process

1. **ARP Request**: Device A checks ARP cache for Device B's MAC address
   - If not found: Broadcasts ARP request to all LAN devices
   - Request format: "Who has IP address X.X.X.X? Send MAC address to [Device A's MAC]"
2. **ARP Response**: Only Device B (owner of requested IP) responds
   - Sends unicast ARP reply directly to Device A
   - Contains Device B's MAC address
3. **Cache Update**: Device A updates its ARP cache with IP-to-MAC mapping

Key Technical Details

- **Broadcast MAC Address**: FF:FF:FF:FF:FF:FF used for ARP requests
- **Gateway Communication**: For external network communication, ARP resolves default gateway's MAC address
- **Cache Management**: ARP entries typically expire after a timeout period

Security Vulnerabilities

ARP Spoofing/Poisoning:

- **Attack Method**: Adversary sends falsified ARP responses claiming ownership of legitimate device's IP address
- **Impact 1**: Traffic redirection → Data interception and manipulation → Potential data breaches
- **Impact 2**: Service disruption → Legitimate traffic sent to attacker instead of intended recipient

3. Link Layer Discovery Protocol (LLDP)

Purpose: Standardized protocol for network device discovery and topology mapping.

LLDP Operation

- **Advertisement**: Devices periodically broadcast LLDP Data Units (LLDPDUs) as multicast packets
- **Information Shared**: MAC addresses, system names, port identifiers, device types
- **Discovery**: Receiving devices update LLDP databases with neighbor information
- **Network Management**: Enables administrators to understand network topology

Security Vulnerabilities

LLDP Spoofing:

- **Attack Method**: Adversary broadcasts forged LLDPDUs claiming to be legitimate network devices
- **Impact**: Unauthorized network access, traffic manipulation, man-in-the-middle attacks

Denial of Service (DoS):

- **Attack Method**: Flooding network with excessive LLDP traffic
- **Impact**: Device processing overload, network slowdown, service disruption

---

Wireless Protocols

Background and Evolution

Timeline:

- **1983**: Wired communication protocols standardized
- **1997**: IEEE 802.11 wireless standard introduced
- **2003**: WPA with TKIP introduced
- **2004**: WPA2 with AES introduced
- **2018**: WPA3 with enhanced security features

Wireless Network Architecture

- **Access Point (AP)**: Central network device managing wireless communications
- **Bridge Function**: AP forwards communications between wireless and wired networks
- **Client Communication**: All mobile devices communicate through AP

Enhanced Security Requirements

Wireless networks require stronger security due to:

1. **Inherent Vulnerability**: Radio wave transmission accessible to anyone within range
2. **Lack of Physical Barriers**: No physical access required for interception
3. **Increased Attack Surface**: Multiple attack vectors available remotely

Common Wireless Attacks

1. **Eavesdropping**: Intercepting data packets transmitted over wireless medium
2. **Man-in-the-Middle (MitM)**: Attacker intercepts and relays communications between parties
3. **Rogue Access Points**: Malicious APs masquerading as legitimate networks
4. **Denial of Service (DoS)**: Network flooding or de-authentication attacks

5. **Session Hijacking**: Stealing session tokens/cookies over wireless transmission
6. **Jamming**: Broadcasting disruptive signals to block legitimate communications

WiFi Frame Structure

WiFi frames are more complex than Ethernet frames due to wireless-specific requirements:

Frame Components

1. **Frame Control (2 bytes)**: Specifies frame type (management/control/data) and includes ACK mechanism
2. **Duration/ID (2 bytes)**: Indicates medium occupation time for collision avoidance
3. **Address Fields (6 bytes each)**:
   - **Address 1**: Receiver MAC address
   - **Address 2**: Transmitter MAC address
   - **Address 3**: BSSID (Access Point MAC address)
   - **Address 4**: Optional, used in Wireless Distribution Systems
4. **Sequence Control (2 bytes)**: Frame reassembly information
   - **Sequence Number**: Unique per packet (same for all fragments)
   - **Fragment Number**: Incremental per fragment within sequence
5. **Frame Body (0-2312 bytes)**: Actual data payload (may be encrypted)
6. **Frame Check Sequence (4 bytes)**: CRC integrity verification

---

Wireless Security Protocols

1. Wired Equivalent Privacy (WEP) - 1997

Design Goal: Provide security equivalent to wired networks using RC4 stream cipher.

WEP Operation

1. **Key Generation**: 40-bit secret key + 24-bit Initialization Vector (IV) = 64-bit total key
2. **Encryption Process**:
   - Message (M) + Integrity Check Value (ICV) using CRC-32
   - RC4 generates keystream from (IV + secret key)
   - Ciphertext = (M || ICV) ⊕ keystream
   - Transmitted data = IV + ciphertext

3. **Decryption Process**:
    - Extract IV from received data
    - Generate keystream using RC4(IV + secret key)
    - Decrypt: (M || ICV) = ciphertext ⊕ keystream
    - Verify integrity using CRC-32

Critical WEP Vulnerabilities

1. **Key Management**: Same shared secret key for all devices
2. **Integrity Weakness**: CRC-32 is non-cryptographic; bit manipulation possible
3. **Confidentiality Issues**:
    - Short key size (40-bit)
    - IV reuse due to 24-bit limitation
    - Keystream reuse enables cryptanalysis

2. WiFi Protected Access (WPA) with TKIP - 2003

Design Goal: Address WEP vulnerabilities while maintaining hardware compatibility.

Key Features

- **Temporal Key Integrity Protocol (TKIP)**: Enhanced key management
- **Backward Compatibility**: Implementable on existing WEP hardware
- **Dynamic Key Generation**: Session-specific encryption keys
- **Improved Integrity**: Michael Message Integrity Check (MIC)

Authentication Methods

1. **Pre-Shared Key (PSK)**: Shared password authentication
2. **IEEE 802.1X**: Enterprise authentication with EAP

3. WiFi Protected Access 2 (WPA2) - 2004

Major Improvement: Advanced Encryption Standard (AES) replaces RC4.

Technical Specifications

- **Encryption**: AES-CCMP (Counter Mode with CBC-MAC Protocol)
- **Key Management**: Robust Security Network (RSN) protocol
- **Authentication**: EAP or PSK methods

- **Security Level**: Strong cryptographic protection

4. WiFi Protected Access 3 (WPA3) - 2018

Enhanced Security Features:

- **Forward Secrecy**: Past communications remain secure even if keys are compromised
- **Improved Key Exchange**: Diffie-Hellman key exchange protocol
- **Enhanced Authentication**: Simultaneous Authentication of Equals (SAE)

WPA3 Key Derivation

- **PMK**: Derived from Diffie-Hellman key exchange
- **PTK**: H(PMK, Password, Snonce, Anonce, MAC1, MAC2)
- **GTK**: Generated by AP, encrypted with KEK from PTK
- **Forward Secrecy**: Unique session keys prevent retroactive decryption

---

IEEE 802.1X Authentication Framework

Components

1. **Supplicant**: Client device seeking network access
2. **Authenticator**: Network access point (typically AP)
3. **Authentication Server**: Centralized credential verification (usually RADIUS)

Port-Based Access Control

- **Controlled Port**: Accepts packets from authenticated devices only
- **Uncontrolled Port**: Passes only 802.1X authentication traffic
- **State Management**: Ports transition from "unauthorized" to "authorized" after successful authentication

EAP Methods

PEAP (Protected EAP)

1. **TLS Tunnel Establishment**: Client and server create secure communication channel
2. **Server Authentication**: Server presents certificate to client
3. **Client Authentication**: Username/password sent through encrypted tunnel
4. **Key Distribution**: Session keys derived and distributed

EAP-TLS

1. **Mutual Authentication**: Both client and server present X.509 certificates
2. **Strong Security**: Certificate-based authentication on both sides
3. **PKI Requirement**: Requires public key infrastructure deployment

Authentication Process Flow

1. **Detection**: Authenticator detects new supplicant
2. **Port State**: Set to "unauthorized" (only 802.1X traffic allowed)
3. **Identity Request**: Authenticator requests supplicant identity
4. **RADIUS Communication**: Authenticator forwards identity to authentication server
5. **Method Negotiation**: Server and supplicant agree on EAP method
6. **Credential Exchange**: Authentication credentials exchanged
7. **Result**: Server sends EAP-Success or EAP-Failure
8. **Port Authorization**: Successful authentication enables normal traffic

---

Pre-Shared Key (PSK) Authentication

Mechanism

- **Shared Secret**: Common password between user and network
- **Key Derivation**: PSK + nonces generate session keys
- **Simplicity**: No dedicated authentication server required
- **Use Cases**: Home and small office networks

PSK Operation

1. **Password Entry**: User enters shared password
2. **Session Key Generation**: Both client and AP derive session key from PSK
3. **Secure Communication**: Session key encrypts all subsequent traffic

Key Derivation Process

- **PMK**: Pre-Master Key (shared secret)
- **PTK**: Pairwise Transient Key = H(PMK, Snonce, Anonce, MAC1, MAC2)
- **GTK**: Group Temporal Key (generated by AP, encrypted with KEK from PTK)
- **MIC**: Message Integrity Check for frame verification

Security Protocol Comparison

Feature	WEP	WPA	WPA2	WPA3
Encryption Algorithm	RC4	RC4-based TKIP	AES	AES
Key Management	Static shared key	Dynamic key	Dynamic key	Dynamic key
Authentication Method	PSK only	EAP or PSK	EAP or PSK	EAP or PSK
Security Level	Insecure	Better than WEP	Strong	Strongest
Forward Secrecy	No	No	No	Yes
Key Exchange	Static	Dynamic	Dynamic	Diffie-Hellman

Key Terminology

- **Static Key**: Same key used for all sessions
- **Dynamic Key**: Session-specific keys derived from master key + nonces
- **Forward Secrecy**: Compromise of long-term keys doesn't affect past communications

Best Practices and Recommendations

Wired Network Security

1. **Network Segmentation**: Isolate critical systems
2. **Physical Security**: Secure cable access points
3. **MAC Address Filtering**: Limited effectiveness but adds layer
4. **Network Monitoring**: Detect ARP spoofing and unusual traffic

Wireless Network Security

1. **Use WPA3**: Deploy strongest available security protocol
2. **Strong PSK**: Use complex, lengthy pre-shared keys
3. **Enterprise Authentication**: Implement 802.1X for organization networks
4. **Regular Updates**: Keep firmware and security patches current
5. **Network Isolation**: Separate guest and internal networks
6. **Monitoring**: Deploy wireless intrusion detection systems

General Security Principles

1. **Defense in Depth**: Multiple security layers

2. **Least Privilege**: Minimum necessary access rights
3. **Regular Audits**: Periodic security assessments
4. **Incident Response**: Prepared response procedures
5. **User Education**: Security awareness training

Conclusion

Link Layer Security is fundamental to network protection, requiring comprehensive understanding of both wired and wireless protocols. The evolution from WEP to WPA3 demonstrates continuous improvement in addressing security vulnerabilities. Proper implementation of these protocols, combined with additional security measures, creates robust network defense against various attack vectors. Regular assessment and updates ensure continued protection against emerging threats.