1 Netzwerkgrundlagen & Sicherheit

1.1 Einführung und Modelle

Dieser Abschnitt behandelt die Grundlagen von Netzwerken, Kommunikationsmodellen und spezifischen Angriffen sowie deren Abwehr auf verschiedenen Schichten.

1.1.1 OSI-Modell (Open System Interconnection)

Das OSI-Modell ist ein Referenzmodell für Netzwerkprotokolle, unterteilt in 7 Schichten. Jede Schicht bietet Dienste für die darüberliegende Schicht an.

- **Layer 7: Application Layer** (Anwendungsschicht)
  Stellt Funktionen für Anwendungen bereit (nicht die Anwendung selbst).
  HTTPS/S, FTP, SMTP, DHCP, DNS
- **Layer 6: Presentation Layer** (Darstellungsschicht)
  Datenformatierung, Kompression, Verschlüsselung.
  SSL/TLS
- **Layer 5: Session Layer** (Sitzungsschicht)
  Sitzungsmanagement (Aufbau, Abbau), Authentifizierung.
  RPC, SMPP
- **Layer 4: Transport Layer** (Transportschicht)
  Ende-zu-Ende Kommunikation, TCP/UDP.
  TCP, UDP
- **Layer 3: Network Layer** (Vermittlungsschicht)
  Logische Adressierung (IP), Routing.
  IPv4, IPv6, ARP, ICMP
- **Layer 2: Data Link Layer** (Sicherungsschicht)
  Physische Adressierung (MAC), Zugriff auf das Medium.
  SDLC, SLIP, NCP
- **Layer 1: Physical Layer** (Bitübertragungsschicht)
  Übertragung von Bits über ein Medium (Kabel, Funk).
  Ethernet, Wi-Fi

1.1.2 TCP/IP Modell vs. OSI

Das TCP/IP-Modell ist eine vereinfachte, praxisorientierte Version des OSI-Modells (oft 4 Schichten).

Vergleich der Dateneinheiten (Encapsulation)

Beim Durchlaufen der Schichten von oben nach unten werden Daten **gekapselt** (Encapsulation). Jede Schicht fügt ihren Header (und teilweise Trailer) hinzu.

- **Application Layer:** Daten / Message (M)
- **Transport Layer:** **Segments** (Header $H_t + M$)
- **Internet Layer:** **Packets** (Header $H_i + H_t + M$)
- **Link Layer:** **Frames** (Header $H_l + \cdots + TrailerT_l$)

1.2 Die Schichten im Detail

1.2.1 Layer 1: Physical Layer

- **Funktion:** Konvertierung von Daten in physikalische Signale zur Übertragung zwischen Geräten.
- **Medien:**
  - Elektrische Impulse (Kupferkabel)
  - Lichtimpulse (Glasfaser)
  - Funksignale (Wi-Fi)

1.2.2 Layer 2: Data Link Layer

- **Funktion:** Verbindung zwischen zwei Geräten im *selben* Netzwerk (Hop-to-Hop).
- **Hardware:** Switches.
- **Adressierung:** **MAC-Adresse** (Media Access Control).
  - Weltweit eindeutig (theoretisch).
  - 48 Bit lang (6 Bytes).
  - **Aufbau:** Erste 3 Bytes = Hersteller-Kennung (OUI), Letzte 3 Bytes = Seriennummer.

1.2.3 Layer 3: Network Layer

- **Funktion:** Logische Adressierung und Weiterleitung (Routing) über Netzwerkgrenzen hinweg.
- **Protokolle:** IPv4, IPv6, ICMP.
- **Hardware:** Router.
- **Wichtig:** IP ist ein **unzuverlässiges** Protokoll (Best Effort). Es gibt keine Garantie für die Ankunft der Pakete.

1.2.4 Layer 4: Transport Layer

Stellt die Ende-zu-Ende-Kommunikation sicher.

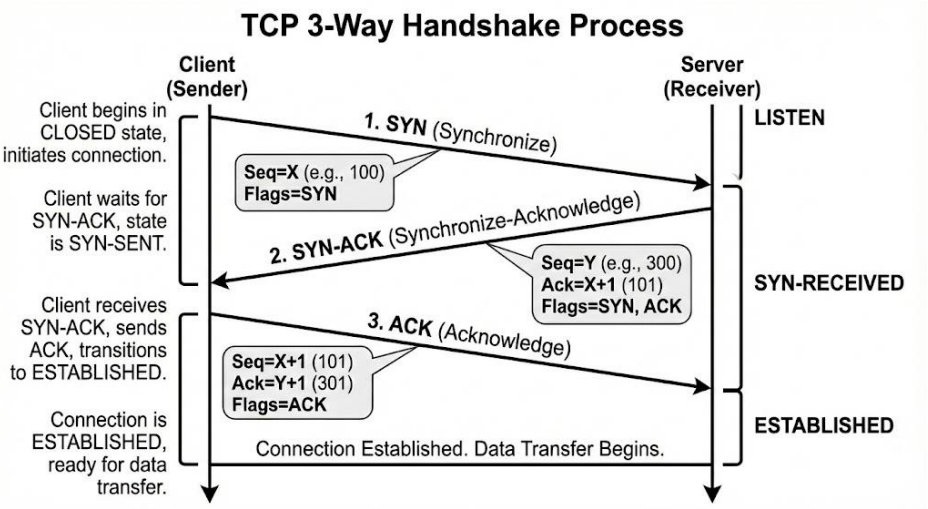
- **Multiplexing:** Nutzung von **Ports**, um verschiedene Dienste (z.B. Web, Mail) gleichzeitig auf einem Host zu betreiben.
- **Segmentierung:** Aufteilen großer Datenmengen.
- **Fehlererkennung:** Checksummen.
- **Flusskontrolle:** Vermeidung von Überlastung des Empfängers.

TCP vs. UDP

TCP (Transmission Control Protocol):
- **Verbindungsorientiert** (Handshake notwendig).
- **Zuverlässig** (ACKs für Pakete, Neuversand bei Verlust).
- **Reihenfolge:** Garantiert (Sequenznummern).
- **Einsatz:** Web (HTTP), Email (SMTP), Dateitransfer (FTP).

UDP (User Datagram Protocol):
- **Verbindungslos** (Fire-and-Forget).
- **Unzuverlässig** (Keine ACKs, kein Neuversand).
- **Schnell:** Geringer Overhead (nur 8 Byte Header).
- **Einsatz:** Streaming, Gaming, DNS, DHCP.

TCP 3-Way Handshake (Verbindungsaufbau) Um eine Verbindung aufzubauen, nutzen Client und Server folgenden Ablauf:



1. **SYN:** Client sendet `Seq=X, Flags=SYN`. (Status: SYN-SENT)
2. **SYN-ACK:** Server antwortet `Seq=Y, Ack=X+1, Flags=SYN,ACK`. (Status: SYN-RECEIVED)
3. **ACK:** Client bestätigt `Seq=X+1, Ack=Y+1, Flags=ACK`. (Status: ESTABLISHED)

TCP Connection Termination (Verbindungsabbau) Der Abbau erfolgt in der Regel über einen 4-Schritte-Prozess unter Nutzung des **FIN**-Flags:

1. **FIN:** Client möchte schließen, sendet `Flags=FIN`. (Status: FIN-WAIT-1)
2. **ACK:** Server bestätigt den Erhalt mit `Flags=ACK`. (Status: CLOSE-WAIT beim Server, FIN-WAIT-2 beim Client)
3. **FIN:** Server ist bereit zum Schließen, sendet ebenfalls `Flags=FIN`. (Status: LAST-ACK)
4. **ACK:** Client bestätigt den Erhalt mit `Flags=ACK`. (Status: TIME-WAIT, danach CLOSED)

1.2.5 Layer 5-7: Höhere Schichten

- **Session Layer:** Authentifizierung, Verwaltung von Sitzungen (z.B. RPC).
- **Presentation Layer:** Datenkonvertierung (z.B. ASCII → ASN.1), Verschlüsselung (SSL/TLS wird oft hier eingeordnet), Kompression.
- **Application Layer:** Protokolle für Anwendungen. Ports definieren den Service:
  - HTTP/S: Port 80/443
  - FTP: Port 20/21
  - SMTP: Port 25

1.3 Angriffsmodelle im Netzwerk

- **Eavesdropping (Abhören):** Passiver Angreifer. Liest Daten mit, verändert sie aber nicht. Abwehr: Verschlüsselung.
- **On-Path / Man-in-the-Middle (MitM):** Angreifer sitzt *auf* dem Kommunikationsweg (z.B. kontrolliert Router). Kann Daten lesen, **verändern**, **blockieren** oder einschleusen.

- **Off-Path:** Angreifer sitzt *nicht* auf dem direkten Weg. Kann Daten nicht mitlesen oder blockieren, aber Daten einschleusen (z.B. Spoofing mit gefälschter Absenderadresse).

1.4 Netzwerkprotokolle und spezifische Angriffe

1.4.1 ARP (Address Resolution Protocol)

Funktion: Auflösung einer bekannten IP-Adresse zu einer unbekannten MAC-Adresse im lokalen Netzwerk (Layer 2).

Ablauf ARP

1. **Request:** "Wer hat IP 10.23.4.38?" → Gesendet als **Broadcast** (FF:FF:FF:FF:FF:FF). Alle Geräte empfangen es.
2. **Reply:** "Ich (10.23.4.38) habe MAC 11:AB:..." → Gesendet als **Unicast** an den Anfragenden.

ARP Spoofing / Cache Poisoning Da ARP **zustandslos** ist (Clients akzeptieren Antworten auch ohne vorherige Anfrage), kann ein Angreifer gefälschte ARP-Replies senden.

- **Angriff:** Angreifer sendet: "Ich bin IP des Routers" an das Opfer und "Ich bin IP des Opfers" an den Router.
- **Folge:** Der ARP-Cache der Opfer wird "vergiftet". Der Angreifer wird zum *Man-in-the-Middle*.
- **Gegenmaßnahmen:**
  - Statische ARP-Einträge (aufwendig).
  - ARP-Monitoring Tools (z.B. Arpwatch, Snort).
  - Nutzung von IPv6 (nutzt NDP + SEND, sicherer).
  - Netzwerksegmentierung.

MAC Spoofing: MAC-Adressen sind in Software leicht änderbar. MAC-Filter sind daher kein verlässlicher Schutz.

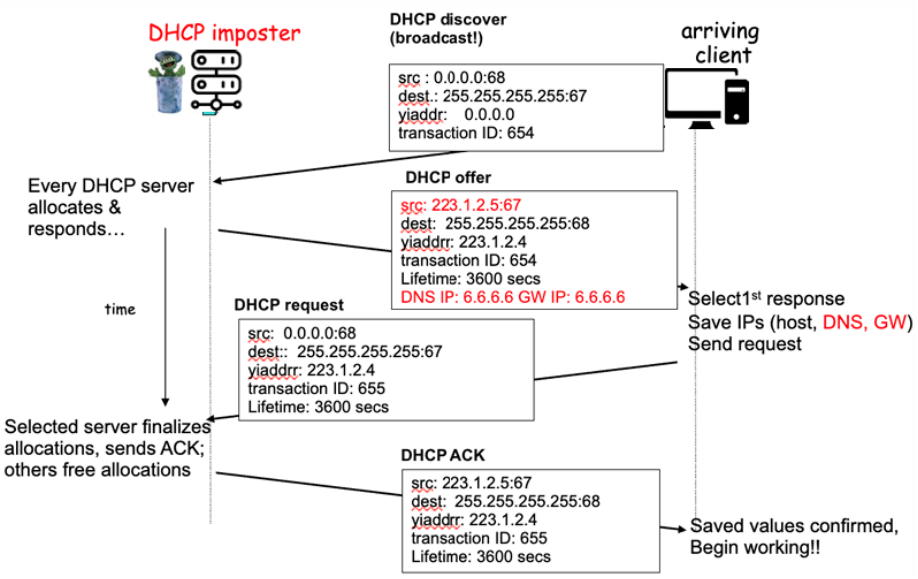
1.4.2 DHCP (Dynamic Host Configuration Protocol)

Funktion: Automatische Zuweisung von IP-Adressen, Subnetzmasken, Gateway und DNS an Clients. Nutzt UDP (Ports 67/68).

Ablauf (DORA-Prinzip)

1. **D**iscover (Broadcast): Client sucht DHCP-Server.
2. **O**ffer (Unicast/Broadcast): Server bietet IP an.
3. **R**equest (Broadcast): Client fordert die angebotene IP an.
4. **A**ck (Unicast/Broadcast): Server bestätigt und verleast IP.

DHCP Spoofing (Rogue DHCP) Ein Angreifer stellt einen falschen DHCP-Server im Netz auf. Wenn er schneller antwortet als der echte Server (Race Condition), übernimmt er die Konfiguration des Clients.



- **Gefahr:** Angreifer setzt sich selbst als Gateway oder DNS-Server (MitM).
- **Gegenmaßnahme: DHCP Snooping** auf Switches.
  - Ports werden in **Trusted** (nur hier darf ein DHCP-Server hängen) und **Untrusted** unterteilt.
  - DHCP-Offers von Untrusted Ports werden blockiert.

1.4.3 ICMP und (D)DoS Angriffe

ICMP (Internet Control Message Protocol): Dient dem Austausch von Informations- und Fehlermeldungen (z.B. `ping` zur Latenzmessung).

(D)DoS - (Distributed) Denial of Service Ziel ist es, die Verfügbarkeit eines Dienstes zu stören.

- **DoS:** Ein Angreifer.
- **DDoS:** Viele Angreifer (Botnet).

Spezifische Angriffe

- **Ping of Death:** Senden von malformierten (z.B. zu großen) ICMP-Paketen, die beim Zusammensetzen den Server zum Absturz bringen. (Heute meist gepatcht).
- **Smurf Attack (Amplification):**
  - Angreifer sendet Ping an die **Broadcast-Adresse** eines Netzwerks.
  - Absender-Adresse ist gefälscht auf die **Opfer-IP**.
  - Alle Hosts im Netz antworten dem Opfer → Überlastung.
  - **Schutz:** Broadcast-Pings im Router deaktivieren.
- **SYN Flood:**
  - Angreifer sendet viele TCP-SYN-Pakete, antwortet aber nie auf das SYN-ACK.
  - Server hält Ressourcen für "halboffene Verbindungen" reserviert, bis er überlastet ist.
  - **Schutz: SYN Cookies** (Zustand wird nicht gespeichert, sondern kryptographisch in der Sequenznummer der Antwort kodiert).

1.5 Netzwerkschutzmechanismen

1.5.1 Firewall

Ein System, das den Netzwerkverkehr zwischen Zonen (z.B. LAN und Internet) überwacht und filtert.

- Filtert basierend auf Regeln (IPs, Ports, Protokolle).
- Ermöglicht Netzwerksegmentierung.

1.5.2 IDS vs. IPS

IDS und IPS Vergleich

IDS (Intrusion Detection System):
- **Passiver** Beobachter (nicht im Datenpfad/Inline).
- Analysiert Kopien des Verkehrs ("Mirror Port").
- Meldet Alarme, blockiert aber nicht selbstständig.

IPS (Intrusion Prevention System):
- **Aktiver** Schutz (Inline im Datenpfad).
- Kann bösartige Pakete in Echtzeit verwerfen/blockieren.