IT-Sicherheit

Netzwerksicherheit

Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun

Sommersemester 2020

Hochschule Augsburg - Fakultät für Informatik

Netzwerke

Um welche Netzwerke handelt es sich?

- Definition zu Rechnernetzen (deutsche Wikipedia)
  - ”Ein Rechnernetz ist ein Zusammenschluss verschiedener technischer, primär selbstständiger elektronischer Systeme [...], der die Kommunikation der einzelnen Systeme untereinander ermöglicht.”

- Beispiele
  - Netzwerke in der IT-Infrastruktur
  - Das Internet (of Things)
  - Netzwerke im Automobil
  - Netzwerke in industriellen Anlagen

Netzwerkschichten

Schicht (layer)	OSI Modell	TCP/IP Modell
7	Anwendungen (application)	Anwendungen
6	Darstellung (presentation)	
5	Sitzung (session)	
4	Transport (transport)	Transport
3	Vermittlung (network)	Internet
2	Sicherung (data link)	Netzzugang
1	Bitübertragung (physical)	

OSI Layer 1: Physical Layer

- Zweck
  - Physikalische Übertragung von Informationen
  - z.B. elektrisch, elektro-magnetisch, optisch
- Komponenten
  - Kabel, Stecker
  - Antennen
  - Repeater
- Sicherheitsrelevant
  - Physikalischer Zugang zum Netz
    $\rightarrow$ passive/aktive Teilnahme am Netzwerk

OSI Layer 2: Data Link Layer

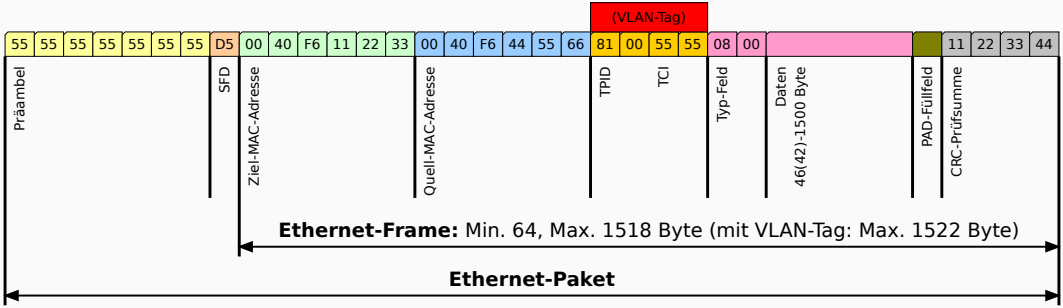
- **Zweck**
  - Aufteilung in Datenblöcke und zuverlässige Übertragung
  - z.B. Frames mit Fehlerkorrektur-Prüfsummen

- **Komponenten**
  - Switch

- **Sicherheitsrelevant**
  - Versenden/empfangen von Daten
    $\rightarrow$ Logische Teilnahme am (lokalen) Netzwerk
  - Evtl. Filterung auf Basis von MAC-Adressen

Ethernet (IEEE 802.3)

- Arbeitet auf Layer 1 und 2
  - Definition von Steckern, Kabeln, etc.
  - Spezifizierung von Datenfeldern und Prüfsummen
  - Enthält Anforderungen für MAC Protokoll (Layer 2)



OSI Layer 3: Network Layer

- **Zweck**
  - Weiterleitung/Routing von Paketen
- **Komponenten**
  - Router, Layer-3-Switch
- **Sicherheitsrelevant**
  - Versenden von Daten über Router hinweg
    $\rightarrow$ Teilnahme am gesamten (weltweiten) Netzwerk
  - Evtl. Filterung auf Basis von IP-Adressen

Internet Protocol (IP)

- Arbeitet auf Layer 3
  - Benutzt Sender- und Empfänger-Adressen
  - Organisiert Paket-Routing vom Sender zum Empfänger
- IP Paket
  - Header
  - Payload

Internet Protocol (IP) - IPv4 Adressen

- 32-bit Adressen
  - Subnetz-ID + Host-ID
  - z.B. 192.168.7.32 mit Subnetzmaske 255.255.255.0
    - ”Klasse C”-Netzwerk
    - Subnetz-ID: 192.168.7
    - Host-ID: 32

- Classless Inter-Domain Routing (CIDR)
  - Zahl gibt ”1”-Bits der Subnetzmaske an
  - z.B. 10.27.153.7/8
    - ”Klasse A”-Netzwerk
    - Subnetz-ID: 10
    - Host-ID: 27.153.7

Worauf verweist die IP-Adresse 127.0.0.1?

Internet Protocol (IP) - Network Address Translation (NAT)

- Verbindung verschiedener Netze
  - Transparentes ersetzen von IP-Adressen in IP-Paketen
  - Übersetzung interner IPs in externe IPs und umgekehrt
  - z.B. Heimnetzwerk mit Router als Verbindung zum Internet
- NAT Router
  - Hält temporäre NAT-Tabelle vor und übersetzt entsprechend
  - Ermöglicht auch Port and Address Translation (PAT)

ARP und ICMP

- Address Resolution Protocol (ARP)
  - Übersetzt IP-Adressen in MAC-Adressen
  - Hält temporäre ARP Tabelle vor
- Internet Control Message Protocol (ICMP)
  - Definiert diverse Steuerungsnachrichten im Internet
  - z.B. ”Echo Request” und ”Echo Reply” für Ping

OSI Layer 4: Transport Layer

- Zweck
  - Datensegmentierung und Stauvermeidung
  - Bereitstellung der Daten für Anwendungen
- Typische Protokolle
  - TCP und UDP
  - Adressierung: Ports
- Sicherheitsrelevant
  - Verbindungsaufbau mit Diensten auf Rechnern
    $\rightarrow$ Nutzung von Diensten im Netzwerk
  - Evtl. Filterung auf Basis von Ports

TCP vs. UDP

- Transmission Control Protocol (TCP)
  - Erstellt Verbindung zwischen Kommunikationsendpunkten
  - Kann mit verlorenen oder vertauschen Paketen umgehen
- User Datagram Protocol (UDP)
  - Verzichtet auf Verbindungen
  - Tauscht Daten über einfache Datagramme aus

OSI Layer 5, 6 und 7

- **Layer 5: Session Layer**
  - Verwaltet Sitzungen/Kommunikation zwischen Prozessen
  - z.B. Remote Procedure Calls (RPCs)

- **Layer 6: Presentation Layer**
  - Regelt Darstellung von Daten auf verschiedenen Systemen
  - z.B. Zeichensatz, Kompression, Verschlüsselung, etc.

- **Layer 7: Application Layer**
  - Unterstützt Dateneingabe und -ausgabe
  - Fungiert als Schnittstelle zur Anwendung

Bekannte Angriffe

Ping Flooding

- Ping
  - Absender schickt ICMP Echo Request
  - Ziel-Host antwortet mit ICMP Echo Reply
- Flooding
  - Angreifer sendet mehr Anfragen als Host beantworten kann
  - Führt zu Denial-of-Service
- Schutz
  - Blocken aller ICMP Echo Requests
  - Erlauben einer bestimmten Anzahl in bestimmter Zeit

Smurf Angriff

- Angriff
  - Angreifer verschickt ICMP Echo Request per Broadcast
  - Angreifer ersetzt Quell-Adresse mit Angriffsziel
  - Alle Netzwerkteilnehmer antworten mit ICMP Echo Reply an gefälschte Adresse
  - Angriffsziel wird überlastet → Denial-of-Service

- Schutz
  - Blockieren von ICMP Echo Requests
  - Deaktivieren der Broadcast-Funktionalität
  - Netzwerkverkehrüberwachung und Filterung

ARP Spoofing

- **ARP-Cache auf Host**
  - Lernt Adressen und speichert diese temporär
  - Akzeptiert alle ARP-Pakete

- **Spoofing**
  - Angreifer sendet manipulierte ARP-Pakete an A und B
  - ARP-Cache wird manipuliert
  - Angreifer erlangt Man-in-the-Middle Position

- **Schutz**
  - Statische ARP-Tabellen (schwer zu verwalten)
  - Sichere Varianten von ARP, z.B. Secure ARP (S-ARP)
  - Überwachen des Netzwerksverkehrs

SYN Flooding

- TCP Verbindung
  - Initiiert durch SYN Nachricht
  - Server bestätigt durch SYN-ACK Nachricht
  - Client bestätigt durch ACK Nachricht
- Flooding
  - Angreifer schickt sehr viele SYN Nachrichten
  - Angreifer schickt aber keine ACK Nachrichten
  - Server muss Zustand von vielen Verbindungen vorhalten
  - Server ist irgendwann überlastet $\rightarrow$ Denial-of-Service
- Schutz
  - Zustand nicht speichern vor Verbindungsaufbau
  - Analyse des Netzwerkverkehrs, ggf. Filterung

Auf der Ebene des Data Link Layer ist keine Filterung der Netzwerk-Teilnehmer möglich, da IP-Adressen vom Network Layer verarbeitet werden.

A) Richtig

B) Falsch

QUIZ: Netzwerkangriffe (twbk.de)

Welche der folgenden Angriffe basiert darauf, dass ein Angreifer ICMP Echo Requests verschickt und dessen Absender-Adresse manipuliert.

A) ARP Spoofing

B) Smurf Angriff

C) Ping Flooding

Netzwerksicherheit

Ziele der Netzwerksicherheit

- Schutz des Netzwerkzugangs
  - Remote, aus anderen Netzwerken heraus
    - aus dem Internet
    - aus anderen Netzwerk-Teilen
  - Lokal, durch physische Nähe zum Netzwerk
    - Kabelgebundene Netze
    - Funknetzwerke

- Schutz von Infrastruktur und Komponenten
  - vor Denial-of-Service (DoS) Angriffen
  - vor Abhören und Manipulation
  - durch Analyse des Netzwerkverkehrs

Netzwerksegmentierung

- Physikalisch
  - z.B. keine Verbindung zum Internet
  - z.B. ”Air-Gap” zwischen Netzen und Systemen
- Virtuell
  - z.B. durch Firewalls
  - z.B. durch VLANs
  - z.B. Zugriff erst nach erfolgreicher Authentifizierung

Virtual Local Area Network (VLAN)

- Port-basiert
  - Physikalischer Port wird VLAN zugeordnet
  - Switch regelt Trennung zwischen Netzen
  - Verbindung mehrerer VLANs durch Router möglich
- Tag-basiert
  - Tags durch Switches/Engeräte hinzugefügt/entfernt
  - Dynamische Varianten möglich
  - Nicht für Netzwerksicherheit geeignet

Netzwerksegmentierung - Vor- und Nachteile

- Vorteile
  - Erfolgreiche Angriffe betreffen nur Teil des Netzwerks
  - Setzt ”Defense-in-Depth”-Konzept um
  - Ermöglicht besseren Überblick, gezieltere Netzwerkanalyse

- Nachteile
  - Evtl. mehr Instrastruktur-Komponenten nötig
  - Administration evtl. komplizierter
  - Prozesse evtl. komplizierter

Firewall

- Zweck
  - Beschränkung des Netzwerkverkehrs zw. Netzen
- Filterung auf Basis verschiedener Kriterien
  - Paketfilter (IP-Adressen und Ports)
  - Stateful Inspection (zustandsbasiert, z.B. Verbindungen)
  - Proxyfilter (stellt Anfragen stellvertretend für Client)
  - Contentfilter (Proxyfilter, der auch Nutzdaten analysiert)
  - Deep Packet Inspection (Analyse diverser Protokolldaten)

Beispiel: Demilitarisierte Zone (DMZ)

- Zone zwischen Internet und internem Netzwerk
  - Ermöglicht Zugriff auf Server in DMZ (z.B. E-Mail-Server) aus dem Internet und aus dem internen Netz
  - Infizierte Server in DMZ sind von internem Netz getrennt

- Üblicherweise zwei Firewalls
  - Erste Firewall erlaubt Verbindungen vom Internet
    z.B. nur auf Port 80 für Web-Server
  - Zweite Firewall erlaubt Verbindungen aus dem Intranet
    z.B. nur auf Port 22 für Administration via SSH

IDS und IPS

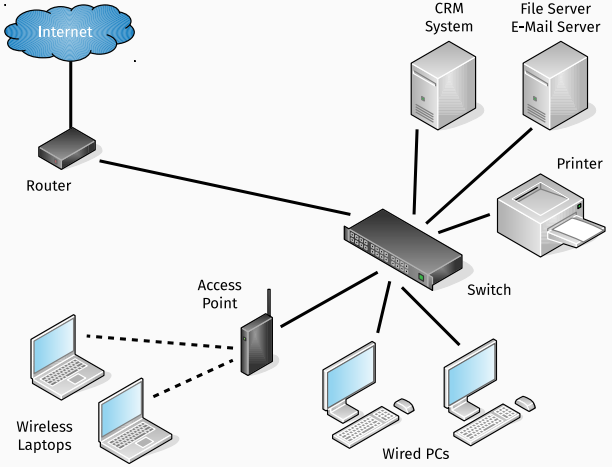
- Intrusion Detection System (IDS)
  - Analysiert Netzwerkverkehr auf Angriffsmuster
  - Alarmiert Administratoren bei potentiellen Angriffen
- Intrusion Prevention System (IPS)
  - Analysiert Netzwerkverkehr und verhindert aktiv Angriffe

Teilnehmer-Authentifizierung (IEEE 802.1X)

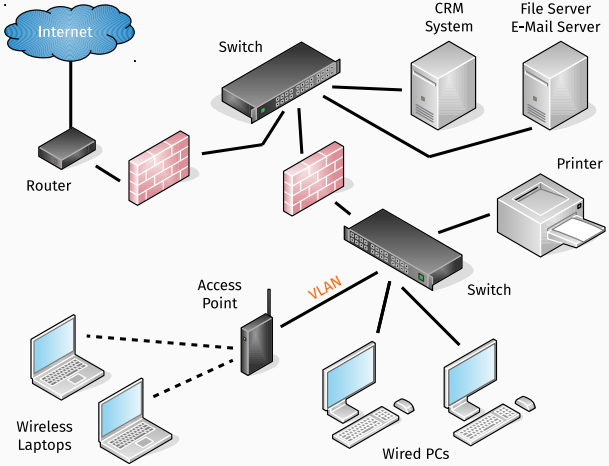
- Authentifizierung beim Netzwerkzugang
  - Physikalischer Port
  - Tagged VLAN (IEEE 802.1Q)
  - WLAN Zugriff
- Bereitstellung von Authentisierungsinformationen
  - Authentifizierungsserver erteilt/verweigert Netzzugang
  - z.B. auch eduroam an der Hochschule

AUFGABE: Konzept für Netzwerksicherheit

Netzwerk eines kleinen Unternehmens ...



Netzwerk eines kleinen Unternehmens ...



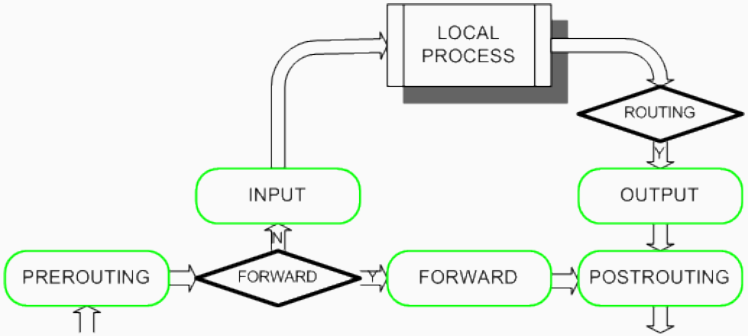
Firewalls

Filtern von Netzwerkverkehr

- **Host-basierte Firewall / Personal Firewall**
  - Schützen ein Endgerät
  - Filtern Netzwerkpakete die von Endgeräten empfangen oder gesendet werden
  - Filterregeln auf IP-Ebene *oder* auf Ebene von Prozessen

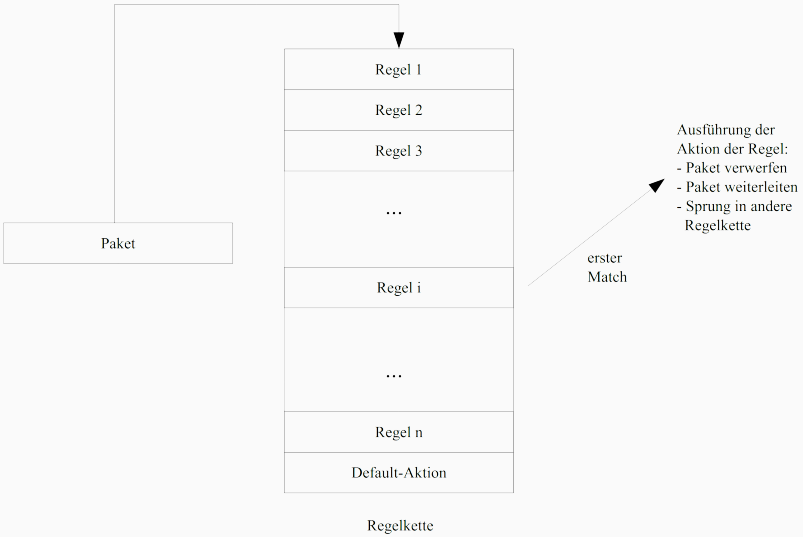
- **Netzwerk-basierte Firewalls**
  - Geräte die Netzwerkverkehr anderer Geräte weiterleiten und filtern
  - Zwei oder mehr Netzwerk-Interfaces
  - Filtern Pakete anderer Teilnehmer im Netzwerk *und* Pakete zu sich selbst

- **Aufgaben einer Firewall mit mehreren Netzwerkkarten**
  - Empfang und Routing-Entscheidung über Weiterleitung von Netzwerkpaketen
  - Anwendung von Filterregeln in Regelketten



Untersuchungspunkte für Pakete innerhalb von Netfilter (Quelle)

Bearbeitung der Regeln innerhalb einzelner Regelketten



Regeln für Linux Netfilter

- Aktionen für Pakete die Weiterleitung beeinflussen
  - **Akzeptieren (*accept*)**: Paket in der Kette als zur Weiterverarbeitung markieren
  - **Verwerfen (*drop*)**: Paket ohne Rückmeldung verwerfen
  - **Zurückweisen (*reject*)**: Paket verwerfen und Rückmeldung an Sender geben

- Matching-Regeln für Pakete
  - Inhalt von Feldern in den Headern der Netzwerkpakete (z.B. IP-Adresse)
  - Eigenschaften der Firewall (z.B. eingehende Netzwerkkarte)
  - Sonstiger gespeicherter Zustand (z.B. Paket gehört zu einer schon akzeptierten Verbindung)

- Default-Aktionen (*Policies*)
  - Regeln für alle Pakete für die keine anderen Regeln definiert sind

Konfiguration von Netfilter über Befehl *iptables* mit Regelsprache

- iptables -P INPUT DROP
  - Setzt *Policy* und verwirft alle eingehenden Pakete auf die Firewall selbst
- iptables -A INPUT -p tcp –source 111.222.121.212 –destination 1.2.3.4 –dport 22 -j DROP
  - Fügt neue Regel für eingehende Pakete zur Firewall hinzu
  - TCP-Segment von IP 111.222.121.212 an IP 1.2.3.4 an Port 22 werden verworfen
- iptables -A FORWARD -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT
  - Fügt Regel für alle weitergeleiteten Pakete hinzu
  - Erlaubt alle Pakete einer akzeptierten oder *verwandten* Verbindung
- Weitere Informationen: *man iptables*

Vorgehen bei der Konfiguration einer Firewall

- **Identifikation von benötigtem Netzwerkverkehr**
  - Sammeln der existierenden Clients und Server
  - Trennung der Systeme nach Gruppen in unterschiedliche Subnetze
  - Welche Systeme müssen wie mit anderen Systemen kommunizieren?

- **Whitelisting von notwendigem Verkehr**
  - *Default-Policy* sollte immer ein Verbot der Kommunikation sein
  - Nur benötigte Verkehrsströme werden erlaubt

Gibt es noch Fragen?