

ESSE Einführung in Security – VO 03: Netzwerksicherheit

Florian Fankhauser, Rafael Vrekar



Einführung

ISO/OSI-Modell

Konkrete Angriffe und Bedrohungen

ARP – Address Resolution Protocol

IP – Internet Protocol

ICMP – Internet Control Message Protocol

TCP – Transmission Control Protocol

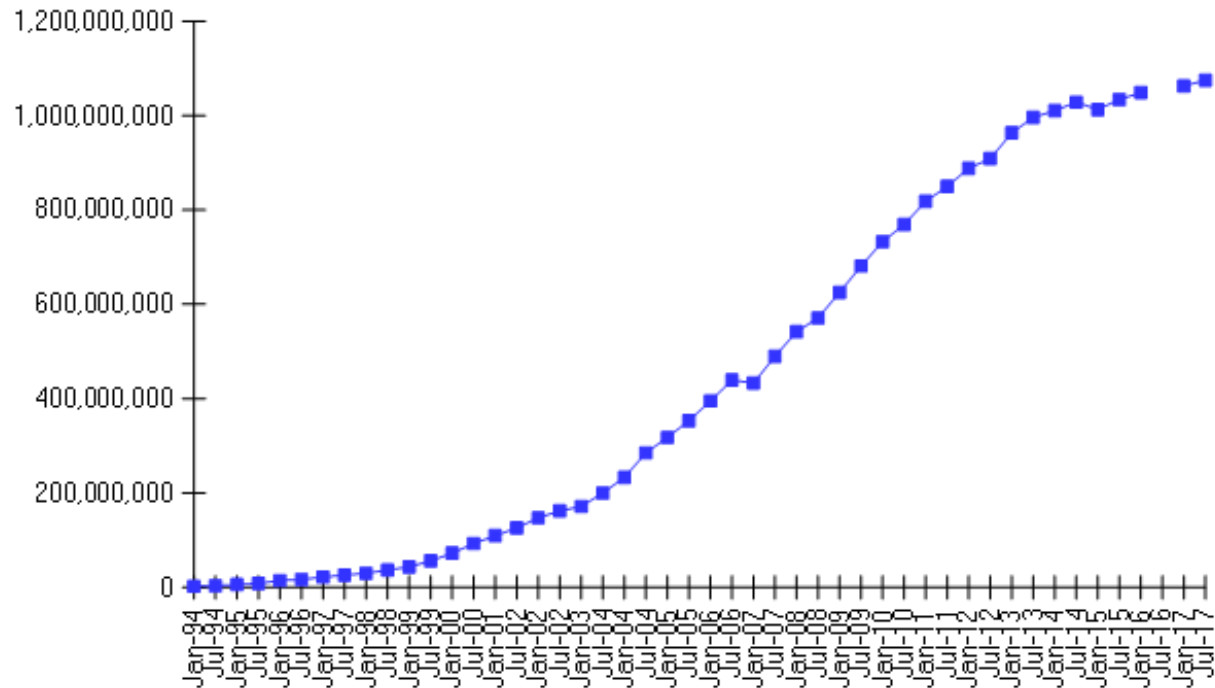
Aspekte von Wireless Netzwerken

Lösungsansätze

Tools, Literatur

Viele Systeme sind im Internet

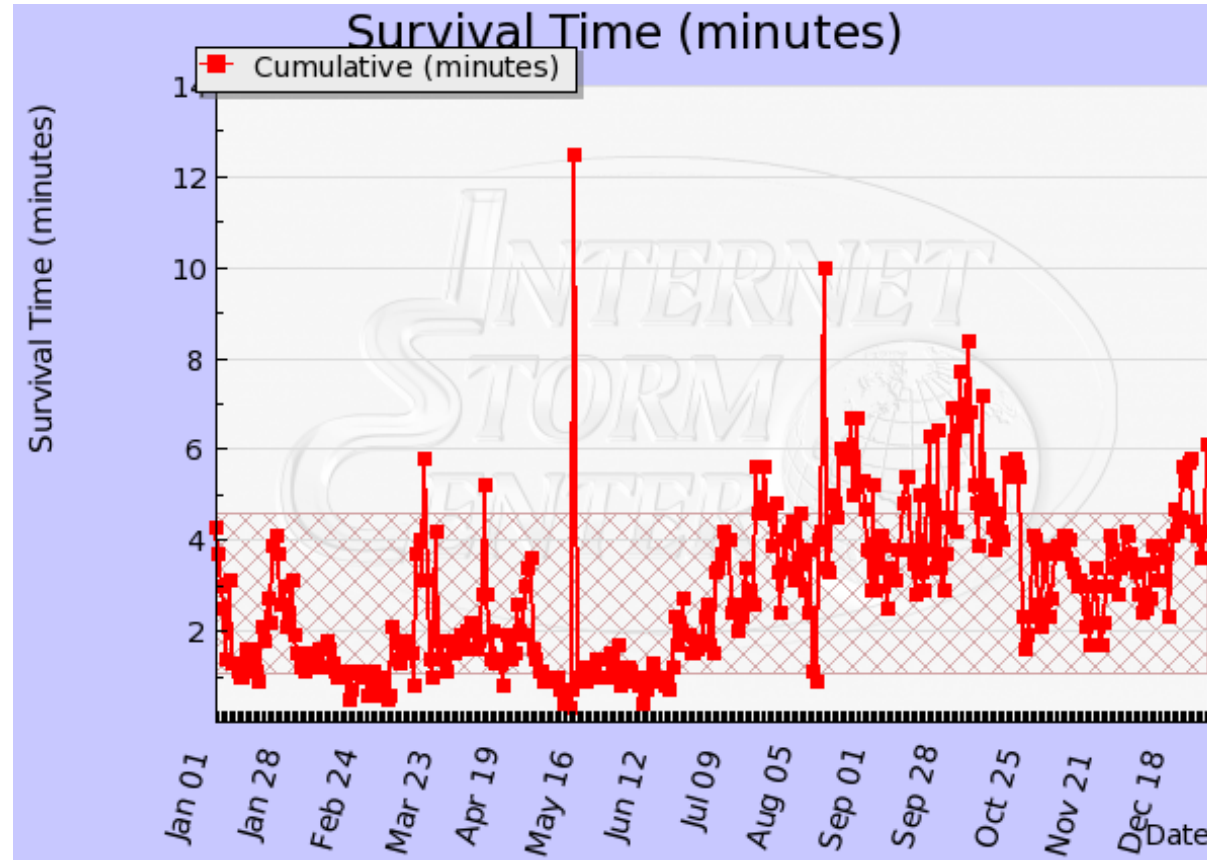
Internet Domain Survey Host Count



Source: Internet Systems Consortium (www.isc.org)

„We had no idea that this would turn into a global and public infrastructure.“

— Vint Cerf, one of the founding fathers of the Internet



(01/2005-10/2013, Quelle: <http://isc.sans.org/survivaltime.html> bzw. <https://isc.sans.edu/survivaltime.html>)

Motivation zur Netzwerksicherheit – 1/2

Oder: Die Verwendung von Wireshark

The screenshot shows the Wireshark interface with a packet list table and a detailed view of an ARP reply packet.

No.	Time	Source	Destination	Protocol	Info
22	4.997359	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
23	5.006302	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
26	19.673895	QuantaCo_	Broadcast	ARP	Who has 10.203.1.1? Tell 10.59.1.143
27	19.703028	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
29	19.722402	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
155	49.475783	QuantaCo_	Handlink_	ARP	Who has 10.203.1.1? Tell 10.59.1.143
156	49.476130	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
157	49.476504	Handlink_	QuantaCo_	ARP	10.203.1.1 is at
178	80.477697	QuantaCo_	Handlink_	ARP	Who has 10.203.1.1? Tell 10.59.1.143
179	80.478061	Handlink_	QuantaCo_	ARP	10.203.1.1 is at

Packet 156 Details:

- Ethernet II, Src: Handlink_ , Dst: QuantaCo_
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (0x0001)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcodes: reply (0x0002)
 - Sender MAC address: Handlink_
 - Sender IP address: 10.203.1.1 (10.203.1.1)
 - Target MAC address: QuantaCo_
 - Target IP address: 10.59.1.143 (10.59.1.143)

Packet 156 Hex Data:

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010  08 00 06 00 01 00 00 00 00 00 00 00 00 00 00 00
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    
```

Address Resolution Protocol (arp), 28 bytes | P: 317 D: 317 M: 0 Drops: 0

Motivation zur Netzwerksicherheit – 2/2

Oder: Die Verwendung von Wireshark

The screenshot shows the Wireshark interface with a packet capture list and detailed view. The packet list shows a sequence of events: a DNS query for security.inso.tuwien.ac.at, a response, a SYN flood attempt from 10.59.1.143 to 128.130.59.99, an ICMP unreachable response, and finally a successful GET request for / HTTP/1.1. The detailed view shows the raw bytes of the HTTP User-Agent header.

No.	Time	Source	Destination	Protocol	Info
34	19.839240	10.59.1.143		DNS	Standard query A security.inso.tuwien.ac.at
35	19.889847		10.59.1.143	DNS	Standard query response A 128.130.59.99
36	19.890134	10.59.1.143	128.130.59.99	TCP	35799 > www [SYN] Seq=0 Len=0 MSS=1460 TSV=9232100 TSER=0 WS=7
37	19.894945		10.59.1.143	DNS	Standard query response
38	19.894973	10.59.1.143		ICMP	Destination unreachable (Port unreachable)
39	19.964830	128.130.59.99	10.59.1.143	TCP	www > 35799 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1166 TSV=494870320 TSEI
40	19.964877	10.59.1.143	128.130.59.99	TCP	35799 > www [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=9232118 TSER=494870320
41	19.965148	10.59.1.143	128.130.59.99	HTTP	GET / HTTP/1.1
42	20.044596	128.130.59.99	10.59.1.143	TCP	www > 35799 [ACK] Seq=1 Ack=222 Win=6912 Len=0 TSV=494870338 TSER=9232118
43	20.082294	128.130.59.99	10.59.1.143	TCP	[TCP segment of a reassembled PDU]

```

▶ Internet Protocol, Src: 10.59.1.143 (10.59.1.143), Dst: 128.130.59.99 (128.130.59.99)
▶ Transmission Control Protocol, Src Port: 35799 (35799), Dst Port: www (80), Seq: 1, Ack: 1, Len: 221
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: security.inso.tuwien.ac.at\r\n
    User-Agent: ELinks/0.11.1-1.2etch1-debian (textmode; Linux 2.6.18-5-686 i686; 90x40-2)\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip\r\n
    Accept-Language: en\r\n
    Connection: Keep-Alive\r\n
    \r\n
0050 0d 0a 48 6f 73 74 3a 20 73 65 63 75 72 69 74 79 ..Host: security
0060 2e 69 6e 73 6f 2e 74 75 77 69 65 6e 2e 61 63 2e .inso.tu wien.ac.
0070 61 74 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 at..User -Agent:
0080 45 4c 69 6e 6b 73 2f 30 2e 31 31 2e 31 2d 31 2e ELinks/0 .11.1-
0090 32 65 74 63 68 31 2d 64 65 62 69 61 6e 20 28 74 2etch1-d ebian (t
00a0 65 78 74 6d 6f 64 65 3b 20 4c 69 6e 75 78 20 32 extmode; Linux 2
00b0 2e 36 2e 31 38 2d 35 2d 36 38 36 20 69 36 38 36 .6.18-5- 686 i686
00c0 3b 20 39 30 78 34 30 2d 32 29 0d 0a 41 63 63 65 ; 90x40- 2)..Acce
00d0 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d pt: */*. .Accept-
00e0 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a Encoding : gzip..
HTTP User-Agent header (http.user_agent), 88 bytes | P: 317 D: 317 M: 0 Drops: 0
    
```

- Vernetzung wichtig
- Kleine LANs – Internet
- Verschiedenste Systeme und Applikationen
- Vernetzung über diverse Landes-/Verantwortlichkeits-Grenzen hinweg

- Probleme und Merkmale
 - Anzahl und Komplexität der beteiligten Systeme
 - Attacken über das Netzwerk sind einfach
 - Nachvollziehbarkeit von Angriffen schwierig
 - (Vermeintliche) Anonymität
 - Angriffsmethoden leicht und schnell verfügbar
 - Angriffe im Netzwerkbereich oft Basis für weitere Angriffe

Beispiele für technische und nicht-technische Angriffe/Bedrohungen in Netzwerken

- Vertraulichkeit
 - Google Hacking
 - Covert Channels
 - Sniffing
- Integrität, Authentizität, Nichtabstreitbarkeit
 - Spoofing
- Verfügbarkeit
 - Session Hijacking
 - Denial of Service (DoS)
 - Distributed Denial of Service (DDoS)

- Entwicklung von TCP/IP lange her
(TCP, IP, ICMP: 1981, UDP: 1980)
- Umfeld anders als heute
- Keine/wenig Sichtweise auf Security/Angriffe
- Grundlage wenige Hosts, Basis-Netz zuverlässig

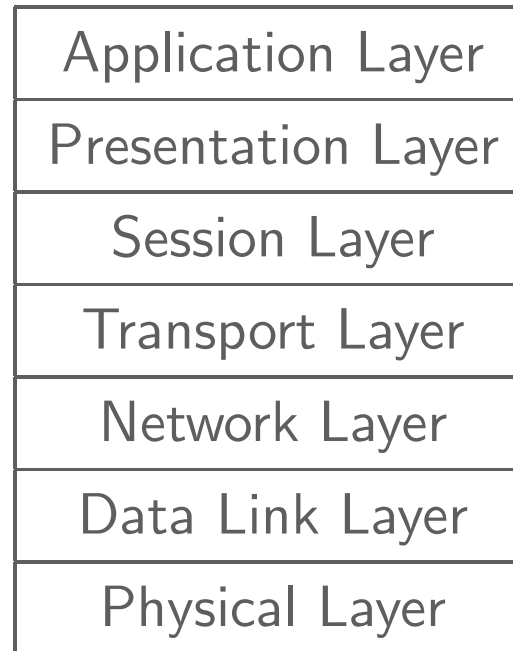
- Spezifikationen tw. unvollständig
- Software Bugs

- Mehr Rechner/Teilnehmer:innen
- Teilnehmer:innen unbekannt
- Das Internet ist nicht anders als die „Real World“

- ISO – International Organization for Standardization
- OSI – Open Systems Interconnection

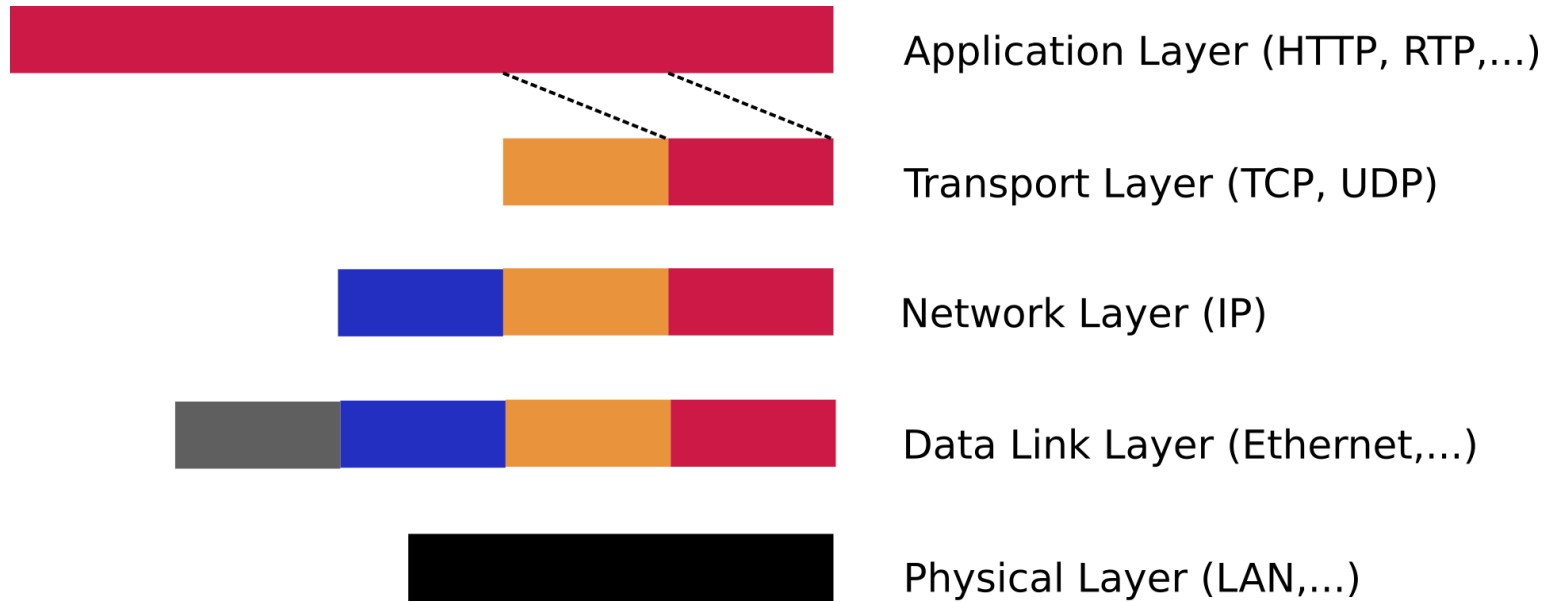
- Schichtenmodell
 - Reduzierung der Komplexität der Abhängigkeiten
 - Trennung der Aufgaben in einzelnen Schichten
 - Schichten weitgehend unabhängig voneinander
 - Genau definierte Schnittstellen zwischen den Schichten
 - Höhere Schichten greifen auf Funktionen niedrigerer Schichten zu

- → Auswirkungen auf die IT-Sicherheit?



(Vergleiche OSI X.200 Basic Reference Model: The Basic Model)

TCP/IP-Schichtenmodell

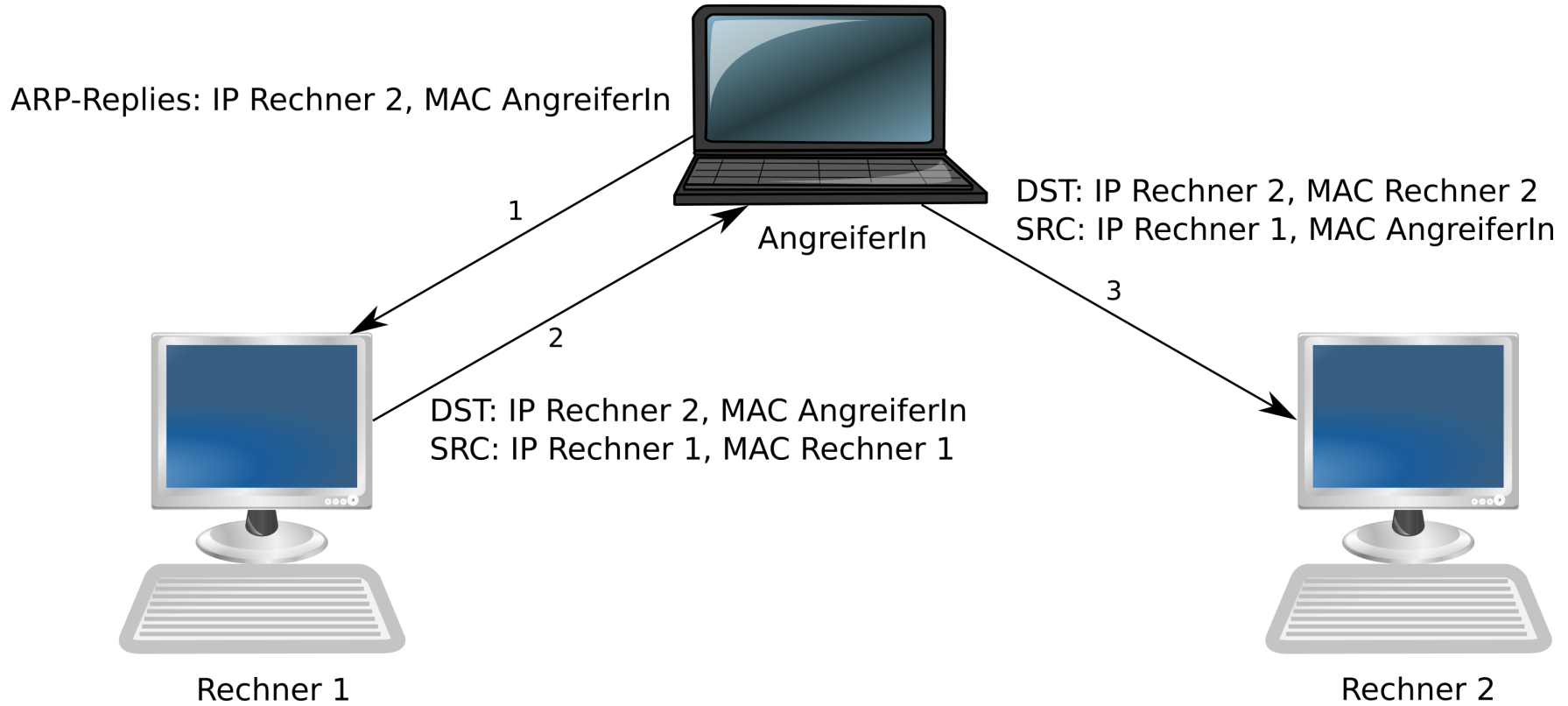


Ausgewählte Angriffe auf ausgewählten Schichten

- ARP
- IP
- ICMP
- TCP

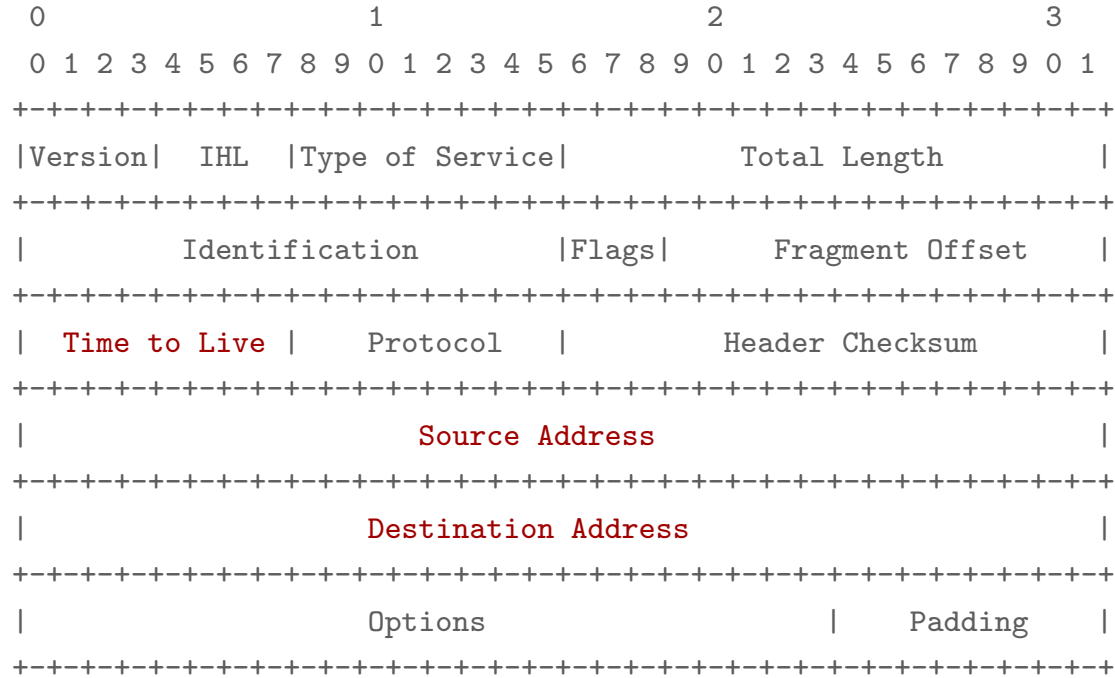
ARP – Address Resolution Protocol

- Basis RFC 826
- Herausforderung logische Adressen/Hardware Adressen
- Umwandlung von IP-Adressen in Hardware Adressen (z.B. Ethernet MAC-Adressen)
- ARP Cache
- Speicherung von eigenen und fremden Anfragen
- ARP Poisoning
 - Black Hole
 - Man in the Middle
- Spoofing von MAC-Adressen leicht möglich!



- Basis RFC 791
- Unzuverlässig, verbindungslos
- Logische Netzwerk Adressen
- Routing
- x.x.x.x (z.B. 192.168.1.1)
- Host Adressen, Broadcast Adressen, spezielle Adressen (u.a. RFC 1918)
- 127.0.0.1 als Adresse für localhost
- IPv4 vs. IPv6

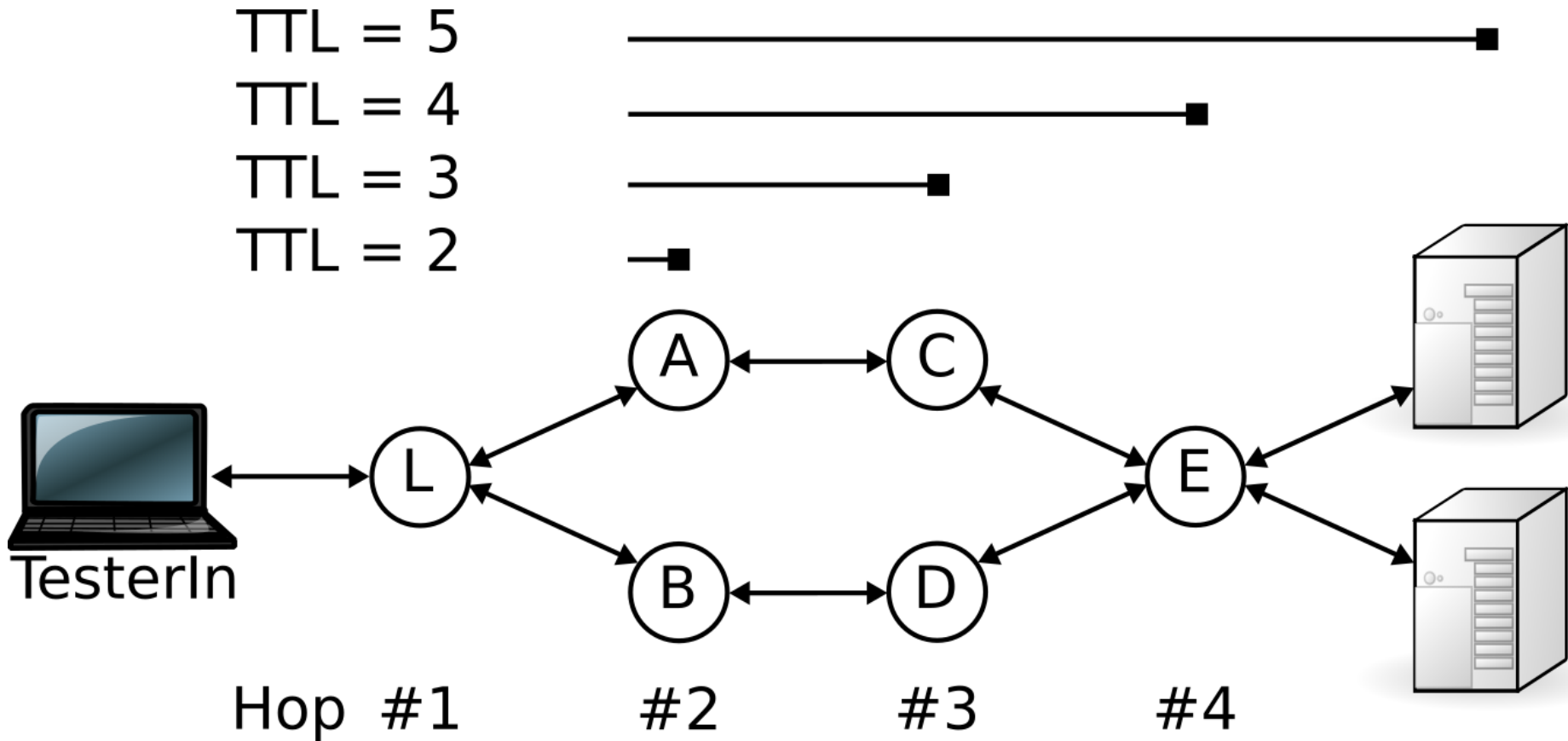
■ Aufbau (aus: RFC 791)



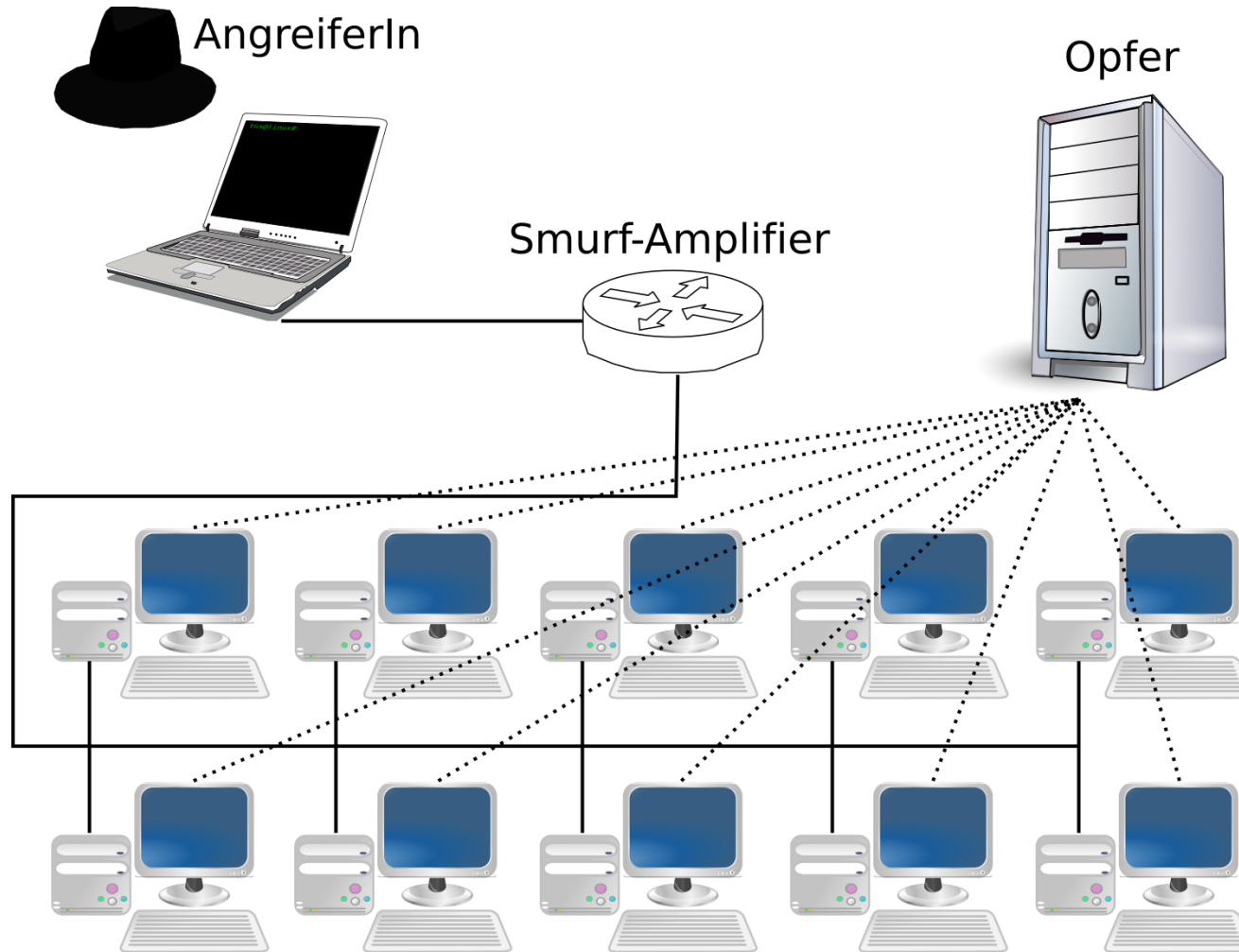
■ Address Spoofing

ICMP – Internet Control Message Protocol

- Basis RFC 792
- Fehlermeldungen
 - Port Unreachable
 - Host Unreachable
 - Time Exceeded
 - ...
- Diverse andere Informationen
 - Uhrzeit
 - Echo Request/Echo Reply
 - ...



ICMP – Smurf-Attacke

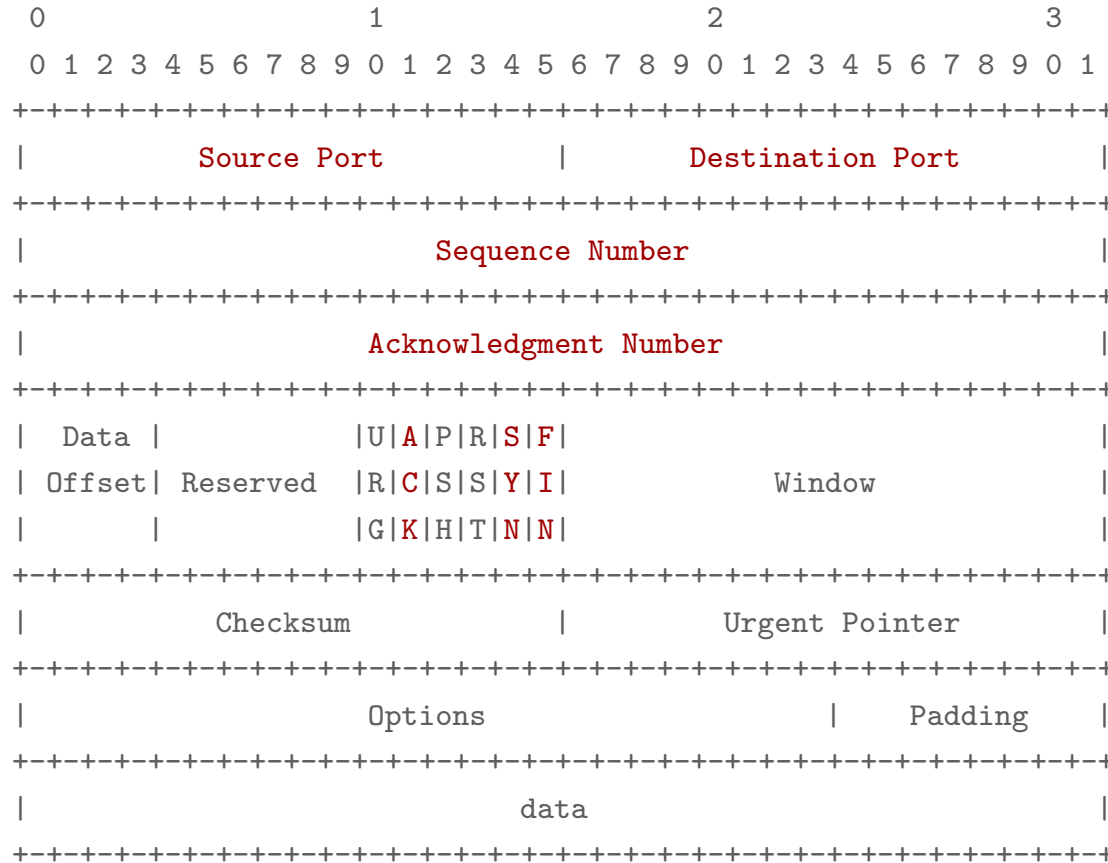


TCP – Transmission Control Protocol

- Basis RFC 793
- Verbindungsorientiert (Three-Way-Handshake), verlässlich (Timeout, Retransmission)
- Flow Control
- Exemplarische Zustände einer TCP-Verbindung: LISTEN, ESTABLISHED, CLOSED
- Keine Broadcast Empfänger:innen möglich – Gegensatz zu UDP
- Anwendung
 - Web (HTTP)
 - SSH
 - e-mails (z.B. POP3, IMAP, SMTP)
 - ...

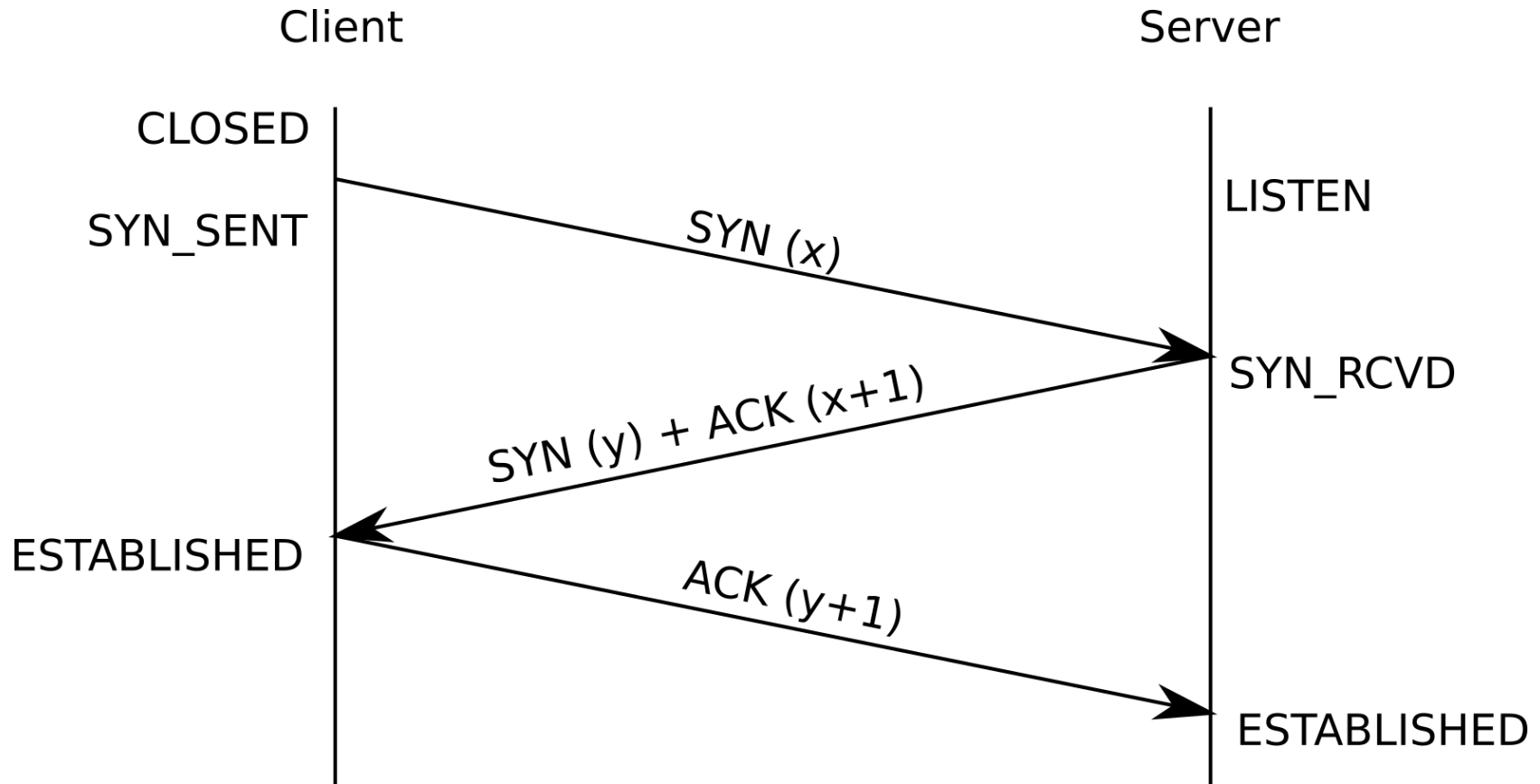
TCP – Header

- Aufbau (aus: RFC 793)

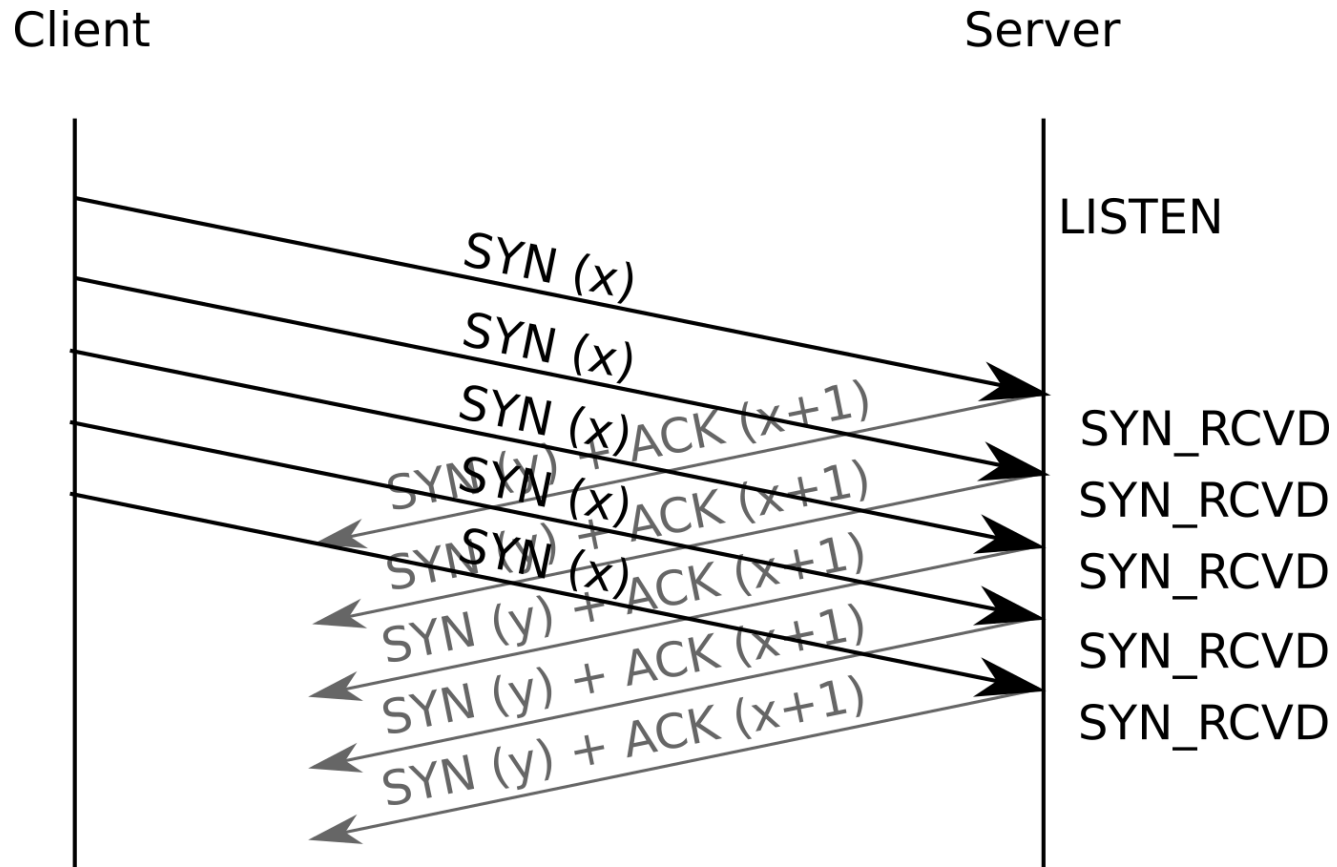


- Land-Attacke (Source Address == Destination Address, Source Port == Destination Port)

TCP – Three-Way-Handshake

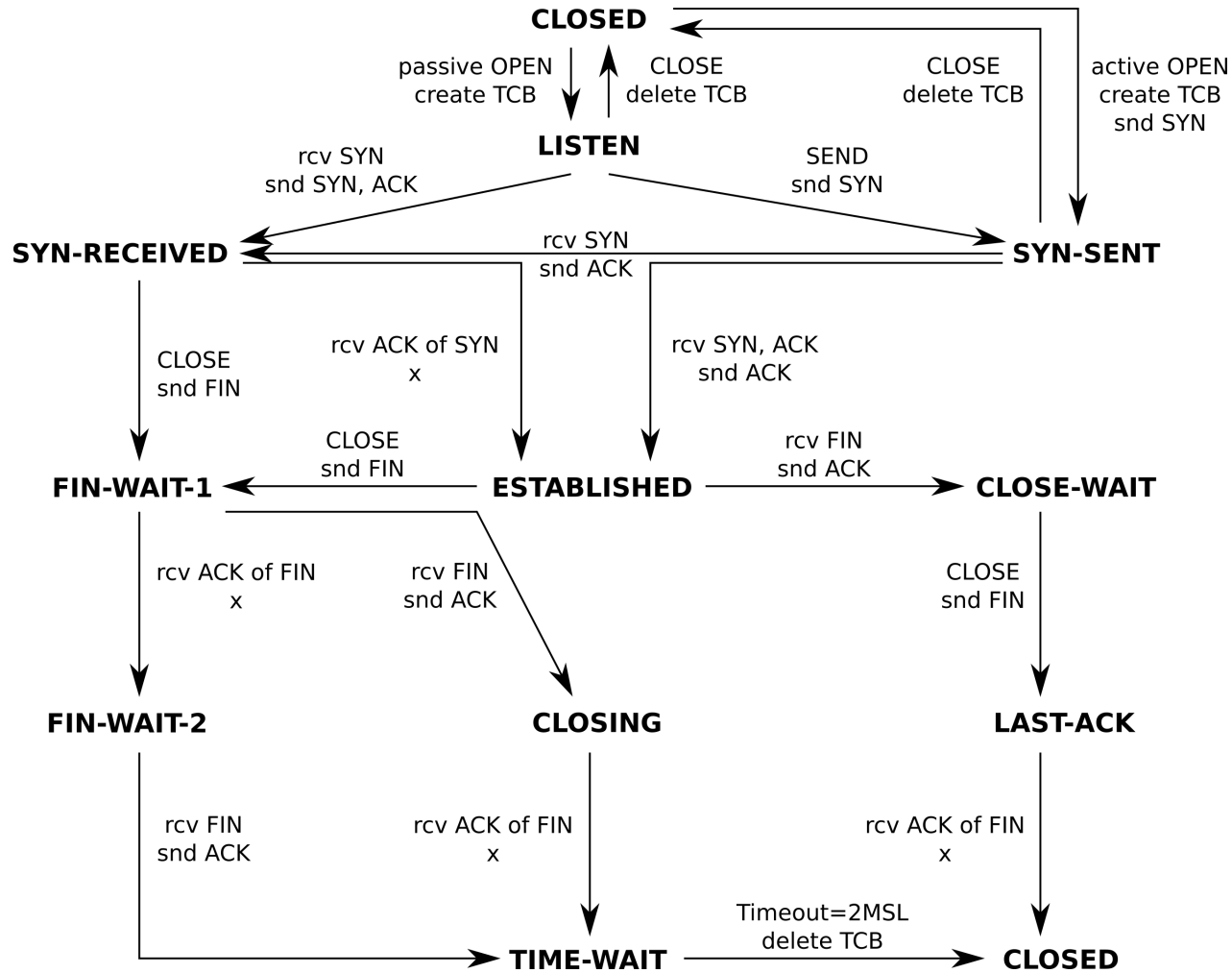


TCP – SYN Flooding



Gegenmaßnahmen z.B. SYN-Cookies u.a., siehe auch RFC 4987

Zustände einer TCP Verbindung



(Vergleiche <https://www.ietf.org/rfc/rfc793.txt>, Figure 6)

- Nicht für jeden Angriff gleich!
- Für Angriffe auf konkrete Systeme oft
 - Host Scan
 - Port Scan
 - OS Detection
 - Vulnerability Scan

 - Scanning
 - Oft auffällig
 - Daher tw. „Slow Scan“, „Stealth Scan“
 - Ablenkung

- Potenziell unsichere Netze
- Angreifer:innen haben Zugriff auf das Übertragungsmedium
- „War-Driving“
- Hotels, Flughäfen, Cafes,...
- Nachbar:innen, Firmen,...
- Angriffe sind z.B.
 - Sniffing
 - Angreifer:in spooft einen Access Point oder Client
 - Denial of Service
- Beispiel: EU-Parlament schaltet sein öffentliches WLAN ab
- Beispiel: Marriott für Blockade persönlicher WLAN-Hotspots bestraft

- Wireless Personal Area Network (WPAN)
 - Radio-Frequency Identification (RFID)
 - Near Field Communication (NFC)
 - IEEE 802.15.4 (Sub-GHz, Basis z.B. für ZigBee, 6LoWPAN)

- Wireless Local Area Network (WLAN)
 - IEEE 802.11a/b/g/n/...

- Wireless Wide Area Network (WWAN)
 - Global System for Mobile Communications (GSM)
 - Universal Mobile Telecommunications System (UMTS)
 - Long Term Evolution (LTE)
 - Fifth Generation Technology Standard (5G)

Absicherung von WLANs, Verringerung der Attack Surface

- WEP – unsicher!
- WPA, WPA2 – gute Kennwörter erforderlich!
- WPA2: 10/2017 neuer Angriff: Key Reinstallation Attack (KRACK)
- WPA3

- VPNs
- Verschlüsselung auf Applikationsebene

- Standard-Passwörter ändern
- Sicherer Schlüssel
- (Regelmäßiger) Wechsel des Schlüssels
- SSID – Service Set Identifier/Network Name
- Richtige Annahmen an Sicherheit von WLANs treffen

- Netzwerkverkehr mitlesen
- Kabelgebundenes Netzwerk vs. WLAN
- root-Rechte
- Netzwerk-Interface im Promiscuous Mode
- tcpdump
- Wireshark
- sslstrip

- Absicherung der Clients/Server
- Separation von Netzwerksegmenten (physisch, logisch)
- Sicherung des Übertragungswegs (Internet, WLAN,...) z.B. via Virtual Private Network (VPN), TLS,...
- Sicherung des Zugangs zum Netzwerk (z.B. Firewalls)
- Sicherung der Nutzdaten (Verschlüsselung von e-mails,...)
- Zusätzliche Maßnahmen wie Intrusion Detection Systems, Intrusion Prevention Systems, Honeypots, -nets, -clients

- Ziel: Unterbindung von unerlaubten Zugriffen
- Unterschiedliche Arten von Firewalls
 - Paketfilter
 - Stateful Inspection
 - Proxy Firewall
- Positionierung von Firewalls i.A. an der Grenze zwischen zwei Netzwerkzonen („Zonenmodell“, DMZ)
- Beispiele
 - iptables/nftables (Linux), pf (packet filter, OpenBSD)
 - Kommerzielle Hersteller: u.a. Cisco, F5, Checkpoint, Fortinet
 - Shorewall, Firewall Builder (fwbuilder)
 - mod_security

Zero Trust Architectures (ZTA)

- Nachteil von Firewalls: Sicherheit an Zonengrenzen
- Angriff innerhalb einer Zone?
- Definition von Zonengrenzen
- Zonengrenzen verschwinden immer mehr, Bedrohungslage ändert sich
- Anbindung von externen Diensten in das Intranet
- → Zero Trust Architecture
- Vertrauen nicht mehr auf Grund einer N/W-Zugehörigkeit, sondern
- Validierung jedes einzelnen Requests als Ziel

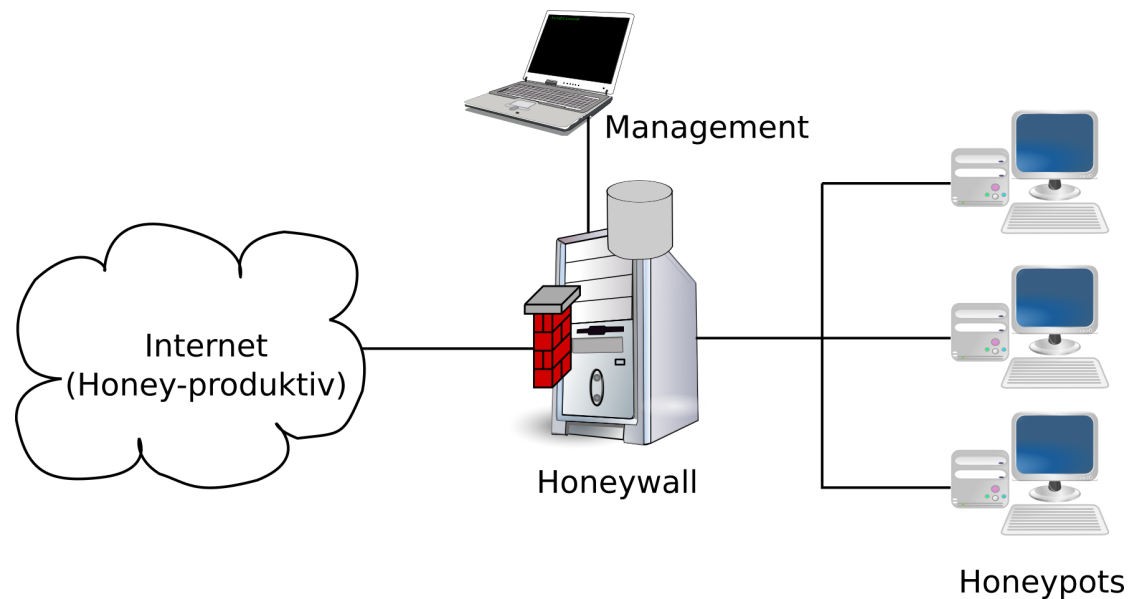
Intrusion (Detection/Prevention) Systeme

- Intrusion Detection System (IDS)
 - Erkennung von Angriffen
 - Signaturen
 - Anomalie-Erkennung
 - Senden eines Alarms bei erkanntem Angriff
- Intrusion Prevention System (IPS)
 - Zusätzlich zur Erkennung: Automatische Ergreifung von Maßnahmen
 - z.B. Aktivierung einer Firewall-Regel
- Beispiel für IDS: Snort, Zeek

- Honeypots sind eine *ergänzende* Sicherheitsmaßnahme
- Definition
 - „A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.“ (Spitzner)
 - „A security resource whose value lies in being probed, attacked or compromised.“ (Spitzner)
- Kein Produktionssystem
- Kein legitimer Zugriff
- Leichtere Analyse von auftretendem Traffic
- Honeynet ist ein Netzwerk von Honeypots

Aufbau eines Honeynets

- So etwas wie eine Firewall bzw. ein Gateway (*Honeywall*)
- Verbund von Honeypots mit diversen Diensten



- netcat
- scapy
- tcpdump
- Wireshark
- ping, traceroute,...
- unicornscan
- Nessus, OpenVAS
- <https://isc.sans.edu/data/port.html?port=80>

- Gerald A. Marin. Network security basics. *Security & Privacy, IEEE*, 3(6):68–72, November/Dezember 2005. ISSN 1540-7993. doi: 10.1109/MSP.2005.153
- Ed Skoudis und Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Pearson Education, Inc., 2. Auflage, 2006. ISBN 0-13-148104-5
- Patrick W. Dowd und John T. McHenry. Network security: it's time to take it seriously. *Computer*, 31(9):24–28, September 1998. ISSN 0018-9162. doi: 10.1109/2.708446
- Stephen M. Bellovin. A look back at security problems in the TCP/IP protocol suite. In *Computer Security Applications Conference, 2004. 20th Annual*, Seiten 229–249, Dezember 2004. doi: 10.1109/CSAC.2004.3

- Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, und Diego Zamboni. Analysis of a denial of service attack on TCP. In *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*, Seiten 208–223, Mai 1997. doi: 10.1109/SECPRI.1997.601338
- Stefan Savage, Neal Cardwell, David Wetherall, und Tom Anderson. TCP congestion control with a misbehaving receiver. *SIGCOMM Comput. Commun. Rev.*, 29(5):71–78, 1999. ISSN 0146-4833. doi: 10.1145/505696.505704
- ITU-T. Information Technology – Open Systems Interconnection – Basic Reference Model: The Basis Model. ITU-T Recommendation X.200, 1994. <http://www.itu.int/rec/T-REC-X.200-199407-I>

- Wesley M. Eddy. RFC 4987: TCP SYN Flooding Attacks and Common Mitigations, 2007. <https://www.ietf.org/rfc/rfc4987.txt>
- Roland Bless, Stefan Mink, Michael Conrad, Kendy Kutzner, Erik-Oliver Blaß, Hans-Joachim Hof, und Marcus Schöller. *Sichere Netzwerkkommunikation 2005*. Springer-Verlag, 2005. doi: 10.1007/3-540-27896-6
- Jürgen Schmidt. Ripple20 erschüttert das Internet der Dinge, 2020. <https://heise.de/-4786249>

- ISO/IEC International Standard - Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *ISO/IEC 8802-11, Second edition: 2005/Amendment 6 2006: IEEE STD 802.11i-2004 (Amendment to IEEE Std 802.11-1999)*, Seiten c1–178, Juli 2004. doi: 10.1109/IEEESTD.2004.311922
- Microsoft, Windows TCP/IP Remote Code Execution Vulnerability, 2020. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-16898>

- Microsoft, Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability, CVE-2023-23415
- BSI Zero Trust Positionspapier
- CERT-EU, HTTP/2 Rapid Reset DDoS Vulnerability, CVE-2023-44487

- Vernetzung alltäglich
- TCP/IP wurde ursprünglich nicht mit Blick auf Sicherheit spezifiziert
- Angriffe finden auf allen ISO/OSI-Ebenen statt
- Verschiedene Angriffstypen (DoS, Sniffing, Man in the Middle, Spoofing, . . .) bei verschiedenen Protokollen (ARP, IP, ICMP, TCP)
- „Kreative Anwendung“ von Protokollen, Möglichkeiten, die nicht spezifiziert wurden
- Herstellung des „Vertrauens“ fehlt
- Unterschiedliche Maßnahmen, um Netzwerksicherheit umzusetzen

Vielen Dank!

<https://establishing-security.at/>

