esse

ESSE Einführung in Security – VO 03: Netzwerksicherheit

Florian Fankhauser, Rafael Vrecar

INSO – Industrial Software
Institut für Information Systems Engineering | Fakultät für Informatik | Technische Universität Wien

Agenda

Einführung

ISO/OSI-Modell

Konkrete Angriffe und Bedrohungen

ARP – Address Resolution Protocol

IP – Internet Protocol

ICMP – Internet Control Message Protocol

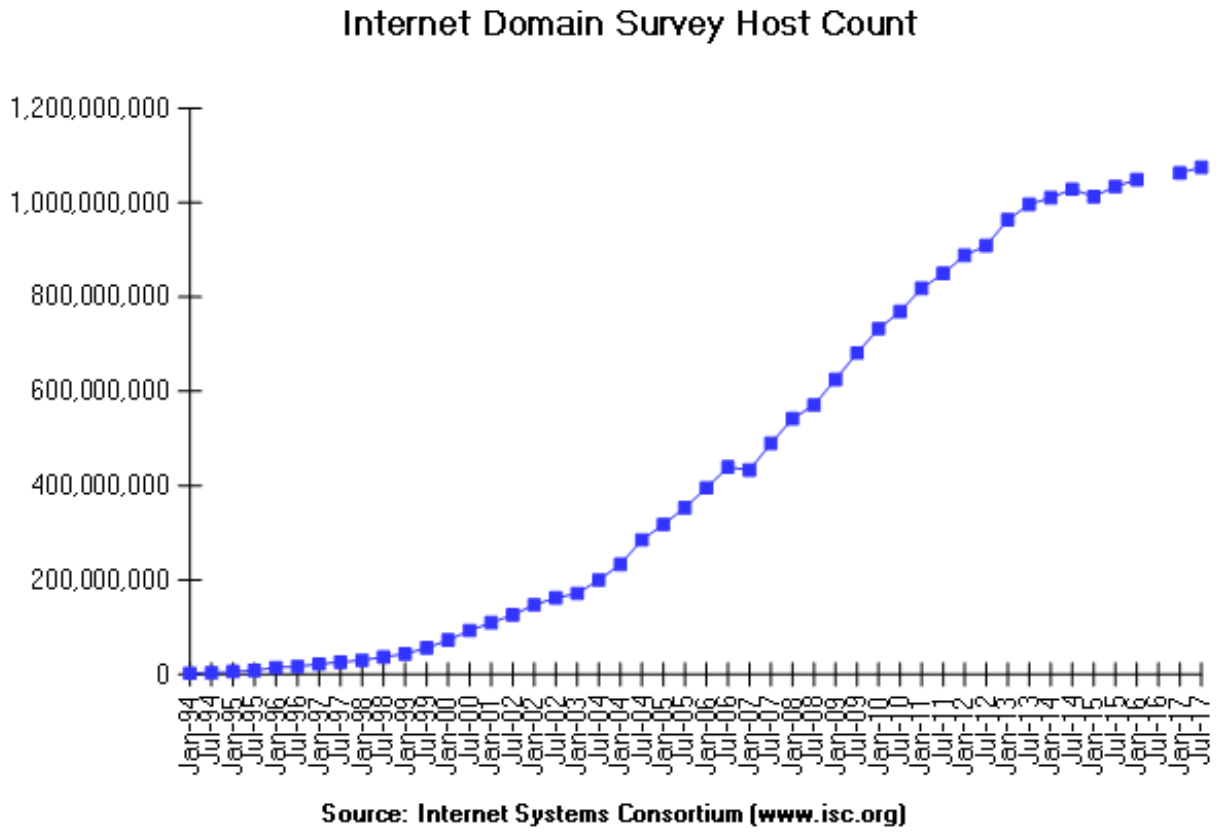
TCP – Transmission Control Protocol

Aspekte von Wireless Netzwerken

Lösungsansätze

Tools, Literatur

Viele Systeme sind im Internet

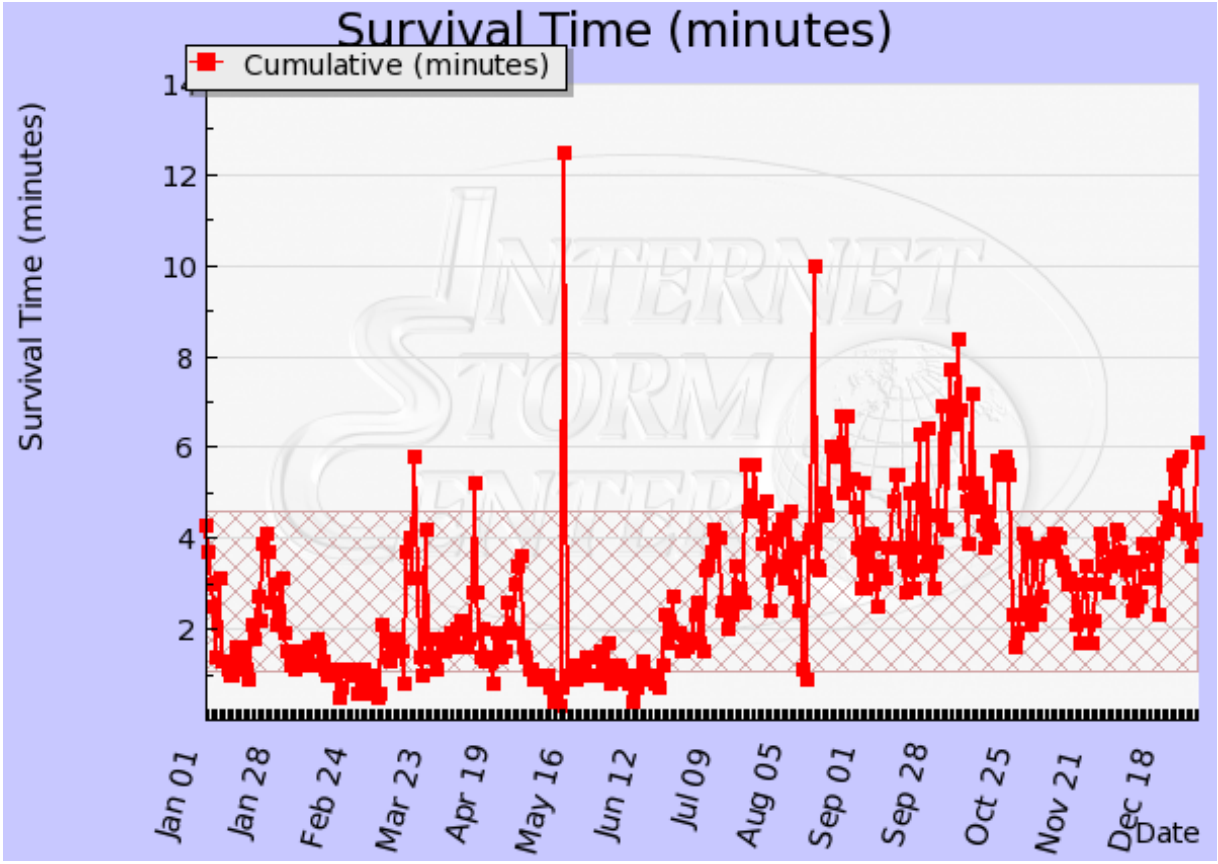


Größe des Internets

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

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

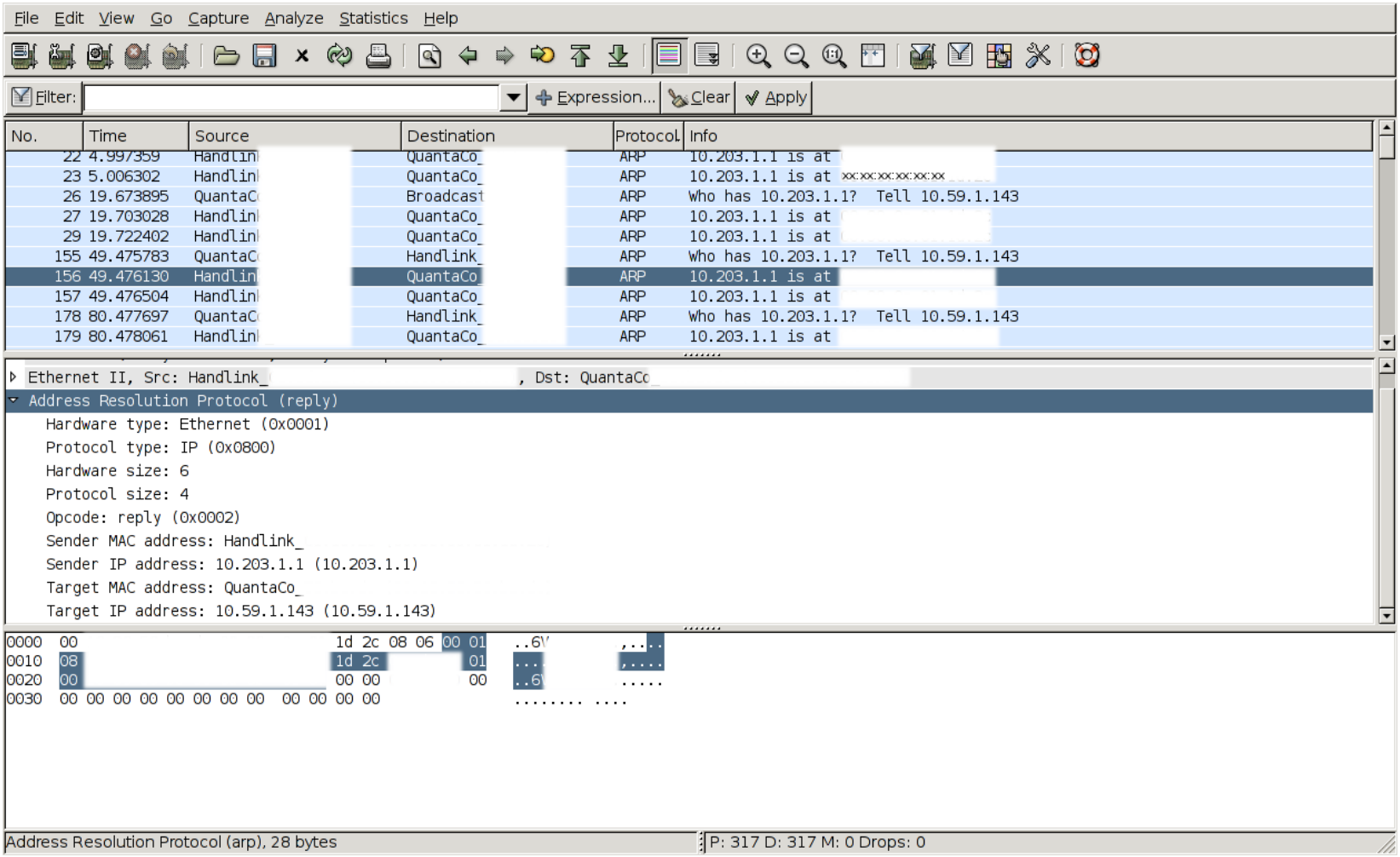
Survival Time im Internet



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

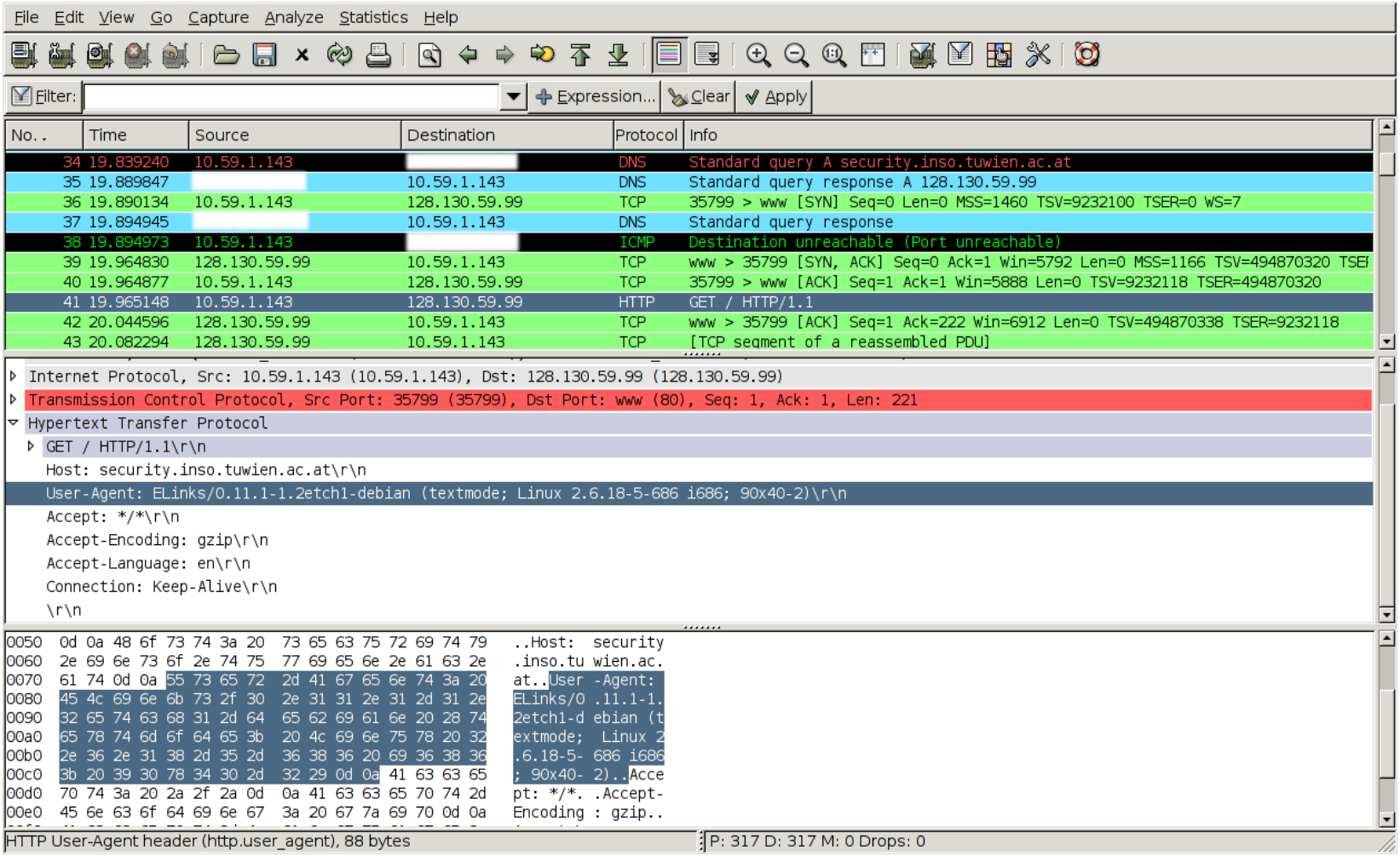
Motivation zur Netzwerksicherheit – 1/2

Oder: Die Verwendung von Wireshark



Motivation zur Netzwerksicherheit – 2/2

Oder: Die Verwendung von Wireshark



Einführung

- 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)

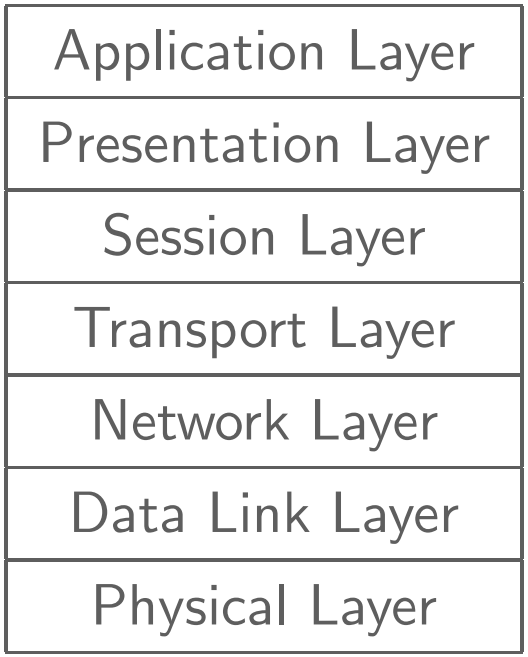
Historie, Grundlagen für IT-Risiken in Netzwerken

- 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/OSI-Modell

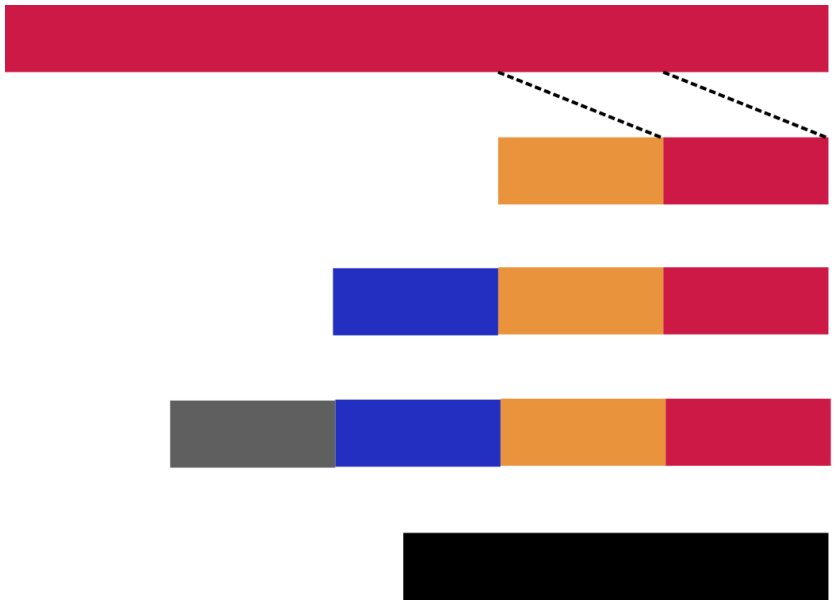
- ISO – International Organization for Standardization
- OSI – Open Systems Interconnection
- Schichtenmodell
  - Reduzierung der Komplexität der Abhängigkeiten
  - Trennung der Aufgaben in einzelnen Schichten
  - Schichten weitgehend unabhängig voneinander
  - Genau definierte Schnittstellen zwischen den Schichten
  - Höhere Schichten greifen auf Funktionen niedrigerer Schichten zu
- → Auswirkungen auf die IT-Sicherheit?

Schichten des ISO/OSI-Modells



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

TCP/IP-Schichtenmodell



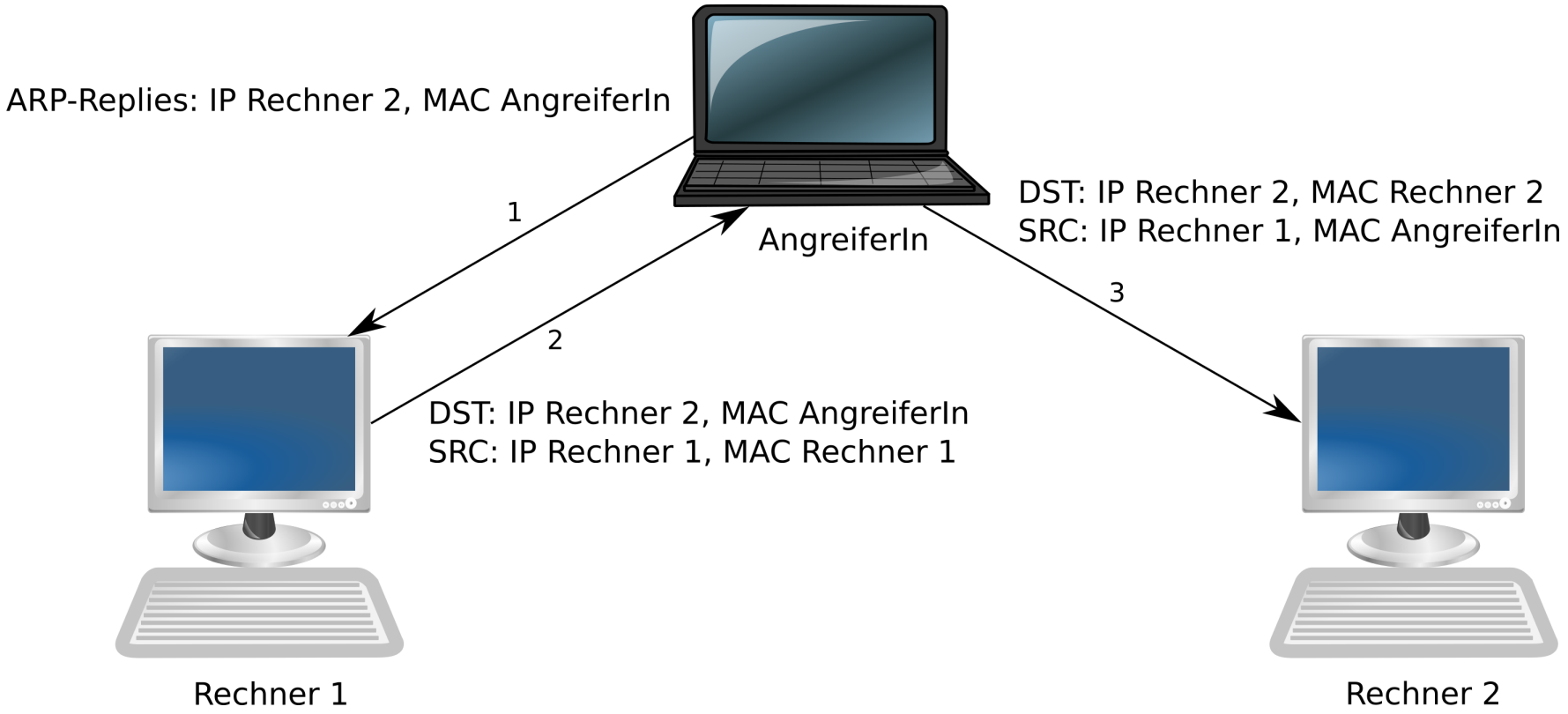
Ausgewählte Angriffe auf ausgewählten Schichten

- 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!

Spoofing

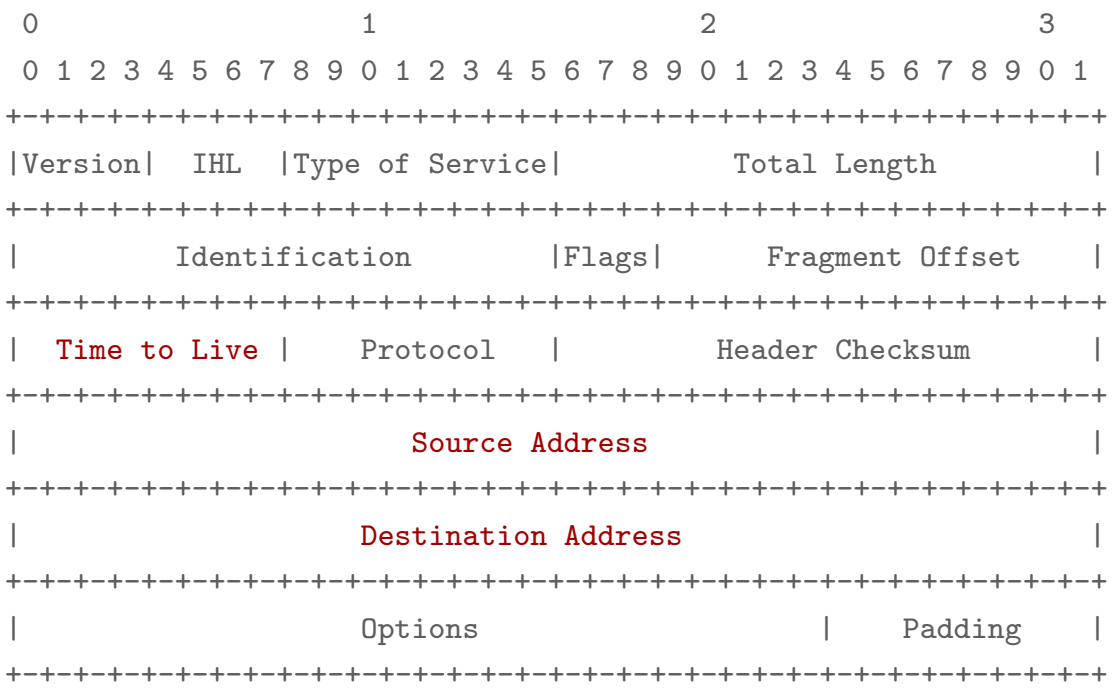

ARP-Replies: IP Rechner 2, MAC AngreiferIn
1
AngreiferIn
DST: IP Rechner 2, MAC Rechner 2
SRC: IP Rechner 1, MAC AngreiferIn
3
2
DST: IP Rechner 2, MAC AngreiferIn
SRC: IP Rechner 1, MAC Rechner 1
Rechner 1
Rechner 2

IP – Internet Protocol

- 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

IPv4

- Aufbau (aus: RFC 791)

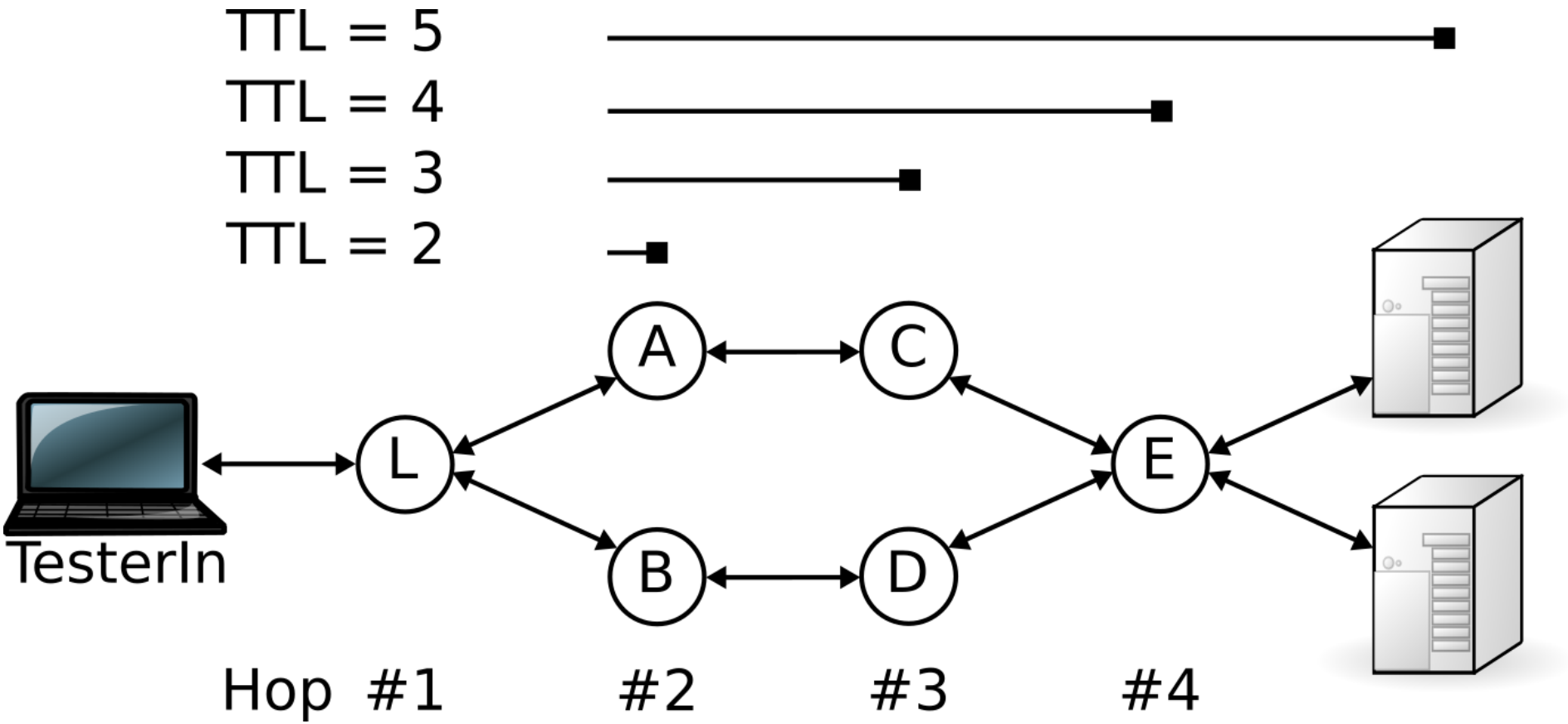


- Address Spoofing

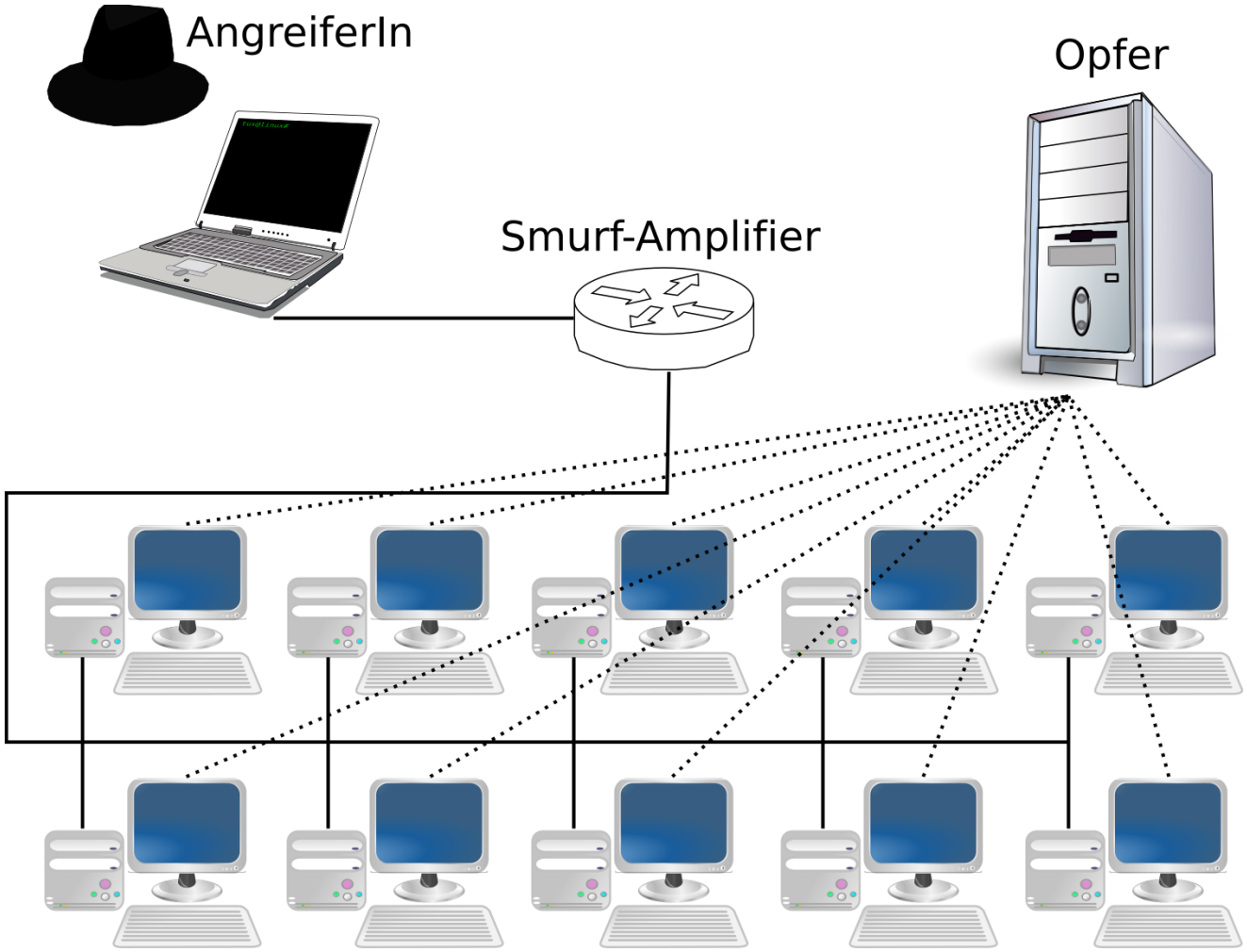
ICMP – Internet Control Message Protocol

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

traceroute



ICMP – Smurf-Attacke

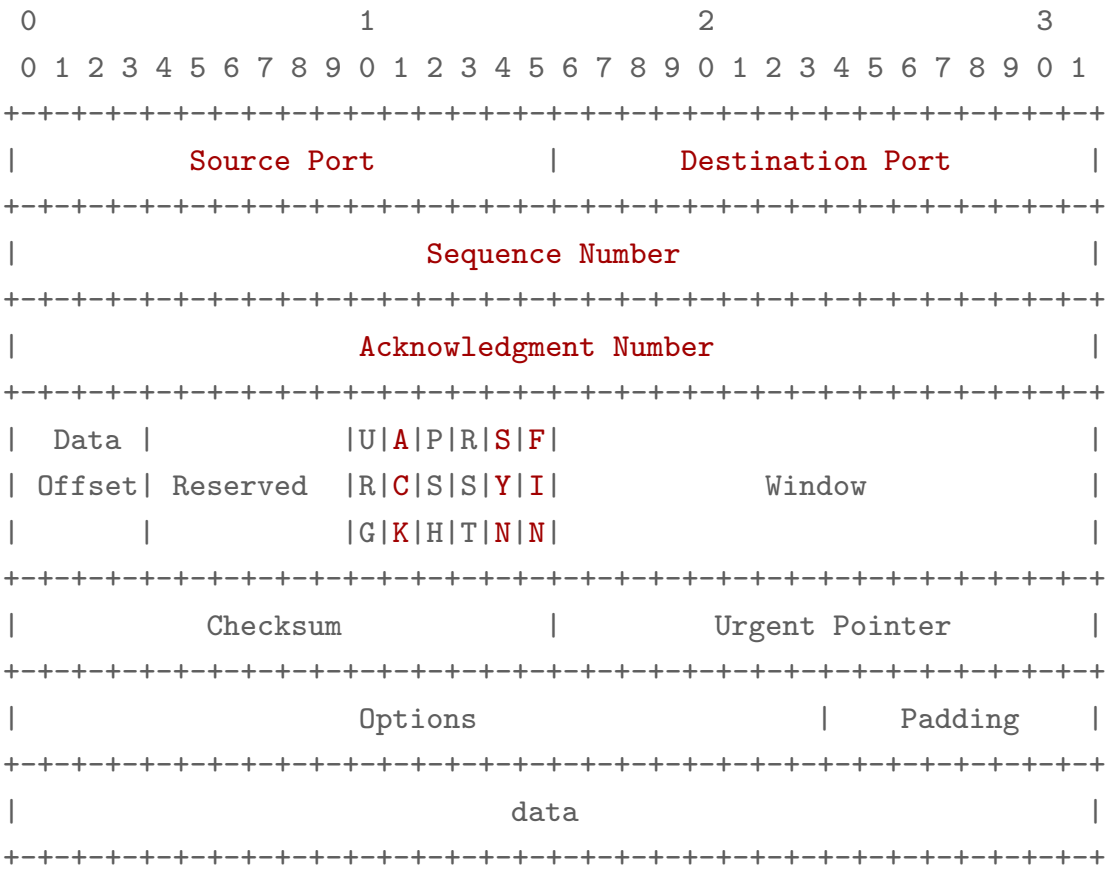


TCP – Transmission Control Protocol

- 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)
  - ...

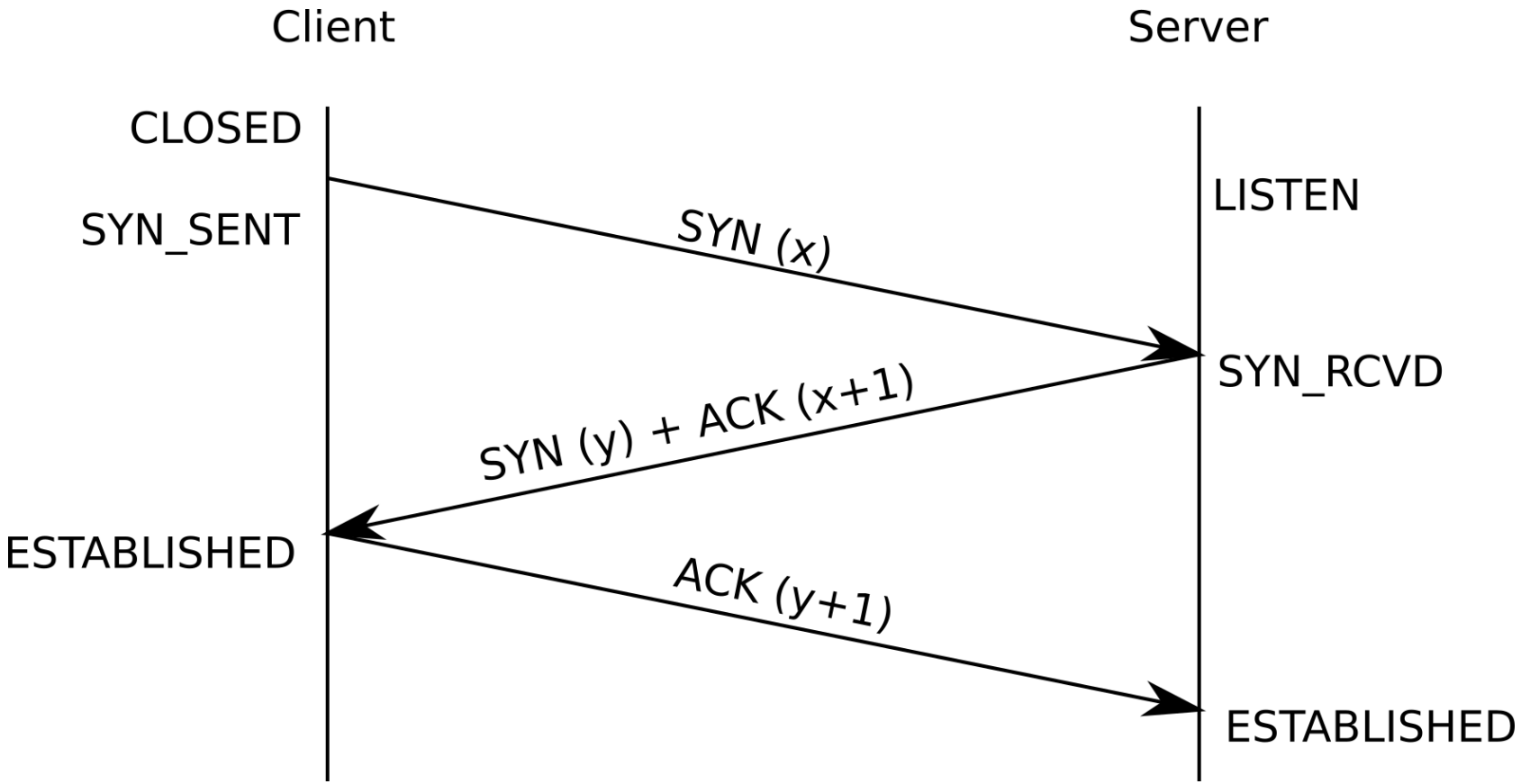
TCP – Header

- Aufbau (aus: RFC 793)

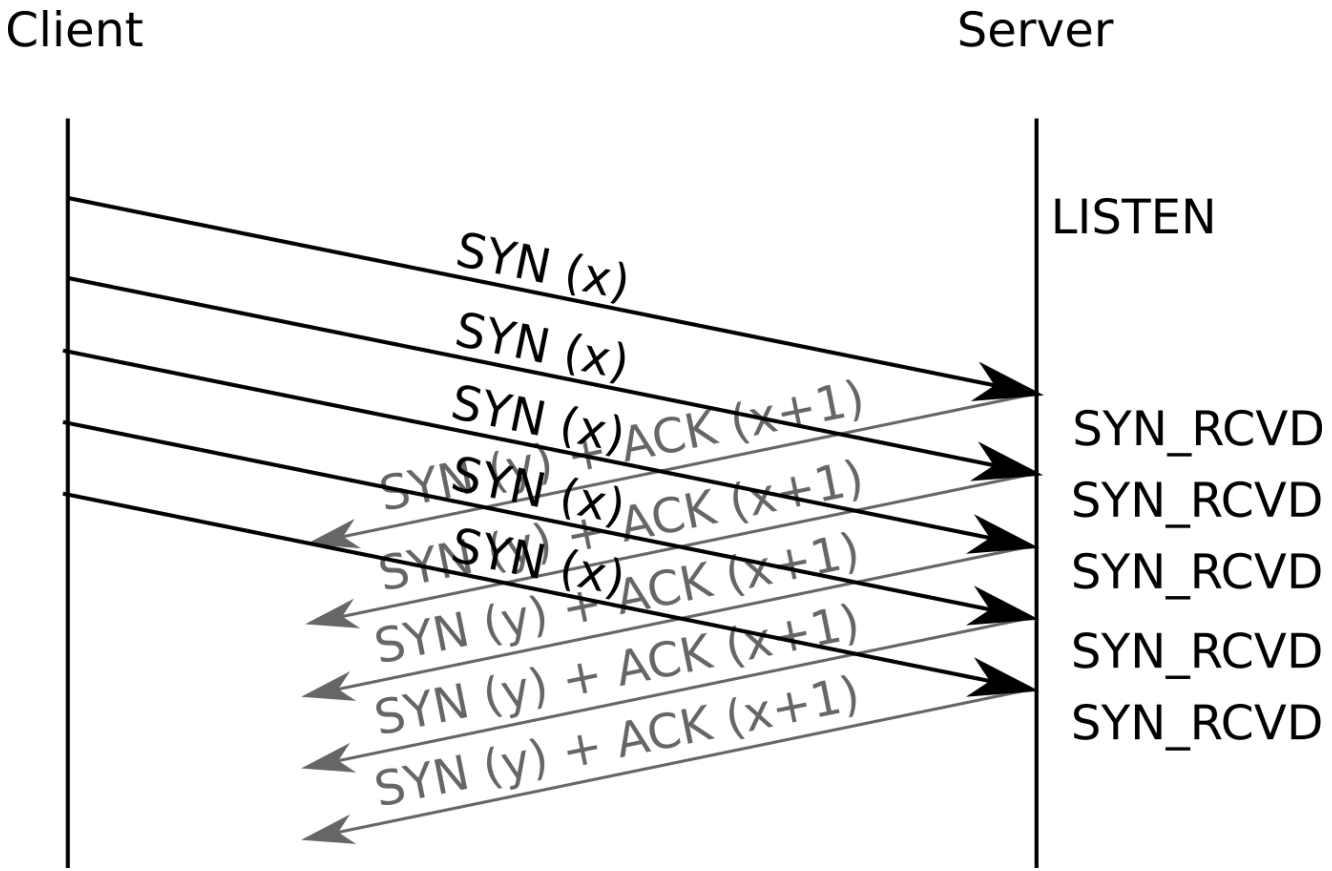


- Land-Attacke (Source Address == Destination Address, Source Port == Destination Port)

TCP – Three-Way-Handshake

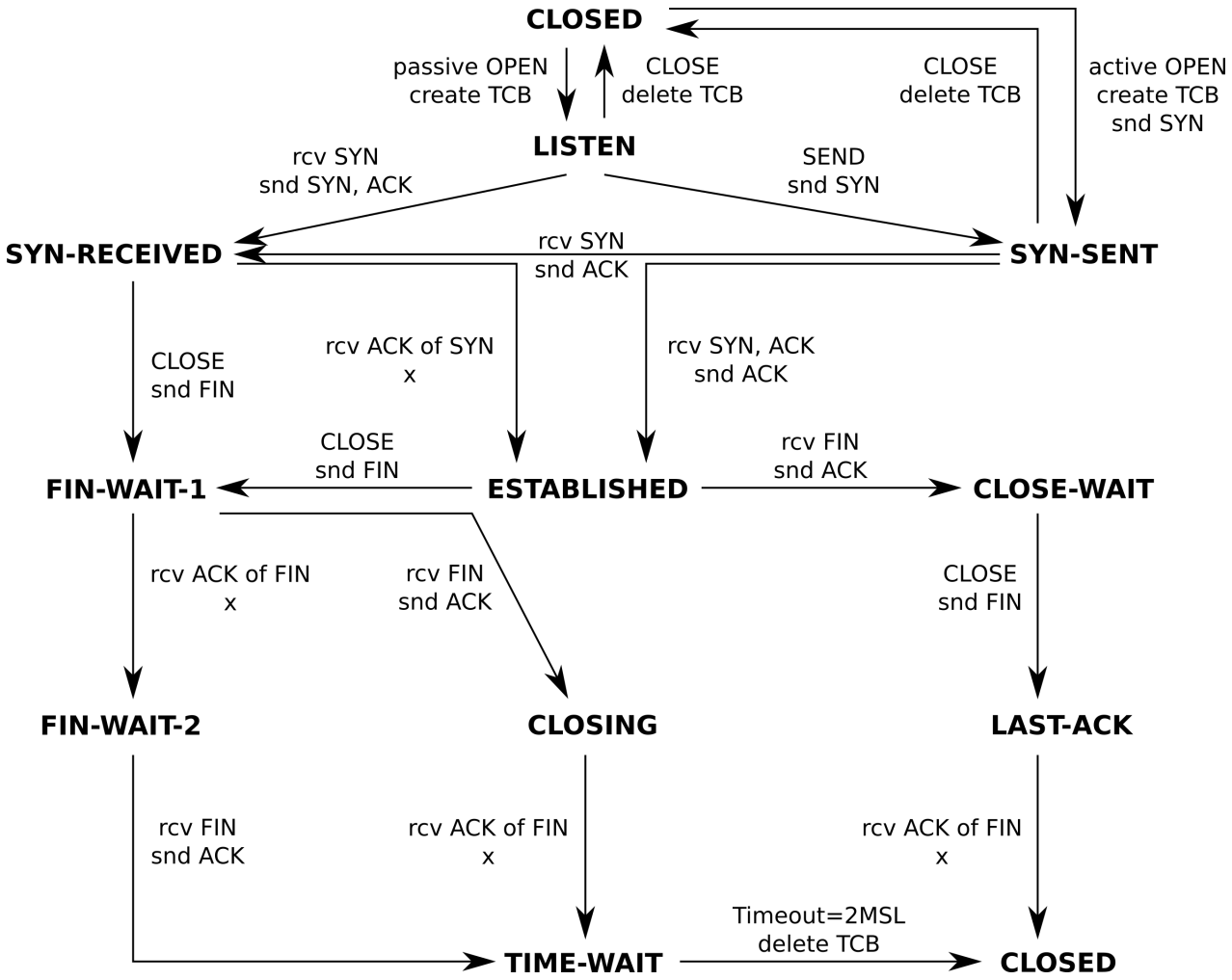


TCP – SYN Flooding



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)

Vorbereitungen für Angriffe auf IT-Systeme

- 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

WLAN

- 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 Technologien

- 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

Sniffing

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

Lösungsansätze

- 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

Firewalls

- 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

- $\rightarrow$ Zero Trust Architecture
- Vertrauen nicht mehr auf Grund einer N/W-Zugehörigkeit, sondern
- Validierung jedes einzelnen Requests als Ziel

Intrusion (Detection/Prevention) Systeme

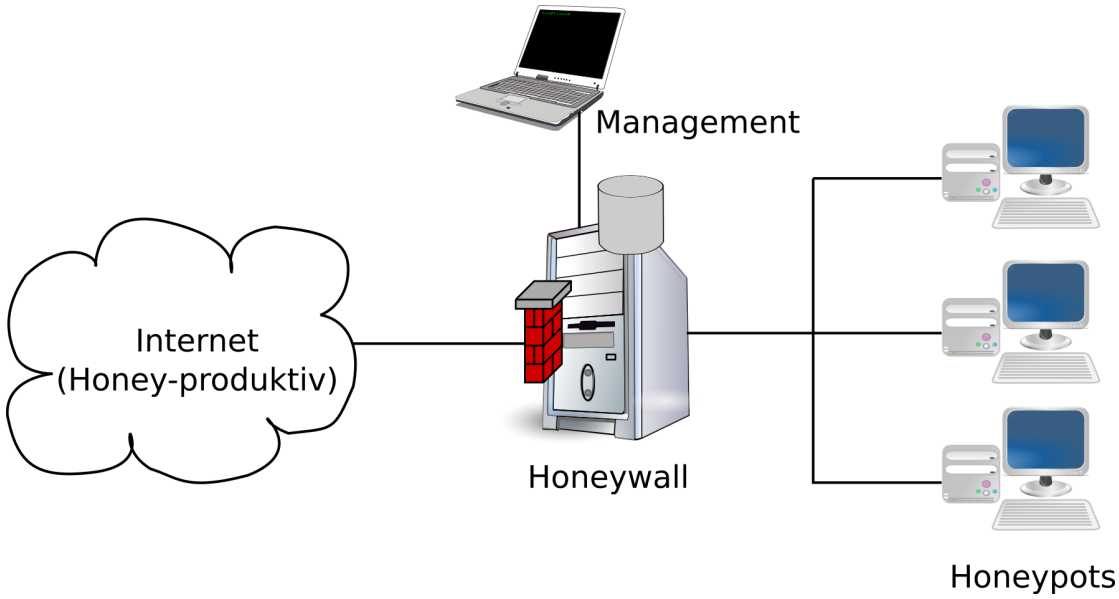
- Intrusion Detection System (IDS)
  - Erkennung von Angriffen
    - Signaturen
    - Anomalie-Erkennung
  - Senden eines Alarms bei erkanntem Angriff
- Intrusion Prevention System (IPS)
  - Zusätzlich zur Erkennung: Automatische Ergreifung von Maßnahmen
    - z.B. Aktivierung einer Firewall-Regel
-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

Honeypot und Honeynet

- 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 who's 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



Tools, weitere Information

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

Literatur, Links 1/5

- 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

Literatur, Links 2/5

- 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`

Literatur, Links 3/5

- 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`

Literatur, Links 4/5

- 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`

Literatur, Links 5/5

- 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

Zusammenfassung und Ausblick

- 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/