esse

ESSE Security for Systems Engineering 2023S
VO 02: Netzwerk-Sicherheit

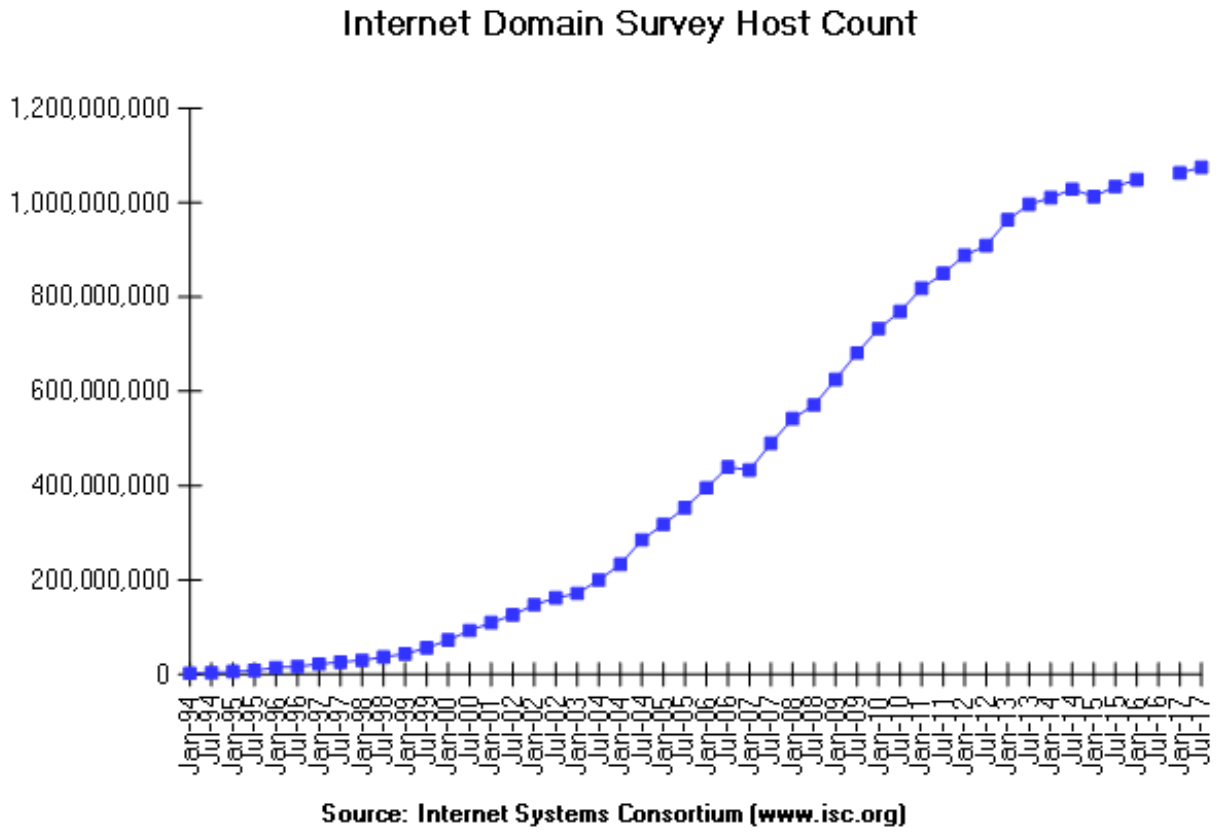
Florian Fankhauser

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

Agenda

- Einführung
- Konkrete technische Angriffe und Bedrohungen
  - ICMP – Internet Control Message Protocol
  - IP – Internet Protocol
  - DHCP – Dynamic Host Configuration Protocol
  - UDP – User Datagram Protocol
  - TCP – Transmission Control Protocol
- N/W-Security Allgemein
- Zonen, Zonenkonzept
- Tools, Literatur

Viele Systeme sind im Internet

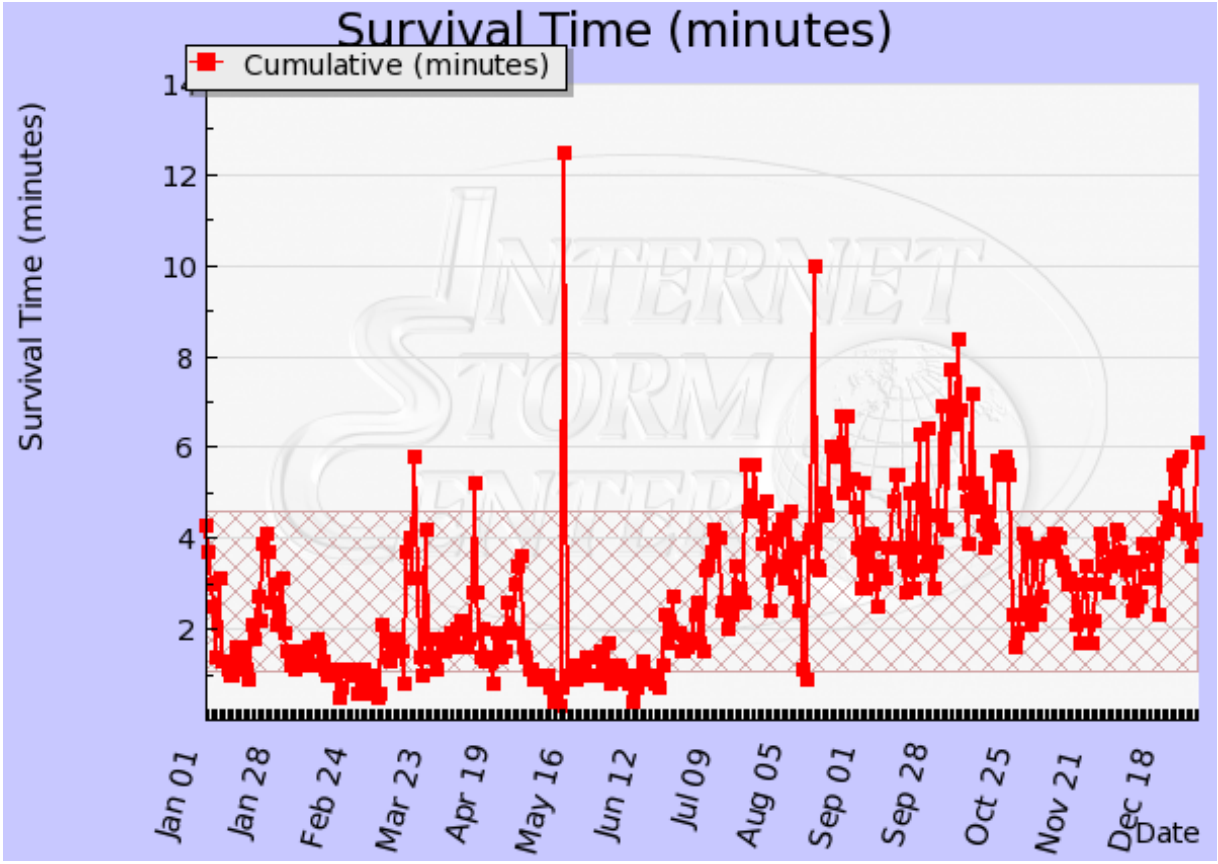


Größe des Internets

„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`)

Real-Life Großangriffe über Netzwerke

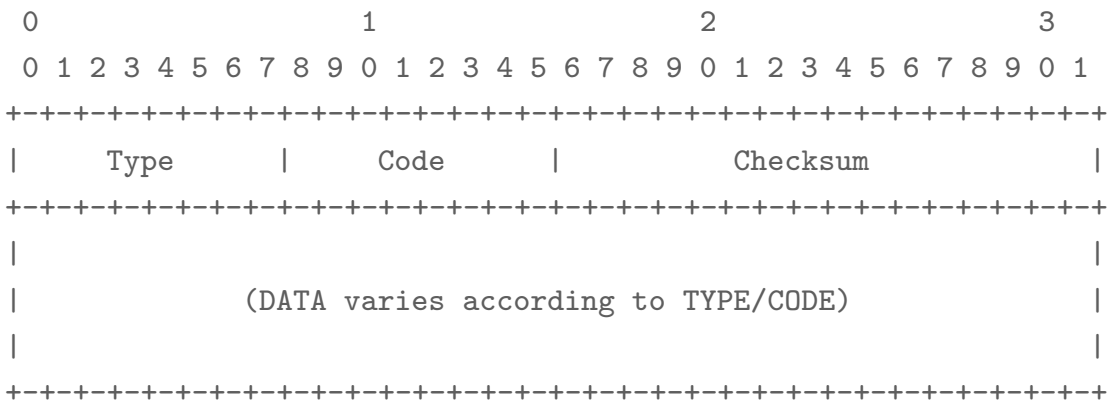
- Microsoft kontert Rekord-DDoS-Attacke mit 3,47 Terabit auf Cloud-Plattform Azure
- Black Hat: DNS-as-a-Service könnte Netzwerkinfrastruktur verraten
- Großstörung bei der Telekom: Angreifer nutzten Lücke und Botnetz-Code port 7547
- Großstörung bei der Telekom: Was wirklich geschah
- Security-Journalist Brian Krebs war Ziel eines massiven DDoS-Angriffs
- Auch Standard-Passwort von Unitymedia-Router leicht zu rekonstruieren

Konkrete technische Angriffe und Bedrohungen auf ausgewählte Schichten und Protokolle

- ICMP
- IP
- UDP
- TCP
- Application Layer

ICMP – Header

- Aufbau (aus: RFC 792)



ICMP Typen und Codes – Auszug

- 0 – Echo Reply
- 3 – Destination Unreachable
  - 0 – Net Unreachable
  - 1 – Host Unreachable
  - 3 – Port Unreachable
- 5 – Redirect
- 8 – Echo
- `https://www.iana.org/assignments/icmp-parameters`

ICMP – Ausgewählte Angriffe

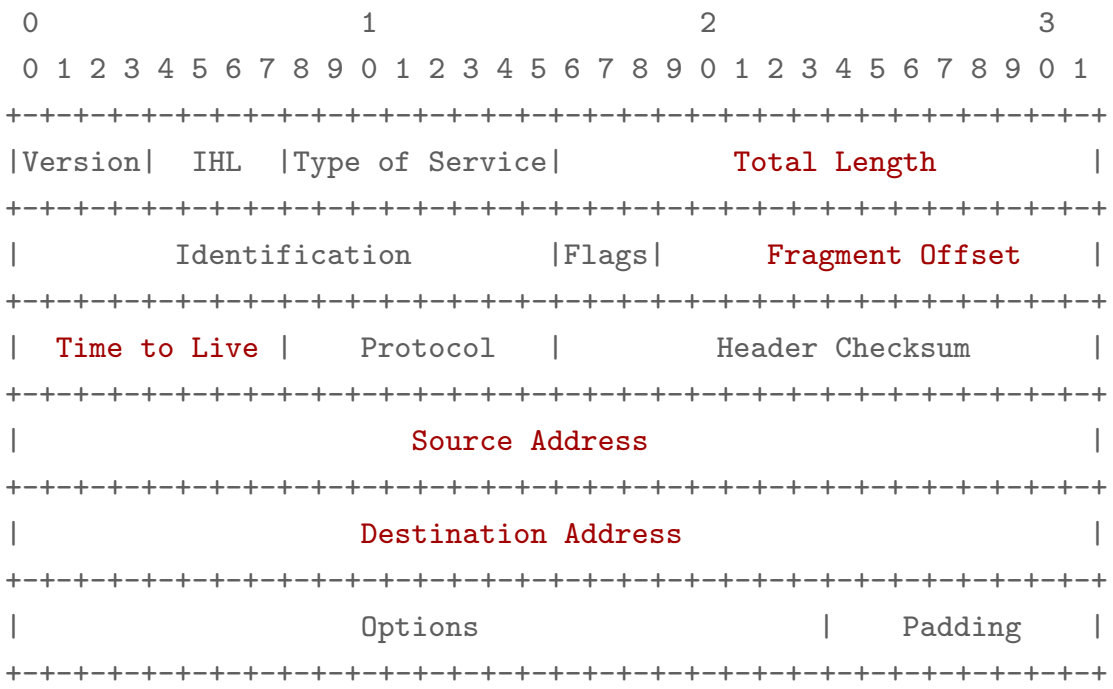
- ICMP echo request/ICMP echo reply (Scannen von N/W, Smurf-Attacke)
- Inverse Mapping (ICMP Reply Message, Fehlermeldung)
- Destination Unreachable, TTL Exceeded
- Route Redirect
- It. Spezifikation zu große Pakete, z.B. mit ping (Ping of Death (IP Fragmentation))
- ICMP Flood
- Tw. Quelle und weitere Informationen: `https://www.sans.org/white-papers/477/`

IP – Internet Protocol (IPv4)

- Basis RFC 791
- Logische Netzwerk Adressen
- x.x.x.x (z.B. 192.168.1.1)
- 127.0.0.1 als Adresse für localhost
- unzuverlässig, verbindungslos

IPv4 – Header

- Aufbau (aus: RFC 791)



IPv4 – Ausgewählte Angriffe auf Fragmentation

- Ping o' Death

  zusammengesetztes IP-Paket zu groß

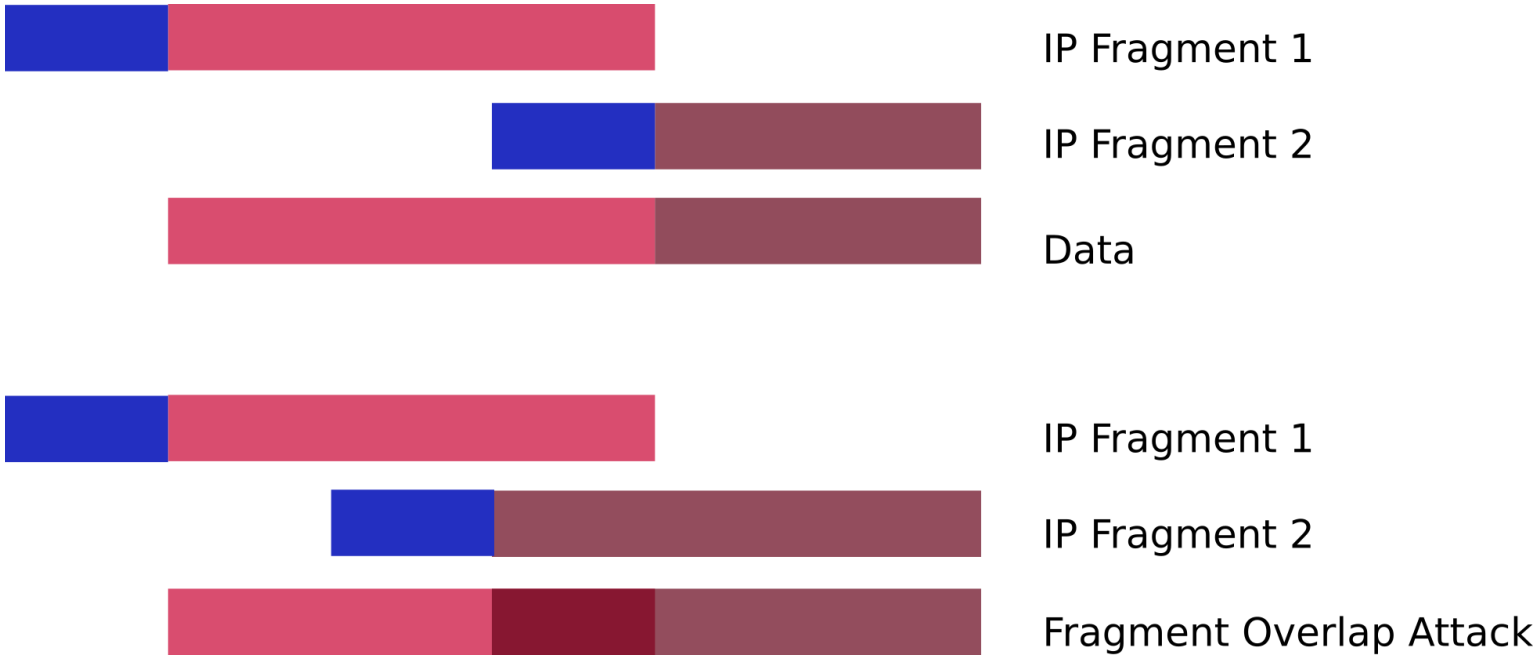
- Fragment Overlap Attack („Teardrop“)

  Überlappen von einzelnen IP-Fragmenten

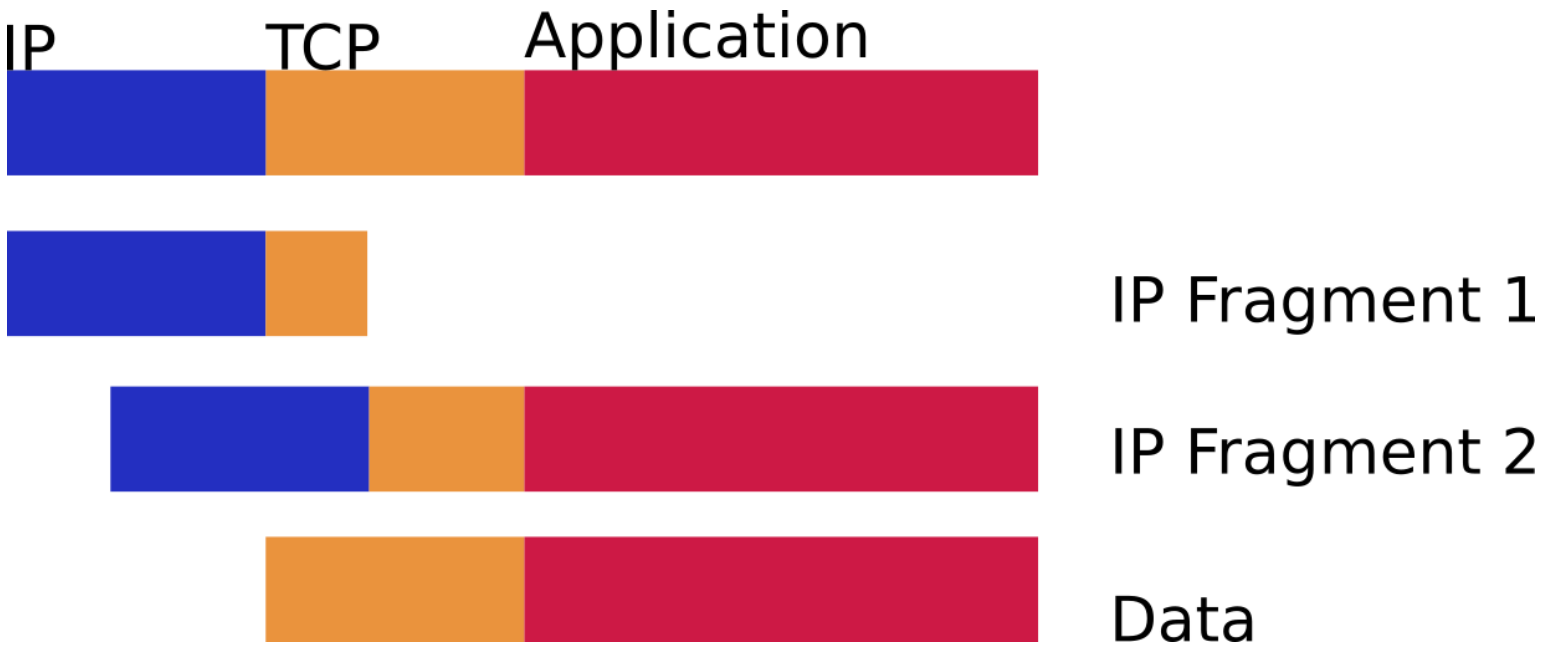
- Tiny Fragment Attack

  IP-Pakete werden absichtlich fragmentiert versendet

IPv4 – Fragment Overlap Attack



IPv4 – Tiny Fragment Attack



Attacke auf Applikationsebene: Dynamic Host Configuration Protocol (DHCP)

- Systeme brauchen IP-Adresse im Netzwerk
- Manuelle Konfiguration
- Automatische Konfiguration via DHCP
- Race Condition
- Wurm mit eingebautem DHCP-Server: https://heise.de/-1255310

Ausblick auf IPv6 – Einführung

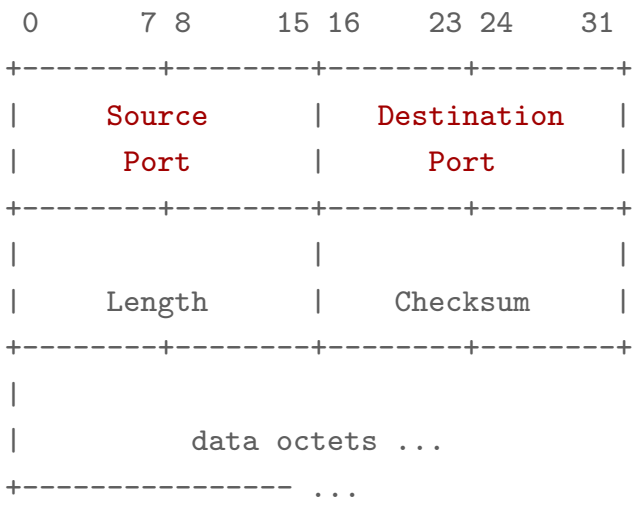
- RFC 2460 1998, mehrere Updates/Errata
- Weitreichende Änderungen im Vergleich zu IPv4, z.B.
  - IP-Adressen 128 Bits lang im Vergleich zu 32 Bits
  - DHCPv6, ICMPv6,...
  - IPv6 Multicast statt Broadcast
  - Autokonfiguration von Hosts mit IP-Adressen
  - zusätzliche, erweiterbare IPv6-Header
- Umstieg von IPv4 auf IPv6 wurde schon lange angekündigt
- Mittlerweile gibt es aber immer mehr produkive Hosts/Netzwerke mit IPv6-Anbindung! :)
- Einige Verbesserungen in Bezug auf IT-Sicherheit

Ausblick auf IPv6 – Ausgewählte Sicherheitsaspekte

- Einige Probleme gelöst, einige gleich geblieben, einige neu
- Koexistenz von IPv4 und IPv6-Netzwerken
- Host-Scans
  - Ca. 4 Mrd. IP-Adressen vs. ca. 340 Sextillionen
  - Aber: Multicast – z.B. sende Anfrage an alle Router im Netzwerk
- IPSec
  - Unterstützung verpflichtend – nicht jedoch der Gebrauch!
  - Lösung einiger Probleme, aber komplex
- DoS weiterhin möglich
  - Auch auf Applikationsebene (z.B. Autokonfiguration)
  - Privacy Extensions
- Weitere, neue Angriffe bestimmt mit höherer Verbreitung :)

User Datagram Protocol (UDP) – Header

- Aufbau (aus: RFC 768)



UDP – Ausgewählte DoS/DDoS-Angriffe

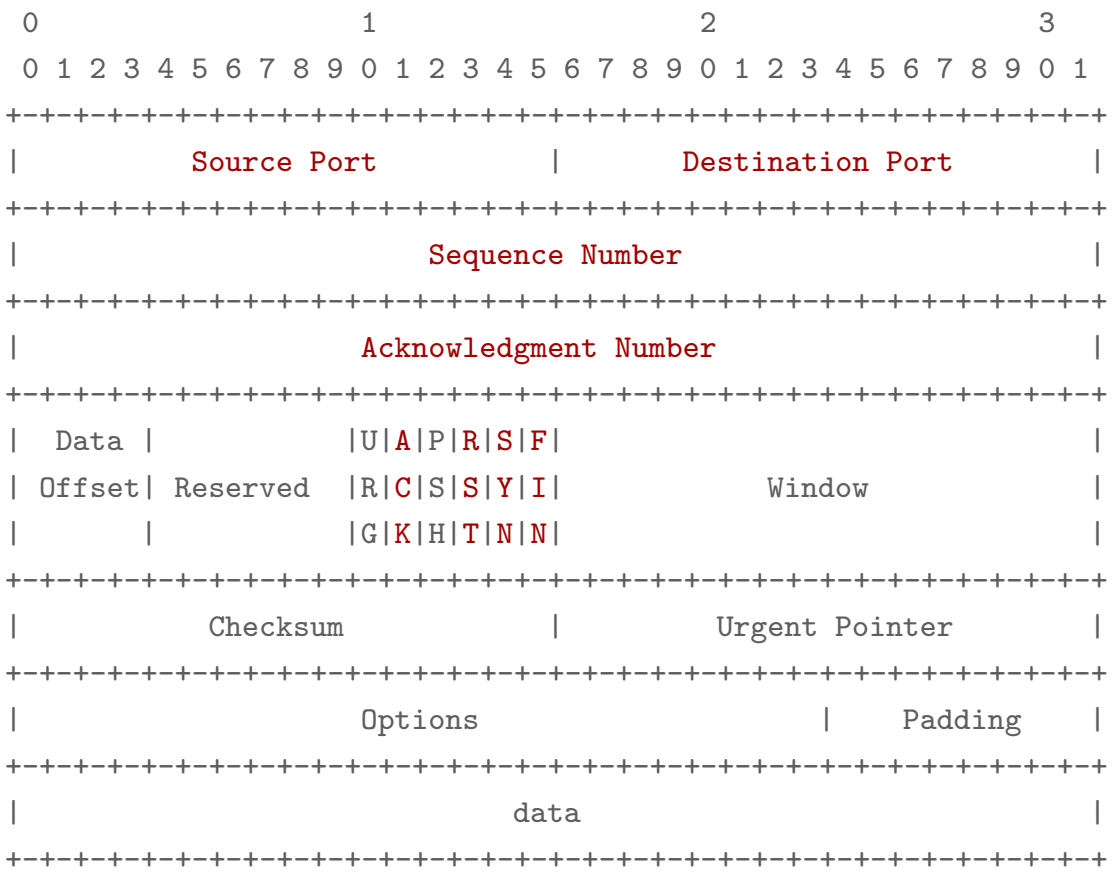
- UDP Flood Attack/UDP Packet Storm, z.B. chargen/echo
  - u.U. an die Broadcast Adresse
  - einfach möglich, da kein Verbindungsaufbau erforderlich wie bei TCP
- US-CERT Alert TA14-013A: NTP Amplification Attacks (`monlist`: Abfrage der letzten Zugriffe (IP-Adressen) und IP-Spoofing)
- US-CERT Alert TA14-017A: UDP-based Amplification Attacks (z.B. DNS, SNMP und viele mehr)

Beispiele für Sicherheitsprobleme von Domain Name System (DNS)

- Mitlesen/Verändern von DNS-Requests/Replies
- Erraten der ID eines DNS-Requests zum Fälschen von Antworten
- Name Chaining
- DoS
- Weitere Beispiele/Details:
  - CCC-DNS-Problem im Februar 2014 (siehe Eikenberg 2014, Schmidt 2014)
  - Details sind z.B. in Atkins und Austein, 2004 zu finden
- Ausblick: DNS über HTTPS (siehe z.B. Ermert, 2018)

TCP – Header

- Aufbau (aus: RFC 793)



TCP – Ausgewählte Angriffe

- Low-Rate DoS
- ACK senden bevor Daten empfangen wurden
- TCP Session Poisoning (z.B. FIN, RST)
- Christmas Tree Packet (Flags)
- TCP Sequence Number Prediction
- TCP Session Hijack (Sniffing + Spoofing)

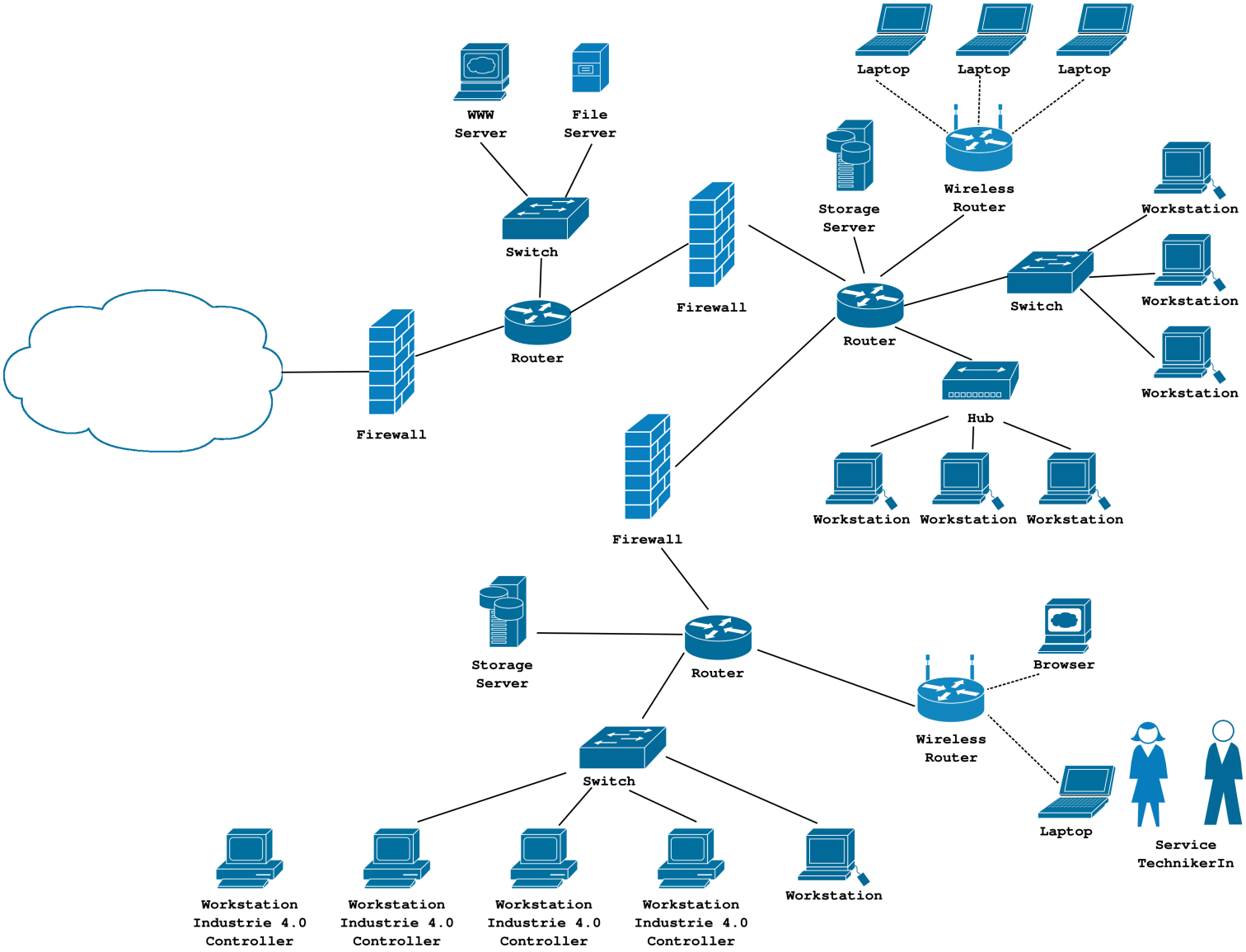
Vorbereitungen für Angriffe auf IT-Systeme

- 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

Netzwerk-Scans: `nmap`

- Portscans
  - ICMP Scan
  - TCP
    - SYN-Scan
    - FIN-Scan
    - ...
  - UDP
- Fingerprinting (OS)
- Services
- → `man nmap`

Sicherheit im Netzwerk: Netzwerk-Plan



Physische und Logische Separation von Netzwerksegmenten

- Netzwerke können physisch unterschiedlich aufgebaut sein
  - Hubs
  - Switches
  - Völlig getrennte Netzwerke, z.B. Produktion/Development, VoIP/Daten
- Netzwerke können logisch getrennt werden
  - Unterschiedliche IP-Adressbereiche
  - VLAN – Virtual Local Area Network
  - Firewalls

Zonen/Zonenkonzept

- Wiederholung: Schutzbedarf
- Unterschiedliche Sicherheitsstufen
- Unterschiedliche Sicherheitsanforderungen und -maßnahmen
- → Trennung nützlich, um Aufwand zu minimieren und Sicherheit zu erhöhen
- → Beispiele für Zonen
  - Webserver vs. interner Fileserver
  - Öffentlicher Bereich vs. Backend einer Public Key Infrastructure (PKI)
  - Interner Domain Name System (DNS) Server und externer DNS Server – Split DNS
  - DeMilitarized Zone (DMZ)

Beispiel für Umsetzung eines Zonenkonzepts: gematik

von			zu		Zone 1		Zone 2					Zone 3		
					1.x	1.9	2.9	2.2	2.3	2.4.1	2.4.2	3.1	3.5	3.6
Zone 1	1.x						2M,RM,PeM,PvS	2M,RM,PeM,PvS	3M,4S,RM,PeM,PvS	3M,4S,RM,PeM,PvS				
	1.9						2M,RM,PeM,PvS	2M,RM,PeM,PvS	3M,4S,RM,PeM,PvS	3M,4S,RM,PeM,PvS				
Zone 2	2.9							1M,2S	1M,2S	1M,2S	1M,2S	2M,PeS,PvM	2M,PeS,PvM	2M,PeS,PvM
	2.2						1M,2S		1M,2S	1M,2S	1M,2S	2M,PeS,PvM	2M,PeS,PvM	2M,PeS,PvM
	2.3						1M,2S	1M,2S		1M,2S	1M,2S	2M,PeS,PvM	2M,PeS,PvM	2M,PeS,PvM
		2.4.1					1M,2S	1M,2S	1M,2S		1M,2S	2M,PeS,PvM	2M,PeS,PvM	2M,PeS,PvM
		2.4.2					1M,2S	1M,2S	1M,2S	1M,2S		2M,PeS,PvM	2M,PeS,PvM	2M,PeS,PvM
Zone 3	3.1						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S		1M,2S	1M,2S
	3.5						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S		
	3.6						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S,PeM,PvM	1M,2S,PeM,PvM	
	3.7						1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM
	3.8						1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM
Zone 4	4.1						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S
	4.5						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S
	4.6						1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S	1M,2S
	4.7						1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM	1M,2S,PeM,PvM
	4.8													
Zone 5							1M,2S	1M,2S	1M,2S	1M,2S	1M,2S			
Zone 6	6.1						1M,2S,RM	1M,2S,RM	1M,2S,RM	1M,2S,RM	1M,2S,RM			
	6.2						1M,2S,RM	1M,2S,RM	1M,2S,RM	1M,2S,RM	1M,2S,RM			

Übergang erlaubt

Verantwortung liegt beim Betreiber, keine abschließenden expliziten Vorgaben durch die gematik

Übergang verboten

nS	Netzwerkschutz Stufe n SOLL umgesetzt werden (S = Soll, M = MUSS)
RM	Regelsatz (siehe [gematik_Inf_Netzerksicherheit]) MUSS der gematik gemeldet werden (R = Regelsatz)
PeM	Erlaubte Verbindungsaufbauten MÜSSEN mit Start- und Zieladresse protokolliert werden (P = Protokollieren, e = erlaubt))
PvM	Der Versuch verbotener Verbindungsaufbaus MUSS mit Start- und Zieladresse protokolliert werden (v = verboten)

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

Grundregeln bei der Nutzung von Firewalls

- Filtern des Traffics
  - ingress
  - egress
  - „Martian Packets“
- Fail Safe
  - → Default Deny
- Logging

Beispiel für Umsetzungsaspekte von Firewalls: netfilter/iptables

- Chains (z.B. FORWARD, INPUT, OUTPUT)
- Targets (ACCEPT, DROP, LOG, REJECT,...)
- Erstellung von Firewall Regeln
  - Texteditor (z.B. Vim, Emacs,...)
  - GUIs (z.B. Firewall Builder)

Beispiele für Netfilter/iptables-Regeln

- Loggen, Droppen von Paketen

```
/sbin/iptables -A INPUT -m state --state INVALID -j LOG \
      --log-prefix "FIREWALL Error: invalid state: "
/sbin/iptables -A INPUT -m state --state INVALID -j DROP
```

- SSH-Zugriff ist erlaubt

```
/sbin/iptables -A INPUT --protocol tcp --dport 22 -m state \
    --state NEW,ESTABLISHED -j ACCEPT
```

- Default-Policy

```
/sbin/iptables -P INPUT DROP
```

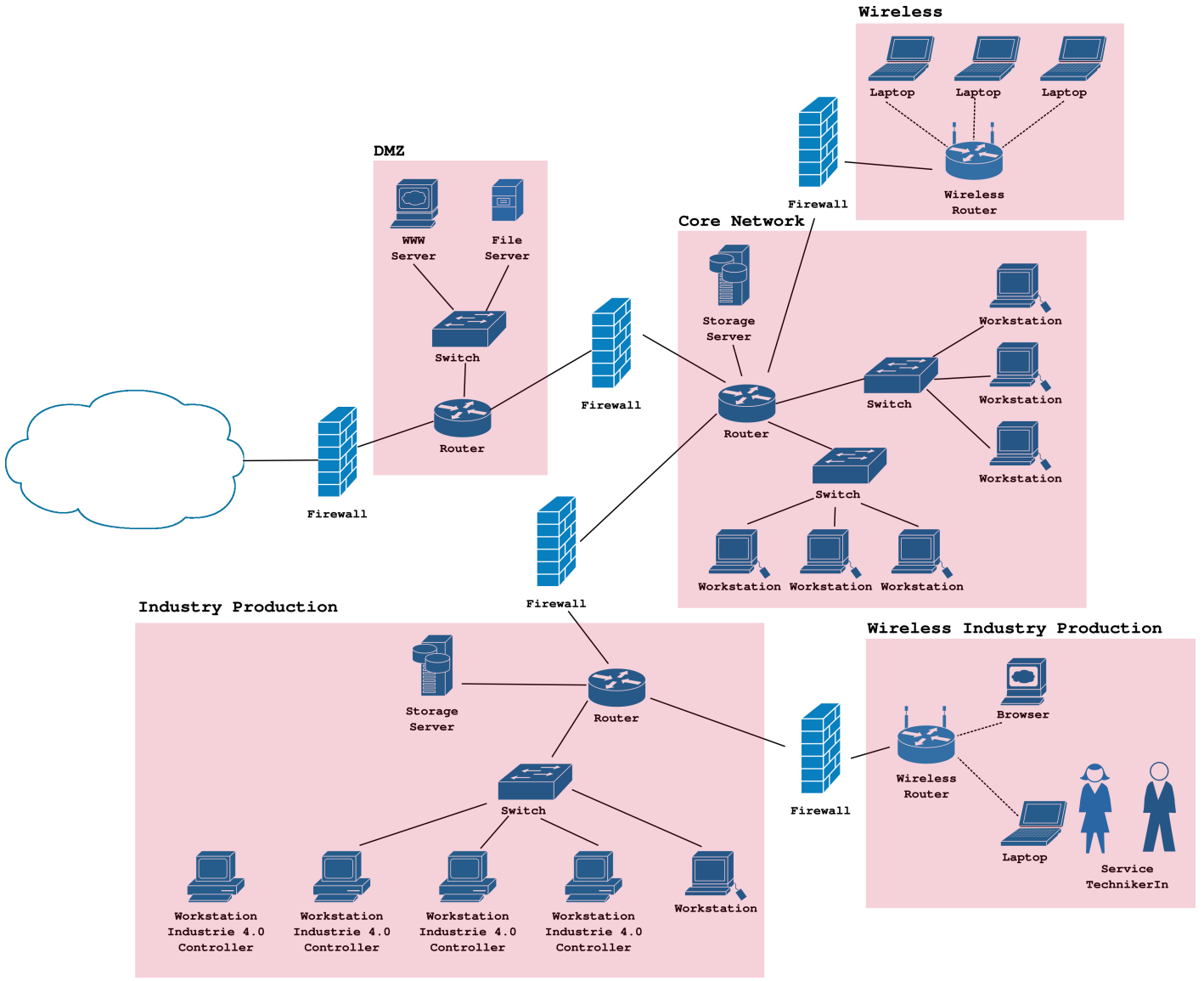
Beispiele für Angriffe auf Firewalls

- Hyper Text Transfer Protocol (HTTP) Tunnel: `https://github.com/larsbrinkhoff/httptunnel`
- Domain Name System (DNS) Tunnel: z.B. dns2tcp, iodine
- $\rightarrow$ Firewall muss auch auf Applikationsebene verstehen wie der Traffic aussieht
- Angriff direkt auf die (Application Layer) Firewall, die ja auch „nur Software“ ist
- Nachteil: Gegebenenfalls Vernachlässigung anderer Schutzmaßnahmen

MetaSploit-Framework als Tool (auch) für Netzwerk-Angriffe

- Open Source
- Fertige „Exploit Umgebung“
- Über Hunderte fertige Exploits
  - Directory Traversal, Windows Bugs usw.
- Entwicklungsbasis für neue Exploits

Sicherheit im Netzwerk: Netzwerk-Plan 2.0



Tools, weitere Information

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

Betroffene Schutzziele

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Nichtabstreitbarkeit
- ...

Literatur 1/6

- The OWASP Foundation. OWASP Top 10 – 2021, 2021. `https://owasp.org/Top10/`
- 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

Literatur 2/6

- 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

Literatur 3/6

- W. Richard Stevens. *TCP/IP Illustrated, Volume 1. The Protocols*. Addison-Wesley, 1994. ISBN 0-201-63346-9
- Niels Ferguson und Bruce Schneier. A Cryptographic Evaluation of IPsec, 1999. `https://www.schneier.com/wp-content/uploads/2016/02/paper-ipsec.pdf`
- Stuart McClure. *Hacking Exposed: Network Security Secrets and Solutions*. Mcgraw-Hill Professional, 2009. ISBN 0071613749
- US-CERT. Alert TA14-013A: NTP Amplification Attacks Using CVE-2013-5211, 2014a. `https://www.us-cert.gov/ncas/alerts/TA14-013A`

Literatur 4/6

- US-CERT. Alert TA14-017A: UDP-based Amplification Attacks, 2014b. https://www.us-cert.gov/ncas/alerts/TA14-017A
- Derek Atkins und Rob Austein. Threat Analysis of the Domain Name System (DNS), 2004. https://www.ietf.org/rfc/rfc3833.txt
- Ronald Eikenberg. Heise Newsticker: DNS-Server des CCC als Werbeschleuder missbraucht, 2014. https://heise.de/-2111501
- Jürgen Schmidt. Heise Newsticker: DNS-Server des CCC: Anfällig wegen veralteter Software, 2014. https://heise.de/-2112171
- Jürgen Seeger. Heise Newsticker: EU-Parlament schaltet sein öffentliches WLAN ab, 2013. https://heise.de/-2057579

Literatur 5/6

- Stephen E. Deering und Robert M. Hinden. Internet Protocol, Version 6 (IPv6) (RFC 2460), 1998. https://www.ietf.org/rfc/rfc2460.txt
- Carlos E. Caicedo, James B.D. Joshi, und Summit R. Tuladhar. IPv6 Security Challenges. *Computer*, 42(2):36–42, Februar 2009. ISSN 0018-9162. doi: 10.1109/MC.2009.54
- Fernando Gont. ICMP Attacks against TCP, 2010. https://www.ietf.org/rfc/rfc5927.txt
- Monika Ermert. IETF: DNS über HTTPS wird zum Standard, 2018. https://heise.de/-4119942

Literatur 6/6

- Fernando Gont. Network Security: IPv6 Security for IPv4 Engineers, 2019. https://www.internetsociety.org/resources/deploy360/ipv6/security/ipv4-engineers
- Jürgen Schmidt. Ripple20 erschüttert das Internet der Dinge, 2020. https://heise.de/-4786249

Zusammenfassung und Ausblick

- (Nicht nur) Computer sind vernetzt
- Angriffe finden auf allen OSI-Ebenen statt
- TCP/IP wurde ursprünglich nicht mit Blick auf Sicherheit spezifiziert
- Unterschiedliche Angriffe auf unterschiedliche Protokolle/Dienste
- „Kreative Anwendung“ von Protokollen; Möglichkeiten, die nicht spezifiziert wurden
- Unterschiedliche Maßnahmen, um Netzwerksicherheit umzusetzen
- Netzwerk-Design, Firewalls
- Zero Trust

Vielen Dank!

https://security.inso.tuwien.ac.at/