
Sniffing, Spoofing, Denial of Service, Internet of Things and Security

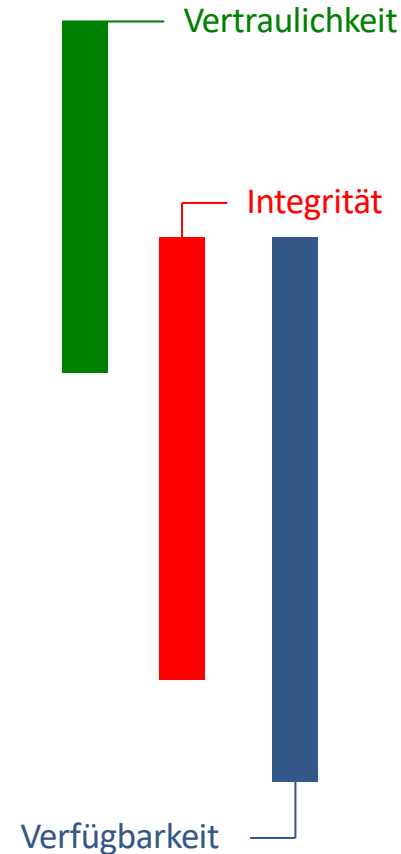
Angriffsformen

■ Passive Angriffe

- Lauschangriff (eavesdropping, sniffing)
- Verkehrsflussanalyse (traffic analysis)

■ Aktive Angriffe

- Maskerade (masquerading)
 - Man-in-the-middle attack
- Verändern von Daten (modification)
- Einfügen von Daten (injection, spoofing)
 - Wiederholen (replay)
 - Fluten (flooding, spamming)
- Dienstverweigerung (denial of service)



Konkrete Beispiele

Broadcast Ethernet und Funkkomm.

Überwachung in Kommunikationsnetzen (Carnivore, XKeyScore, Cambridge Analytica, Strava Heatmap, ...)

ARP-Spoofing (Switched Ethernet)

DNS-Spoofing

Recht auf Vergessenwerden

Distributed Denial of Service (DDos)

Vertraulichkeit

Integrität

Verfügbarkeit

Sniffing-Angriffe: Funktionsweise (Ethernet)

a) Ethernet: Alle Stationen erhalten alle Datenpakete

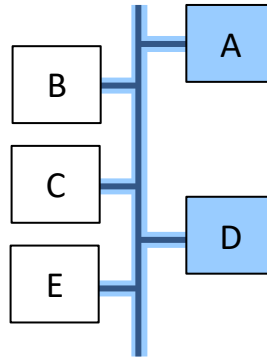
- lokale Filterfunktion
- Abschalten des Filters in Ethernetadapter möglich: »promiscuous mode«

b) Switched Ethernet: Sniffing beschränkt sich auf die Netzsegmente, in denen der Angreifer verbreitet ist

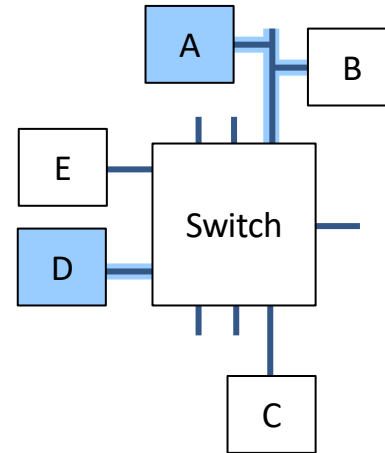
- Angriff über ARP-Spoofing für nicht direkt abhörbare Netzsegmente

Rechner **A** und **D** kommunizieren miteinander

a) im Ethernet



b) im Switched Ethernet



 Ausbreitung der übertragenen Daten

Sniffing-Angriffe: Vorgehen

- 1. Schritt – Beschaffung der Daten
 - Konfiguration der Netzwerkschnittstelle (promiscuous mode)
 - Auslesen sämtlicher Datenpakete
- 2. Schritt – Informationsgewinnung
 - Auswahl der »interessanten« Pakete anhand der Protokoll-Informationen (Sender- bzw. Empfängeradresse, TCP-Port etc.)
- 3. Schritt – Auswertung des Datenteils



```
/usr/bin/login (ttty1)
SourceName=
WARNING: Short packet. Try increasing the snap length

11:46:50.885110 arp who-has 160.45.110.189 tell router-110.inf
11:46:51.099430 titanus.inf.fu-berlin.de.49156 > fubinf.inf.fu
11:46:51.100215 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:51.214719 arp who-has 160.45.110.189 tell router-110.inf
11:46:52.112502 titanus.inf.fu-berlin.de.49156 > fubinf.inf.f
11:46:52.113040 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:52.113293 titanus.inf.fu-berlin.de.49156 > fubinf.inf.f
11:46:52.113706 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:52.885123 arp who-has 160.45.110.189 tell router-110.inf
11:46:57.010498 jefe.inf.fu-berlin.de > dvmp.mcast.net: igmp
11:46:58.363997 arp who-has 160.45.110.189 tell router-110.inf
11:46:59.884553 arp who-has 160.45.110.189 tell router-110.inf
11:47:01.884507 arp who-has 160.45.110.189 tell router-110.inf
11:47:03.734152 silver.inf.fu-berlin.de.2611 > 255.255.255.255
11:47:03.884505 arp who-has 160.45.110.189 tell router-110.inf
11:47:05.884498 arp who-has 160.45.110.189 tell router-110.inf
```

Sniffing-Angriffe: Vorgehen

■ 3. Schritt – Auswertung des Datenteils

- Im Beispiel ASCII-Textdarstellung eines Ethernet-Datenpaketes gewählt (Punkte stehen für Steuerzeichen)

```
....Ih..OyB..OyB...E...S'@.....QP\..G<..C.H.M../(~.P....>.*... ..
..E.....w.R$.6..f%A....4.6.f%A.....
.....U.....MailSaveOptions...O.U.....SECUREMAIL..
U.....tmpReview...U.....Form MemoU.....Type..
MemoU.....DeletionPeriod.....>@U.....HoldPeriod..
.....U.....ReturnReceiptS..OnU.....DeliveryReport
--B=U.....Sign..liU.....DefaultMailSaveOptions..lrU.
D.....ReplyToa..U.....Body.....Hallo,.....
.....,.....das ist ein Test f.r unsere Sneaker.....
.....-.....THE MAGIC WORDS ARE FEEBLE GIBBERISH.....
.....Gru.,.....Matthias
Mueller.....U.....ReminderDate..U.....Dele
tionDate..U.....Encrypts..OtU.....$Folders..U.....
....PreparedToSend..O U.....DeliveryPriority..NMU.....
..$KeepPrivate..U.....Subject ..Testmail fuer SniffingU.E.
..6.....SendTo..CN=Andreas Maier/OU=DuD/OU=Datenschutz/O=TUD@TU-Dresd
enU.E.....CopyTo..U.D.....BlindCopyTo..U.E..../.Fr
om..CN=Matthias Mueller/OU=DuD/OU=Datenschutz/O=TUD.EU.....Po
stedDate..}.6..f%AU.....i.....$Signature.....X6..f%A.....O...
.....6...H.....j8..d%.....&...@.....$.
.a%...$.t.%.....O=TUD.....O=TUD.....BV...l.O.BC...BA..0BL..v.NN
P...w...%m...]i.u....;,.ys}.}.4].yl.). ....c...|ohi<'5L.r..B...
BZ%;m<....L...Q])..EN..D..MA..l...So;|.PURSAFO..d.YK.....<>3.....
.#->k.....|.Jj/..R..|.U...ka..Ofz.....@@
```

Sniffing-Angriffe: Abwehr

schwacher
Angreifer



starker
Angreifer

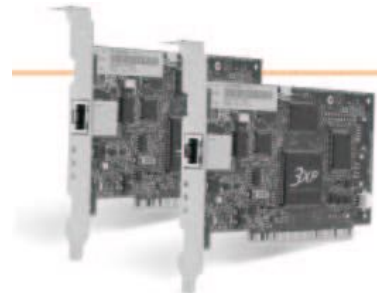
- **Physischer Schutz**
 - auch physischer Schutz des Übertragungsmediums
- **Netzwerkadapter**
 - ohne »promiscuous mode«
 - Signalisierung des Umschaltens in »promiscuous mode«
 - switched networks
- **Schutz gegen einen relativ starken Angreifer**
 - kann Datentransfer über das Medium belauschen
 - Einsatz von Verschlüsselungsverfahren

Sniffing-Angriffe: Abwehr

■ Hardwareverschlüsselung direkt auf Netzwerkkarte

– Historisches Beispiel:

- 3COM 10/100 Secure Network Interface Cards
 - IPSec-Verschlüsselung mit 3DES und DES
 - IPSec-Authentifikation (RFC 2402 Authentication Header) mit SHA-1 und MD5
 - enthält Kryptoprozessor
 - Variante für Client-PCs und Server
 - Speichert bis zu 700 bzw. 1000 Security Associations (Schlüssel der Gegenstelle)
- wird nicht mehr vertrieben



Quelle:
http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3CR990-TX-97

Das Recht auf Vergessen im Internet

■ Allgemeines Ziel

- Verbotenes und Unerwünschtes im Internet soll

nicht möglich

nicht mehr vorhanden

wenigstens nicht mehr erreichbar

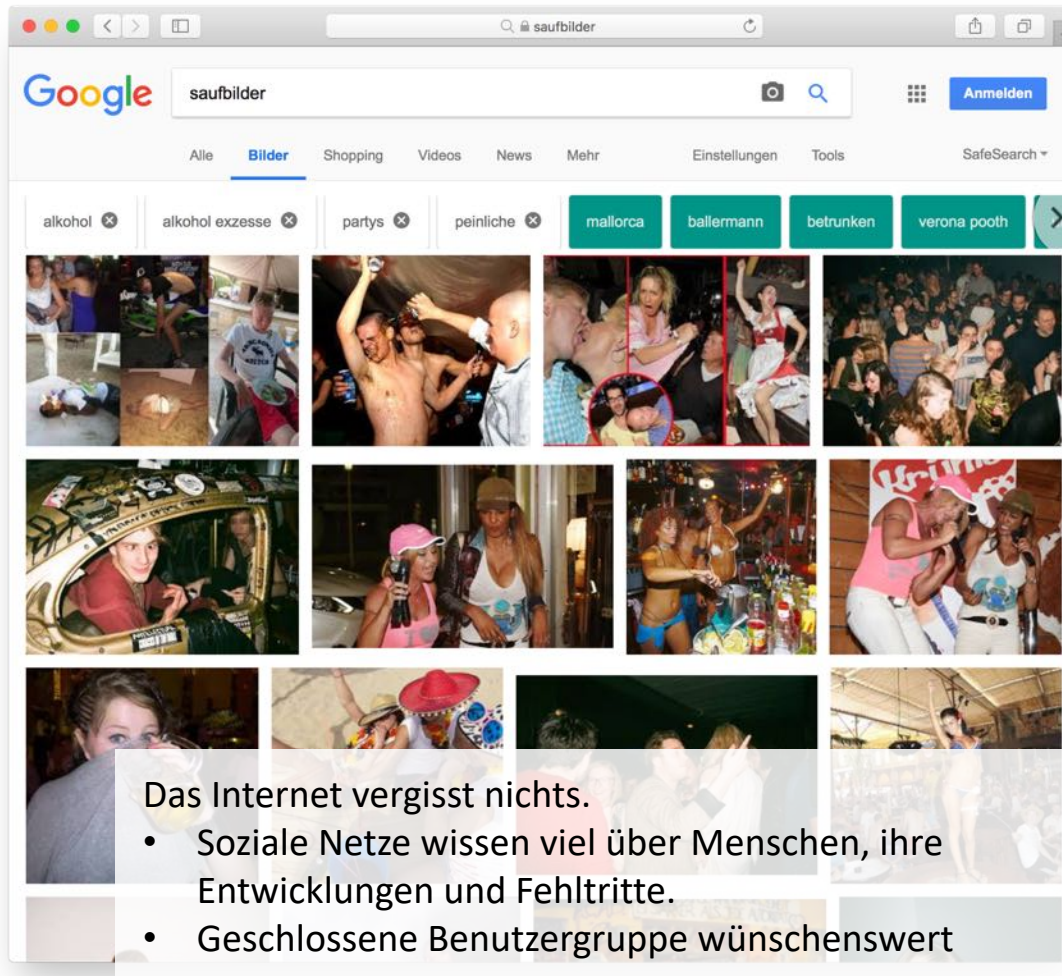
(Untaugliche) Lösungsansätze

[Juristisch: Verbote]

Technisch: x-pire!

Technisch: DNS-Sperre

- sein.



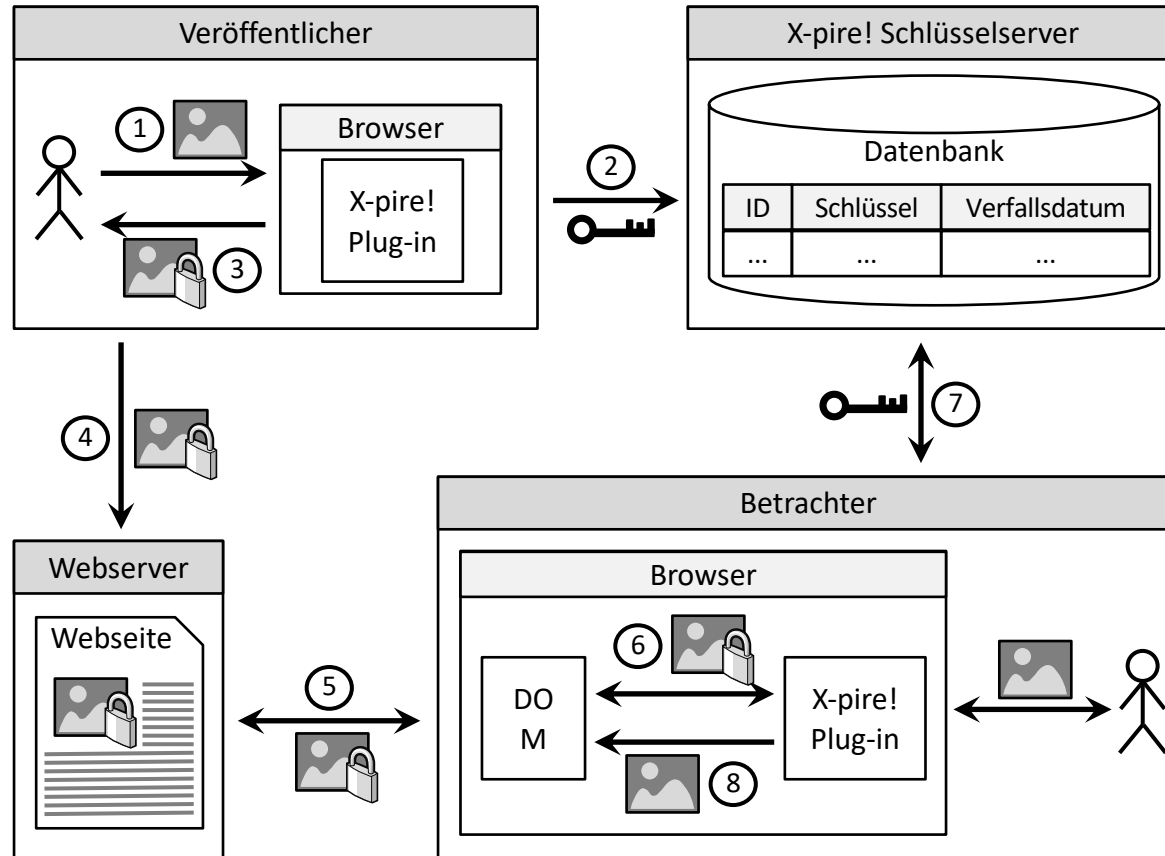
Das Internet vergisst nichts.

- Soziale Netze wissen viel über Menschen, ihre Entwicklungen und Fehlritte.
- Geschlossene Benutzergruppe wünschenswert

X-pire!



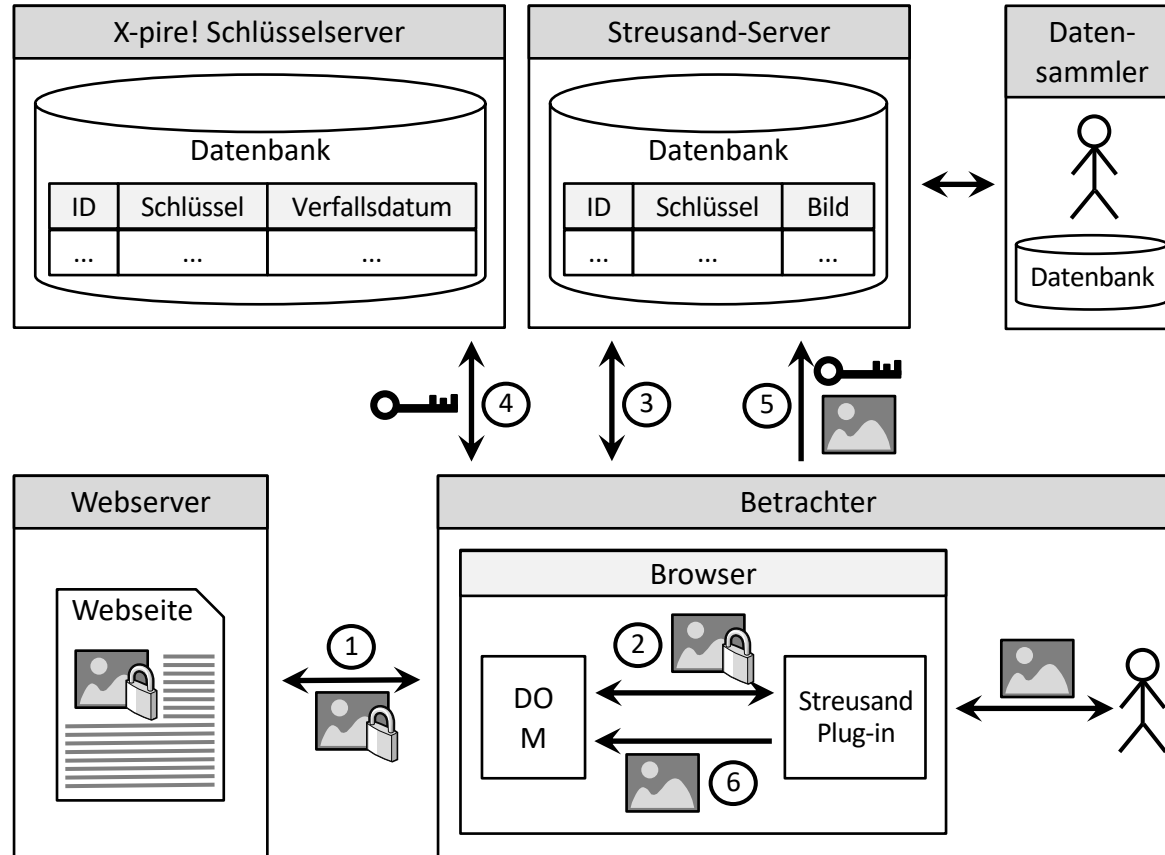
Funktionsweise X-pire!



Sicherheitsaspekte

- Zentraler Schlüsselservers
 - Verfügbarkeit: single-point-of-failure
 - Vertraulichkeit: Datenbank-Betreiber kennt alle Schlüssel
 - Erweiterungen denkbar:
 - Verteilte Datenbanken
 - Verwendung von Secret-Sharing-Verfahren und Anonymitätstechniken
- Kein Schutz gegen Angreifer in der Rolle »Betrachter«
 - Software im Verfügungsbereich des Betrachters (Browser) erhält Zugriff auf Schlüssel und unverschlüsselten Inhalt
 - Weder Verschlüsselung noch CAPTACHs helfen hier!
- Streisand-Effekt
 - Insbesondere Inhalte, die wieder aus dem Netz verschwinden sollen, halten sich möglicherweise besonders lange.

Funktionsweise Streusand-Erweiterung



Streusand-Erweiterung

- Nutzung von X-pire! kann sogar schädlich sein
 - Streusand-Galerie: längst verschwundene Bilder archiviert

01.02.2011 08:25:36	4d4d75d742863ab9656f3d5f76dfff858	a7385c51a13dd53030ee2f18c7fcb689ad4094b06ffb90c601c3abac722f1f5c	
31.01.2011 20:24:00	ab897fbdedfa502b2d839b6a56100887	eee65472de6234f647cf5c25d959e2f116707f76bcb7a5a5de2ad1a99e1d4628	
31.01.2011 20:23:12	ab897fbdedfa502b2d839b6a56100887	17150bb7b618f8e11358b5d8b7d6be438394213eb2a5e582703d8ee733c198e1	
31.01.2011 20:21:08	ab897fbdedfa502b2d839b6a56100887	2b4c6711793140ea5fa88c27f61354034f69dbdbaaac82f6c88490fcd019bd09	
27.01.2011 18:29:03	e6f207509afa3908da116ce61a757695	fb1c038c912c46c41181c8cb32b39e396abacdb0abf1d0683b6ca3d12ee386ba	

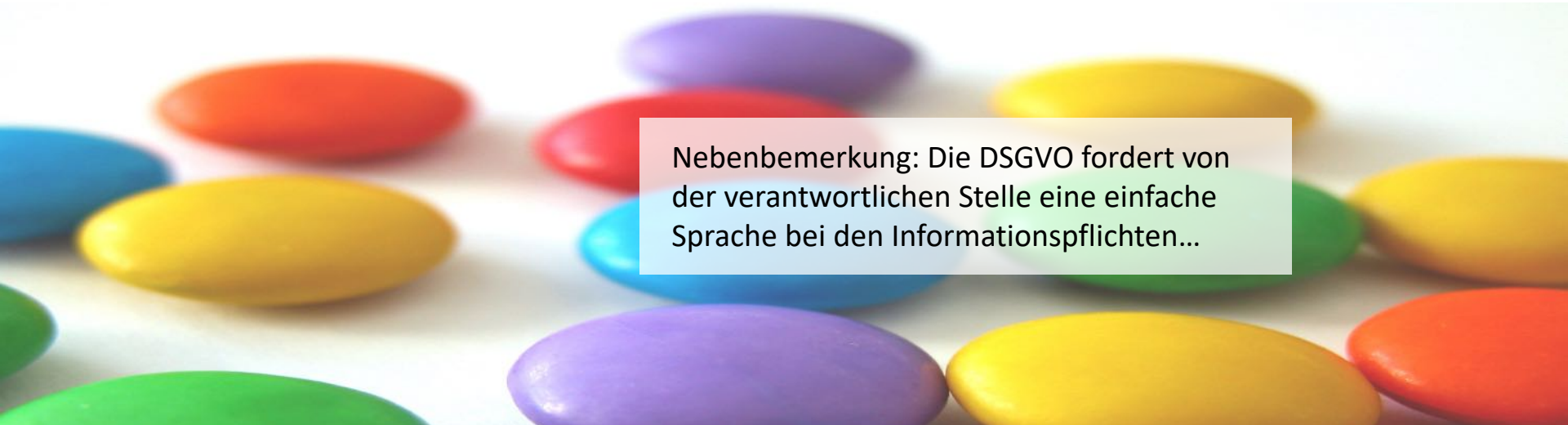
- Softwarelösungen zur Durchsetzung des Rechts auf Vergessen sind untauglich.

Auszug aus Artikel 17 DSGVO

Art. 17 DSGVO Recht auf Löschung (»Recht auf Vergessenwerden«)

(1) ...

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.



Nebenbemerkung: Die DSGVO fordert von der verantwortlichen Stelle eine einfache Sprache bei den Informationspflichten...

support.google.com

Anträge auf Entfernung von Inhalten - Hilfe für Rechtliche Hinweise

Entfernen von Inhalten aus Google - Hilfe für Rechtliche Hinweise

Google


Anmelden

Hilfe für Rechtliche Hinweise

RECHTLICHE HINWEISE

Anträge auf Entfernung von Inhalten

When users ask us to remove content

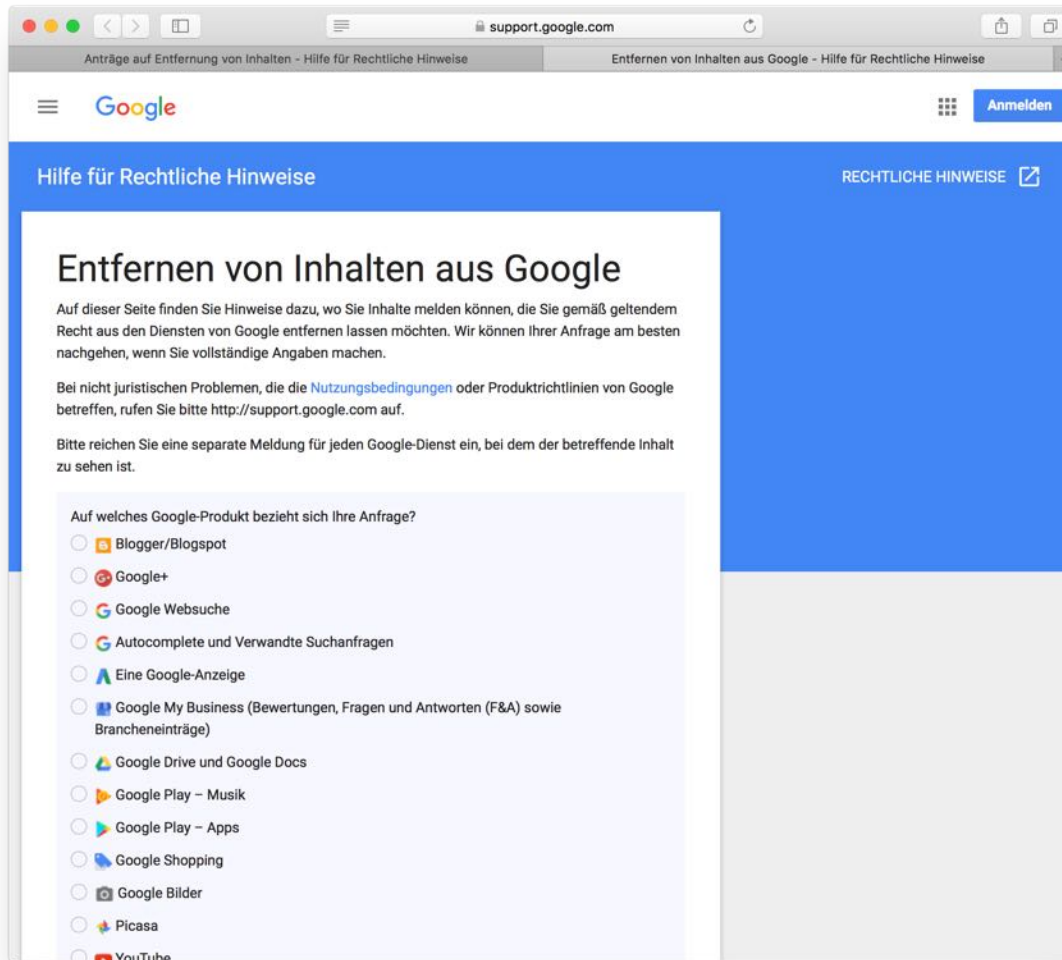


Falls Sie auf Google Inhalte finden, die mutmaßlich rechtswidrig sind, informieren Sie uns. Wir werden das Material dann sorgfältig prüfen und gegebenenfalls den Zugriff darauf sperren oder beschränken bzw. das Material entfernen. Missbräuchliche Inhalte in den Google-Diensten verstoßen möglicherweise auch gegen die [Produktrichtlinien von Google](#). In diesem Fall können Sie die betreffenden Inhalte melden, bevor Sie einen Antrag auf Entfernung der Inhalte einreichen. Die Inhalte werden dann von unseren Teams geprüft. Im Folgenden finden Sie weitere Informationen zu unseren Produktrichtlinien und Datenschutzerklärungen sowie unserem Bekenntnis zu Transparenz. Zudem können Sie hier nachlesen, wie Sie eine gültige rechtliche Mitteilung bei Google einreichen.

[Problemspezifische Unterstützung finden](#)

Informationen zur Entfernung von Inhalten

- [Fehlerbehebung bei Datenschutzproblemen](#)
- [Hilfe zum Urheberrecht](#)
- [Häufig gestellte Fragen](#)



support.google.com

Anträge auf Entfernung von Inhalten - Hilfe für Rechtliche HinweiseEntfernen von Inhalten aus Google - Hilfe für Rechtliche Hinweise

Google

Anmelden

Hilfe für Rechtliche HinweiseRECHTLICHE HINWEISE

Entfernen von Inhalten aus Google

Auf dieser Seite finden Sie Hinweise dazu, wo Sie Inhalte melden können, die Sie gemäß geltendem Recht aus den Diensten von Google entfernen lassen möchten. Wir können Ihrer Anfrage am besten nachgehen, wenn Sie vollständige Angaben machen.

Bei nicht juristischen Problemen, die die [Nutzungsbedingungen](#) oder Produktrichtlinien von Google betreffen, rufen Sie bitte <http://support.google.com> auf.

Bitte reichen Sie eine separate Meldung für jeden Google-Dienst ein, bei dem der betreffende Inhalt zu sehen ist.

Auf welches Google-Produkt bezieht sich Ihre Anfrage?

Google Websuche

Wobei können wir Ihnen helfen?

Ich möchte, dass meine personenbezogenen Daten aus den Google-Suchergebnissen entfernt werden.

Beachten Sie, dass in unseren Suchergebnissen möglicherweise ein Hinweis angezeigt wird, dass einige Ergebnisse entfernt wurden.

Treffen Sie eine Auswahl aus folgenden Optionen.

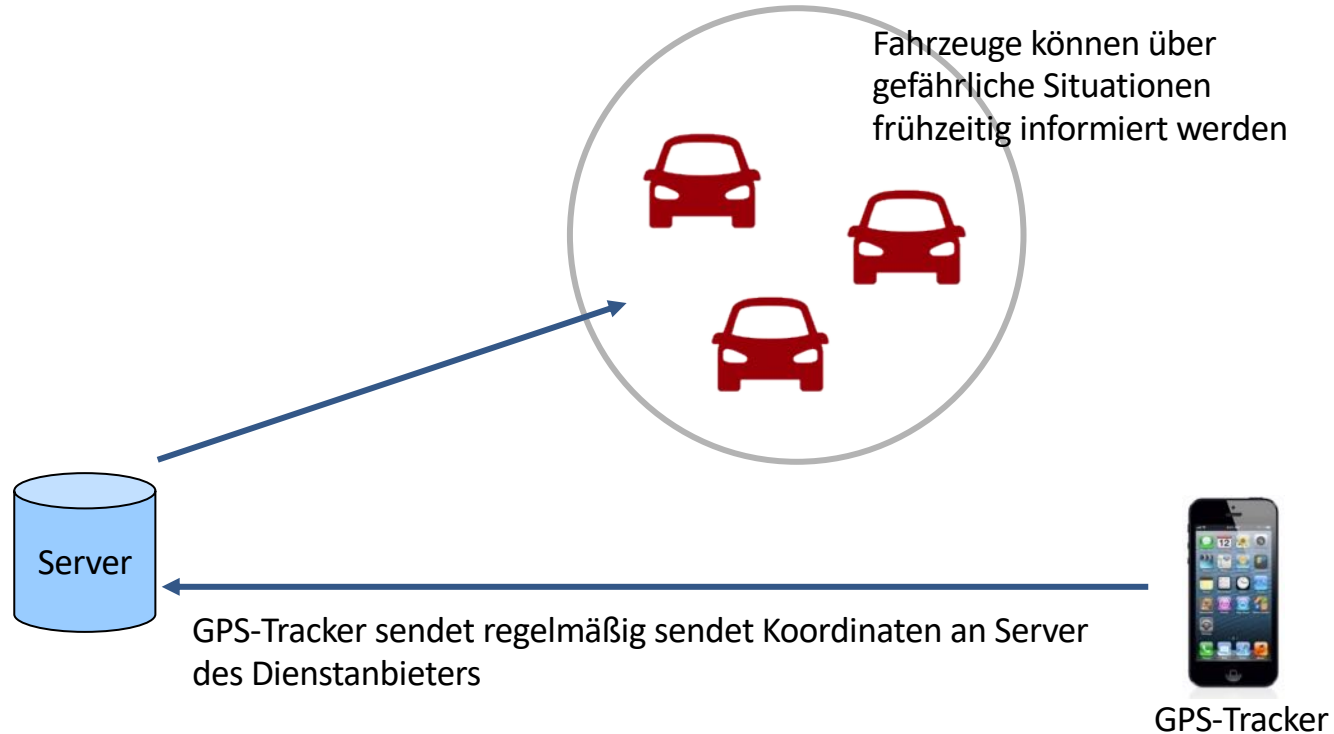
☐ Ich möchte gemäß den europäischen Datenschutzgesetzen bezüglich des "Rechts auf Vergessen" einen Antrag auf Entfernung von Informationen einreichen.

☐ Ich möchte, dass meine vertraulichen personenbezogenen Daten aus den Google-Suchergebnissen entfernt werden (z. B. Sozialversicherungs- oder Ausweisnummer, Konto- oder Kreditkartennummer oder ein Bild meiner handschriftlichen Unterschrift, ein Nacktbild oder -video bzw. sexuell explizite Bilder oder Videos von mir, die ohne mein Einverständnis veröffentlicht wurden).

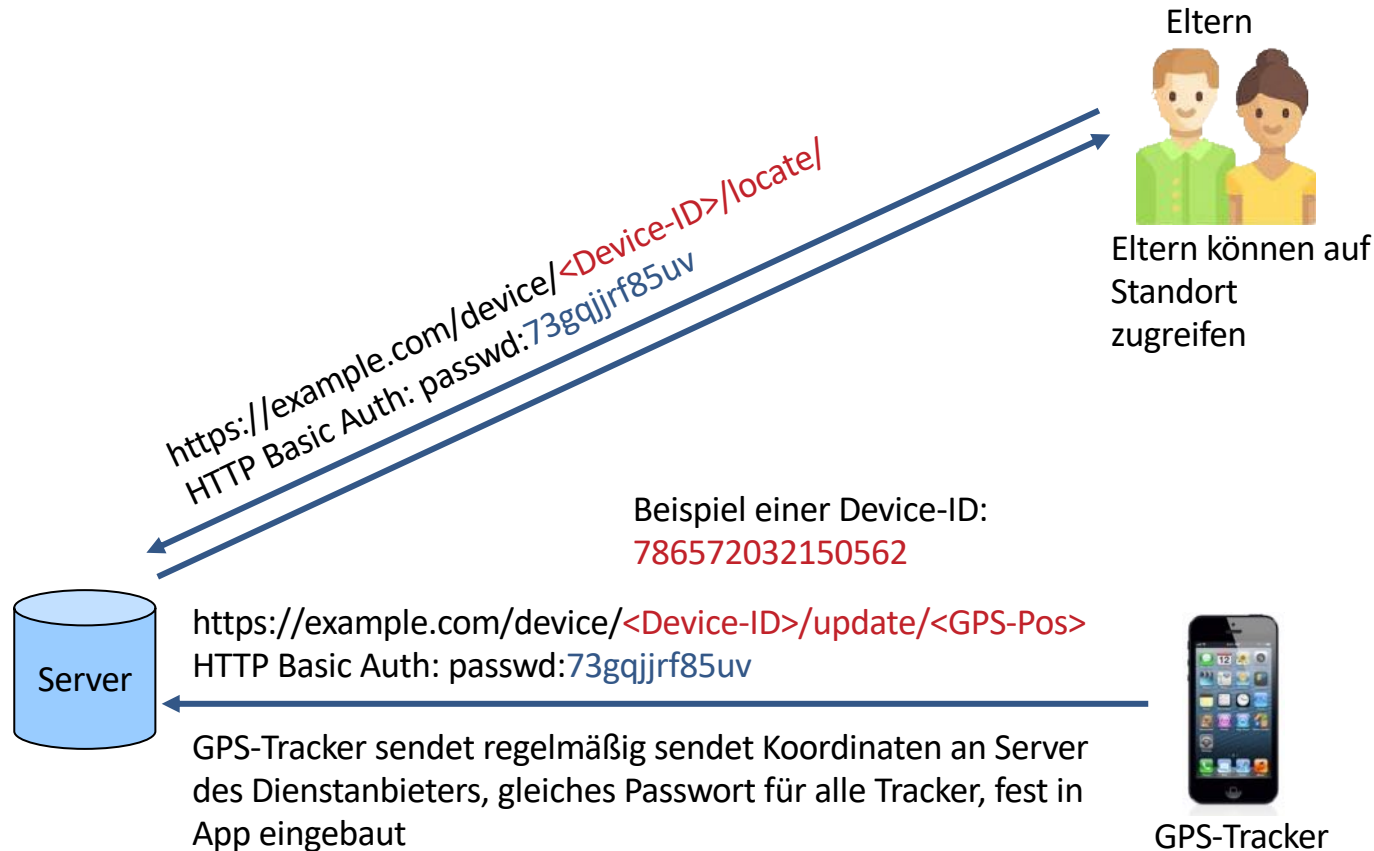
☐ Ich möchte den Webmaster einer in den Suchergebnissen enthaltenen Seite, die falsche oder ungenaue Informationen enthält, auffordern, diese vollständig aus den Google-Suchergebnissen zu entfernen.

Unzureichende Implementierung von Schutzmaßnahmen
kann Vertrauen in IT gefährden

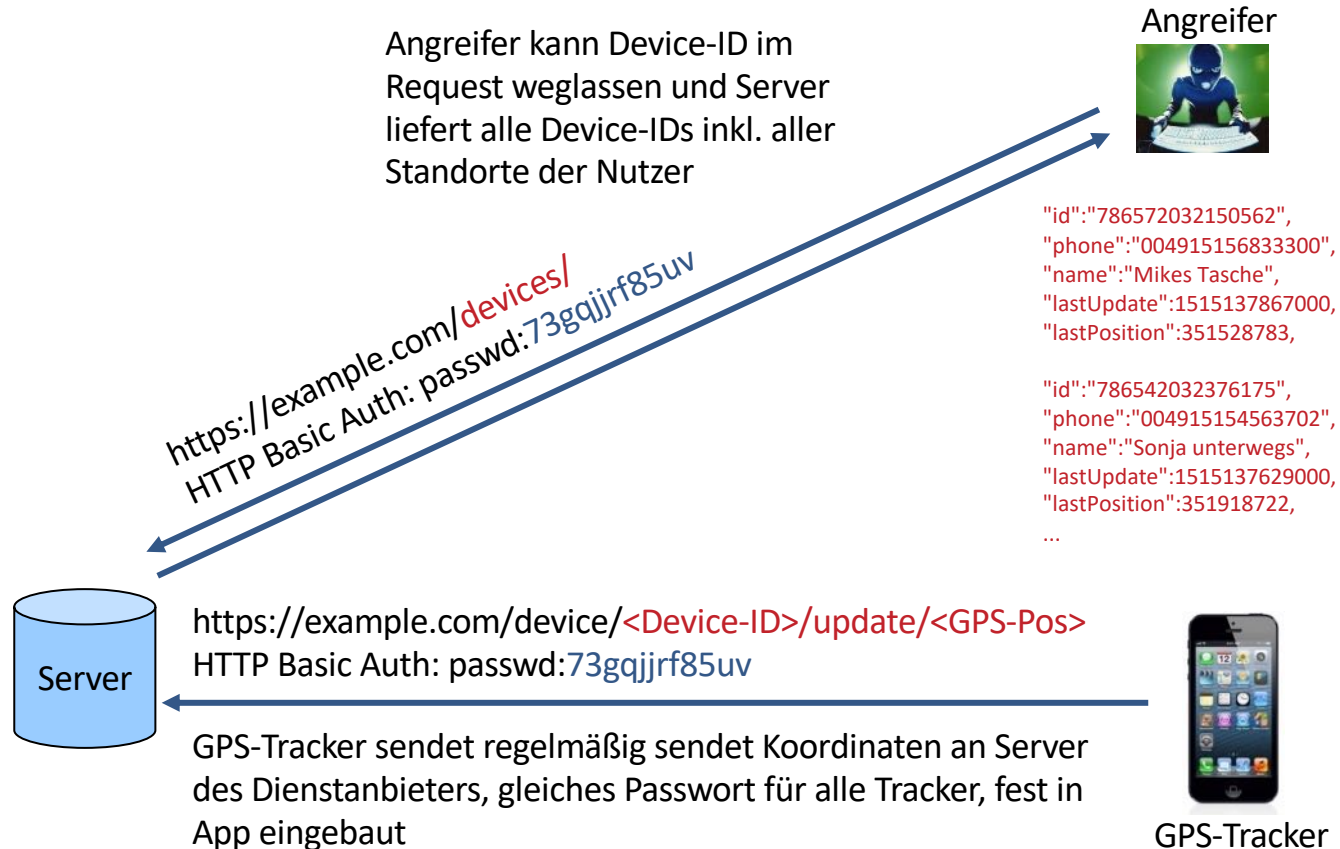
Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT



Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT



Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT



Spoofing

Integrität: Spoofing

■ Was ist Spoofing?

- Vortäuschen falscher Information
- Angriffe gegen die Integrität
- auch mit dem Ziel, schließlich die Vertraulichkeit zu verletzen

■ Arten von Spoofing

- Mail-Spoofing
- IP-Spoofing

- DNS-Spoofing
- ARP-Spoofing

- SSID-Spoofing

• Szenario 1:

- ISP greift an
- DNS-Sperre als Beispiel

• Szenario 2:

- Angriff im LAN
- ARP- und DNS-Spoofing mit Tool Cain&Abel

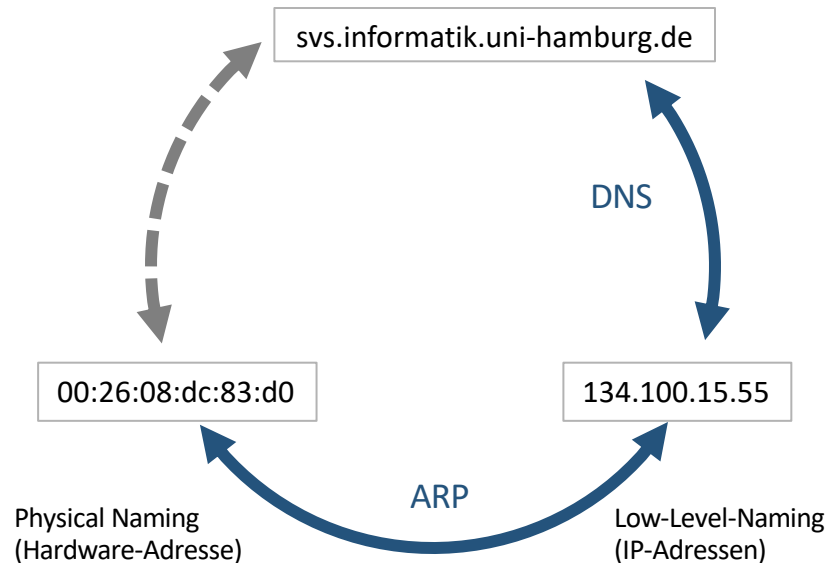
Einordnung ARP, IP, DNS

■ DNS: Domain Name System

- Abbildung des Rechnernamens auf IP-Adresse
- Anfrage an Nameserver
- typischerweise in WANs

■ ARP: Address Resolution Protocol

- Abbildung von IP-Adresse auf Hardwareadresse
- Anfrage an das lokale Netz (Broadcast)
- nur in lokalen Netzen



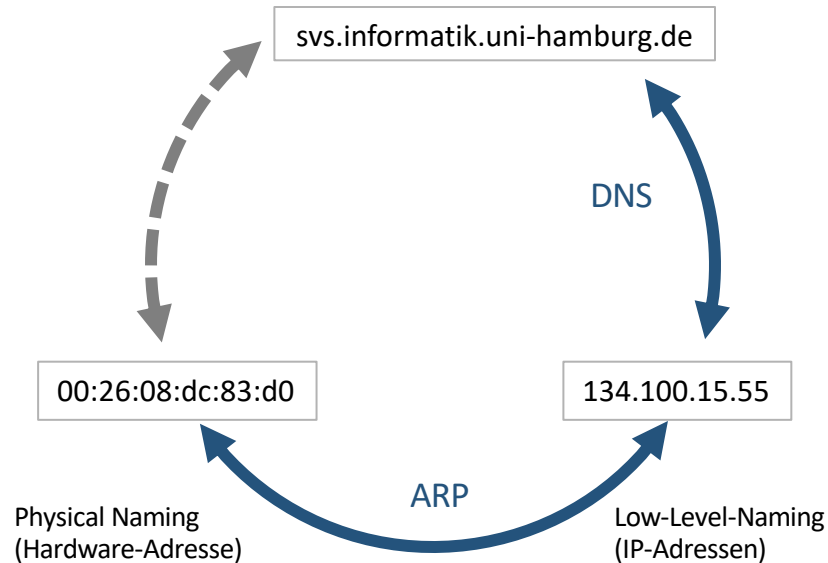
Sicherheit im Domain Name System (DNS)

■ DNS: Domain Name System

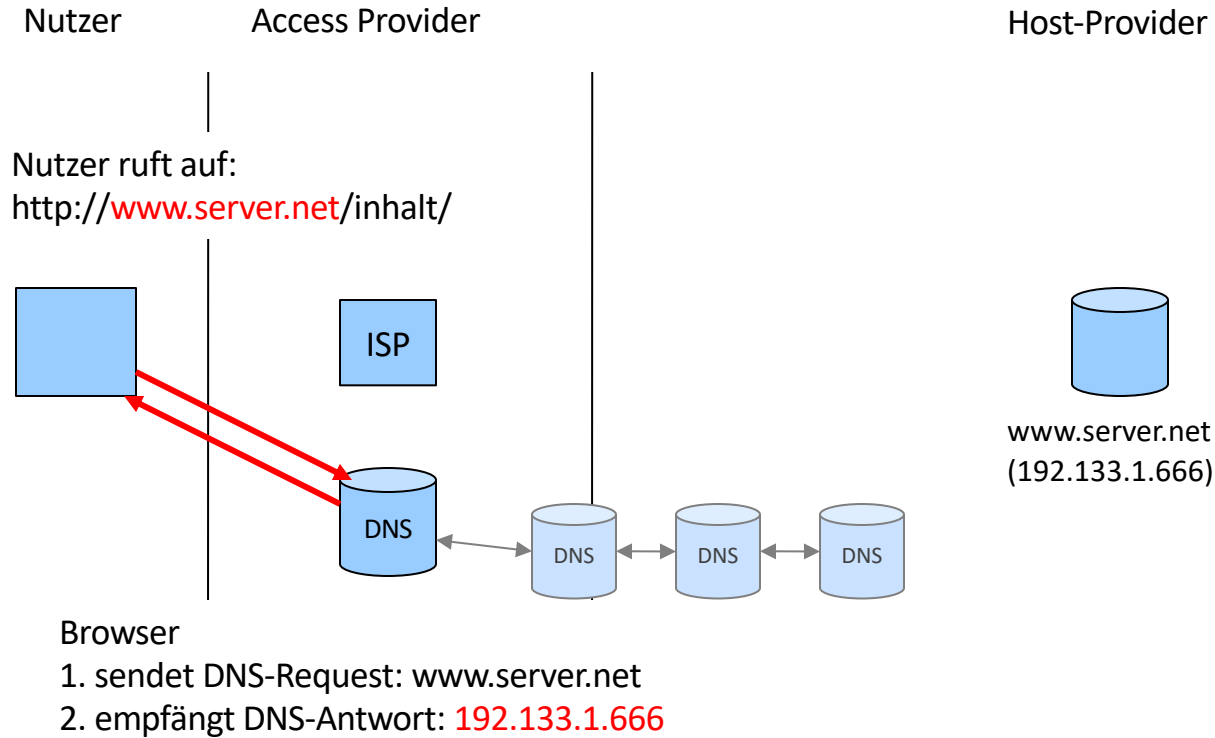
- Abbildung des Rechnernamens auf IP-Adresse
- Anfrage an Nameserver
- typischerweise in WANs

■ Angriffe auf DNS

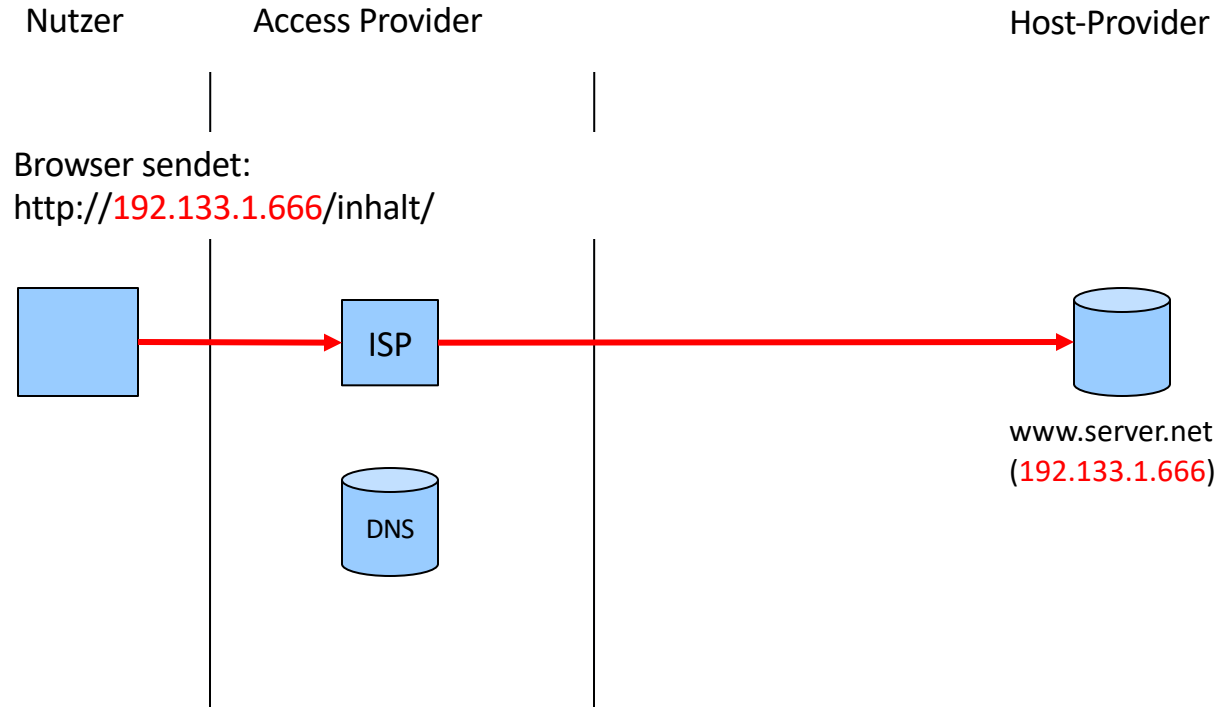
- Sniffing von DNS-Anfragen
- Fälschen der DNS-Antworten
- Denial-of-Service



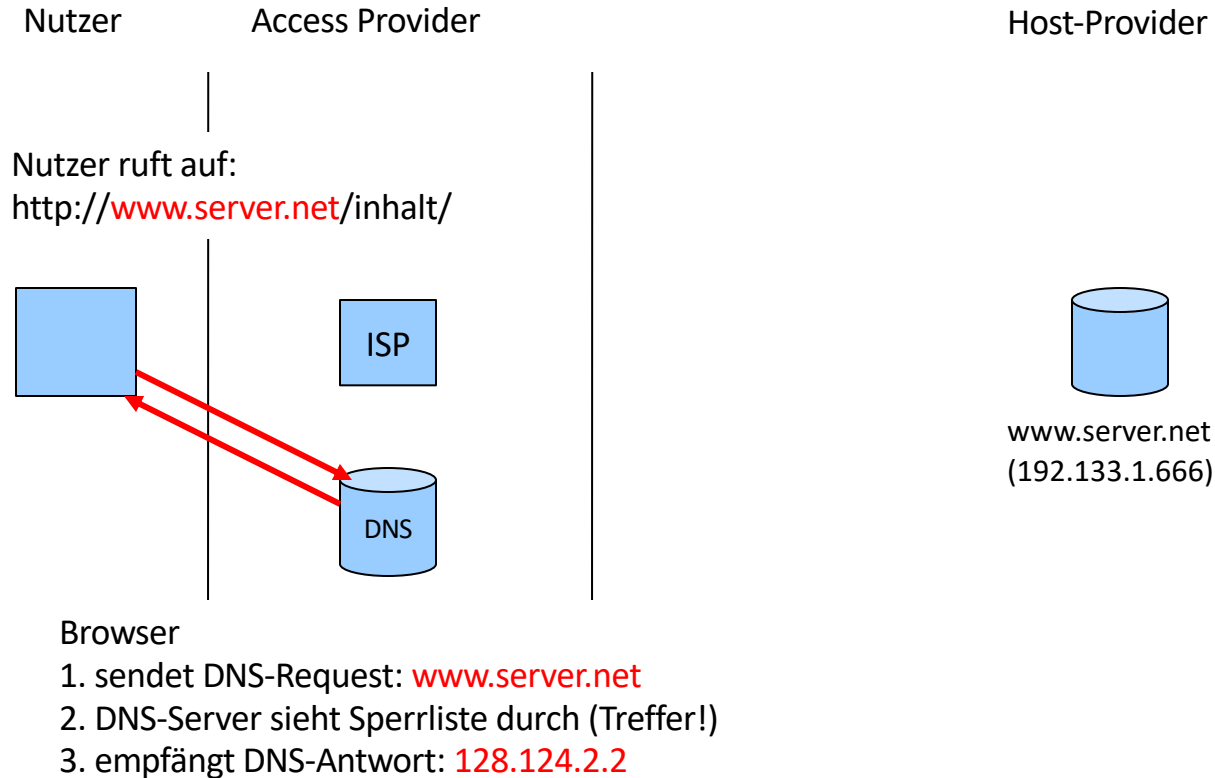
Zunächst wird DNS-Server angefragt



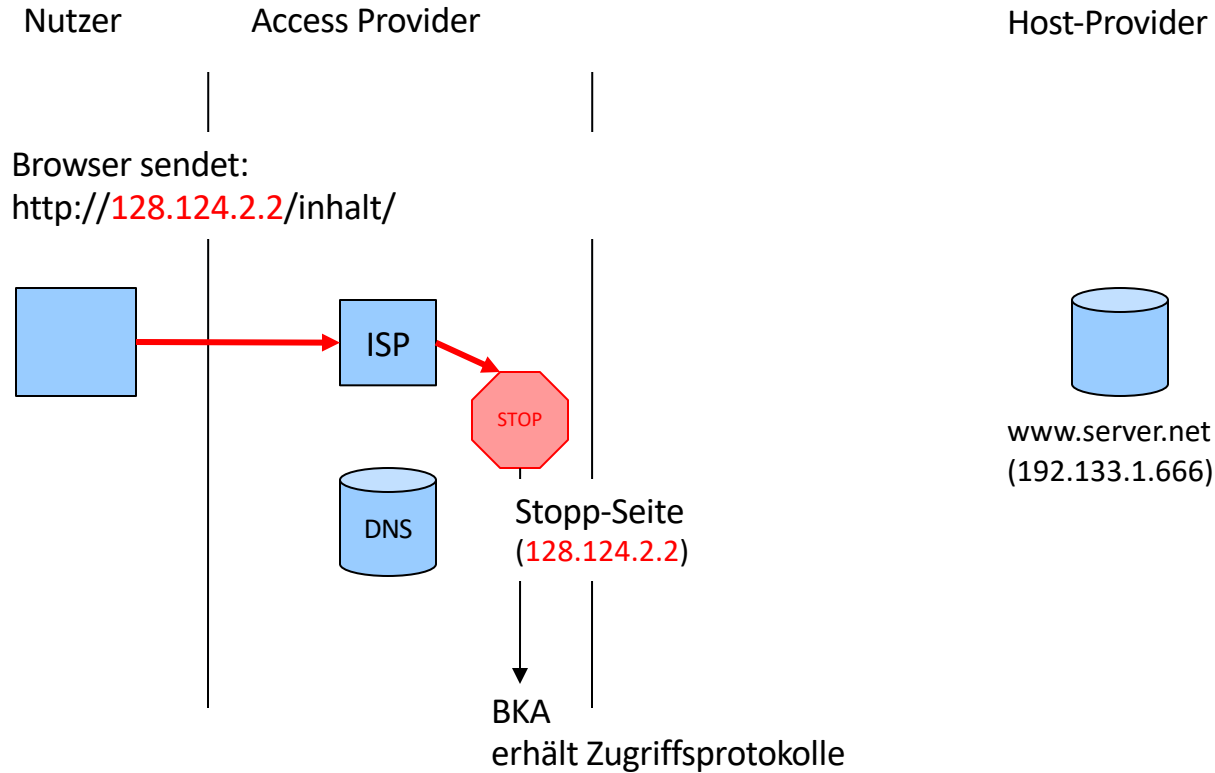
Anschließend wird Inhalt abgerufen



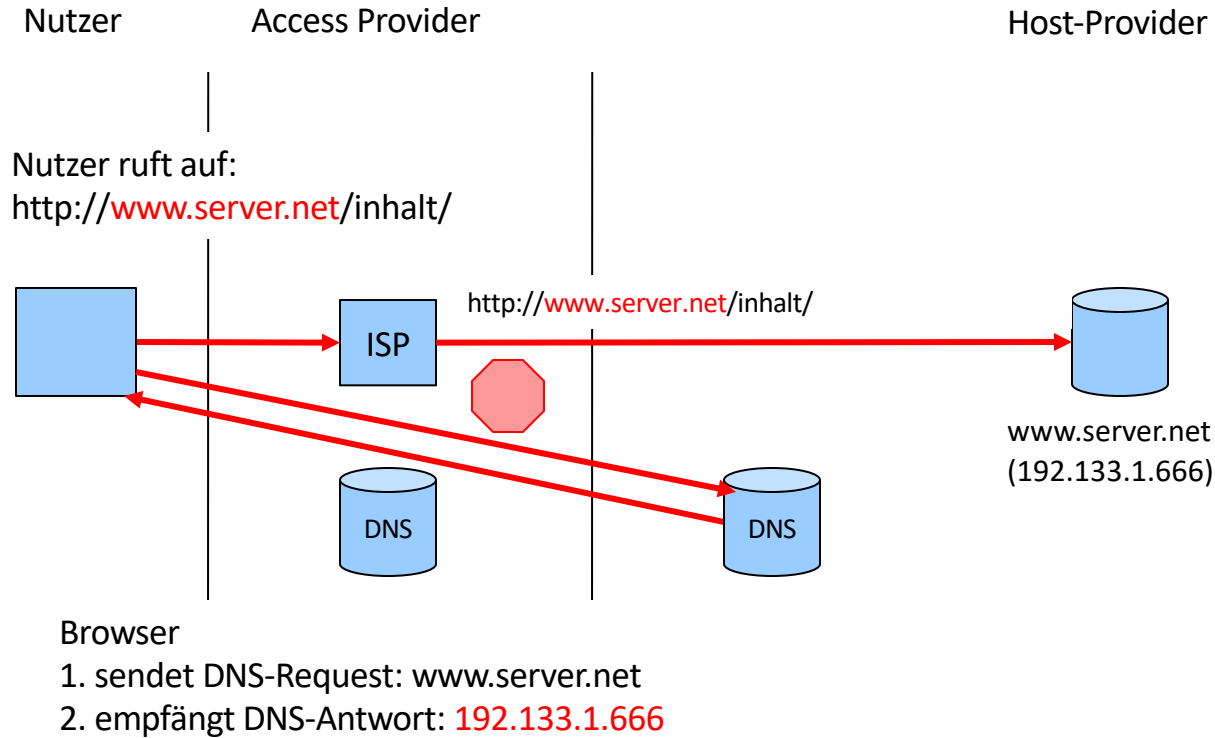
DNS-Sperre: DNS-Server sendet »falsche« Antwort



Mit DNS-Sperre landet der Nutzer im WWW auf Stopp-Seite



Mit DNS-Sperre und Open DNS



Open DNS

The screenshot shows the OpenDNS website in a web browser. The browser's address bar displays <https://www.opendns.com/start/>. The website has an orange header with the OpenDNS logo and navigation links: HOME, SOLUTIONS, USE OPENDNS, CUSTOMERS, SUPPORT, ABOUT US, and BLOG. Below the header, the main heading is "Use OpenDNS (Step 1 of 3: Change DNS settings)". A subheading reads "It only takes 2 minutes. Change DNS on your:". Three options are presented: "Computer" (with a laptop icon), "Router" (with a router icon and a green badge saying "Best for home users"), and "DNS Server" (with a server rack icon). Each option has a brief instruction. To the right, a vertical flowchart shows three steps: 1. Change your DNS settings, 2. Create a free OpenDNS account (optional), and 3. Manage settings in your Dashboard (optional). Below the flowchart, there is a "Video Tutorial" section and a "Find out how OpenDNS complements your existing network setup" section. The footer contains four columns of links: Solutions, Use OpenDNS, Support, and About Us, along with the OpenDNS logo and contact information.

OpenDNS > Use OpenDNS

<https://www.opendns.com/start/> Q open dns


OpenDNS.com Dashboard Community Sign In or Create account Your IP: 92.116.160.129

OpenDNS

HOME SOLUTIONS USE OPENDNS CUSTOMERS SUPPORT ABOUT US BLOG

Use OpenDNS (Step 1 of 3: Change DNS settings)


It only takes 2 minutes. Change DNS on your:



Computer

Get instructions for Windows, Mac, mobile phones, and more.


OR



Router

Enable OpenDNS on your router so every computer benefits.

OR



DNS Server

Learn how to use OpenDNS with your existing DNS servers.

- 1 Change your DNS settings
- 2 Create a free OpenDNS account (optional)
- 3 Manage settings in your Dashboard (optional)

Video Tutorial

Take a few minutes to watch our step-by-step [video](#) on getting started with OpenDNS.

Find out how OpenDNS complements your existing network setup

Read our IT Administrator [Best Practices](#).

The straight dope

Our nameservers are **208.67.222.222** and **208.67.220.220**.

Solutions

- [For Home Network](#)
- [For K-12 School](#)
- [For Small/Medium Business](#)
- [For Enterprise](#)

Use OpenDNS

- [On your computer](#)
- [On your router](#)
- [On your DNS server](#)
- [Best Practices](#)
- [Create a free account](#)

Support

- [Knowledge Base](#)
- [Forums](#)
- [System Status](#)
- [CacheCheck](#)
- [Contact](#)

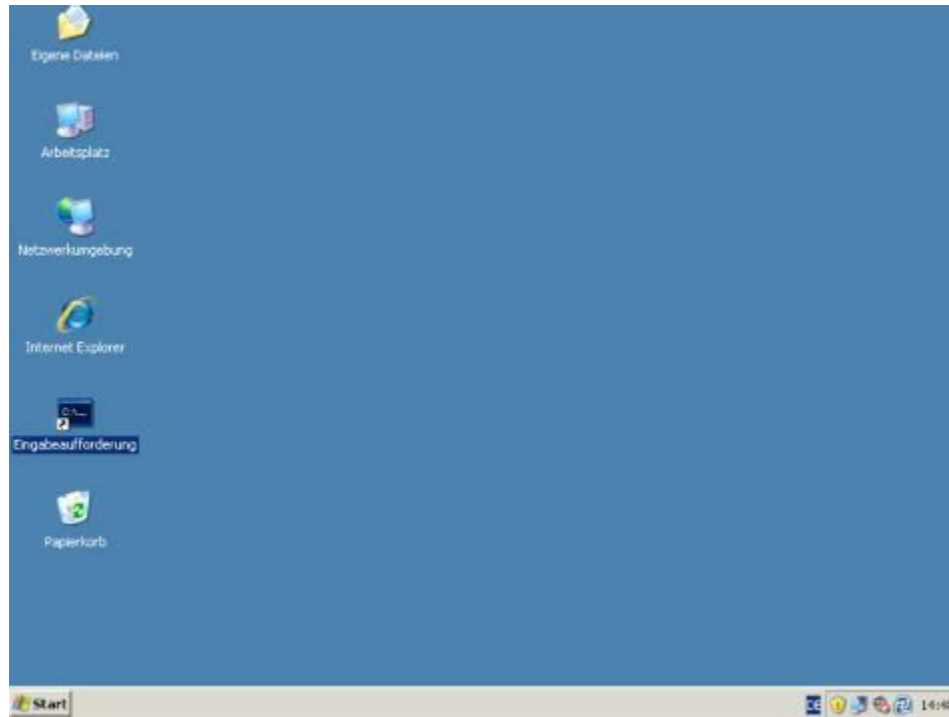
About Us

- [Overview](#)
- [Management](#)
- [Press Center](#)
- [Awards](#)
- [Careers](#)

OpenDNS

208.67.222.222
208.67.220.220

DNS-Sperre und Windows (27 Sekunden)



Quelle: <http://www.youtube.com/watch?v=1NNG5I6DBm0>

Spoofing-Angriffe: Funktionsweise (Switched Ethernet)

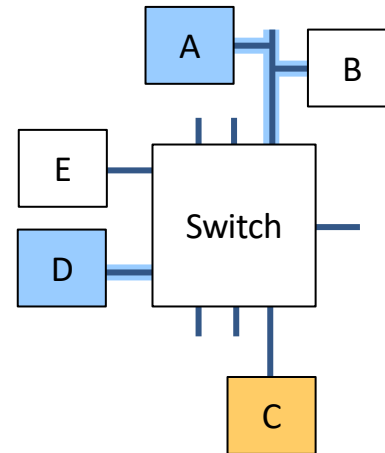
Rechner **A** und **D** kommunizieren miteinander

Switch verteilt Daten nur auf
Netzabschnitt des Empfängers

b) Switched Ethernet: Sniffing beschränkt
sich auf die Netzsegmente, in denen der
Angreifer verbreitet ist

- Angriff über ARP-Spoofing für nicht
direkt abhörbare Netzsegmente

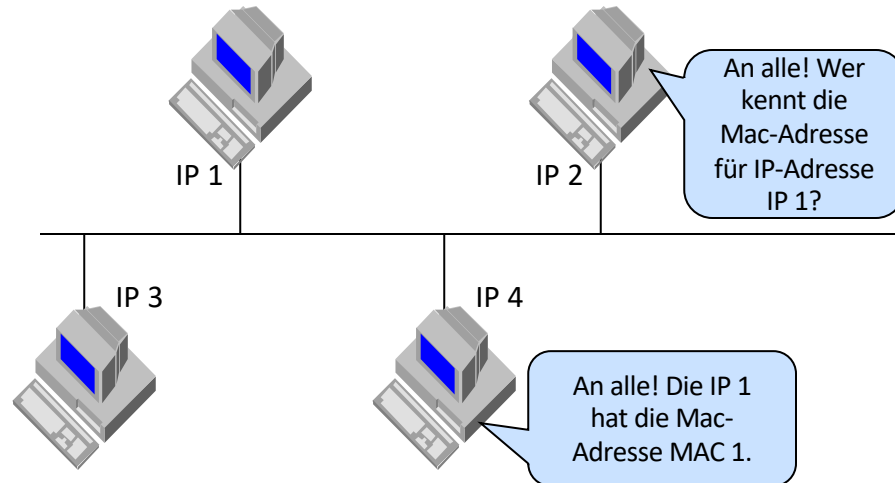
b) im Switched Ethernet



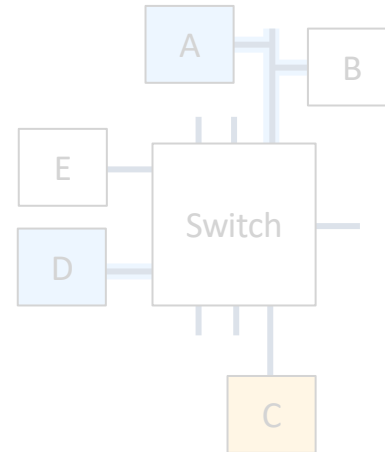
 Ausbreitung der übertragenen Daten

ARP: Address Resolution Protocol

- **ARP-Anfrage**
 - Anfrage wird an das gesamte lokale Netz gestellt (Broadcast)
 - Mitteilen der eigenen Adresse(n) in der Anfrage
- **ARP-Antwort**
 - Jeder Rechner kann antworten

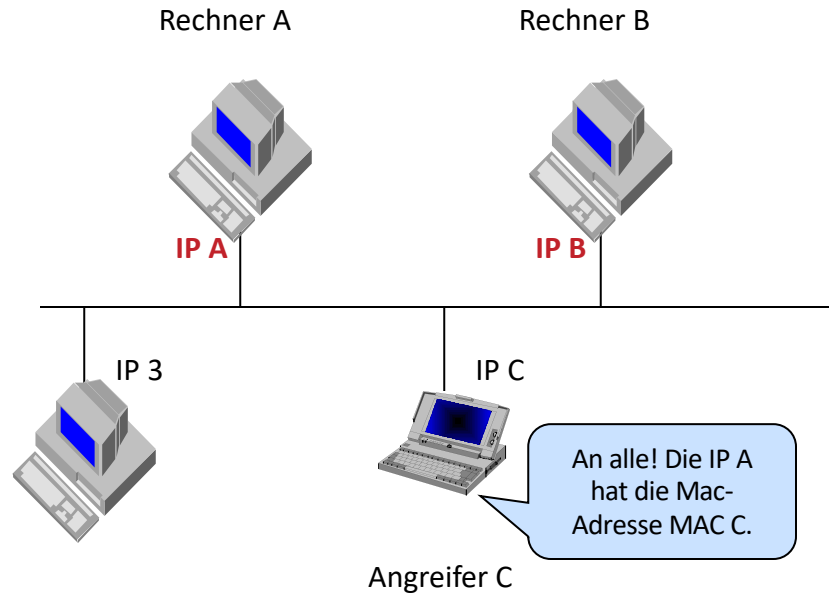


b) im Switched Ethernet

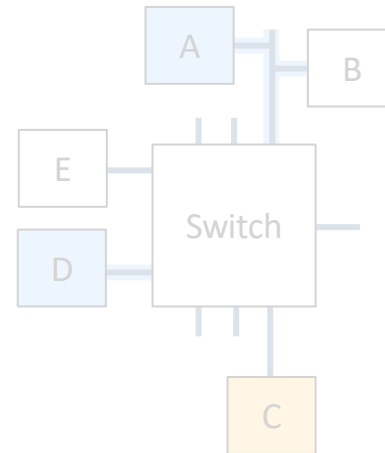


ARP Spoofing

- Angreifer C sendet gefälschte ARP-Response

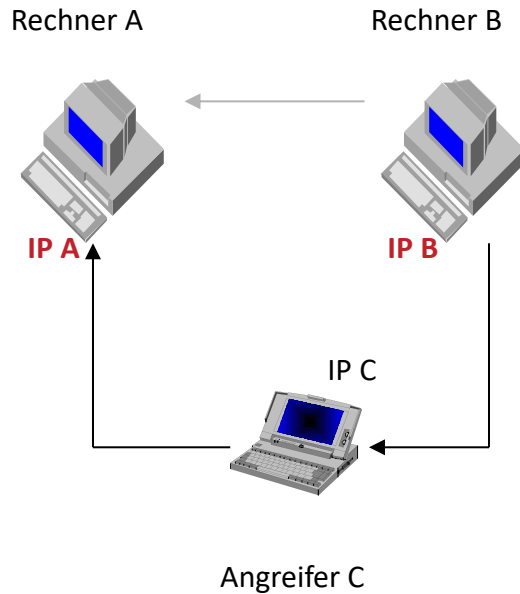


b) im Switched Ethernet

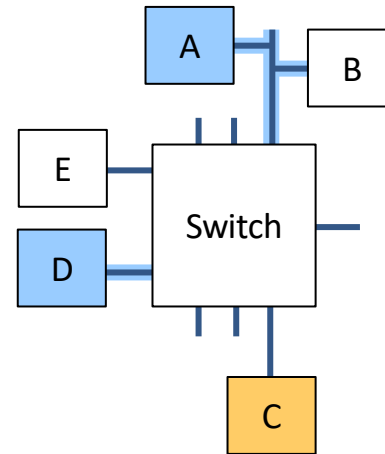


ARP Spoofing

- B adressiert an IP A
- Ethernetkarte von Rechner B schickt die Daten jedoch an MAC C

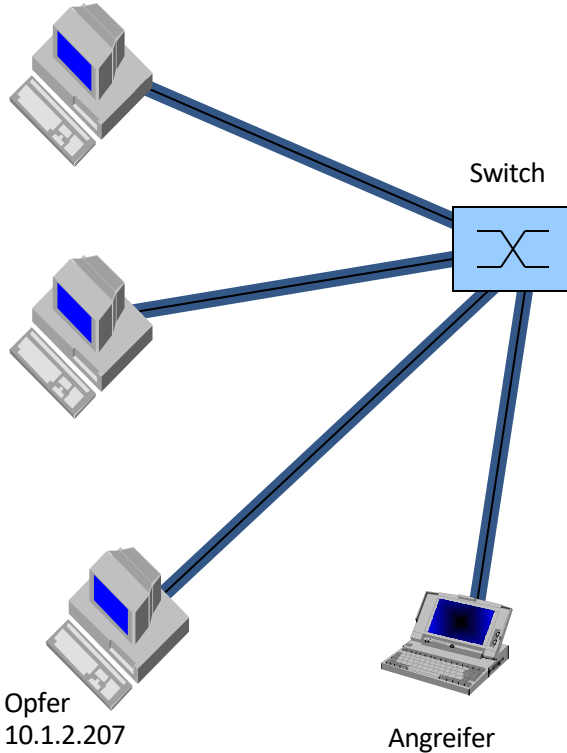


b) im Switched Ethernet



ARP-Spoofing-Demonstration: Vorbereitung

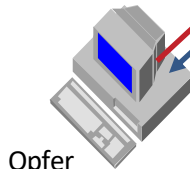
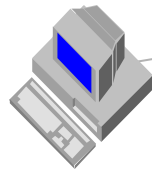
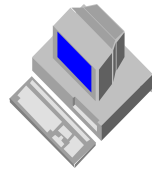
Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



- Angreifer gibt sich gegenüber dem
 - Opfer als Standardgateway aus
 - Standardgateway als Opfer aus

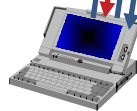
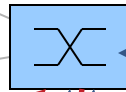
ARP-Spoofing-Demonstration: Opfer sendet IP-Paket ins Internet

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



Opfer
10.1.2.207

Switch



Angreifer



Standardgateway
10.1.1.254

Internet

- Angreifer gibt sich gegenüber dem
 - Opfer als Standardgateway aus
 - Standardgateway als Opfer aus

ARP-Spoofing

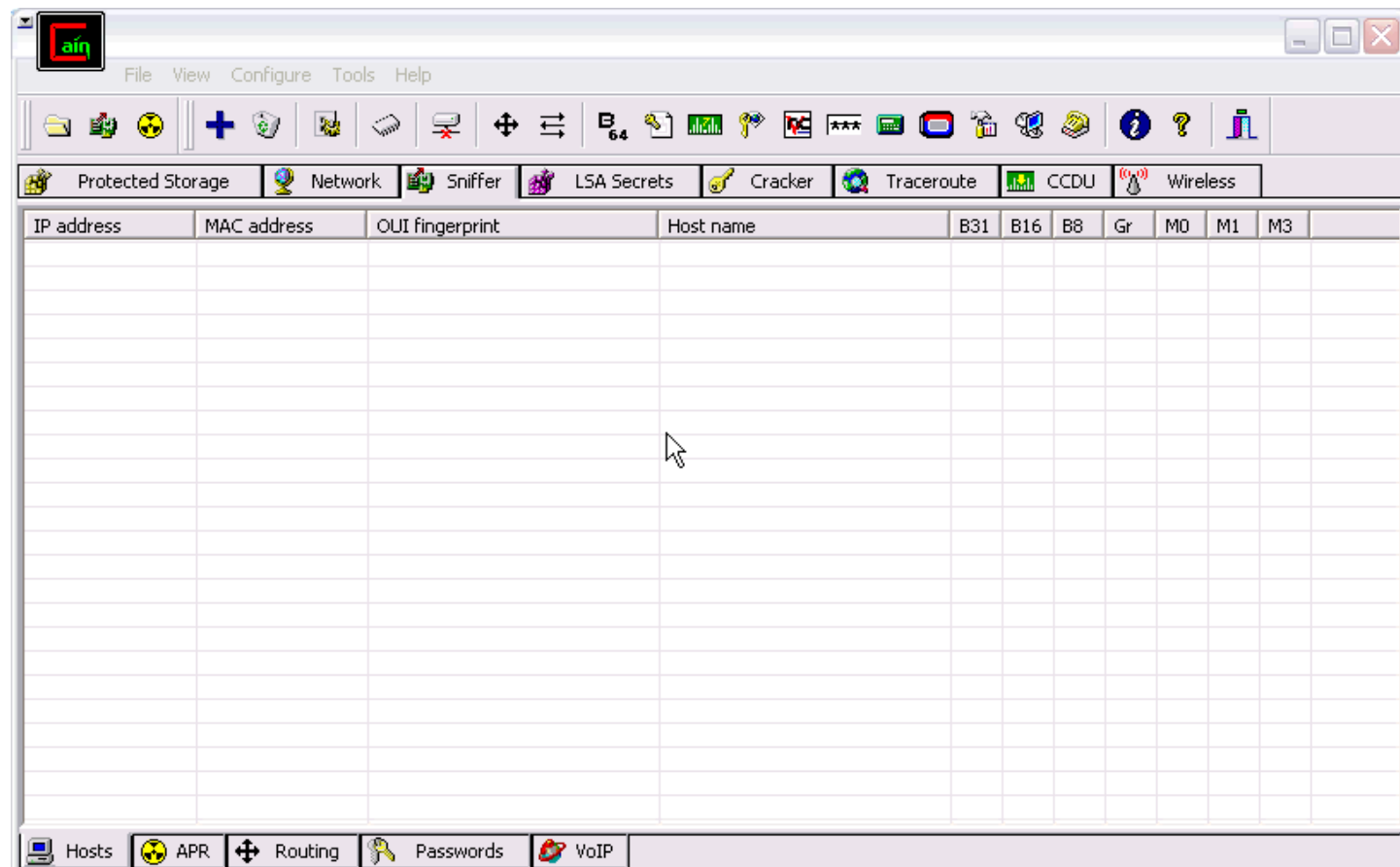
■ Angreifer

- empfängt den gesamten Netzwerkverkehr
 - vom Opfer zum Internet
 - vom Internet zum Opfer
- kann diese Datenpakete beliebig manipulieren

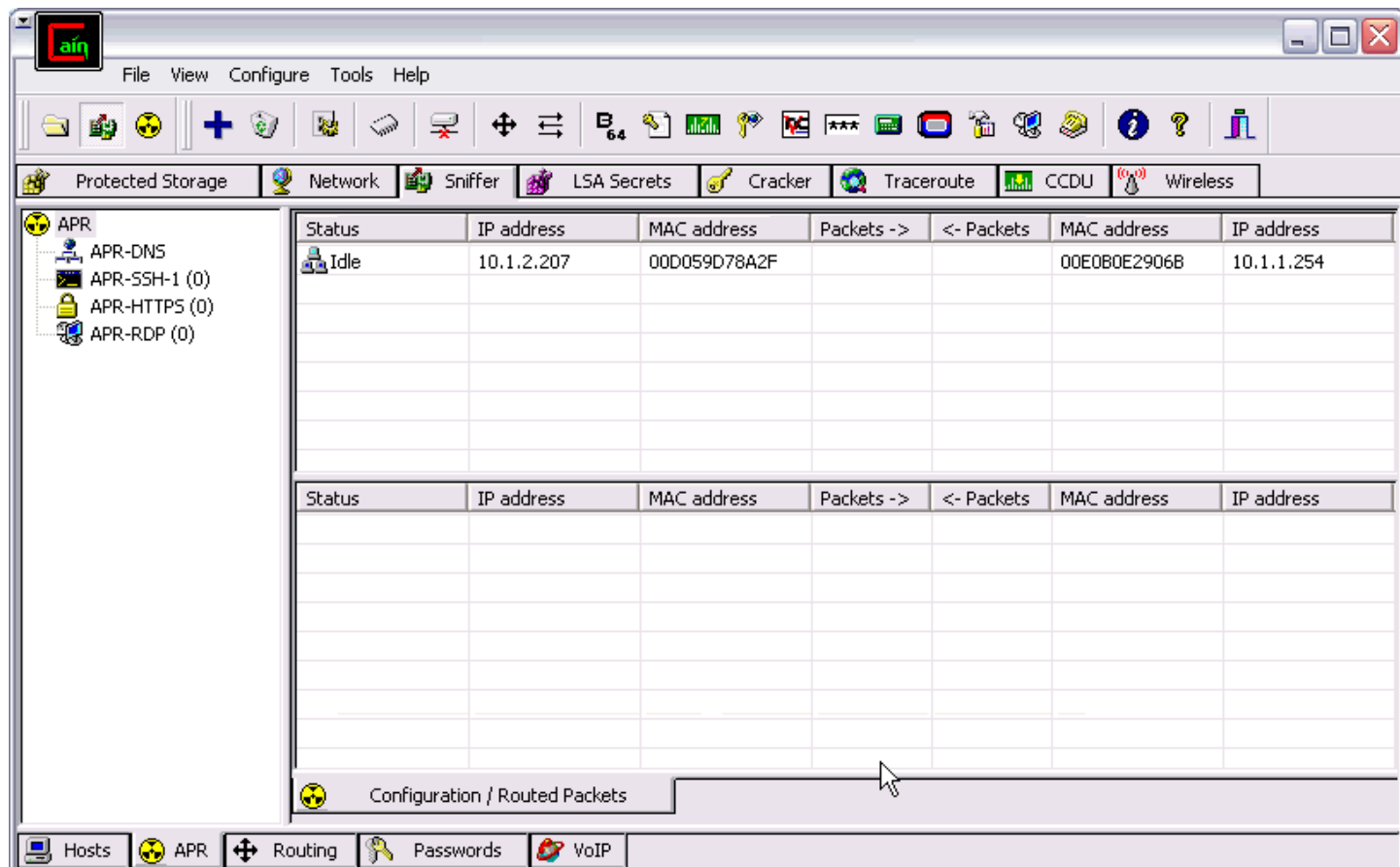
■ Demonstration:

- Windows Tool »Cain & Abel«
 - <http://www.oxid.it/cain.html>
- ARP-Spoofing:
 - Opfer: 10.1.2.207
 - Standardgateway: 10.1.1.254
- DNS-Spoofing:
 - Umleitung von www.bsi.de nach jap.inf.tu-dresden.de

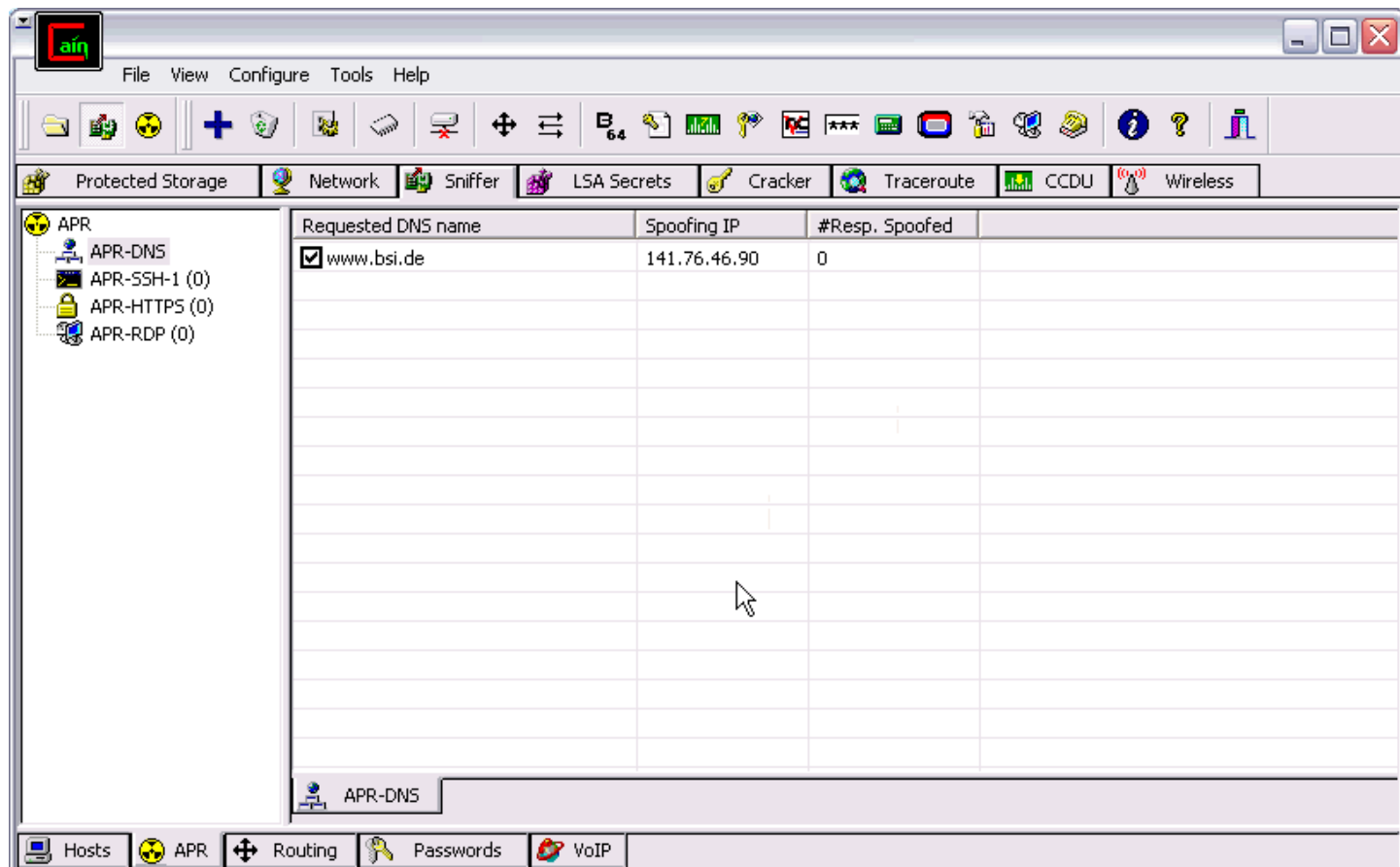
Rechner im Netzwerk identifizieren



Einrichten des DNS-Spoofing

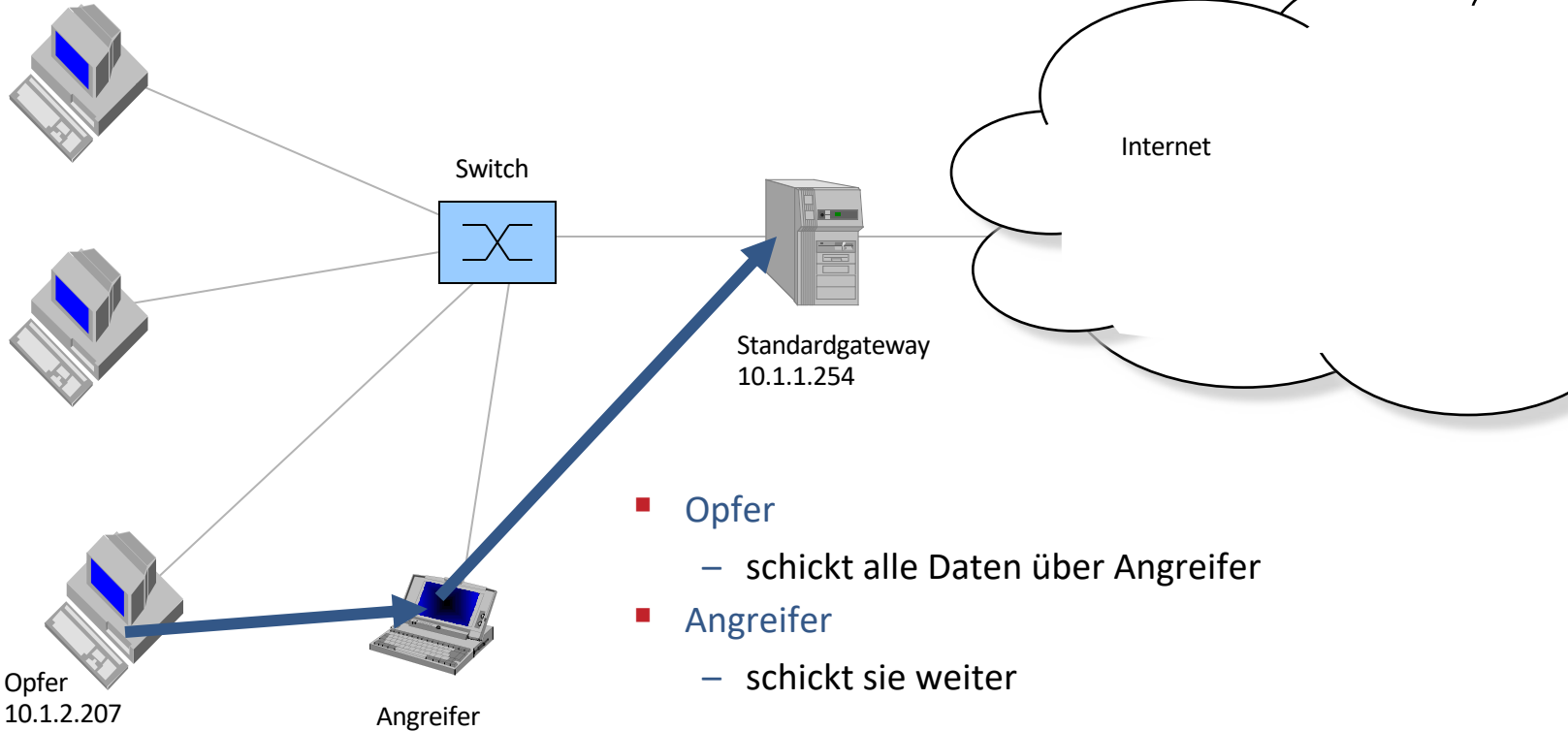


Start des ARP- und DNS-Spoofings



Erreichte Situation

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0




Sicht des Opfers

Lehrveranstaltungsangebote - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://www-sec.uni-regensburg.de/teaching/ Go

 **IT-Sicherheitsmanagement** Lehrstuhl Management der Informationssicherheit

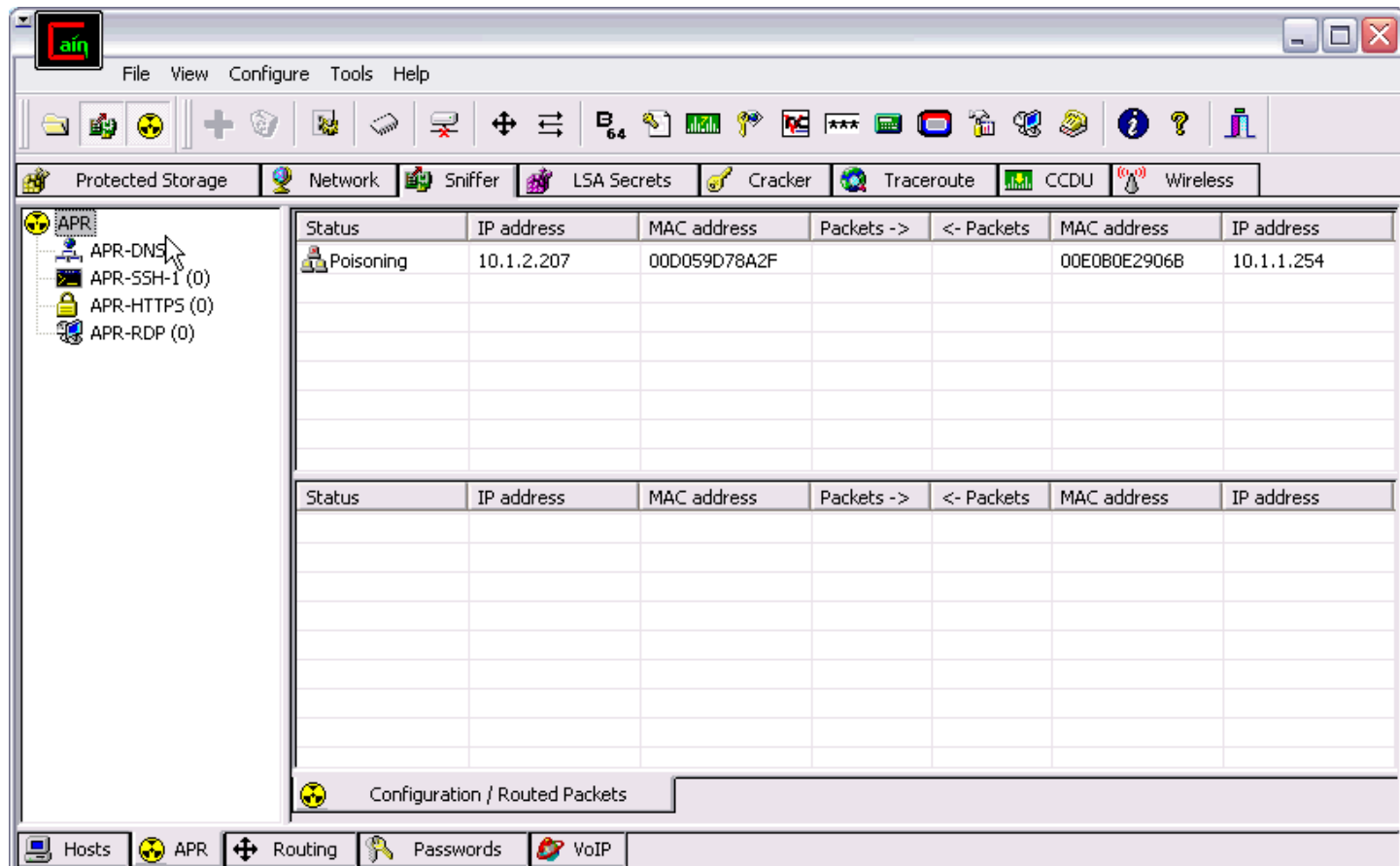
Universität Regensburg > Wirtschaftswissenschaften > Wirtschaftsinformatik

Lehrveranstaltungsangebote

[Lehrveranstaltungsangebote des Lehrstuhls](#) [Vorlesungsfolien in der VUR](#) [Themen für Diplomarbeiten](#) [Schwerpunkt Informationssicherheit](#) [Modellstudienplan Informationssicherheit](#)

Wintersemester	SWS	Art
VL Informatik III (Algorithmen und Datenstrukturen)	2/2	Grundstudium
VL Allgemeine Wirtschaftsinformatik (Datenkommunikation)	2/1	Hauptstudium
Seminar IT-Sicherheit	2	Hauptstudium
Diplomanden- und Doktorandenseminar	2	Hauptstudium
VL Sicherheitsmanagement	2/1	Schwerpunkt Informationssicherheit
VL Sicherheit mobiler Systeme	2/-	Schwerpunkt Informationssicherheit
VL Praxis der IT-Sicherheit (bedarfswise)	1/3	Schwerpunkt Informationssicherheit
Sommersemester		
VL Informatik IV (Objektorientierte Programmierung)	2/1	Grundstudium

Sicht des Angreifers



Schutz vor ARP-Spoofing

■ Arpwatch

- verfolgt Änderungen der Zuordnung von Ethernetadressen und IP-Adressen
 - Erstmaliges Erscheinen einer neuen Ethernetadresse
 - Wechseln der Zuordnung von der »üblichen« auf eine neue Zuordnung (Ethernetadresse–IP-Adresse)
- Alarmiert Systemadministrator bei Auffälligkeiten per E-Mail
- Manpage
 - http://linuxcommand.org/man_pages/arpwatch8.html
- Package
 - <http://packages.debian.org/unstable/admin/arpwatch.html>

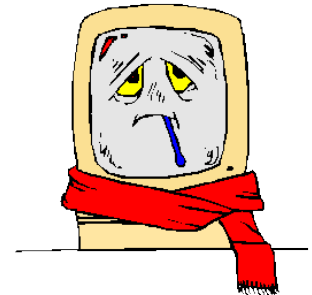
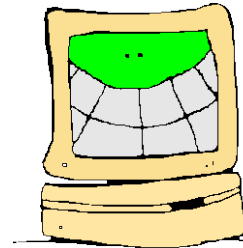
Schutz vor DNS-Spoofing

- DNSSEC (DNS Security Extensions)
 - vorgeschlagen im März 2005 als RFC 4034 (und weitere)
 - <http://www.dnssec.net/>
 - Kernidee:
 - Nutzung digitaler Signaturen zur Authentifizierung der DNS-Antwort
 - Schutzziele
 - Schutz der Integrität und Zurechenbarkeit
 - Kein Schutz der Vertraulichkeit und Verfügbarkeit

Denial-of-Service Angriffe

Verfügbarkeit: Denial-of-Service

- DoS-Angriffe auf Schwachstellen im Systemdesign (insb. Protokolle)
 - Mail-Bombing – Spamming
 - Broadcast-Storm
 - SYN-Flooding
- DoS-Angriffe auf Implementationsfehler
 - WhatsApp text bomb freezing smartphones worldwide (Mai 2018)
<https://www.gadgetsnow.com/tech-news/this-message-is-freezing-whatsapp-across-the-world/articleshow/64058468.cms>
 - WinNuke, Teardrop und Nachfahren (Windows NT, Windows 95, bis ca. 1997)
 - Ping of Death (Windows, Unix, bis ca. 2013)



Distributed Denial-of-Service Angriffe im Internet

■ Charakterisierung

- Ziel wird von mehreren Quellen gleichzeitig angegriffen

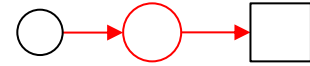
■ Typische Angriffsmuster

- Reflexion, Spoofing
- Amplification
- Distribution (Botnets)

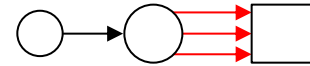
■ Beispiele

- Smurf IP Denial-of-Service Attack von 1998
- Mirai-Botnet (2016)
- Memcached-Angriff von 2017

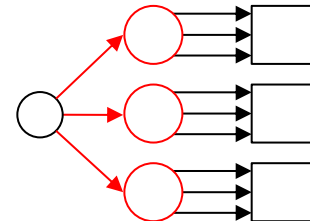
Reflexion



Amplification



Distribution

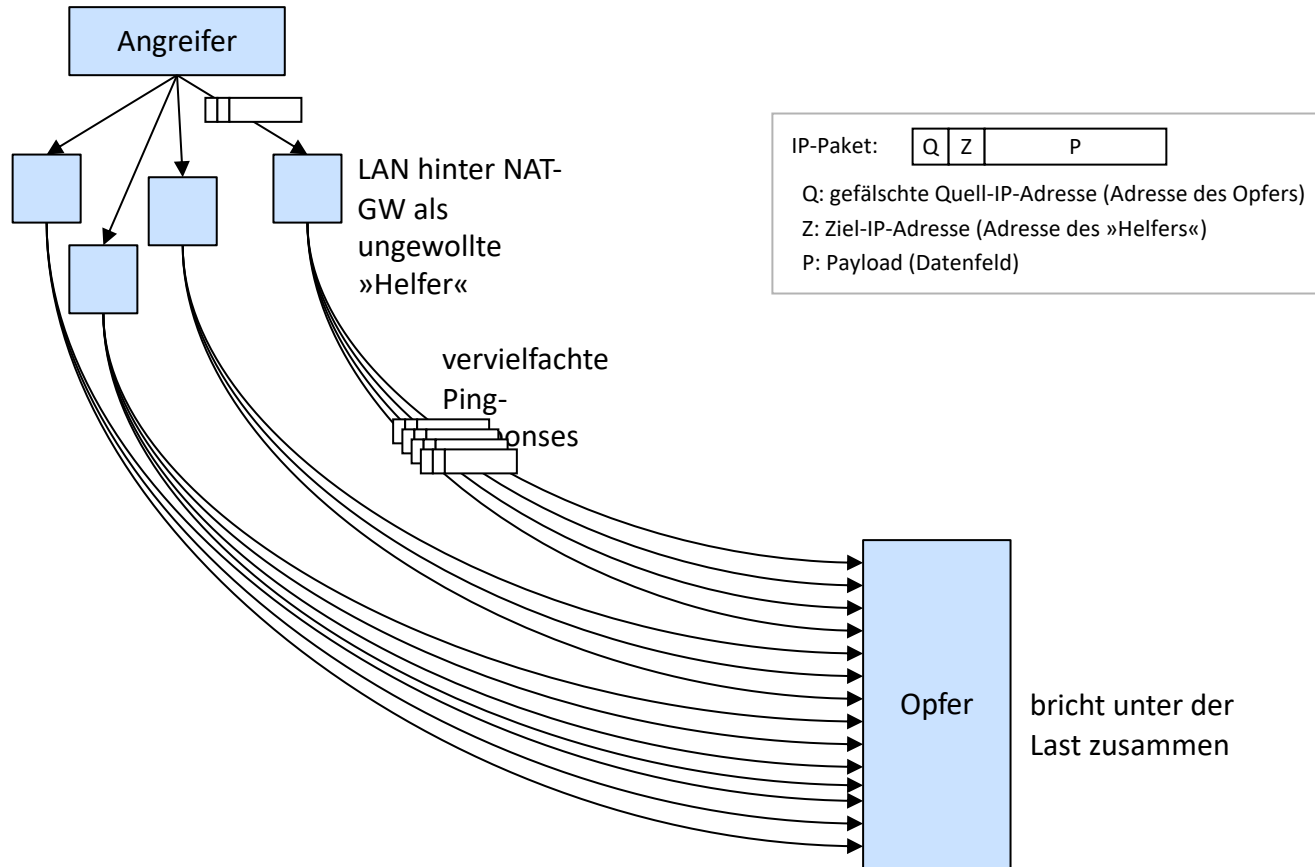


Smurf IP Denial-of-Service Attack (CERT Advisory CA-1998-01)

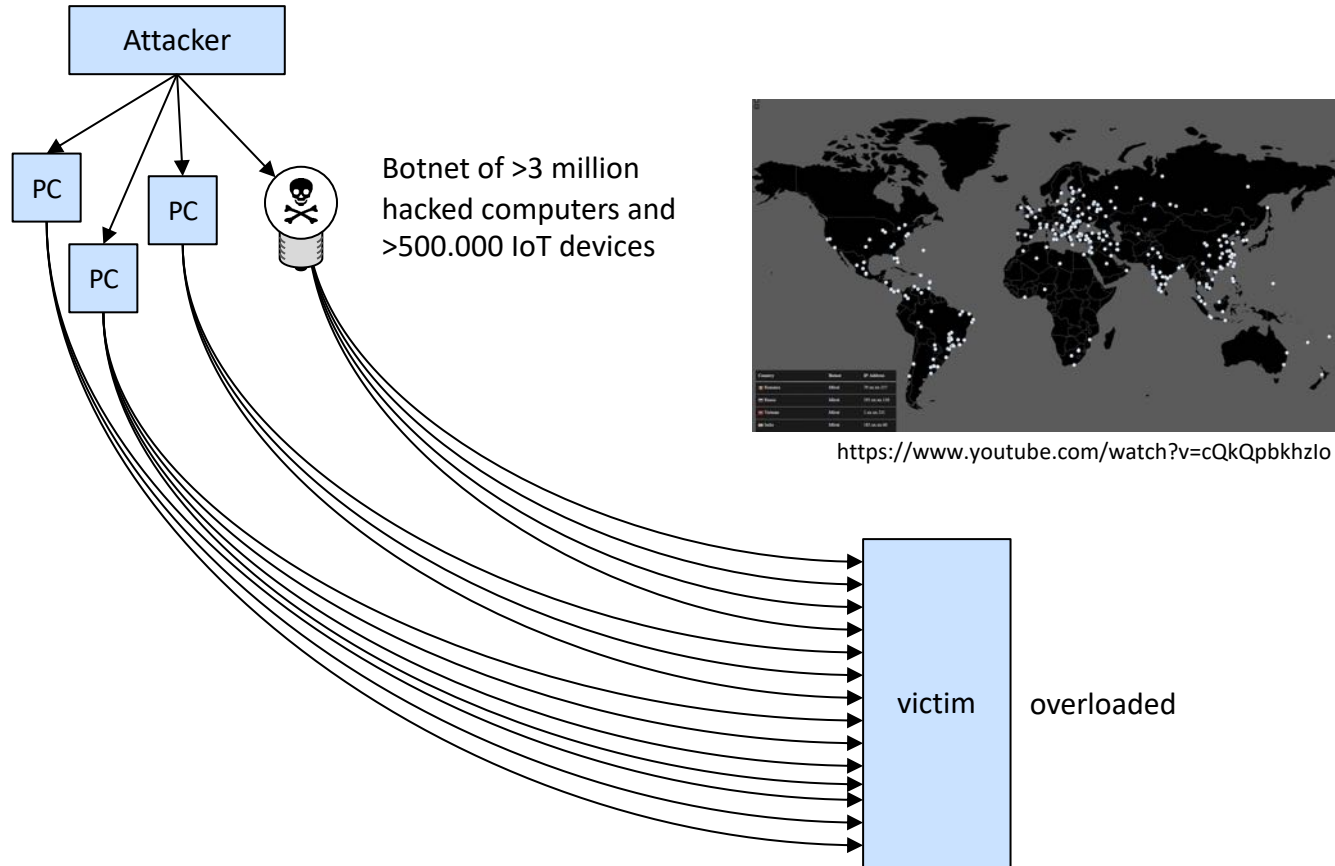
- DDos-Angriff basierend auf Flooding mit Ping-Paketen
 - Ping: Management-Service zur Überprüfung der Empfangsbereitschaft eines Rechners
 - Smurf IP DDos ist Beispiel für IP-Spoofing und Amplification

- Vorgehen
 - Angreifer schickt Ping-Pakete mit gefälschter Absender-Adresse an schlecht administriertes LAN/Intranet
 - Konfigurationsfehler im LAN vervielfacht Ping
 - Weiterleitung an alle Rechner des LAN hinter dem Gateway
 - Jeder Rechner des LAN antwortet mit Pong

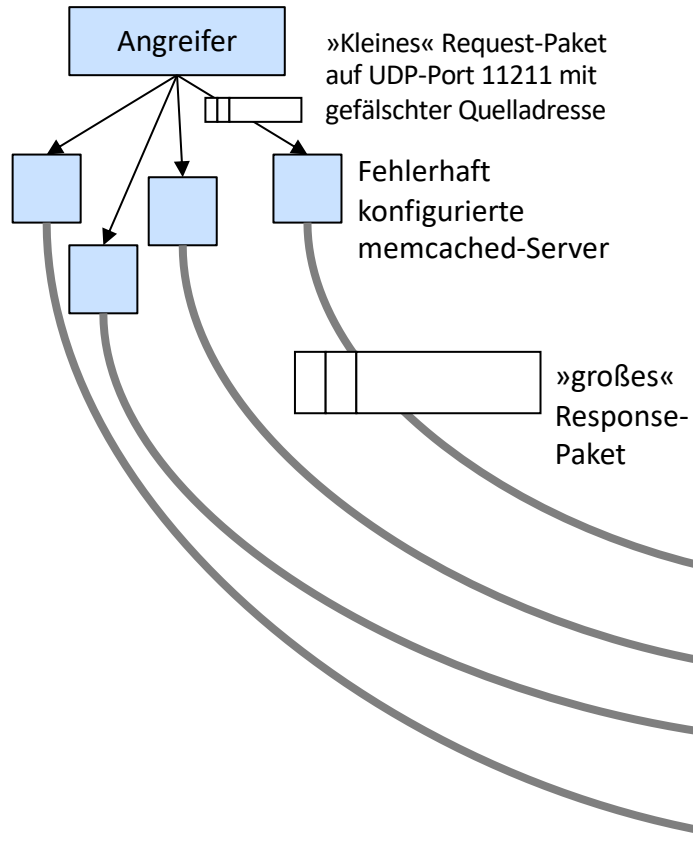
Smurf IP Denial-of-Service Attack (1998)



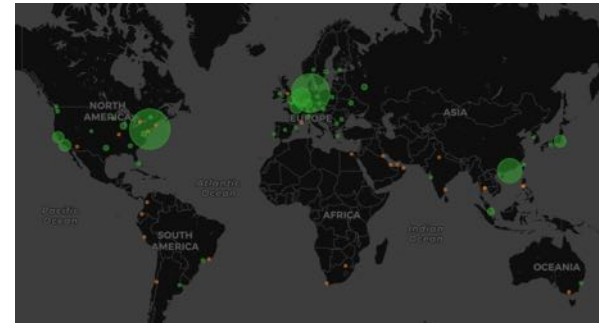
Mirai Botnet (2016)



Memcached-Angriff (2017)

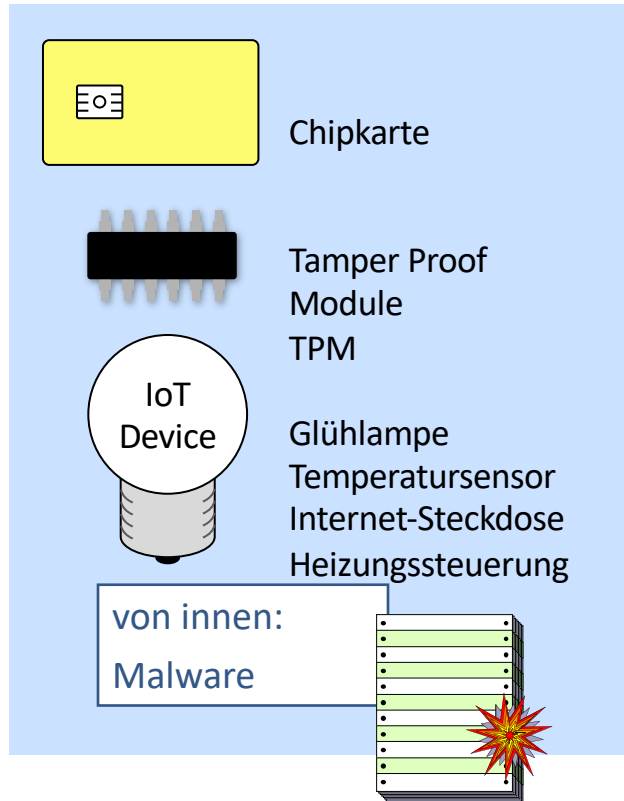


Herkunft der fehlerhaft konfigurierten Memcached-Server



<https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/>

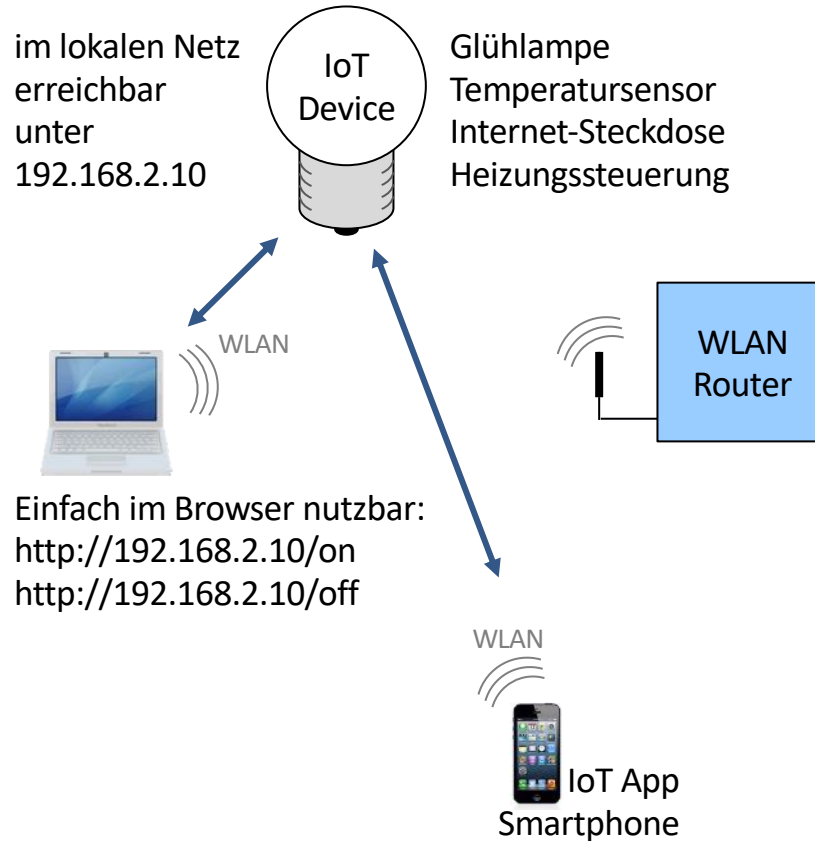
Internet of Things Security



Angreifer kann alle drei
Schutzziele verletzen:

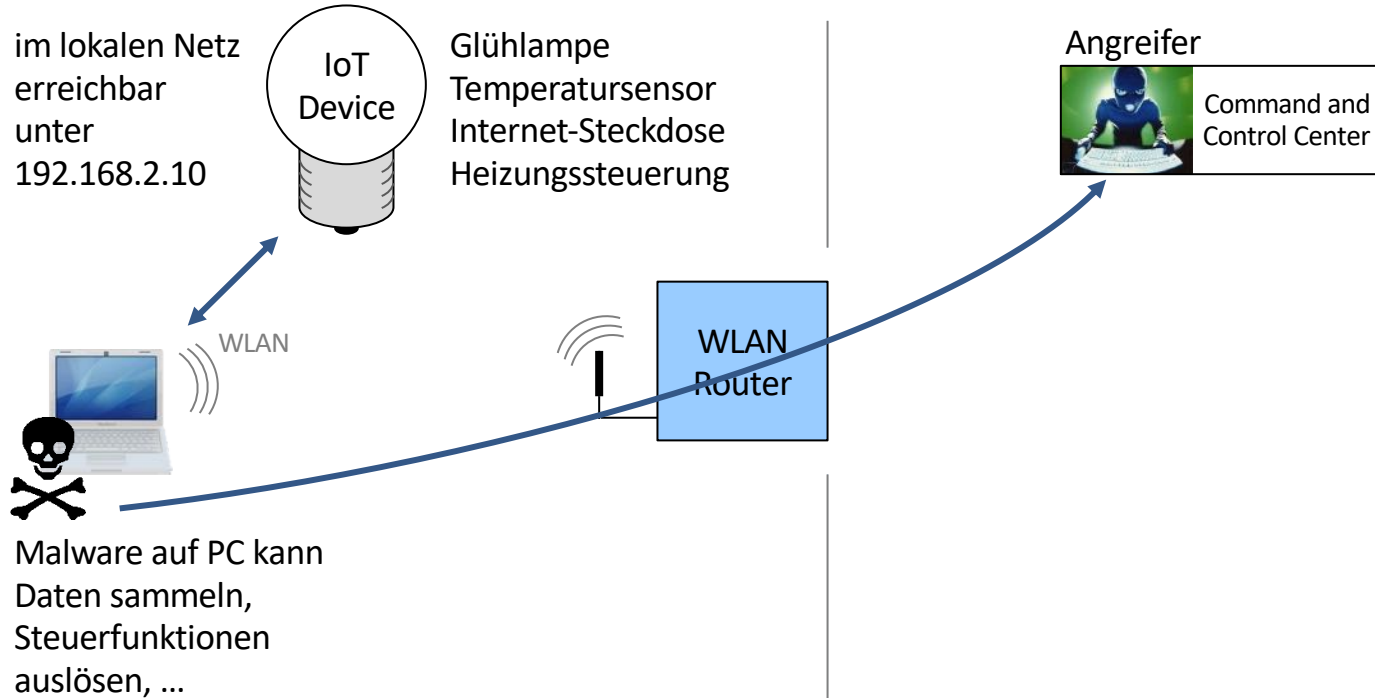
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Internet of Things – im lokalen Netz

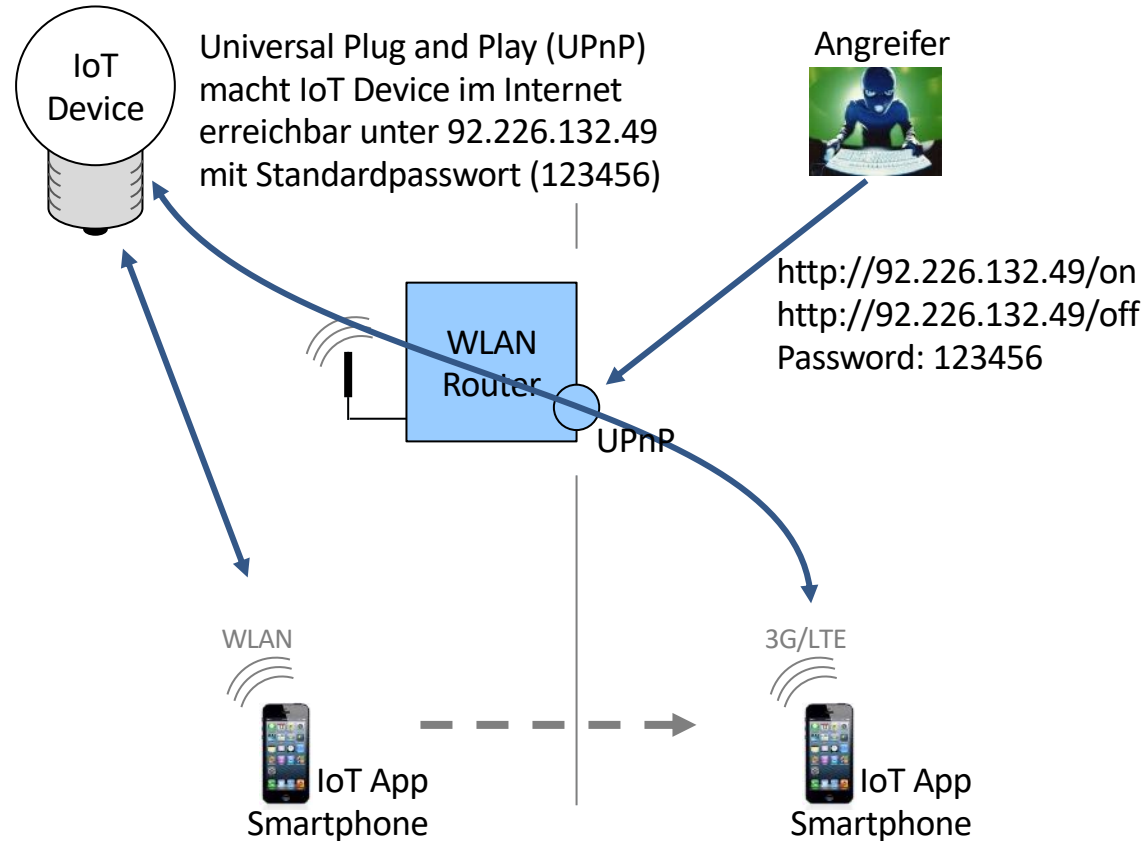


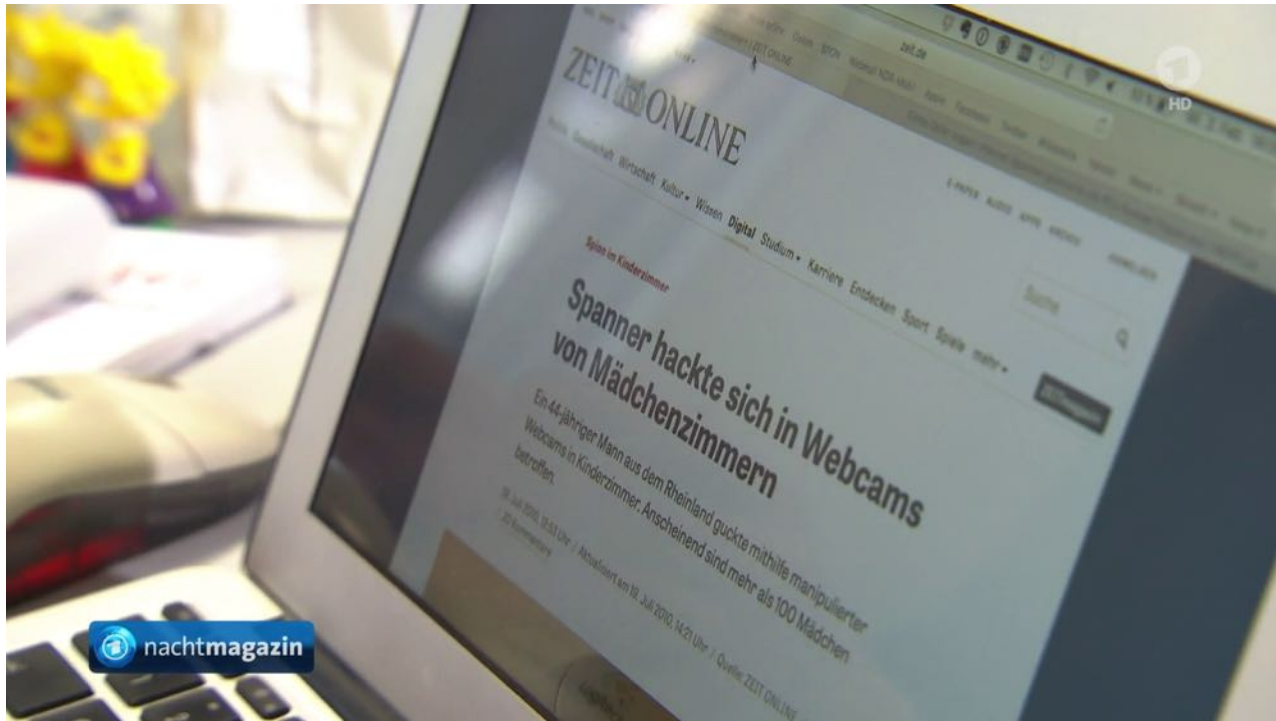
Internet

Internet of Things – im lokalen Netz angreifbar

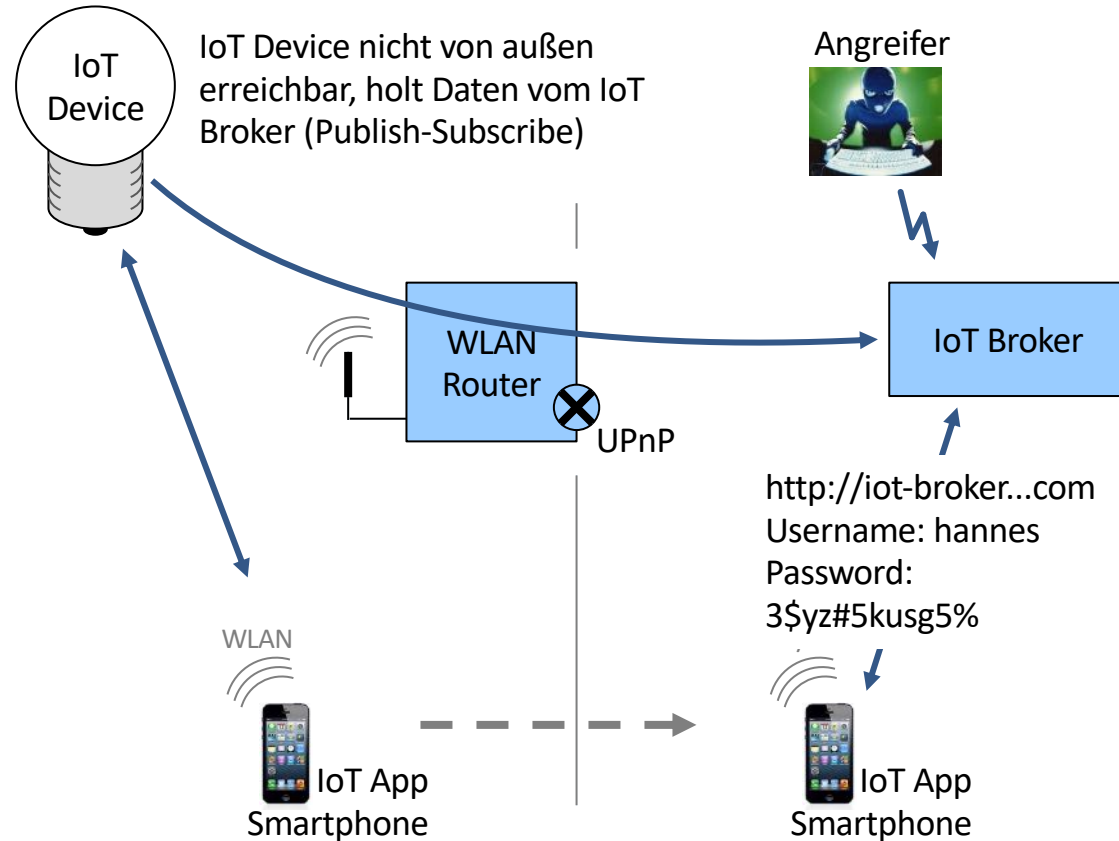


Internet of Things – Angriff über Universal Plug and Play (UPnP)

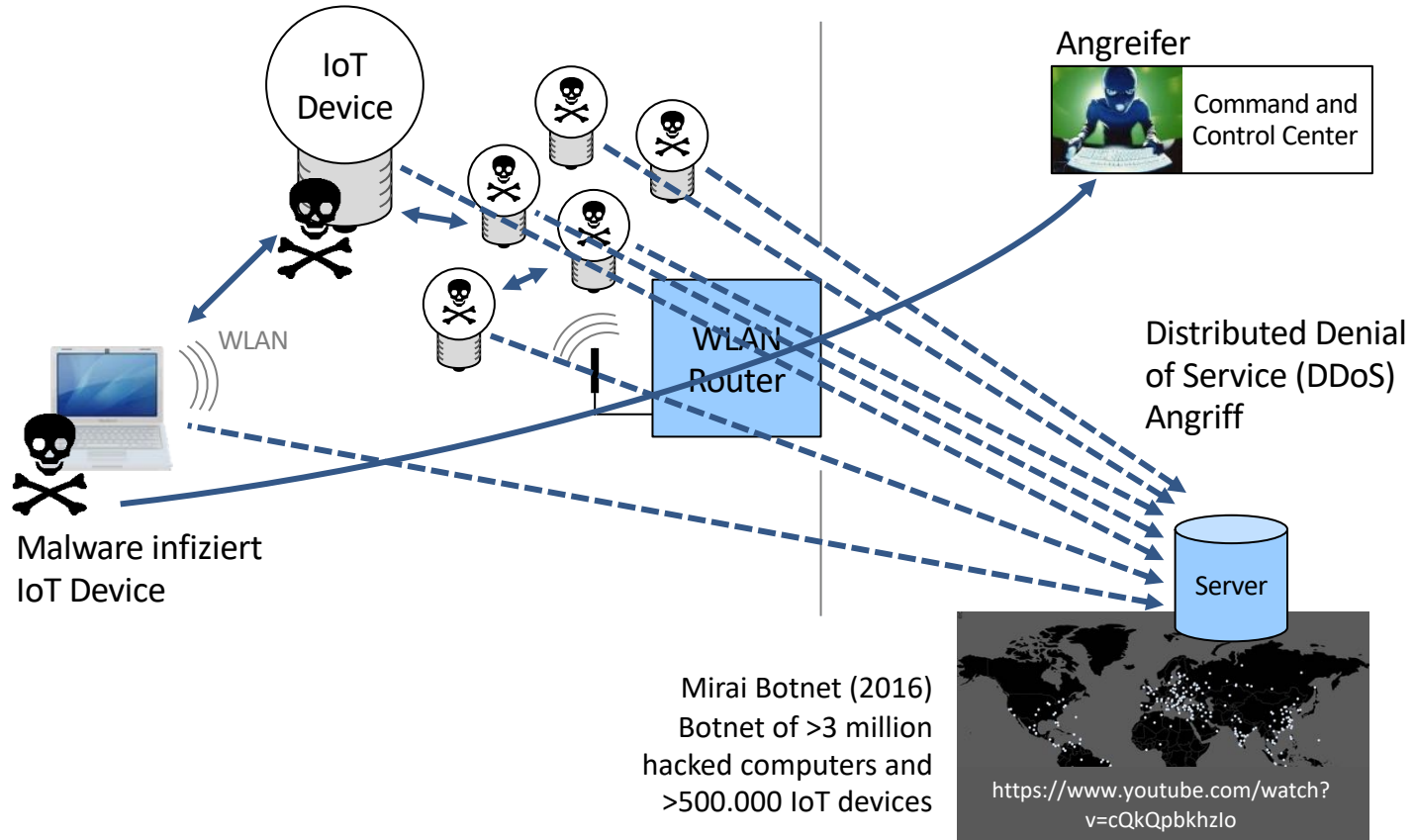




Internet of Things – Sichere Kommunikation über IoT Broker



Internet of Things – IoT Devices als Teil eines Botnetzes



Internet of Things – Over The Air (OTA) Update

