Sicherheit am Strand

Netzwerksicherheit

— Risiken und Schutzmöglichkeiten —

Prof. Dr. Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit

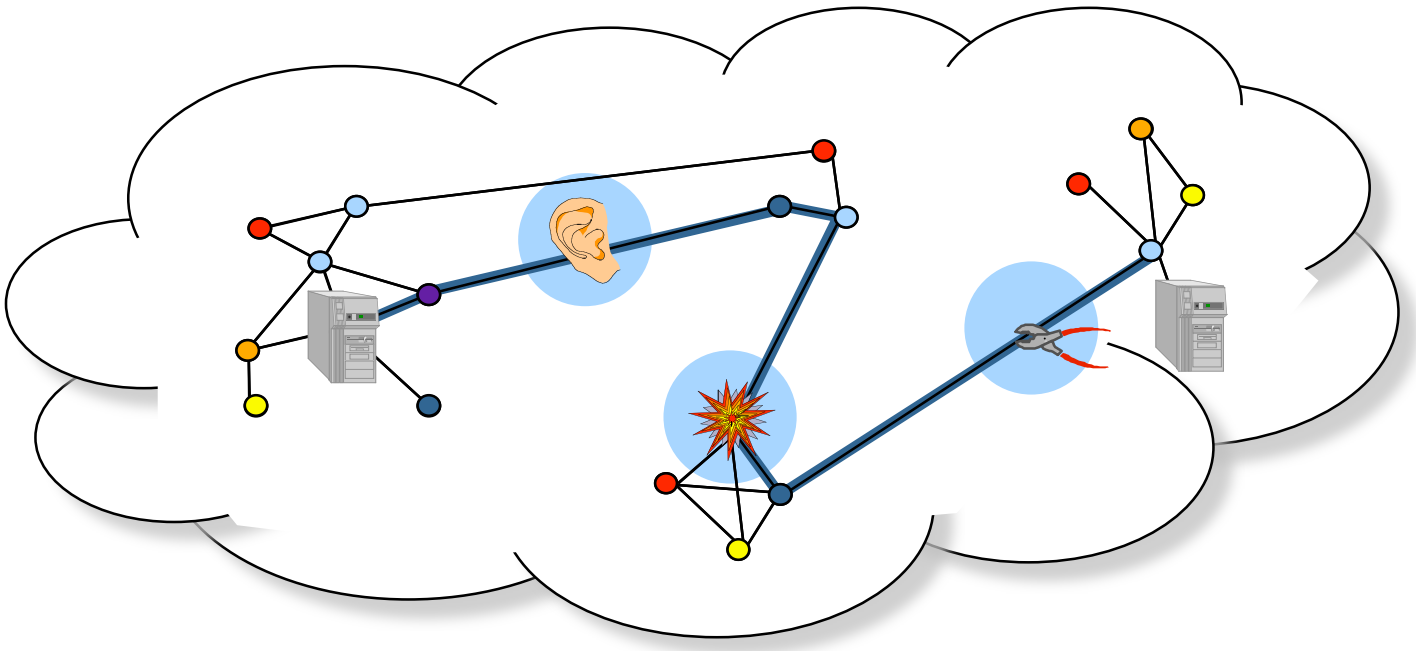
http://www-sec.uni-regensburg.de/

Gliederung

- Einordnung
  - Netzwerksicherheit – Rechnersicherheit
  - Schutzziele
- Angriffe: Fallbeispiele
  - Viren, Würmer, trojanische Pferde
  - Phishing
  - Sniffing und Spoofing

Netzwerksicherheit – Rechnersicherheit

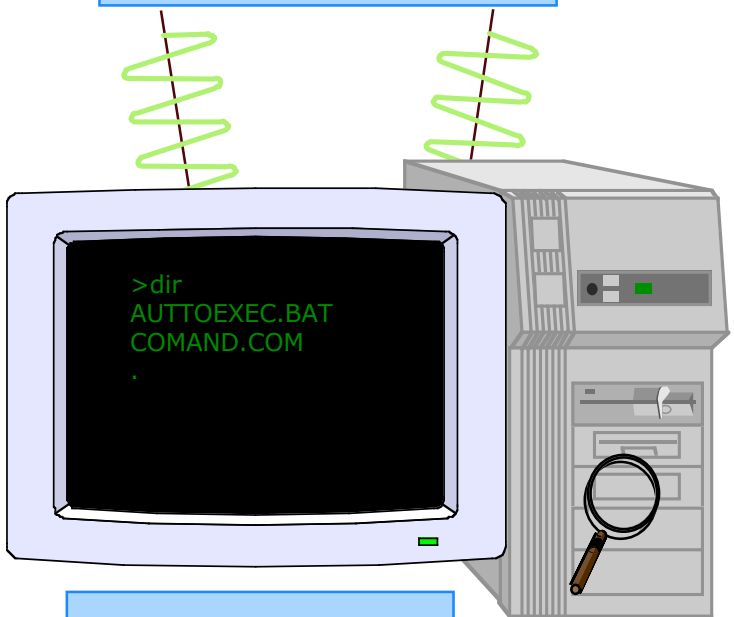
- Knoten: Rechner
- Kanten: Übertragungsstrecken



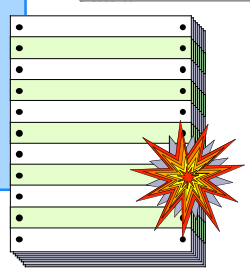
Angriffspunkte

Rechnersicherheit

Abstrahlung

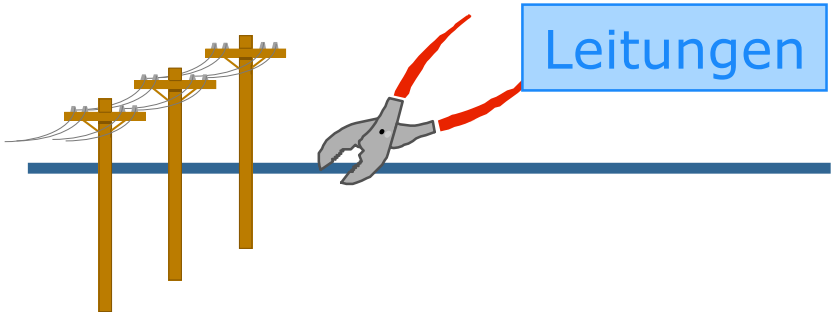


innen (Trojanische Pferde)

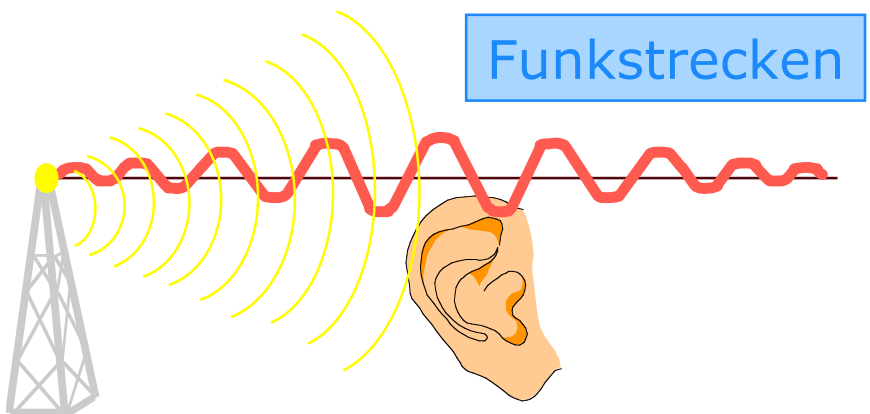


Netzwerksicherheit

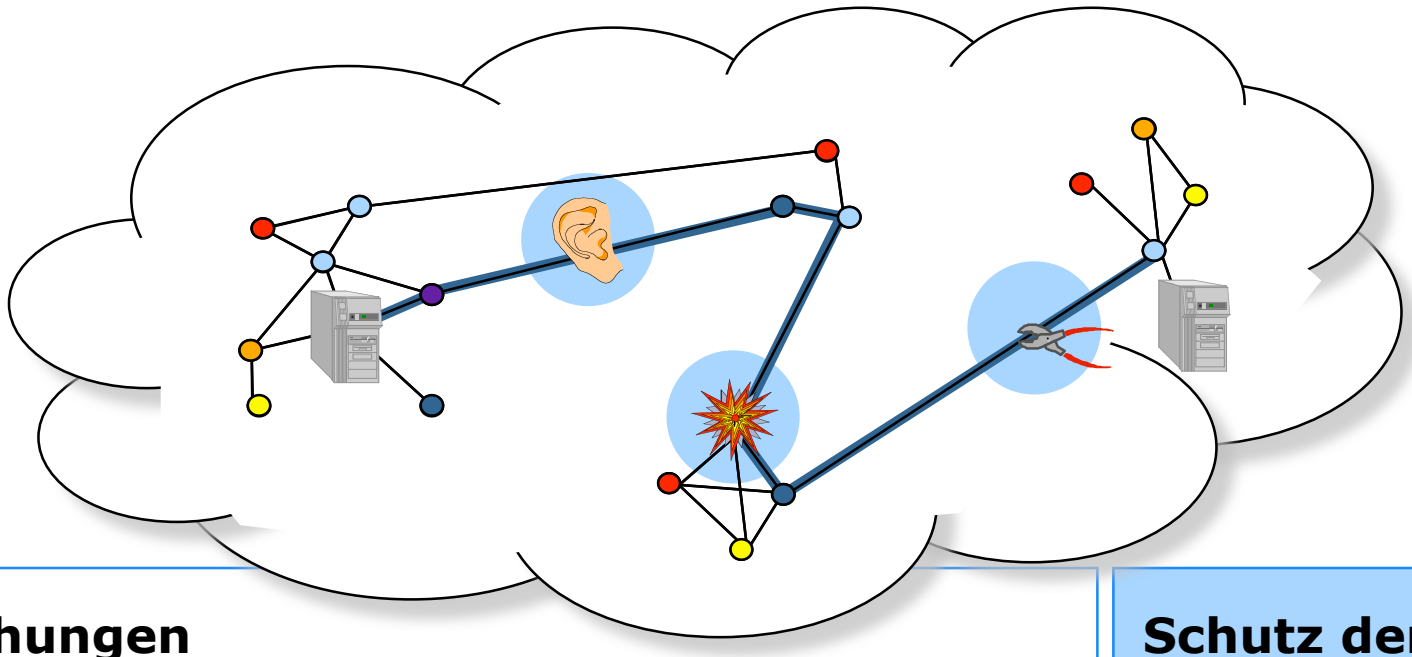
Leitungen



Funkstrecken



Sicherheit in Rechnernetzen



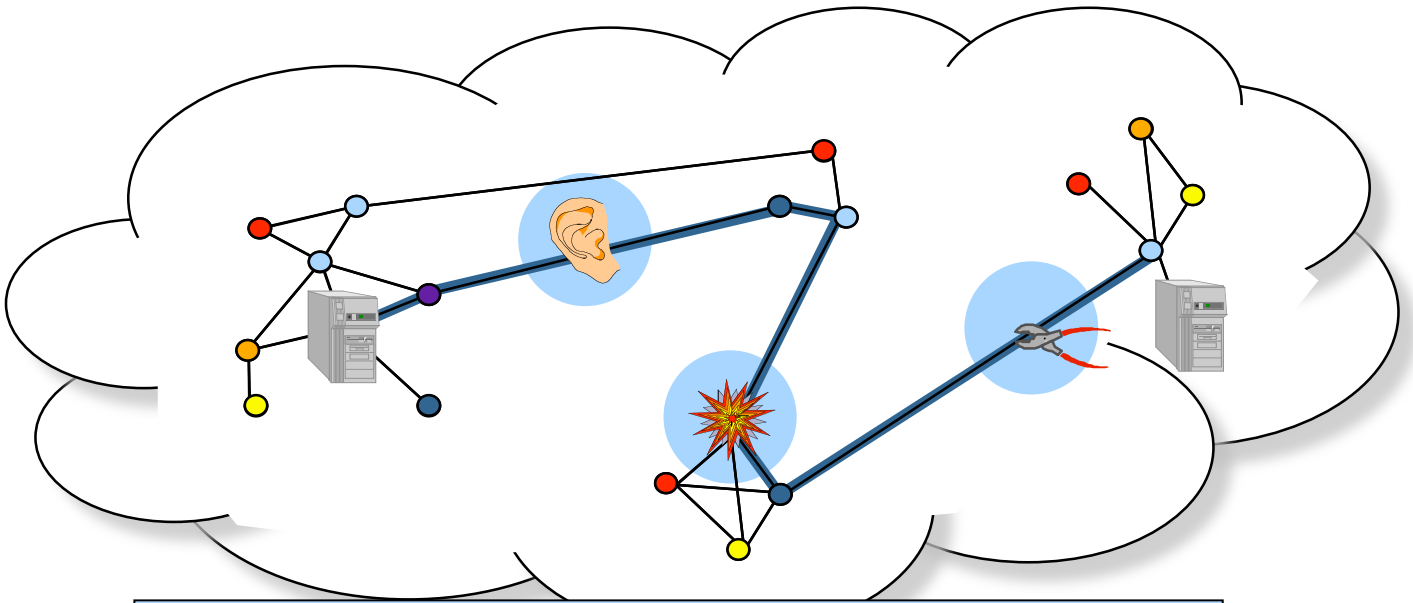
Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

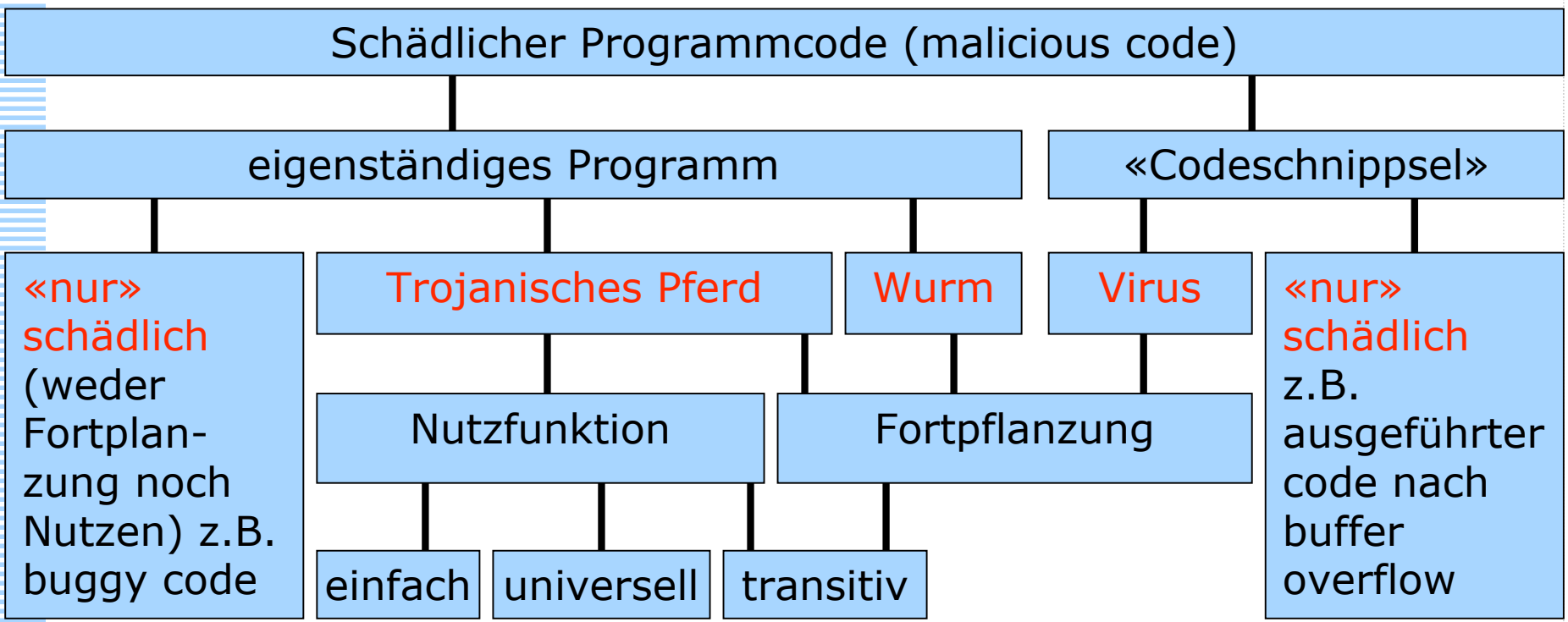
Angriffe: Fallbeispiele



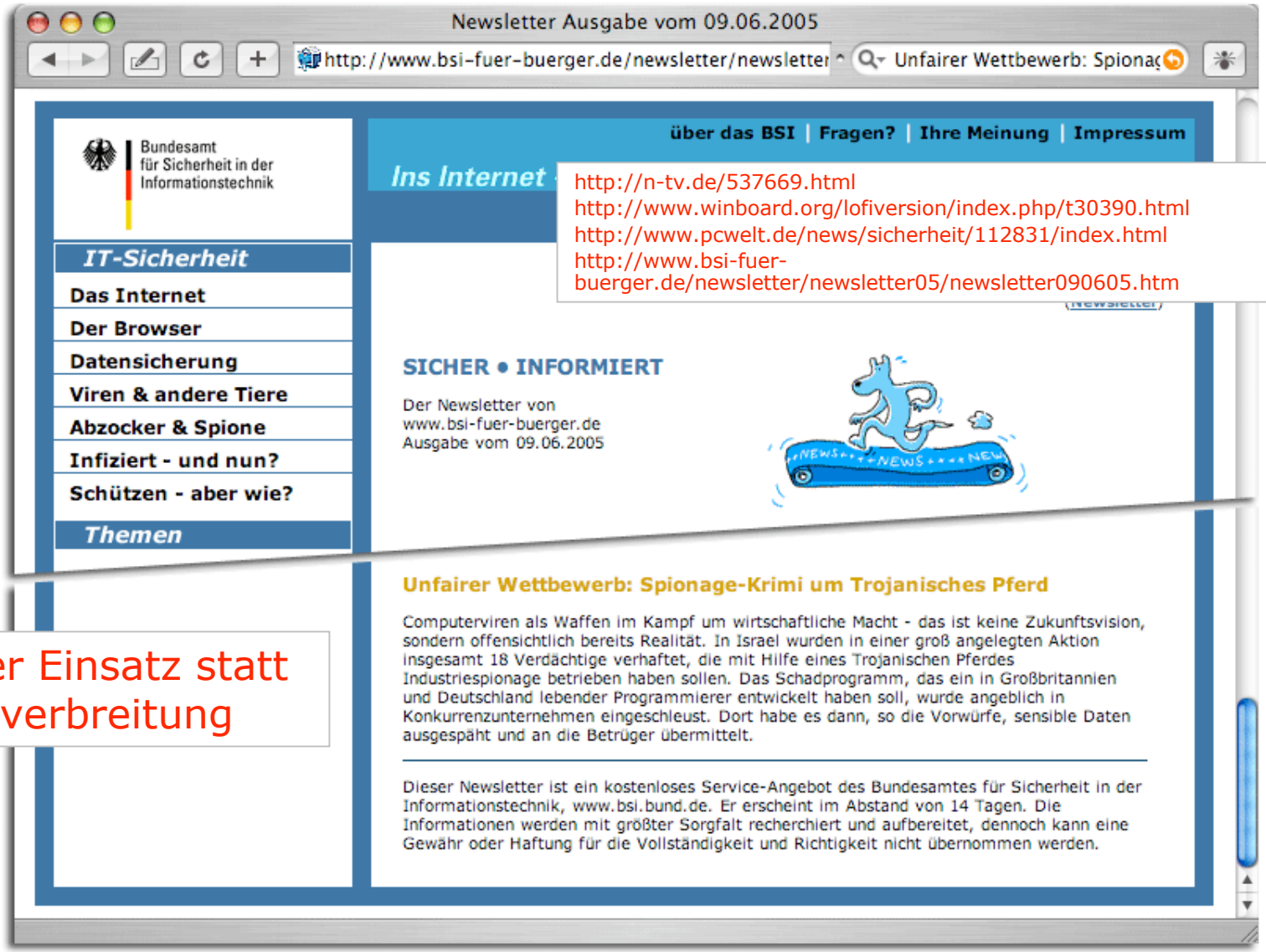
V: Viren, Würmer, trojanische Pferde

P: Phishing

S: Sniffing und Spoofing


Schädlicher Programmcode (malicious code)
eigenständiges Programm
«Codeschnippsel»
«nur» schädlich (weder Fortplan-zung noch Nutzen) z.B. buggy code
Trojanisches Pferd
Wurm
Virus
«nur» schädlich z.B. ausgeführter code nach buffer overflow
Nutzfunktion
Fortpflanzung
einfach
universell
transitiv

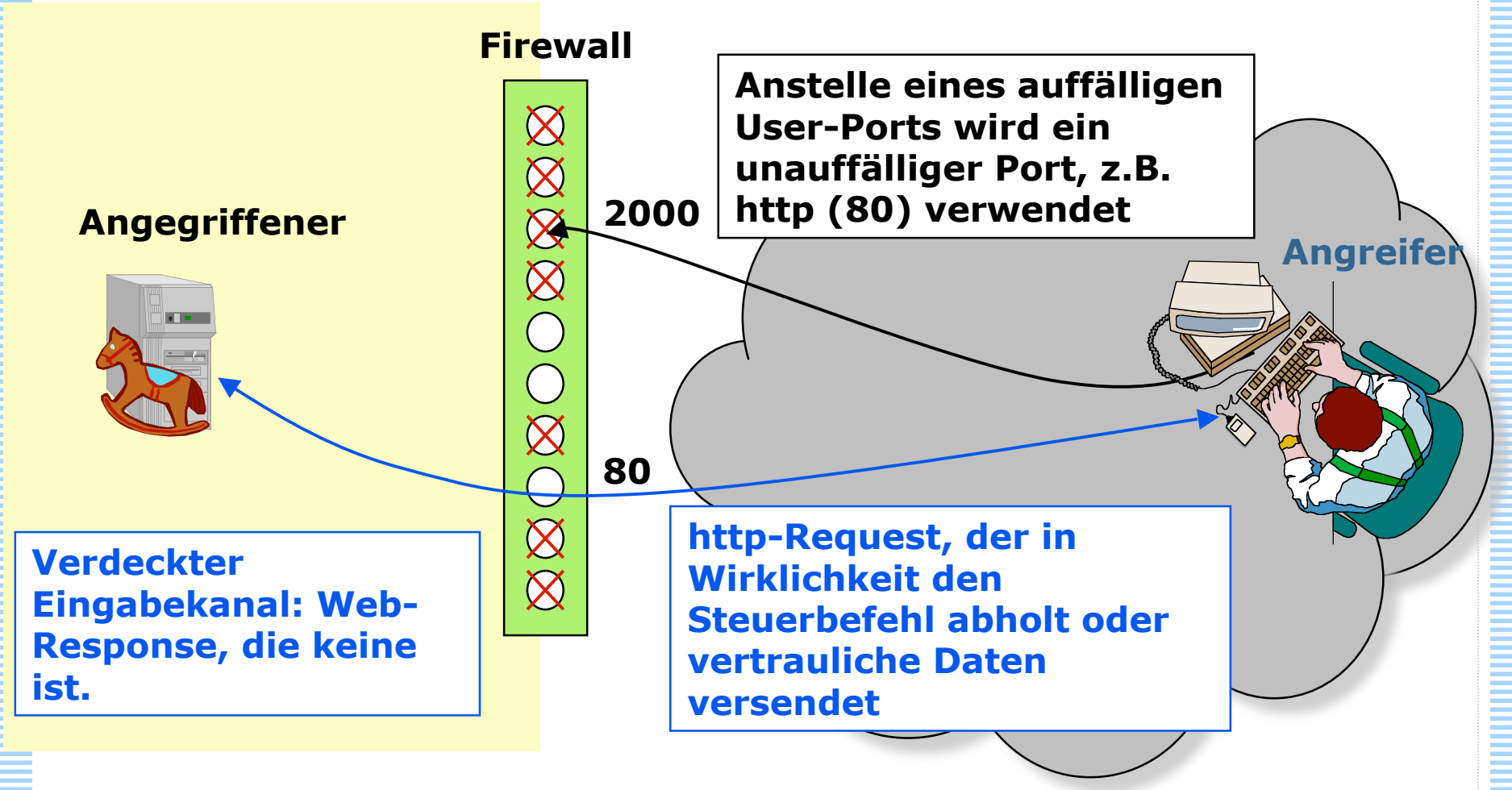
Trojanische Pferde



http://n-tv.de/537669.html
http://www.winboard.org/lofiversion/index.php/t30390.html
http://www.pcwelt.de/news/sicherheit/112831/index.html
http://www.bsi-fuer-buerger.de/newsletter/newsletter05/newsletter090605.htm

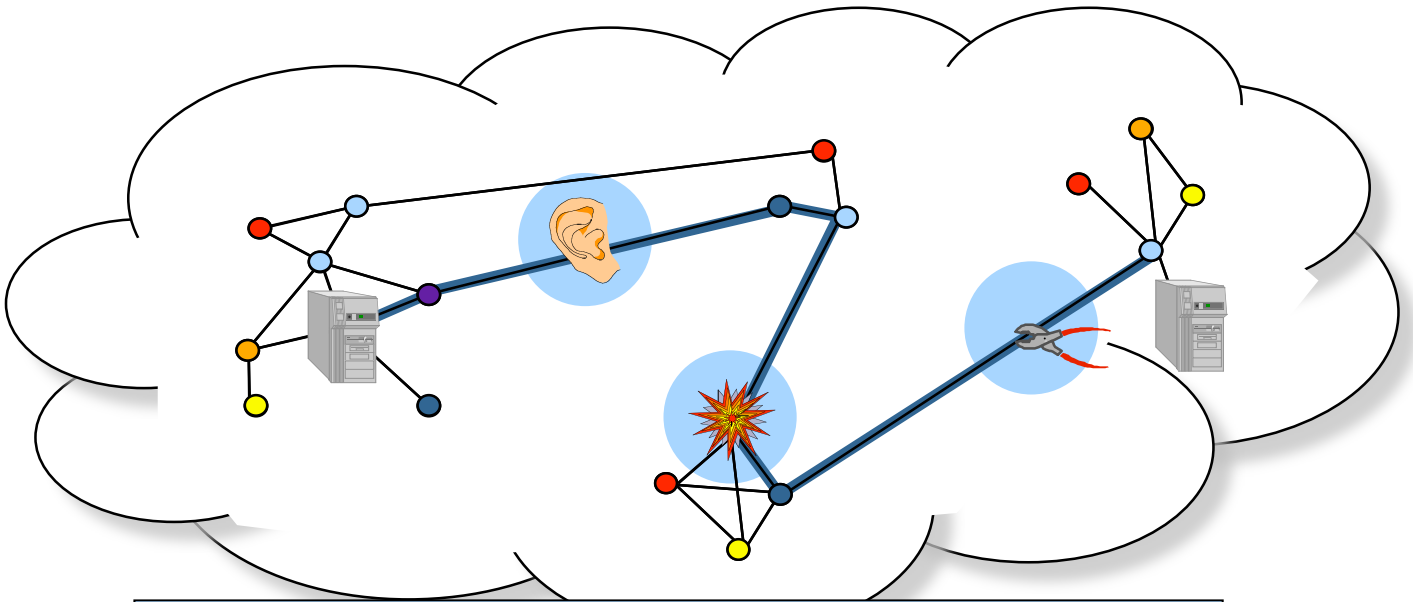
gezielter Einsatz statt Massenverbreitung

Untertunneln einer Firewall durch Troj. Pferd



⇨ Firewall verhindert nicht die Wirkung des trojanischen Pferdes

Angriffe: Fallbeispiele



V: Viren, Würmer, trojanische Pferde

P: Phishing

S: Sniffing und Spoofing

Identifikation von Menschen durch IT-Systeme

- Was der MENSCH IST:
  - Handgeometrie
  - Fingerabdruck
  - Aussehen*
  - eigenhändige Unterschrift*
  - Retina-Muster
  - Stimme
  - Tipp-Charakteristik
  - DNA-Muster
- Was der MENSCH HAT:
  - Papierdokument*
  - Metallschlüssel
  - Magnetstreifenkarte
  - Chipkarte
  - Taschenrechner
- Was der MENSCH WEIß:
  - Passwort
  - Antworten auf Fragen
  - Rechenergebnisse für Zahlen

*=Ausweis

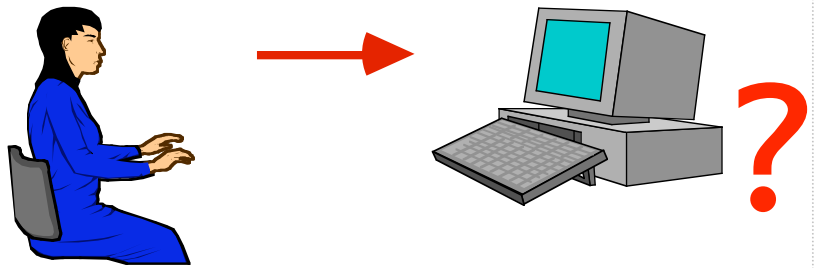


Bild:
http://www.rsasecurity.com

Bild: ntz, Heft 3-4/2006, S. 35

Welche Passwörter werden tatsächlich genutzt?

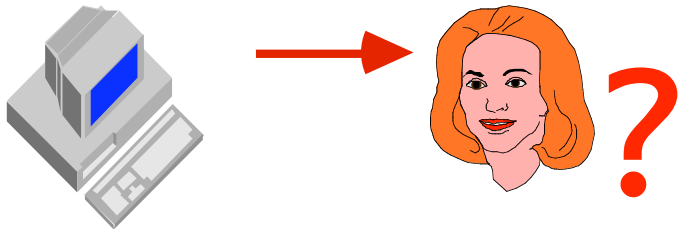
- Kompromittierte Passwörter eines Internet-Dating-Portals wurden auf einer Mailingliste veröffentlicht:
  - Ein blinder Log-in-Versuch mit "123456" führt in fast 1,4 % der Fälle zum Erfolg.
  - Insgesamt rund 2,5 % der Passwörter beginnen mit der Ziffernfolge "1234".
  - Rund 40 % der Passwörter trat nur einmal auf.

Rang	Passwort	Häufigkeit
1	123456	1375
2	ficken	404
3	12345	367
4	hallo	362
5	123456789	260
6	schatz	253
7	12345678	215
8	daniel	215
9	askim	184
10	nadine	177
11	1234	176
12	passwort	173
…		

Quelle: ct 2006, Heft 13, S.64

Identifikation von IT-Systemen durch Menschen

- Was es ist:
  - Gehäuse
  - Siegel
  - Hologramm
  - Verschmutzung



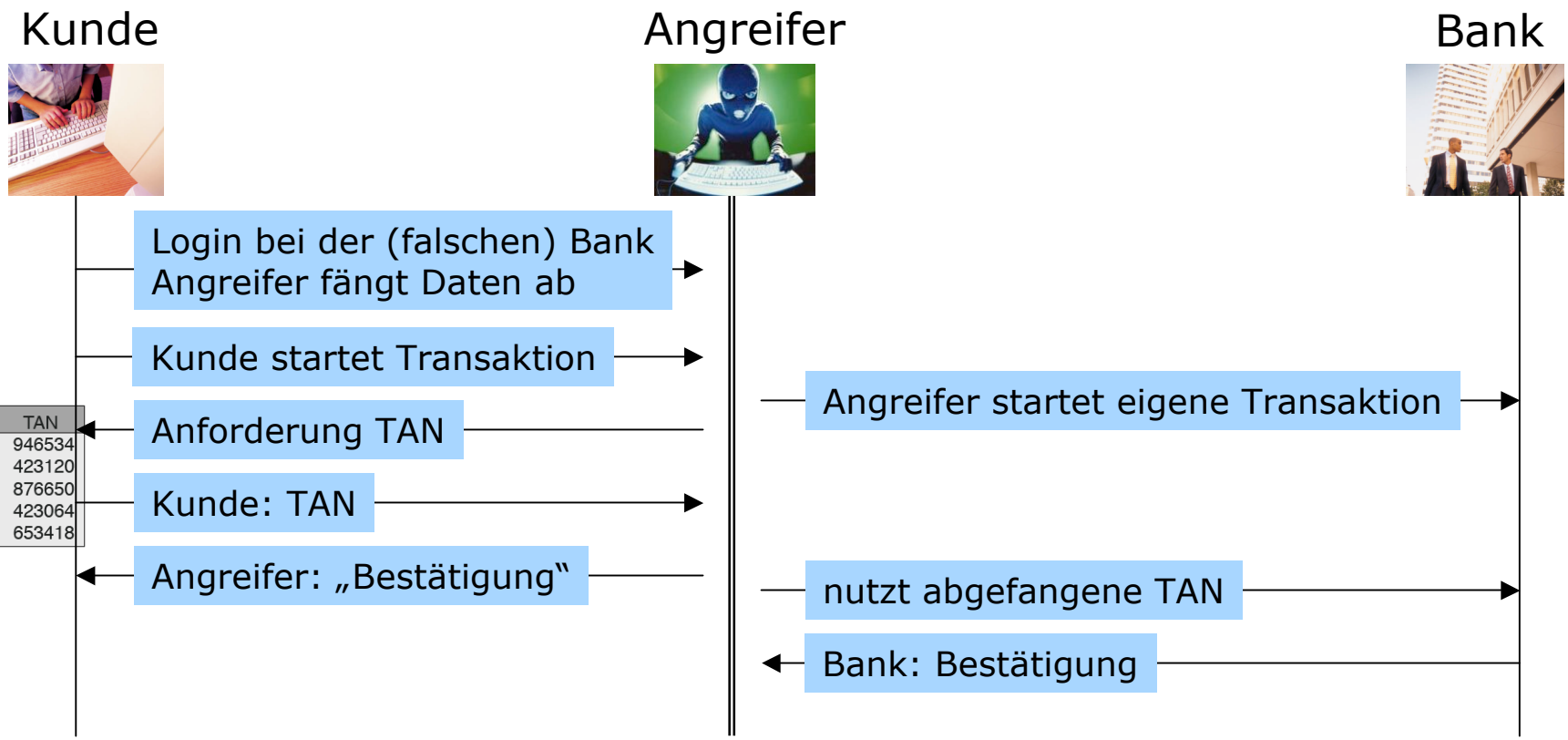
- Was es weiß:
  - Passwort
  - Antworten auf Fragen
  - Rechenergebnisse für Zahlen

- Wo es steht.

Warum ist das relevant?
- Faked Login-Screen
- Phishing

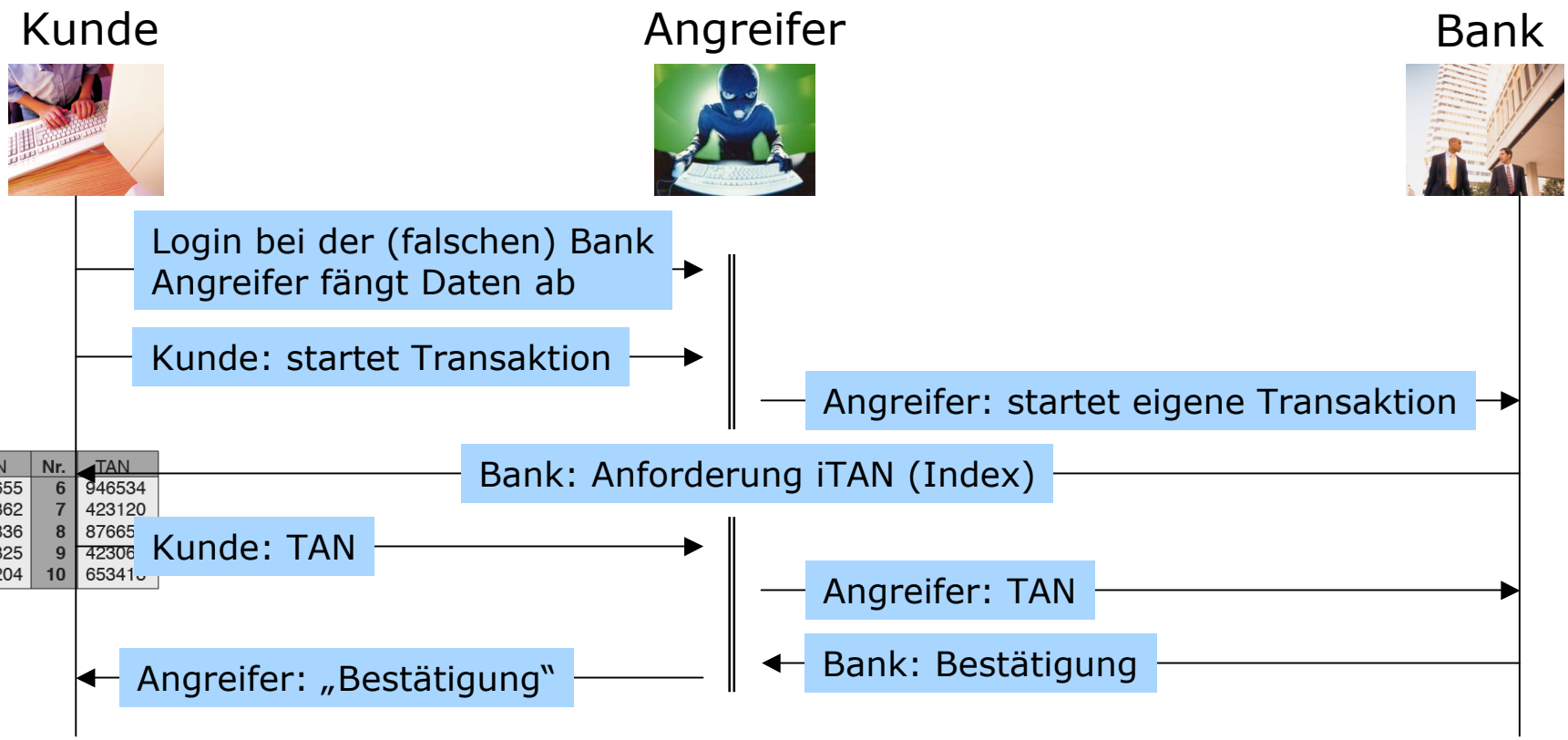
Man-in-the-middle-attack auf TAN-Verfahren (Skizze)

- Voraussetzung: Angreifer
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite



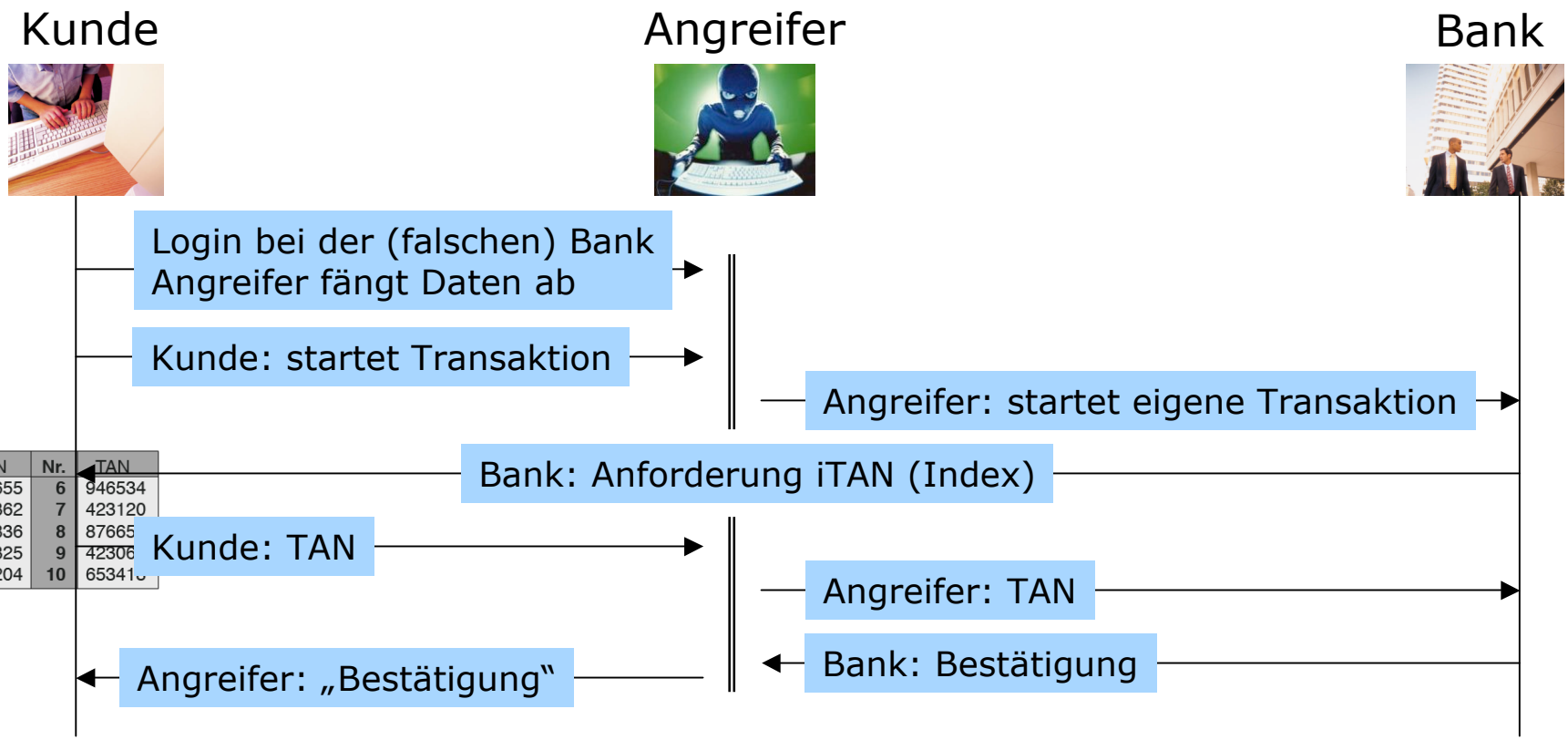
Man-in-the-middle-attack auf iTAN-Verfahren (Skizze)

- Voraussetzung: Angreifer
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite

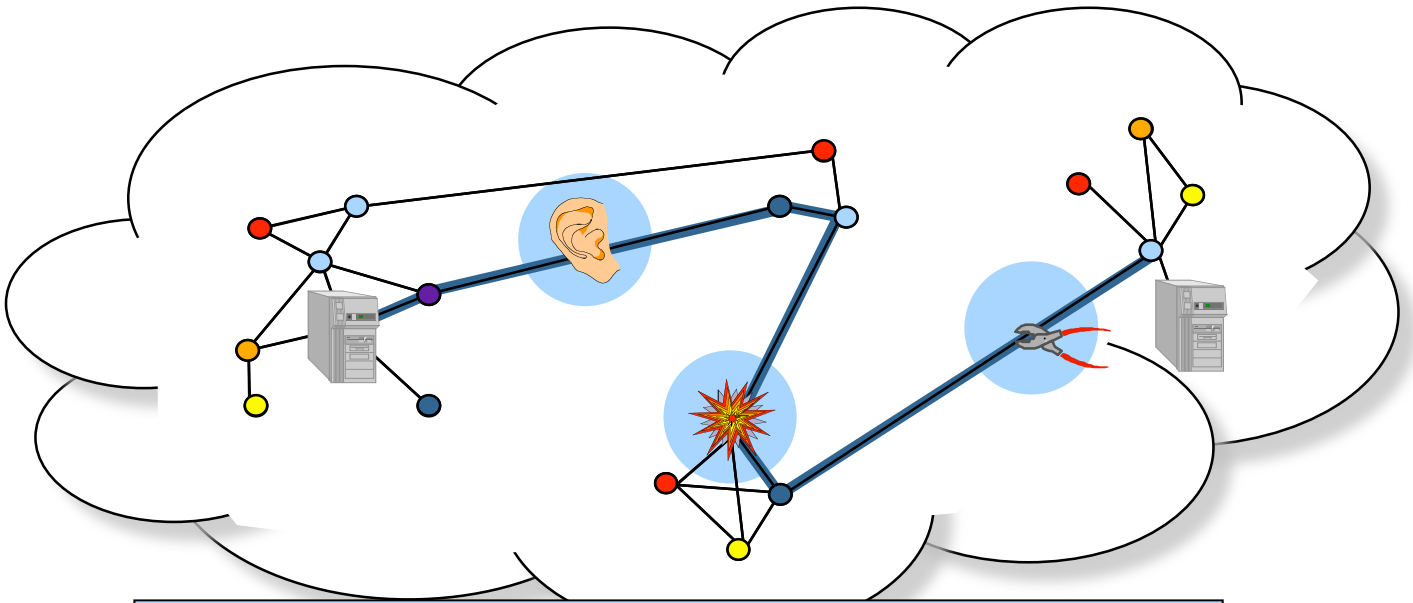


Man-in-the-middle-attack auf iTAN-Verfahren (Skizze)

- Verbesserungen gegenüber normalem TAN-Verfahren:
  - Angreifer benötigt «Online-Hilfe durch Kunden», d.h. er kann nur Transaktionen erfolgreich durchführen, wenn Kunde dies selbst gerade tun will



Angriffe: Fallbeispiele



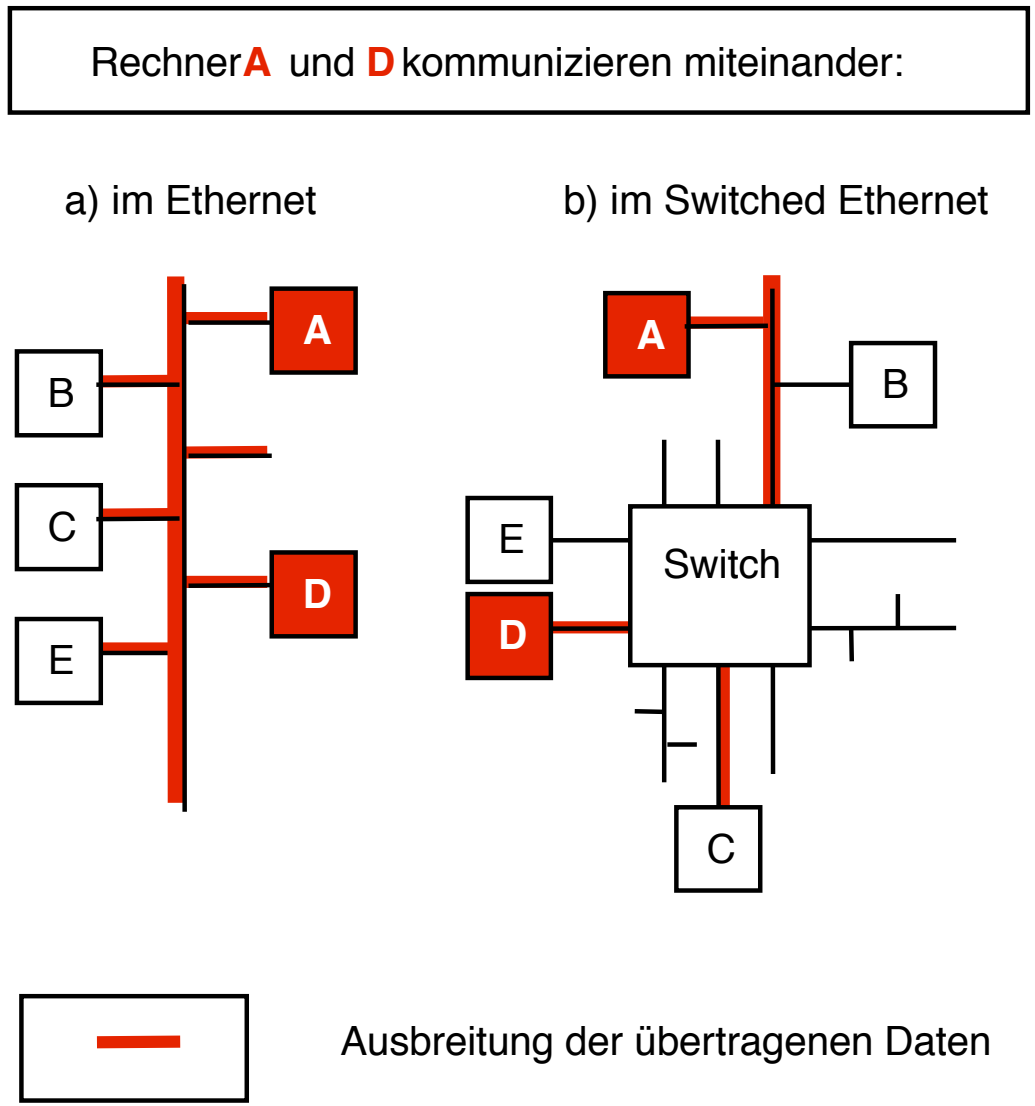
V: Viren, Würmer, trojanische Pferde

P: Phishing

S: Sniffing und Spoofing

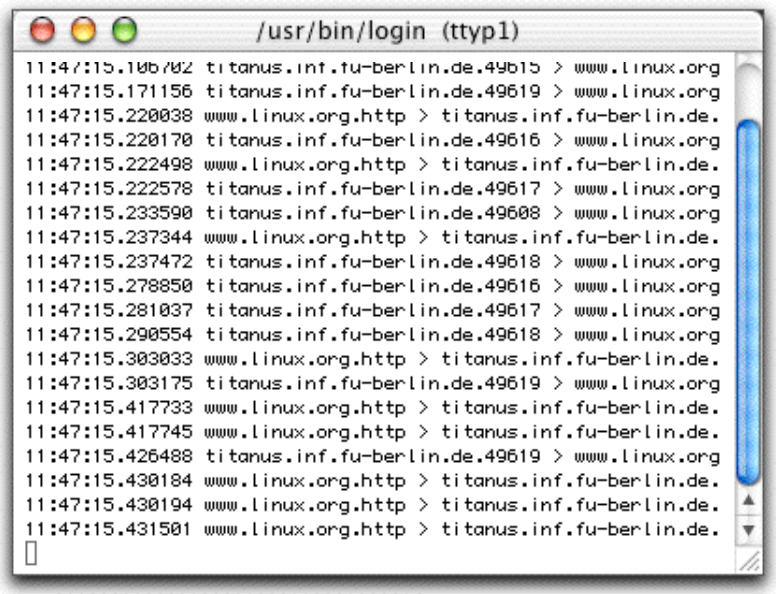
Sniffing-Angriffe: Funktionsweise (Ethernet)

- alle Stationen erhalten alle Datenpakete (im Ethernet)
- lokale Filterfunktion
- Abschalten des Filters möglich: **»promiscuous mode«**
- Sniffing im Switched Ethernet erschwert



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



Sniffing-Angriffe: Vorgehen

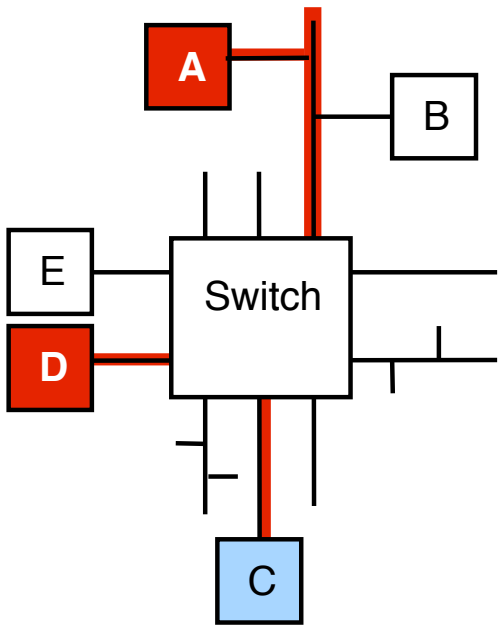
- 3. Schritt – Auswertung des Datenteils
  - Im Beispiel ASCII-Textdarstellung eines Ethernet-Datenpaketes gewählt (Punkte stehen für Steuerzeichen)

```
....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.0.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......@@
```

Spoofing-Angriffe: Funktionsweise (Ethernet)

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

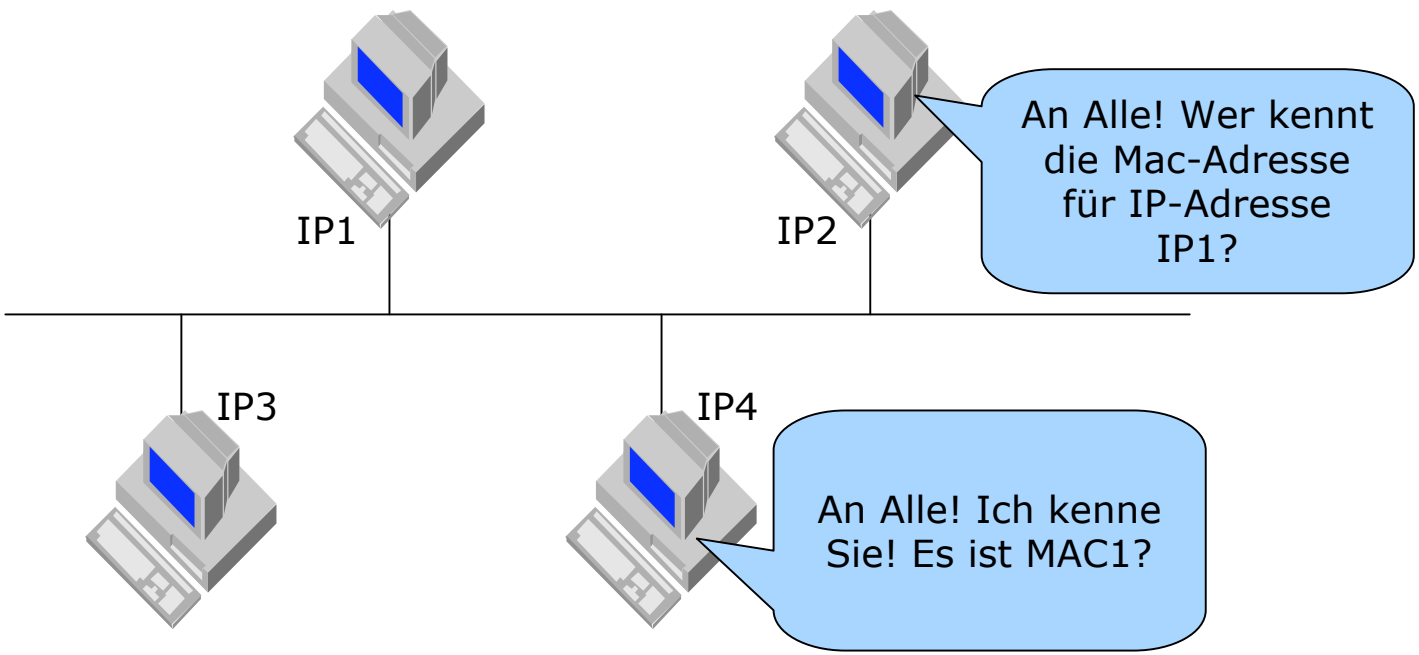
b) im Switched Ethernet



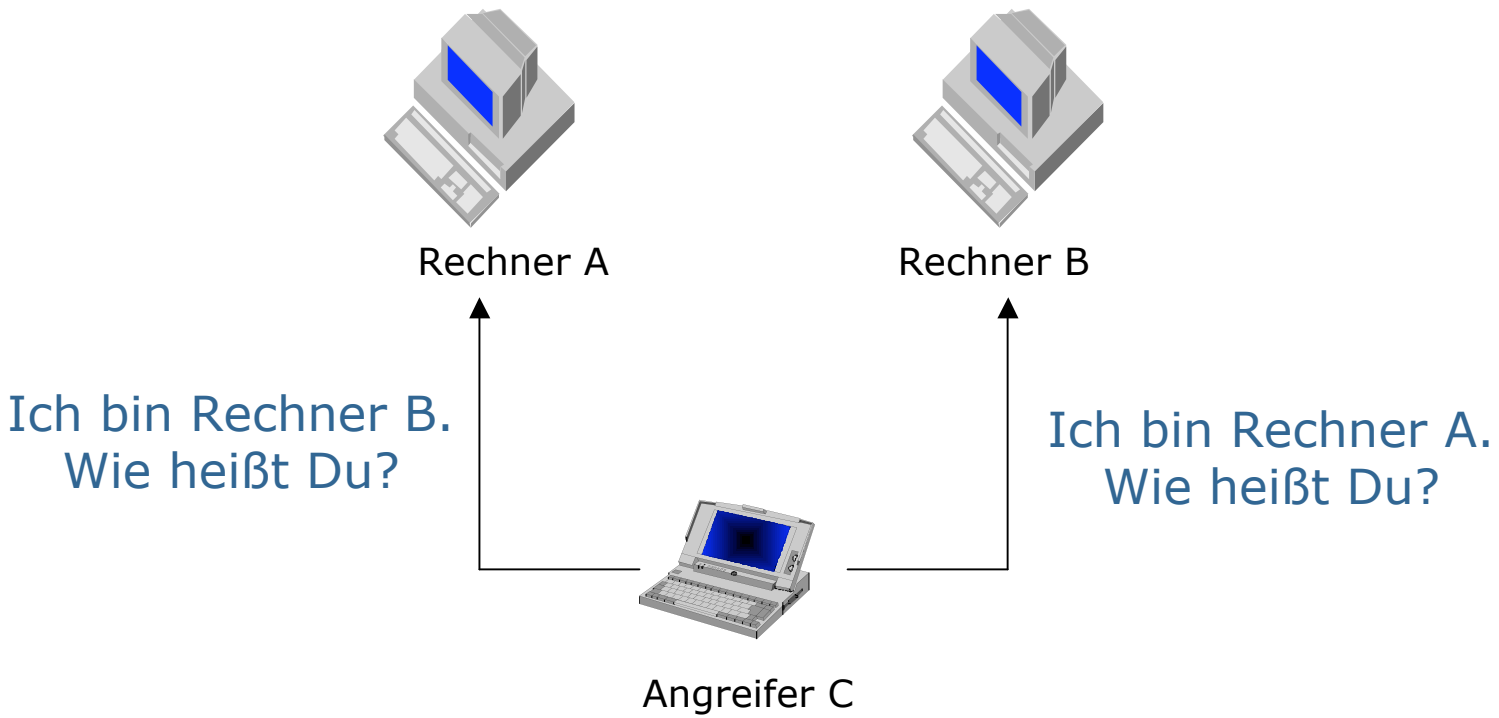
C greift an

ARP: Address Resolution Protocol

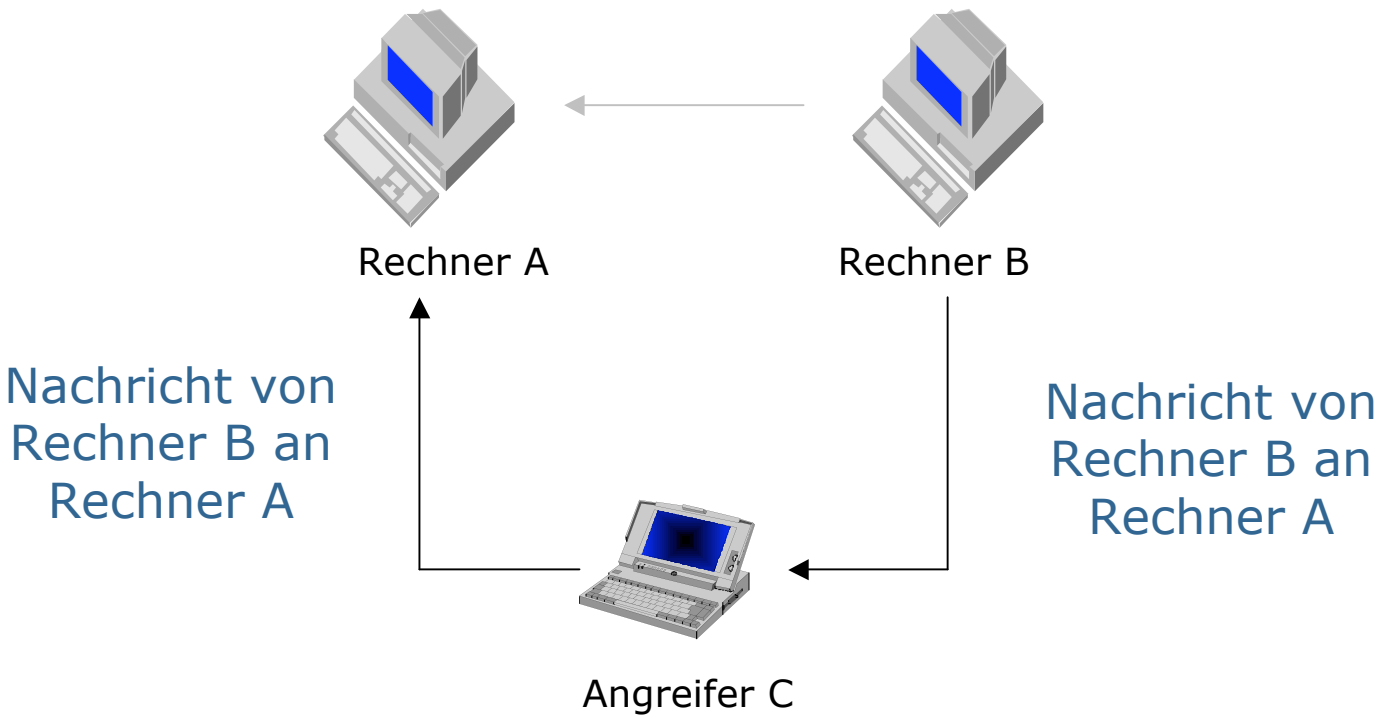
- ARP-Anfrage
  - Anfrage wird an das gesamte lokale Netz gestellt (Broadcast)
  - Mitteilen der eigenen Adresse(n) in der Anfrage
- ARP-Antwort
  - Jeder Rechner, der die Zuordnung kennt, kann antworten



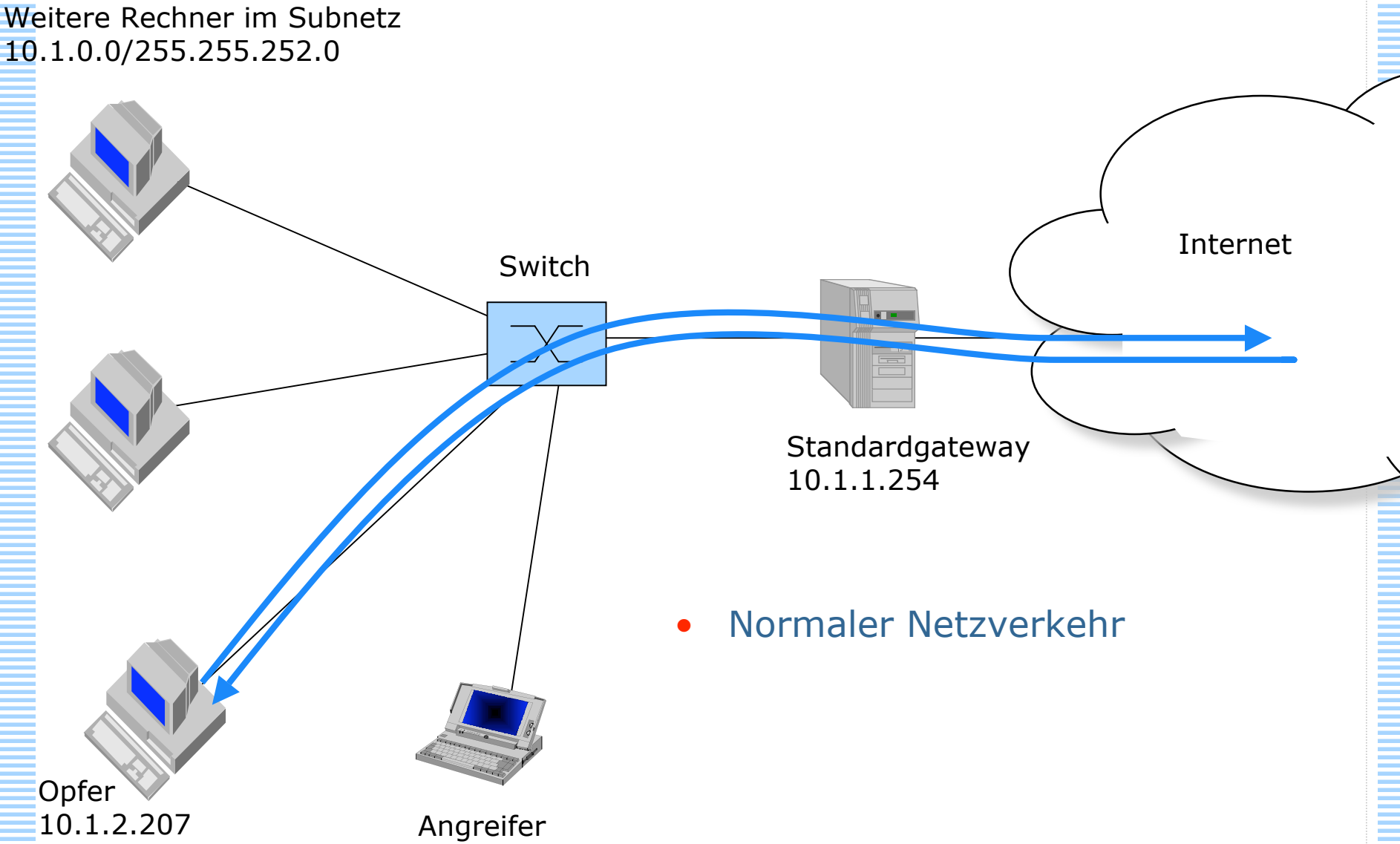
> ARP-Spoofing



>> ARP-Spoofing



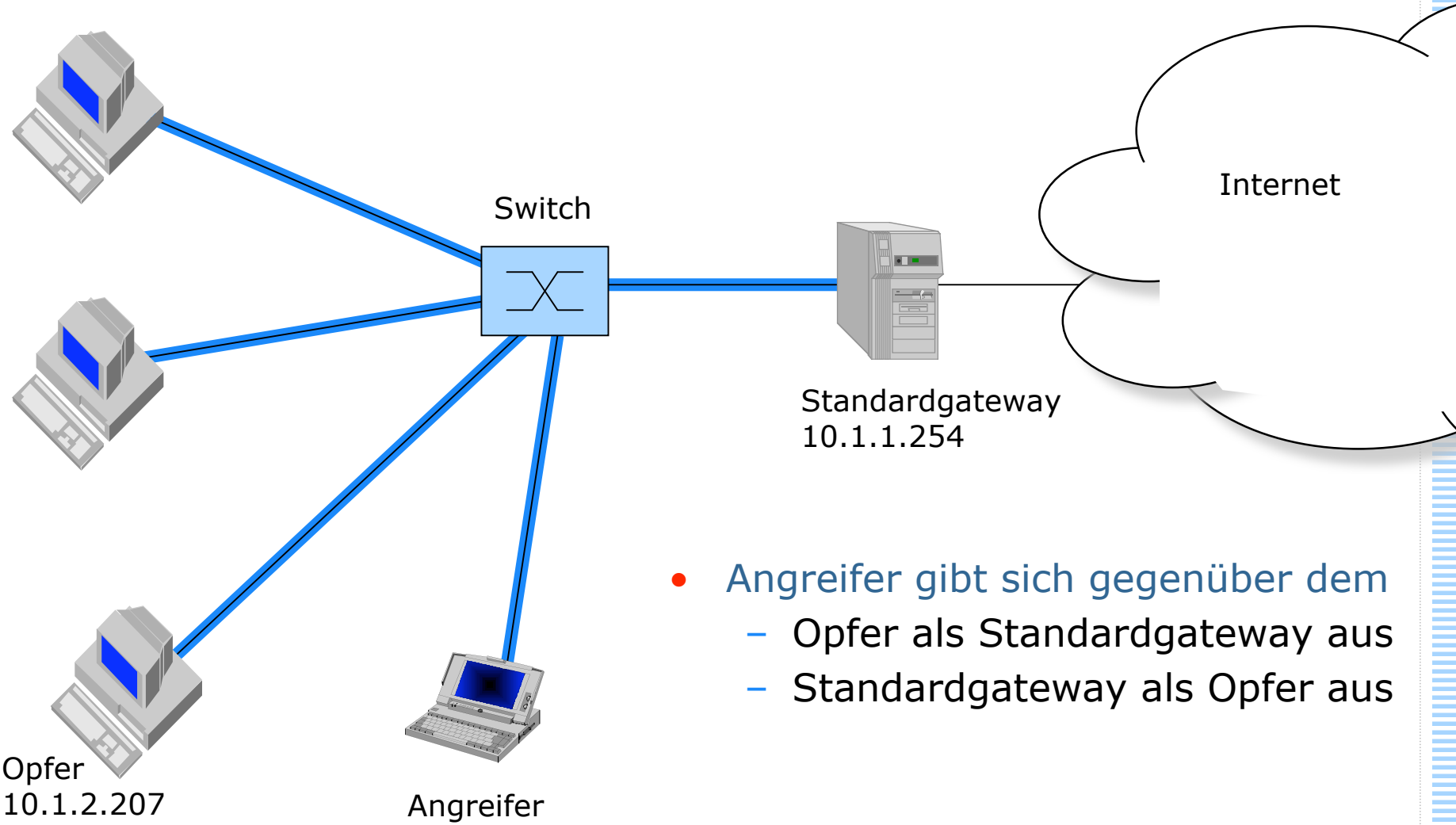
Netzwerktopologie ARP-Spoofing-Demonstration



- Normaler Netzverkehr

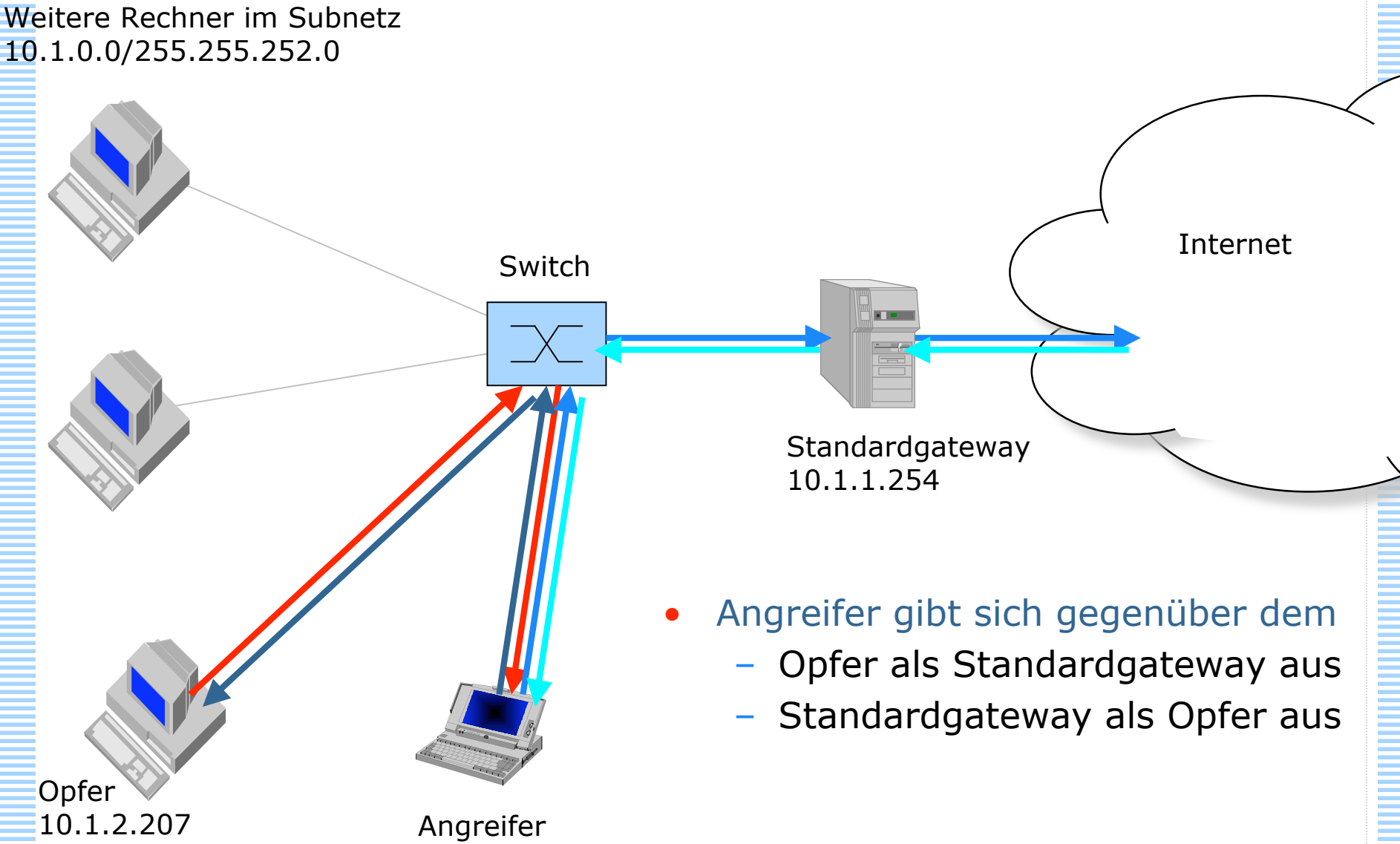
ARP-Spoofing: Vorbereitung

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: Opfer will IP-Paket ins Internet senden



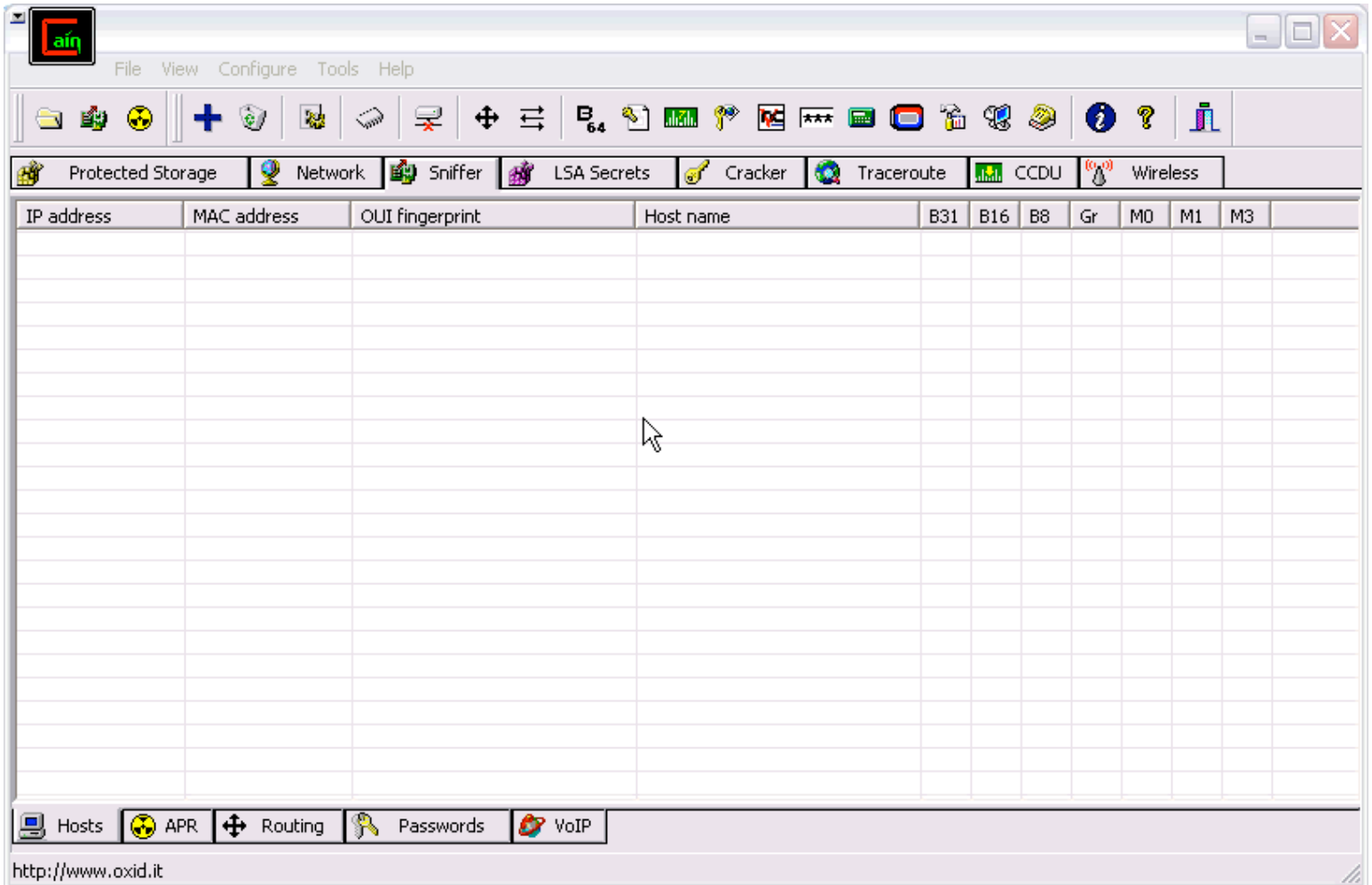
- Angreifer gibt sich gegenüber dem
  - Opfer als Standardgateway aus
  - Standardgateway als Opfer aus

ARP-Spoofing

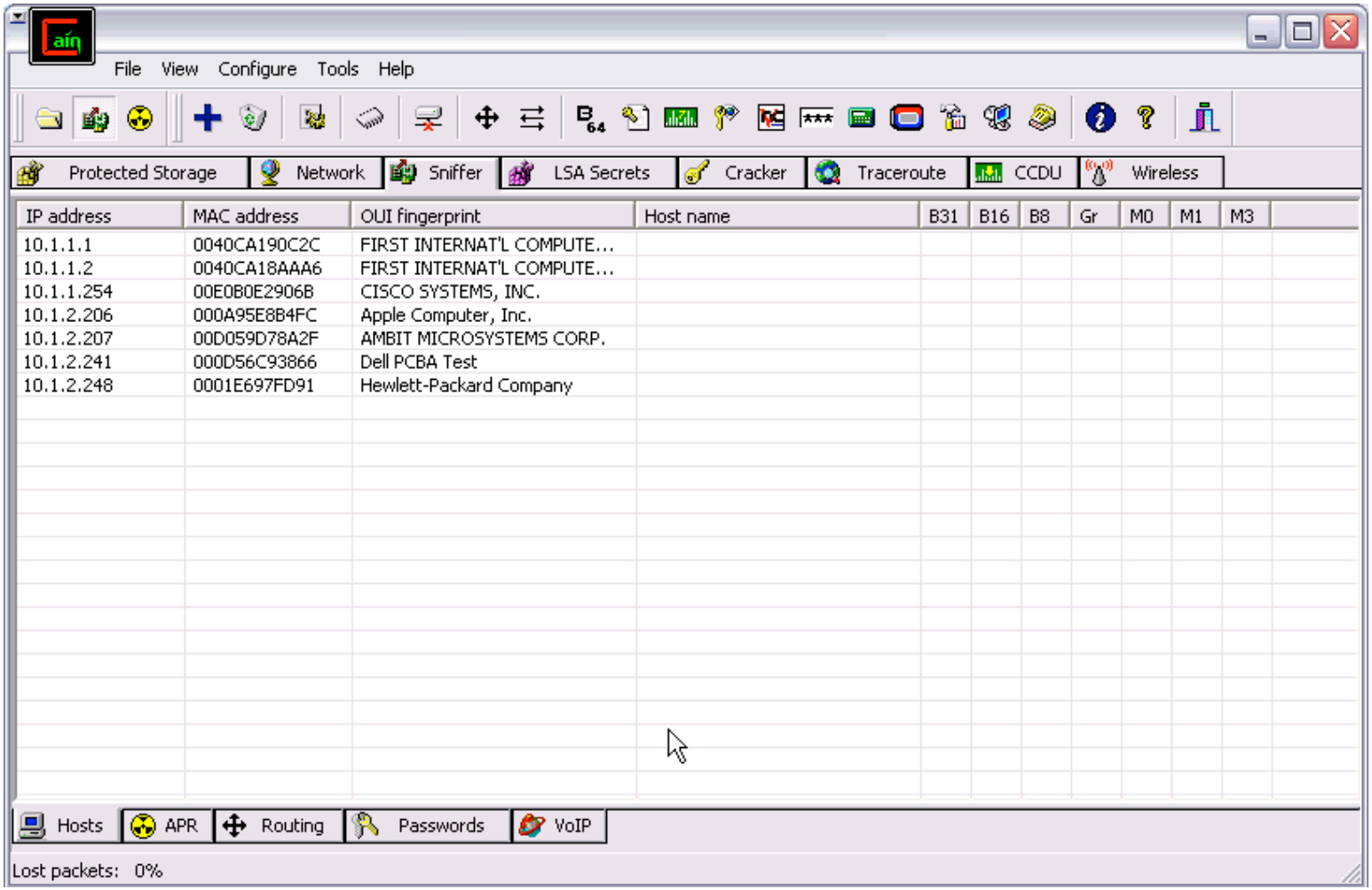
- Angreifer
  - empfängt den gesamten Netzwerkverkehr
    - vom Opfer zum Internet
    - vom Internet zum Opfer
  - kann diese Datenpakete beliebig manipulieren

- 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

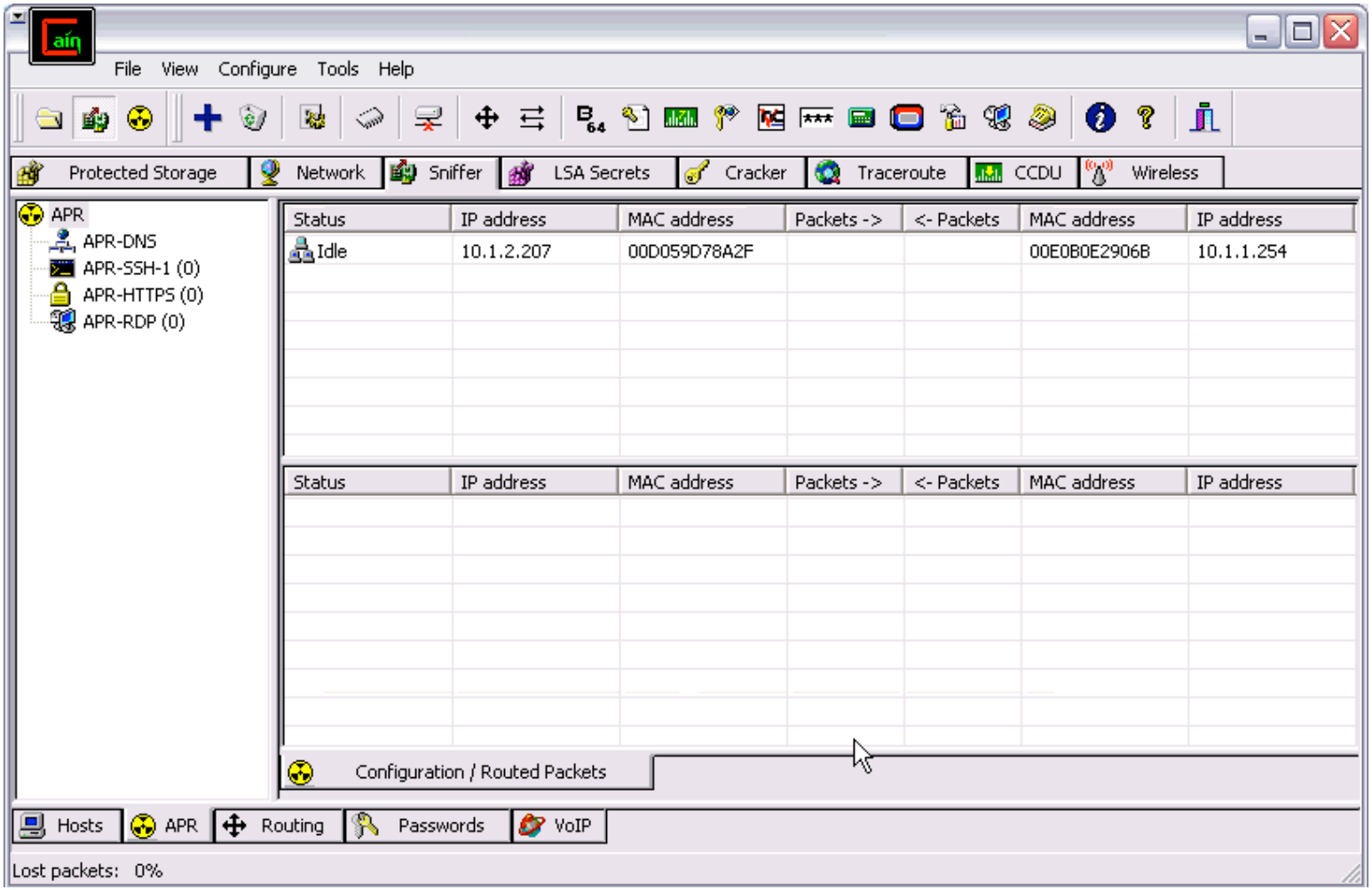
Rechner im Netzwerk identifizieren



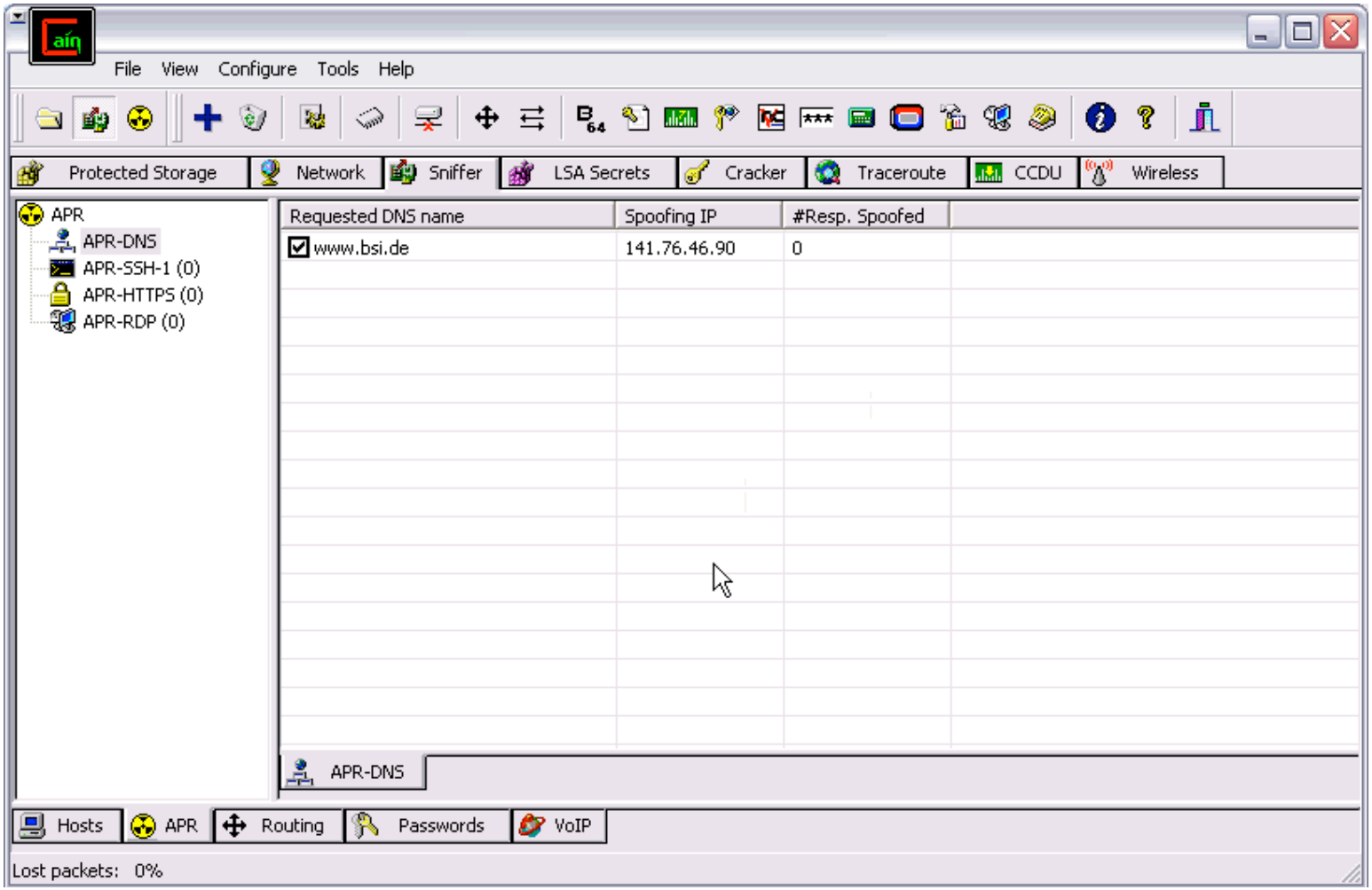
Auswahl der Rechner für das ARP-Spoofing



Einrichten des DNS-Spoofing

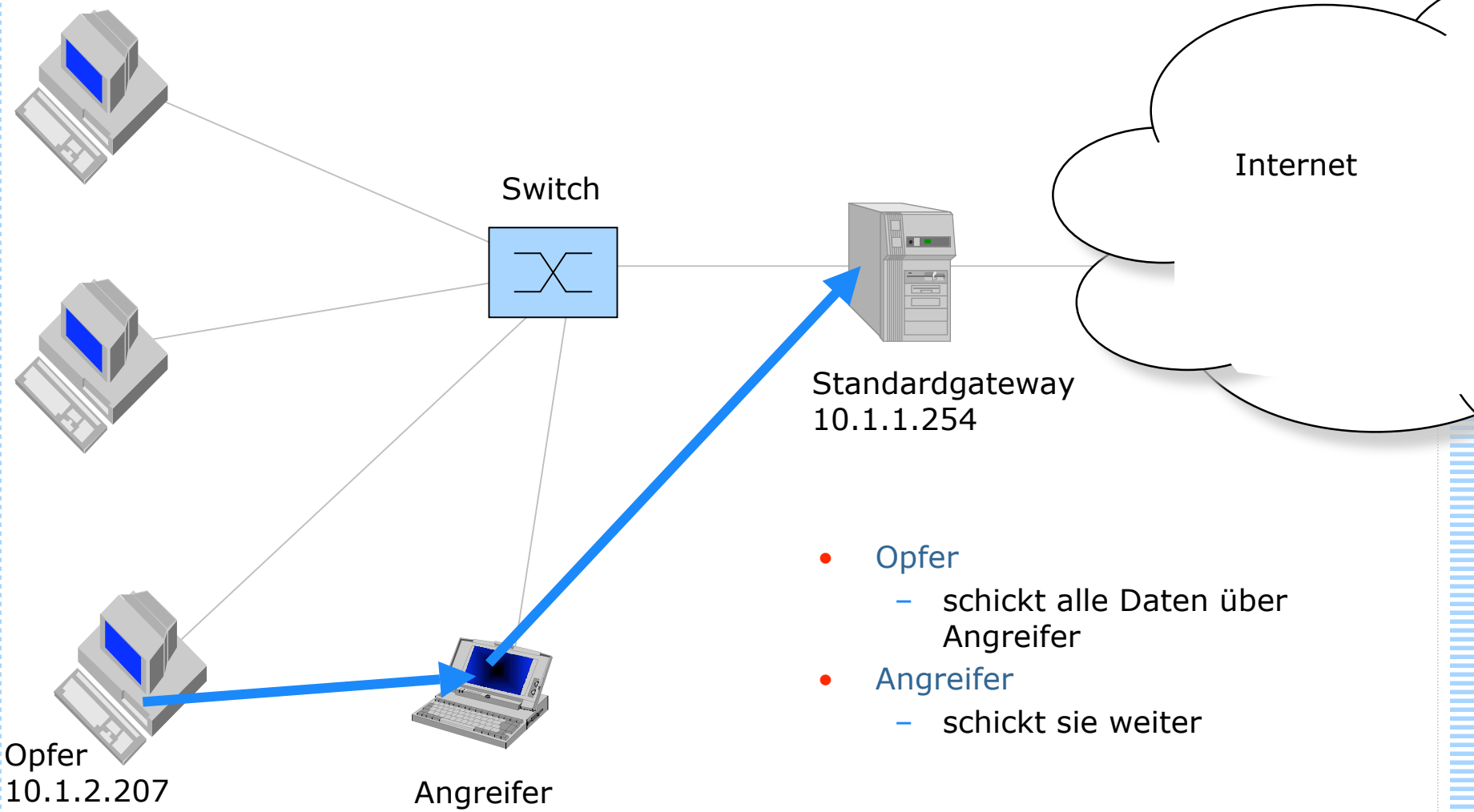


Start des ARP- und DNS-Spoofings



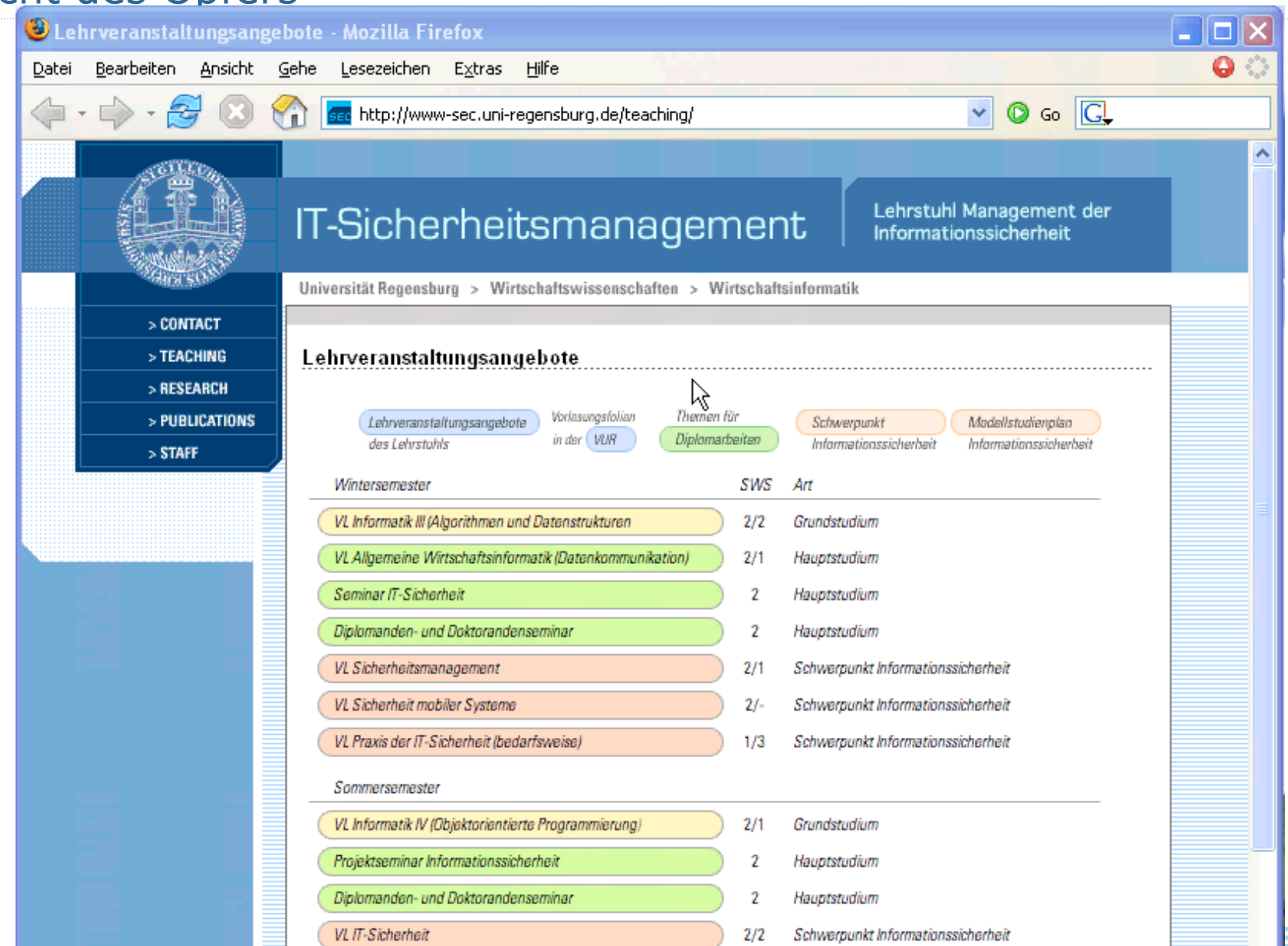
Erreichte Situation

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0

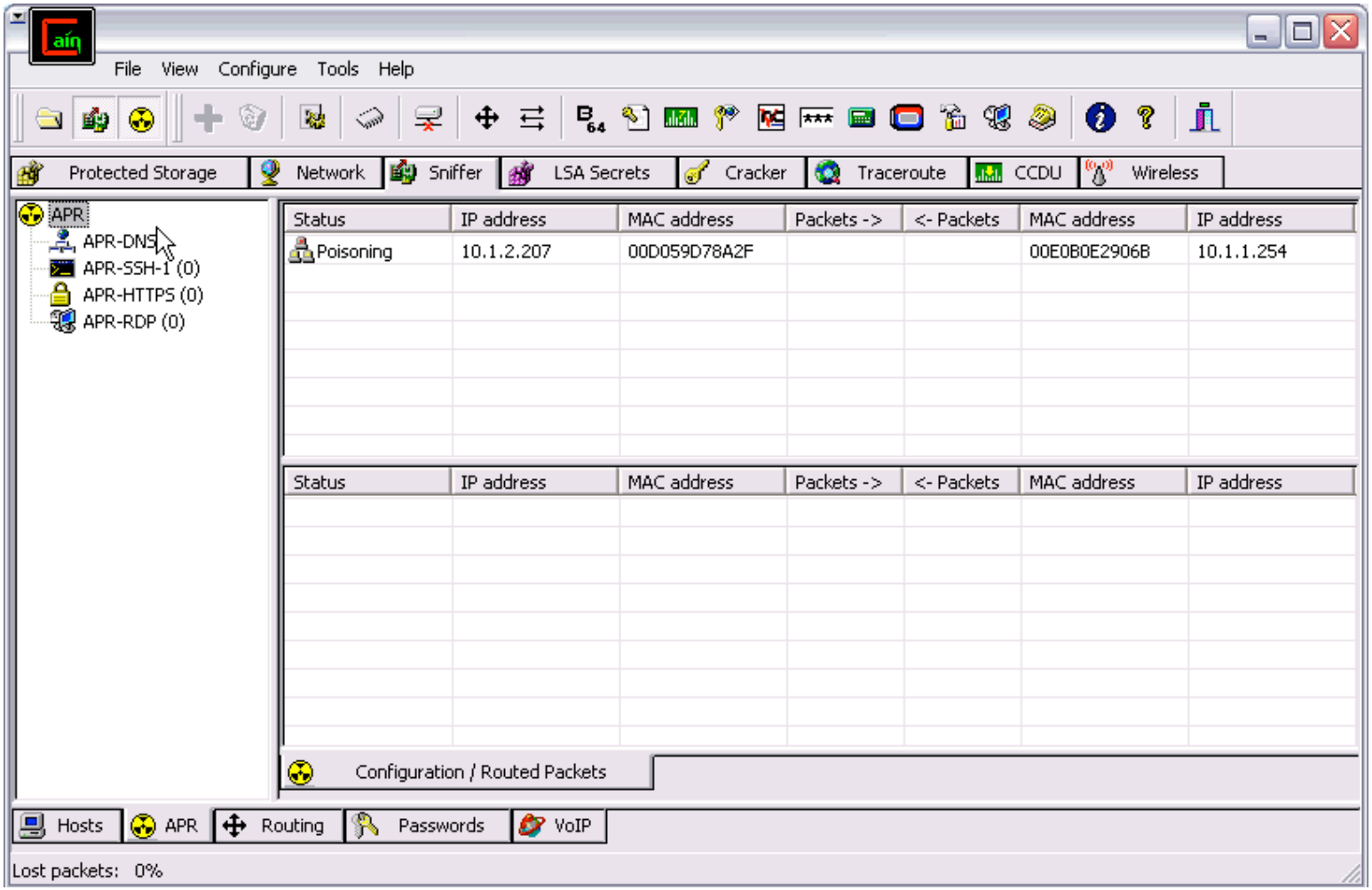


- Opfer
  - schickt alle Daten über Angreifer
- Angreifer
  - schickt sie weiter

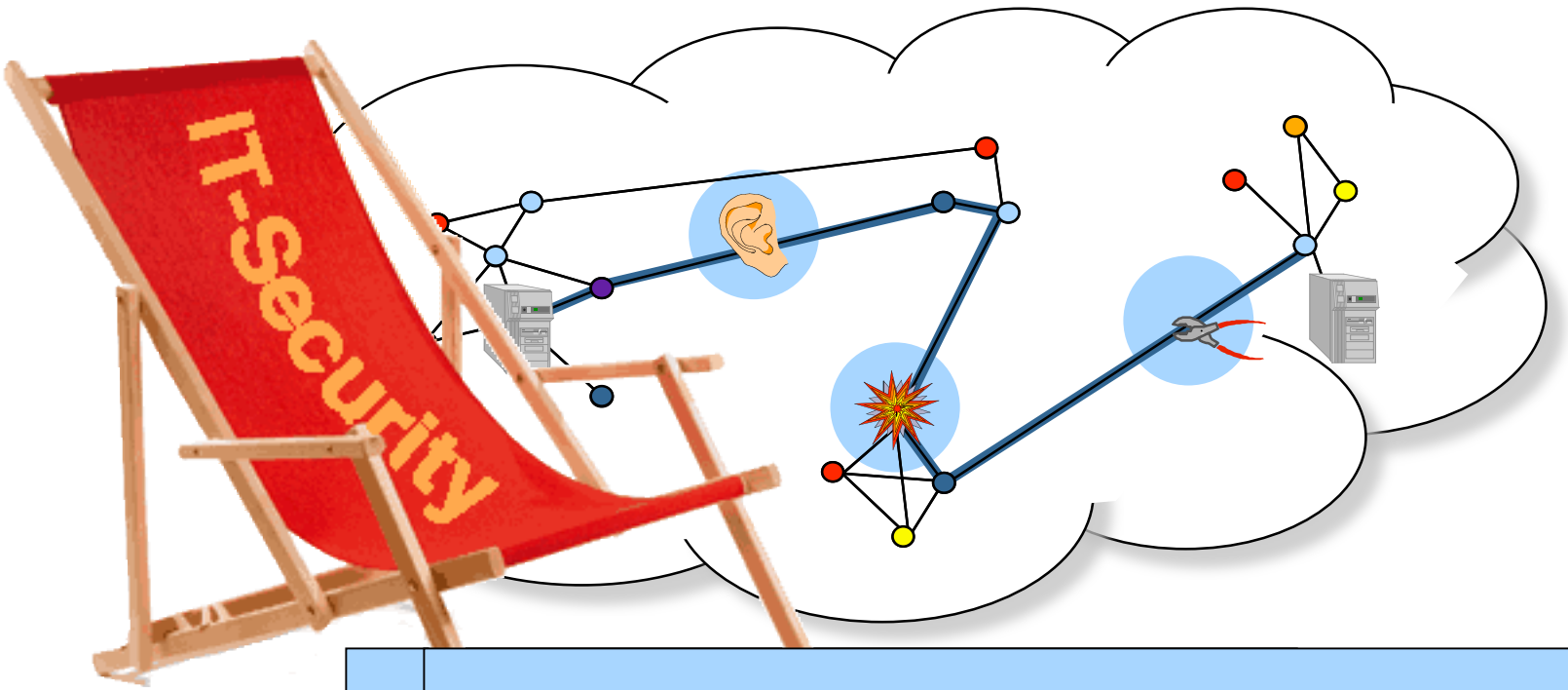
Sicht des Opfers



Sicht des Angreifers



Abwehr



V:	Offene Systeme, Diversität, Berechtigungskonzepte
P:	Kryptographie, insb. PKI
S:	Kryptographie, insb. Verschlüsselung