„Wie man das Internet abschaltet“

Ingo Blechschmidt
<iblech@web.de>

LUGA

2. November 2005

Rekapitulation: Domainnamen

Eingabe im Browser:

`http://www.pugscode.org/`

Auflösung übers Domain Name System (DNS)

3.141.592.6535

TCP-Verbindung

HTTP-Request

Aber: Wie Verbindung nach außen?

„Router wird's schon wissen“

Aber: Wie zum Router kommen?

Über seine IP-Adresse?

Problem: Netzwerkkarten kennen nicht IP

Stattdessen: MAC-Adressen

Jede Karte hat eine eindeutige MAC-Adresse

Live-Demo

Wir wollen zum Router

Aber wir kennen seine MAC noch nicht

Abhilfe: Address Resolution Protocol (ARP)

Also Broadcast
ins gesamte LAN:
„Wer die IP a.b.c.d hat,
bitte bei mir mit seiner
MAC melden, danke“

„Ja hi, ich hab' die `a.b.c.d`;

meine MAC ist `aa:bb:cc:dd:ee:ff`“

Effizienz?

ARP-Cache

Temporäre Speicherung der Zuordnung IP $\leftrightarrow$ MAC

Live-Demo

„Wie man das Internet abschaltet“

Einschub: Hubs

Weiterleitung des Eingangs zu allen Ausgängen

Auch unbeteiligte Rechner erhalten den Traffic

Effizienz...?

Sicherheit...?

Besser: Switches

Erinnerung der Zuordnung MAC $\leftrightarrow$ Port

Nur Weiterleitung an Ziel-Port; Erkennung an Ziel-MAC

„Wie man das Internet abschaltet“

Einschub:
„Wie man einen Switch zum Hub macht“

Einfacher als man vermuten könnte

Überflutung mit vielen ARP-Replys

. . . mit so vielen Paketen,

dass die Tabelle

des Switches

überfüllt wird

$\longrightarrow$ Verlust der Zuordnung MAC $\longleftrightarrow$ Port

→ Umschalten in Hub-Modus

„Wie man das Internet abschaltet“

Einfacher als man vermuten könnte

Szenario: Router-IP ist 192.168.0.1

„Hört mal alle her,

die MAC von `192.168.0.1` ist

`de:ad:be:ef:13:37`!“

de:ad:be:ef:13:37

gibt es aber gar nicht

Aber: blindes Vertrauen!

„Ok, wenn du das sagst, wird's schon stimmen“

Zukünftige Pakete an den Router gehen nun zu `de:ad:be:ef:13:37`

Also nach /dev/null

Ziel-Adresse des ARP-Spoofs beliebig wählbar;

Ausschalten des Internets. . .

. . . für alle Rechner

Ausschalten des Internets. . .

. . . für einige ausgewählte

Aber natürlich
nur innerhalb
eines lokalen Netzes!

Live-Demo

Geht noch besser

Umleitung des Traffics zum Router zum eigenen Rechner

„Hört mal alle her,

die MAC von `192.168.0.1` ist

MAC des Angreifers“

Client → Angreifer → Router → Internet

$\rightarrow$ Problemloses Mitschneiden des gesamten Traffics zum Internet!

Weitere Idee:
Umleitung
des Traffics
zu einem Terabit-Router
zu einem 10 MBit-Rechner

$\rightarrow$ Kein Internet-Zugang mehr

$\rightarrow$ Blockierung des 10 MBit-Rechners

Gegenmaßnahmen

Statische ARP-Einträge

„192.168.0.1 hat *immer* die MAC aa:bb:cc:dd:ee:ff“

```
# arp -s \
    192.168.0.1 \
    aa:bb:cc:dd:ee:ff
```

umständlich

großes LAN?

neuer Computer?

neue Netzwerkkarte?

Überwachung des Traffics und Alarm bei unbekannter MAC

ebenfalls umständlich

Lösung:

IPv6 mit IPsec

Schutz durch starke Verschlüsselung

Fragen?

Danke!