IT Security Workshop 2014

DANE für den Instituts-Mailserver

Christoph D. und Sven S.

Institut für Informatik der Humboldt-Universität zu Berlin

02.10.2014

CA Hack

Über 500 Zertifikate: Ausmaß des CA-Hacks schlimmer als erwartet

- digiNotar kompromittiert
- google.com, addons.mozilla.org, torproject.org, microsoft.com, windowsupdate.com, skype.com, facebook.com, ...
- Die Mozilla-Entwickler kritisieren [...]: "Die Statements, die DigiNotar und der Mutterkonzern VASCO über das Ausmaß und die Auswirkungen der Kompromittierung gemacht haben, waren bestenfalls unvollständig und schlimmstenfalls bewusst irreführend."

Quelle: `http://heise.de/-1336603`

Bisherige Ansätze

- PKIX
- in Verbindung mit DNS
- Keypinning

Unzulänglichkeiten

- Zuständigkeit CA
- schwache Bindung Common Name (CN) zu IP-Adresse
- Vertrauensmodell (CA)
- bootstrapping (CA-Listen)

DANE kurzgefasst

Was ist eigentlich DANE?

öffentliche Schlüssel im Domain Name System

$\Rightarrow$ erfordert Authentizität der DNS-Antworten

Records (RR)

- A
- NS
- MX
- AAAA
- ...

Beispiel DNS-Zone

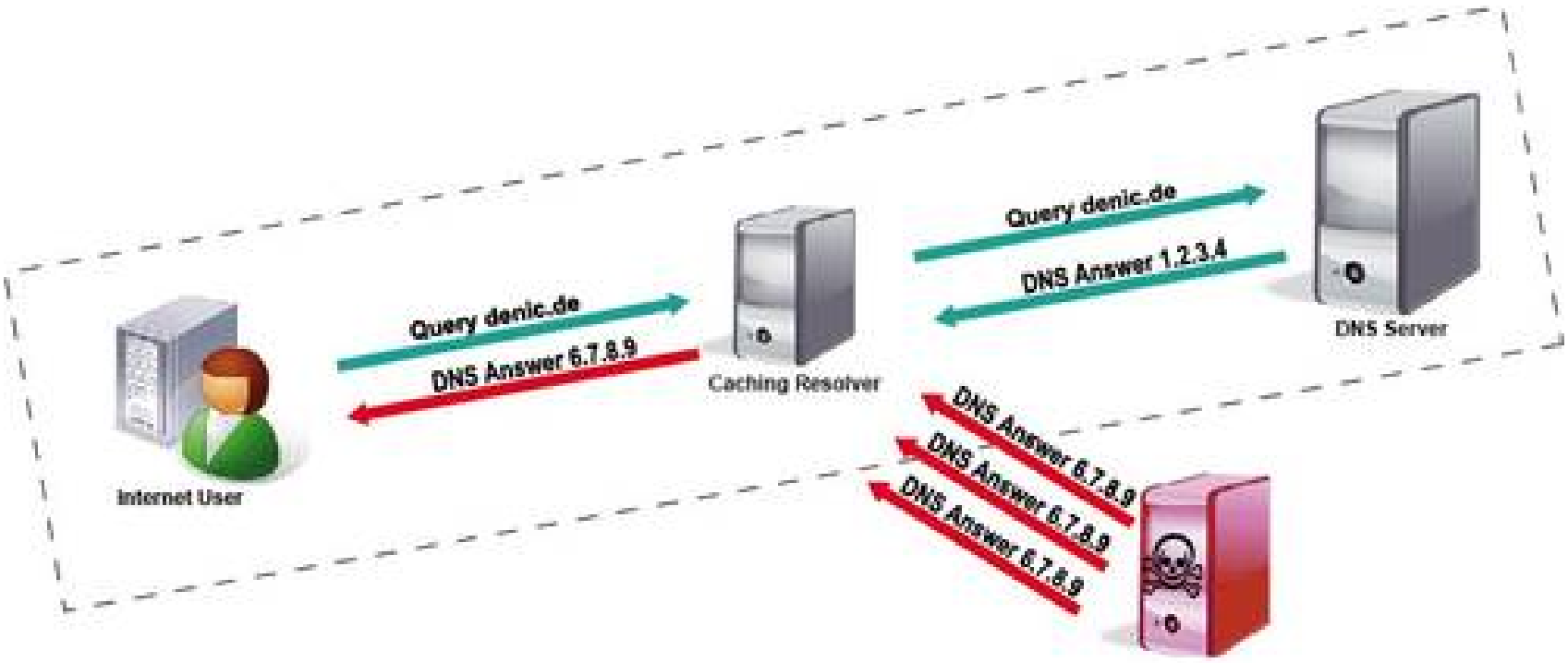
```
itsec. IN SOA itsec.nic. itsec.nic. (
                2014093009 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                1209600    ; expire (2 weeks)
                7200       ; minimum (2 hours)
)

itsec.          NS      itsec.nic.
mail.itsec.     A       141.20.20.131
```

Sicherheitsversprechen von DNS

Angriffsvektoren auf DNS

- DNS Cache-Poisoning (eventual consistency)
- bösartige DNS-Server (Administratoren)
- ungesicherte Übertragung (MITM-anfällig)

DNS Cache-Poisoning



DNS unzureichend ⇒ DNSSEC

- zusätzliche RRs, dadurch DNS kompatibel
  - RRSIG
  - DNSKEY
  - DS
- 15.07.2010 Rootzone signiert (`http://heise.de/-1039401`)
- seit Mai 2011 .de (`http://denic.de/domains/dnssec.html`)

Vertrauensmodell

1. die ICANN in Verbindung mit VeriSign signiert die Rootzone
2. Vertrauen gegenüber jeder übergeordneten Zone in der Hierarchie (z.B. DENIC für TLD .de)

Beispiel DNSSEC-Zone

```
$ less zonefile.signed
```

Zugewinn durch DNSSEC

Validierbarkeit der Auflösung/Zuordnung Name $\rightarrow$ IP-Adresse

DANE im DNS

```
_PORT._PROTO.domain.tld.  TLSA  x  y  z  WERT
```

- x Usage Field
- y Selector Field
- z Matching-Type Field
- WERT sha256 || sha512 || x509

```
_25._tcp.mail.itsec.  TLSA  3  0  1  8107bd7c...
```

DANE im DNS

```
_PORT._PROTO.domain.tld.  TLSA  x  y  z  WERT
```

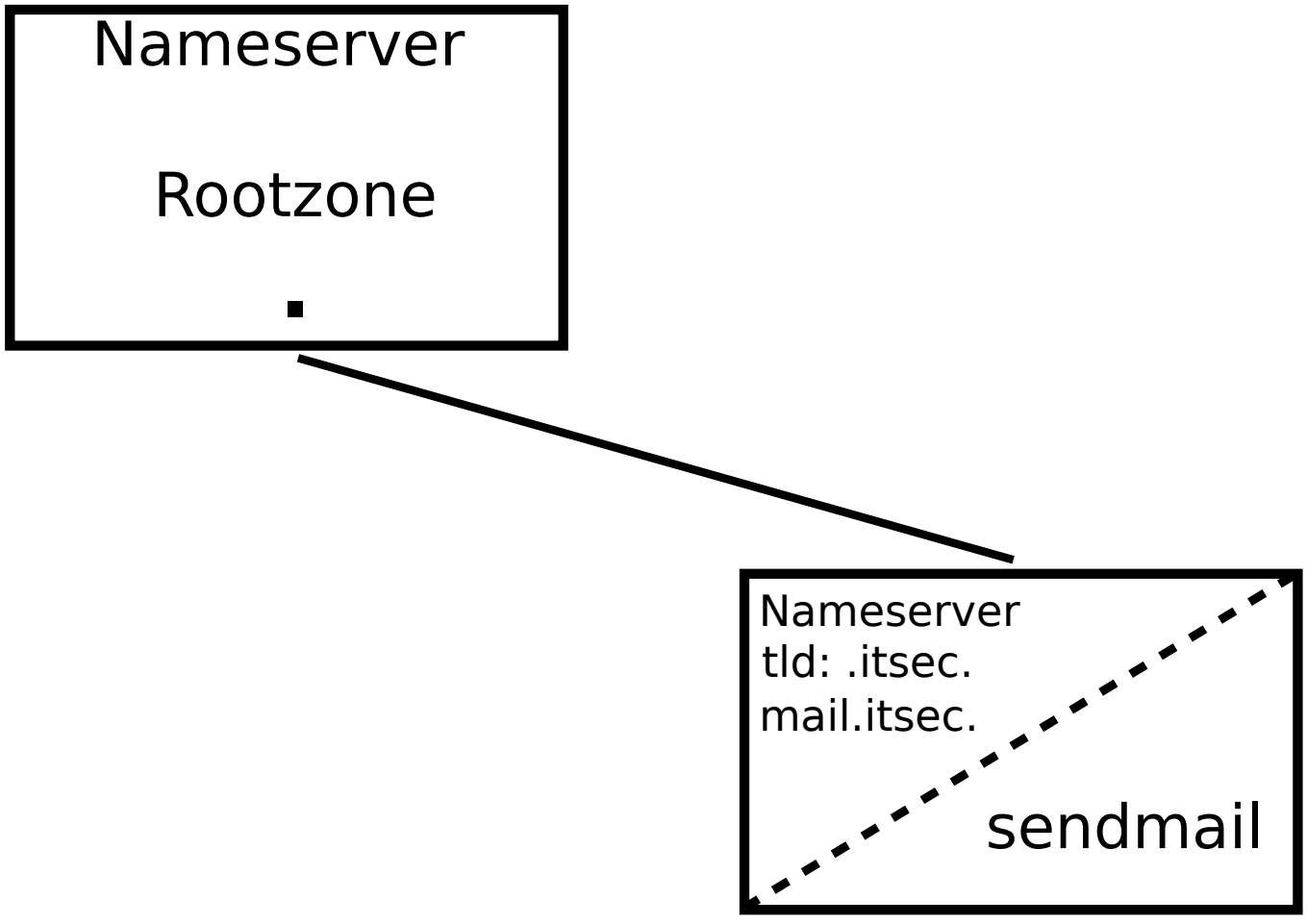
- x Usage Field
- y Selector Field
- z Matching-Type Field
- WERT sha256 || sha512 || x509

```
_25._tcp.mail.itsec.  TLSA  3  0  1  8107bd7c...
```

"TLSA" does not stand for anything; it is just the name of the RRtype. (RFC 6698 p. 4)

- Usage Field
  - 0 einschränken auf CA (PKIX)
  - 1 einschränken auf Zertifikat (PKIX)
  - 2 Vertrauensanker verwenden
  - 3 Zertifikat nutzen
- Selector Field
  - 0 ganzes Zertifikat
  - 1 öffentlicher Schlüssel
- Matching-Type Field
  - 0 ungehashter Selector
  - 1 sha256
  - 2 sha512

Versuchsaufbau – Solariszonen



Konzeptuelle Schritte

- named/BIND einrichten (DNS)
- Rootzone anlegen
- DNSSEC einrichten
  - Schlüssel generieren
  - Zonen signieren
  - Zonen delegieren
- DANE einrichten (TLSA RR)
- sendmail einrichten

- DANE in Programmen/Resolvern verwenden
- Wartung (Zonen regelmäßig neusignieren, sowie bei Bedarf) $\rightarrow$ CMS

Fazit

- serverseitige Unterstützung nicht immer notwendig
- Softwareunterstützung noch eingeschränkt (sendmail, Endanwender)
- Tools zur Einrichtung/Wartung vorhanden vorhanden und überwiegend komfortabel nutzbar

Fallstricke:

- sendmail
- dig, gnutls/**danetool** (oft ohne DNSSEC-Unterstützung)
- Solaris (Konfigurationsdatenbank)

FRAGEN!

HowTo kommt ins Wiki

Quellen

- RFC 6698
- `http://www.denic.de/domains/dnssec.html`