Barcamp Mitteldeutschland

DNSSEC – Vertrauen ins DNS

Lutz Donnerhacke

```
dig NAPTR 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa. +dnssec
```

Domain Name System

- Verteilte Datenbank **öffentlicher** Daten
- Effiziente Abfrage durch *hierarchische Gliederung* und starken Einsatz von *Caches*
- Ausfallsicher durch *Secondaries*
- System ist sehr robust und skalierbar
- Vorwärts: Namen nach Daten (IPs)
- Rückwärts: Namen (IPs) nach Daten (Namen)

Angriffe auf DNS

- MitM: Pakete abfangen und ändern
- ID-Raten: Schneller andere Anworten schicken
- Poisioning: Falsche Antworten cachen lassen
- Letzte Meile: MitM zum dummen Client
- DoS: Vorspieglung der Nichtexistenz
- Wildcards: Vorspieglung der Existenz
- Redirects: Falsche Server konfigurieren

→ ca. 10 bis 30% der Server angreifbar

DNS Security

- Klassische Publickey Signaturen: RRSIG
- Signaturen der Nichtexistenz: NSEC*3*
- Signaturen der Wildcards: extra RRSIG
- Einbettung der Schlüssel: DNSKEY
- Zertifikate entlang der Hierarchie: DS
- Zertifikate außerhalb der Hierarchie: DLV
- Updates an Server: TSig und SIG(0)
- Extra Bits zur Abfrage, Validiertheit, Unchecked

DNSSEC – Fallen

- Signaturen laufen aus
- Seriennummer muß automatisch erhöht werden
- Schlüssel werden kompromittiert
- Datenpakete werden zu groß
- Zeitsynchonisation nötig
- Zonewalking
- Schlüsselwechsel der Startpunkte

DNSSEC – Kompromiß

- Einsatz validierender rekursiver Resolver
- Stub-Resolver der letzten Meile bekommen nur validierte Angaben, bei Fehlern gar keine mehr
- Sicherheit auf der letzte Meile zwingend nötig
- Damit: Aufbrechen des Ende-Ende-Prinzips
- Intelligentere Resolver können aber unvalidierte Daten anfordern

DNSSEC – Verbreitung

- Derzeit ca. 2000 signierte Domains
- Signierte TLDs: bg, br, pr, se, se, um, (fr, ru, .)
- Top: 717 ru, 290 arpa, 233 de, 166 com
- Hier auf dem Barcamp:
  - DNSSEC signierte Root im Einsatz
  - Validierende rekursive Resolver
  - Vor allem die Rückwärtsauflösung ist validierbar

DNSSEC – Cool Stuff

- SSH Fingerprints
- X.509 – Zertifikate
- IPSec – Public Keys
- OpenPGP – Public Keys
- VoIP: e164.arpa ist signiert
- Effektiveres Caching: Beweis der Nichtexistenz
- Schutz vor Pharming Angriffe

DNSSEC – Vertrauen bilden

Können Sie sich falsche Adressbücher leisten?

Fragen!