Domain Spotlight 2008

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 antworten
- Poisioning: Falsche Antworten cachen lassen
- Letzte Meile: MitM zum dummen Client
- DoS: Vorspiegelung der Nichtexistenz
- Wildcards: Vorspiegelung der Existenz
- Redirects: Falsche Server konfigurieren

→ ca. 30% der Server angreifbar

DNS Security

- Klassische Public-Key Signaturen: RRSIG
- Signaturen der Nichtexistenz: NSEC*3*
- Signaturen der Wildcards: extra RRSIG
- Verteilung der Schlüssel: DNSKEY
- Zertifikate entlang der Hierarchie: DS
- Zertifikate außerhalb der Hierarchie: DLV
- Updates an Server: TSig und SIG(0)
- Bits zur Abfrage, Korrektheit, Eigenprüfung

Cool Stuff

- SSH – Zentraladministration statt known_hosts
- SSL/HTTPS – Zertifikate kostenfrei statt CAs
- VPN/IPSec – Public Keys aktuell halten
- OpenPGP – Public Keys aktuell halten
- VoIP – e164.arpa ist signiert
- Spamschutz – Domainkeys, SPF etc. validierbar
- Schutz vor Pharming, Poisoning – Haftung?

Maintainance – Tägliche Arbeiten

- Signaturen laufen aus: Nächtlich neu signieren
- Seriennummer muß *automatisch* erhöht werden
- Notfallplan: kompromittierte Schlüssel
- Datenpakete werden zu groß: EDNS0, Firewalls
- Zeitsynchonisation nötig
- Zonewalking: Sind Ihre Zonen *so* öffentlich?
- Regelmäßige Schlüsselwechsel: DS aktualisieren

Validierung als Kompromiß

- Einsatz validierender rekursiver Resolver
- Stub-Resolver der letzten Meile bekommen nur korrekt validierte Angaben oder SERVFAIL
- Sicherheit auf der letzte Meile zwingend nötig

➔ Aufbrechen des Ende-Ende-Prinzips

- Intelligentere Resolver können aber unvalidierte Daten anfordern und selbst validieren

DNSSEC – Verbreitung

- Derzeit ca. 2500 signierte Domains
- Signierte TLDs: bg, br, cz, pr, se, (org, fr, ru, at)
- Top: 672 ru, 316 br, 310 arpa, 262 de, 220 com
- Produktiv vorhanden:
  - DNSSEC signierte Root von IKS (IANA 2009)
  - DLVs von IKS und ISC
  - Vor allem die Rückwärtsauflösung ist validierbar

Outsourcing

- Umstellung ist zeit- und kostenintensiv
  - Tool chains und Hardware anpassen oder austauschen
  - Admins, Hotline und Vertrieb schulen
  - Organisiationprozesse anpassen
- Outsourcing gewinnt Zeit, ist kein Dauerzustand
  - Hidden primary Konzept: Extern bleibt alles gleich
  - Zonen Konzept: Intern bleibt alles gleich
  - Aktualisierung der DS möglich (Autorisierung)
  - QoS: Maximale Verzögerung, Livesignierung

DNSSEC – Vertrauen bilden

Können Sie sich falsche Adressbücher leisten?

Fragen!