Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

DNS and DNSSEC Basics

IT Service Support Team Meeting

Thursday, 16th October 2014 15:00 – 17:00

BFH – Conference Room HAL 9000 (Dammweg 3, Bern)

Daniel Baumann <daniel.baumann@bfh.ch>

IT System Engineer Linux, Team Infrastructure Services

Overview

- **DNS Basics**
- **DNSSEC Basics**
- **Pointers**

DNS Basics

Domain Name System (1/2)

Problem

- Computer can only talk to IP Addresses (e.g. 147.87.250.111)
- Humans like Hostnames (e.g. www.bfh.ch)

Solution

- Phone book for IP Addresses/Hostnames
- Technically: DNS, a hierarchical distributed naming system for computers
- DNS is both a Service and a Protocol (UDP and TCP over port 53)

Domain Name System (2/2)

Structure

- Zone Files
- Resource Records (SOA, A, CNAME, MX, NS, etc.)

- Forward Mapping: Hostnames to IP Addresses (Surjective function; M:1)
- Reverse Mapping: IP Addresses to Hostnames (Bijective function; 1:1)

Implementation

- Regular Lookups via Caching Resolvers (e.g. dd-int1.bfh.ch)
- Recursive Lookups for e.g. bfh.ch

  via Root Servers ([a-m].root-servers.net, see http://root-servers.org),

  via TLD Registry ([a-h].nic.ch, see http://nic.ch),

  to the Authoritative Servers (e.g. ns1.bfh.ch).

- Reverse Lookups via special zone in-addr.arpa.

Practical dig/drill Usage (without DNSSEC)

- Get IP for a specific hostname: **dig www.bfh.ch**
- Get empty answer (NXDOMAIN): **dig a.ch**

- Get start of authority for a zone: **dig soa bfh.ch**
- Get list of authoritative name servers: **dig ns bfh.ch**
- Get mail exchange (MX) records: **dig mx bfh.ch**
- Get entire zone (Zone Transfer): **dig AXFR bfh.ch**

- Show result only: **dig +short bfh.ch**
- Show recursive lookups: **dig +trace bfh.ch**
- Show reverse entry: **dig -x 147.87.250.111**

- Ask different (e.g. Google) nameserver: **dig @8.8.8.8 bfh.ch**

DNSSEC Basics

DNSSEC

Problem

- DNS is insecure
- It is not possible to trust the answering server
- It is not possible to trust the answer received

- Why needed for us? Use DNS as Inventory

Solution

- DNSSEC: Domain Name System Security Extensions
- Asymetric Cryptography with (implicit) Trust Anchor on root server level
- Hierarchically signed (from Root Servers to TLD Registries to individual Authoritative Nameservers)
- Fully backwards compatible by using new, additional ressource records

Resolver: without DNSSEC

- $ dig @localhost switch.ch

```
;; QUESTION SECTION:
;switch.ch.                     IN      A

;; ANSWER SECTION:
switch.ch.              43      IN      A       130.59.108.97
```

Resolver: with DNSSEC (1/2)

- $ dig @localhost DNSKEY switch.ch

```
;; QUESTION SECTION:
;switch.ch.                     IN      DNSKEY

;; ANSWER SECTION:
switch.ch.              30022 IN      DNSKEY      256 3 8 AwEAAcNwge48Ga2wqRG273f/ocGQNclX[...]
switch.ch.              30022 IN      DNSKEY      257 3 8 AwEAAdXUSV5o2+FVpyI+oXxaCfiqXmou[...]
switch.ch.              30022 IN      DNSKEY      256 3 8 AwEAAavDtKXSjChbdDr7PlZO+ZtGIfusH9[...]
```

Resolver: with DNSSEC (2/2)

- $ dig @localhost +dnssec switch.ch

```
;; QUESTION SECTION:
;switch.ch.                     IN      A

;; ANSWER SECTION:
switch.ch.              43      IN      A       130.59.108.97
switch.ch.              57      IN      RRSIG A 8 2 60 20140928094602 20140901040525 56796 switch.ch.
XCSoIaA36+pial71UtCZBPbM6vDE3AL8dUzcdY0fBfyAsXhmT4k7XLBc
rmFJy+ViUi/j69ScEOhIDqlaw/BZ53XgalB50q75Yd6aMwERIBjUcW+x
aXbc55RPinxp084SLsX1seB8on4sI88sPIDcdpsW+VgagTwYV1s8JbmS Xug=
```

DNSSEC Information for BFH

- IT Infrastructure Meeting with a **more technical Introduction and Procedures** to DNSSEC on 2014-10-22 (13:30, Room HAL 9000, Dammweg)
- **Temporary** enabling DNSSEC during Maintenance Window (tentative: 2014-10-22 or 2014-10-29)
- **Definitive** enabling DNSSEC on 2014-11-01

- **If DNSSEC fails, you get NXDOMAIN – aka „the website is down“**

- Full DNSSEC-enabled Recursive Name Resolution on all „new“ Linux Servers,

  see https://linux.bfh.ch/servers/

- Full DNSSEC-enabled Recursive Name Resolution on all BFH Linux Standard Desktops

  (availability on 2014-11-13, presentation in Biel, see https://linux.bfh.ch for more information)

- DNSSEC Validation on Windows Servers and Windows Clients is up to their respective maintainers and to be defined by them at their own schedule (for now :)

Pointers

Pointers

Interesting Stuff

- Qualified NXDOMAIN: NSEC and NSEC3 Ressource Records
- DNSSEC KSK and ZSK Rollover
- DNSSEC lookaside Verification (DLV Entries)
- Additional stuff to put into the DNS: TLSA, SSHFP, DKIM, etc.

Further Information

- Wikpedia Articles about DNS and DNSSEC
- The usual RFCs at rfc-editor.org

Thank You for Your Attention.

❤ Source Code is freely available

git clone git://git.bfh.ch/git/staff/bad9/other/talks.git