Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

DNSSEC@BFH

IT Infrastructure Team „Special“ Meeting

Wednesday, 22th October 2014 13:30 – 14:30

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

Andre Kaufmann <andre.kaufmann@bfh.ch>

Peter Spycher <peter.spycher@bfh.ch>

Daniel Baumann <daniel.baumann@bfh.ch>

IT System Engineers, Team Infrastructure Services

Overview

- **What?**
- **Why?**
- **How?**
- **BFH!**
- **Questions?**

Pointers...

What?

Vocuabulary (1/2)

DNS

- Zones and Zone Files (e.g. bfh.ch)
- Resource Records (SOA, A, CNAME, MX, NS, etc.)

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

- Authoritative Servers
- Stub Resolvers
- Recursive Resolvers

Vocuabulary (2/2)

DNSSEC

- Network Information Center (NIC) or Registry
- Registrar
- Top Level Domain (TLD)

- Key Signing Key
- Zone Signing Key
- Trust Anchor

Domain Name System Security Extensions (DNSSEC)

- Asymmetric Cryptography with (implicit) Trust Anchor on Root Server Level
- Hierarchically signed (chain from Root Servers to TLD Registries to individual Authoritative Nameservers)
- Fully backwards compatible by using new, additional ressource records

Timeline

- 1999: Initial Draft for the Domain Name System Security Extensions (DNSSEC)
- 2005: Final Specification published, initial deployments for some TLDs (e.g. .se)
- 2010: Deployment on all Root Servers completed, Trust Anchor published
- 2011: DNSSEC for .ch Zone enabled

Why?

Trust your DNS

Problem

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

Reasons for a secure DNS

- General: MiM Attacks, DNS Spoofing
- General: Use Advanced, State of the Art Security Technologies (SSHFP, TLSA, DKIM, etc.)
- Specifically: DNS as Inventory

How?

DNSSEC Components

- Recursive DNS Lookups
- Trust Anchor on Root Server Level („pre-shared secret“)
- Key Signing Keys in DNS at TLD Registry (usually offline)
- Zone Signing Keys in DNS at TLD Registry (usually online on Name Servers or hidden master)

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 (1/3)

- $ dig @localhost DS switch.ch

;; QUESTION SECTION:

;switch.ch. IN DS

;; ANSWER SECTION:

switch.ch. 3397 IN DS 4369 8 1 39737AE7341AB1CC4A1C0AD5F04234679CB3C9E4

switch.ch. 3397 IN DS 4369 8 4 1DFD1EB90F65FB9ABC67D42CE5100DD72F9F1CA5A754219[...]

switch.ch. 3397 IN DS 4369 8 2 3CCC9D582DFF9CC91EC2D15897455DFD740763D3D45717C[...]

switch.ch. 86345 IN RRSIG DNSKEY 8 2 86400 20141109122148 20140924112148 4369 switch.ch.
WvbDknwdXH4X/jov27QXzPMvjN8g0N38kq5pFsh7wQDIdx/QSlxt94Z8
k8gkKaVzu4JsxIxWsefSKd76nH8LbYZZ5dpkikACrMDs8ubdOGoiqIAA
OVFJKc/jFuPLkIGvDRciLGctHbMiWwugQKNtvg206htRVSH4/mVsH0QR
1L8xdLVv8pt/aIrrtUcpqCeX8PmogkGasszf/bnBHI5ZPZtFRZBm2Pu5
c0CE4jcIlhnJonzYeNBNdoZ1nDRWyv5ufBH0vDpQd8vXl/vHju2mKFlH
r18UnxVc3vFgBXQOYbRlR03ydwFc16Wx1hktgDc4o3JqCxf+L6yU0Xgn WX1W/g==

Resolver with DNSSEC (2/3)

- $ 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[...]

switch.ch. 86345 IN RRSIG DNSKEY 8 2 86400 20141109122148 20140924112148 4369 switch.ch.
WvbDknwdXH4X/jov27QXzPMvjN8g0N38kq5pFsh7wQDIdx/QSlxt94Z8
k8gkKaVzu4JsxIxWsefSKd76nH8LbYZZ5dpkikACrMDs8ubdOGoiqIAA
OVFJKc/jFuPLkIGvDRciLGctHbMiWwugQKNtvg206htRVSH4/mVsH0QR
1L8xdLVv8pt/aIrrtUcpqCeX8PmogkGasszf/bnBHI5ZPZtFRZBm2Pu5
c0CE4jcIlhnJonzYeNBNdoZ1nDRWyv5ufBH0vDpQd8vXl/vHju2mKFlH
r18UnxVc3vFgBXQOYbRlR03ydwFc16Wx1hktgDc4o3JqCxf+L6yU0Xgn WX1W/g==

Resolver with DNSSEC (3/3)

- $ 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=
```

BFH!

Name Server without DNSSEC

External Authoritative Name Servers

(**External** DNS View **only**)

NS1 .254.20

NS2 .250.20

NS3 .de

Internal Authoritative Name Servers

(**Internal** DNS View **only**)

DD-INT1 .224.20

DD-INT2 .96.20

Name Server with DNSSEC (1/2)

External Authoritative Name Servers

(**External and Internal** DNS Views)

NS1
.254.20

NS2
.250.20

NS3
.de

Internal Authoritative Name Servers

(**Internal** DNS View **only**)

DD-INT1
.224.20

DD-INT2
.96.20

Name Server with DNSSEC (2/2)

External Authoritative Name Servers

NS1
.254.20

NS2
.250.20

NS3
.de

Internal Validating (Caching) Recursive Resolvers

DD-INT1
.224.20

DD-INT2
.96.20

BFH Specifics (1/2)

Policy

- 1 KSK and 1 ZSK is active at the time
- Ideally 2 KSK and 2 ZSK pairs at all times in DNS
- Ideally 2 KSK and 2 ZSK pairs at all time in escrow
- Only strong algorithm combinations, see https://linux.bfh.ch/services/dns/dnssec-keys/

Processes

- Key Generation: Linux Team (responsible), Security Team (backup)
- Key Rollover: Network Team (responsible), Linux Team (backup)
- Key Escrow: Security Team, ITS IS and ITS Management (backup)

BFH Specifics (2/2)

Key Rollover (e.g. KSK)

- ZSK rollover (sample dates taken) will be done like that:
  - 2016-01-01: New ZSK is added to DNSKEY.
  - 2016-01-07: New ZSK is used to sign zones in addition, zones have two signatures of both the old and the new ZSK at the same time.
  - 2016-01-14: Old ZSK is not used to sign zones anymore, zones have only one signature from the new KSK.
  - 2016-01-21: Old ZSK is marked as revoked.
  - 2016-01-31: Old ZSK is removed from DNSKEY.

- KSK rollover goes the similar way.

BFH Timeline

- DNSSEC Tests with Test Domain (bfh.li)

22th October 2014

- DNSSEC Introduction Meeting for ITS

29th October 2014

- **Temporarily** enabling DNSSEC for bfh.ch during Maintenance Window (18:00 – 20:00)

5th November 2014

- **Permanently** enabling DNSSEC for bfh.ch during Maintenance Window (18:00)

At any later point...

- Enabling DNSSEC Verification on Stub Resolvers (dd-int1/dd-int2) by Network Team
- Enabling DNSSEC Verification on Clients and Servers for recursive lookups by individual Teams/Persons
- Enabling DNSSEC for „third-party“ Zones hosted by BFH name server by Network Team

Possible Problems.. which we don't have or can deal with ;)

- General Complexity increases
- Potential for catastrophic failures on signature handling errors

- Validation costs ressources on clients
- Validation costs ressources on name servers (only recursive lookups from now on)

- **Your Input Here**

Questions?

Pointers...

Further Information

BFH

- https://linux.bfh.ch/software/unbound
- https://linux.bfh.ch/services/dns

Manual pages

- man unbound.conf

Wikipedia

- http://en.wikipedia.org/wiki/DNSSEC
- http://de.wikipedia.org/wiki/DNSSEC

RFC

- http://rfc-editor.org

Interesting Stuff

- DNSSEC Lookaside Verification (DLV)
- Qualified NXDOMAIN: NSEC and NSEC3 Ressource Records
- TLSA, SSHFP, DKIM, etc.
- ...

Thank You for Your Attention.

❤ Source Code is freely available

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