Praktische Beispiele zu DNSSEC

Arsen Stasic
arsen.stasic@univie.ac.at

9. Dezember 2022

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert
- gTLD .berlin wurde 2014-01-08 delegiert

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert
- gTLD .berlin wurde 2014-01-08 delegiert
- gTLD .versicherung wurde 2014-05-22 delegiert

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert
- gTLD .berlin wurde 2014-01-08 delegiert
- gTLD .versicherung wurde 2014-05-22 delegiert
- gTLD .hamburg wurde 2014-06-04 delegiert

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert
- gTLD .berlin wurde 2014-01-08 delegiert
- gTLD .versicherung wurde 2014-05-22 delegiert
- gTLD .hamburg wurde 2014-06-04 delegiert
- Aufgabe: Finden Sie Gemeinsamkeiten der gTLDs heraus

gTLDs

- gTLD .wien wurde 2014-01-03 delegiert
- gTLD .berlin wurde 2014-01-08 delegiert
- gTLD .versicherung wurde 2014-05-22 delegiert
- gTLD .hamburg wurde 2014-06-04 delegiert
- Aufgabe: Finden Sie Gemeinsamkeiten der gTLDs heraus
- `http://ntldstats.com/`

DNSSEC Rootkey Rollover

- 2017-07-11: Publication of new KSK in DNS
- ~~2017-10-11: New KSK begins to sign the root zone key set (the actual rollover event)~~
- 2017-09-27: KSK Rollover Postponed
- ~~Rollover will take place in Q1 2018~~
- 2018-10-11: 16:00 UTC KSK Rollover was performed
- 2019-01-11: Removal of old KSK - increasing queries for old KSK

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuAOe50`

Gegenmaßnahmen:

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuAOe50`

Gegenmaßnahmen:

- Filter:

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuAOe50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuAOe50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853
- **Filter skalieren nur bei kleinen und mittel-großen Netzen**

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuA0e50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853
- **Filter skalieren nur bei kleinen und mittel-großen Netzen**
- RPKI (Resourse Public Key Infrastructure): RFC6480, 6481, 6482, 6810, 6811

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuA0e50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853
- **Filter skalieren nur bei kleinen und mittel-großen Netzen**
- RPKI (Resourse Public Key Infrastructure): RFC6480, 6481, 6482, 6810, 6811
- **zentralistischer Ansatz steht im Gegensatz zum dezentralen BGP**

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuA0e50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853
- **Filter skalieren nur bei kleinen und mittel-großen Netzen**
- RPKI (Resourse Public Key Infrastructure): RFC6480, 6481, 6482, 6810, 6811
- **zentralistischer Ansatz steht im Gegensatz zum dezentralen BGP**
- BGPsec: RFC8205, 8206, 8207, 8208, 8209

Internet Routing

- BGP-Hijack: `https://youtu.be/IzLPKuA0e50`

Gegenmaßnahmen:

- Filter:
  - whois AS15169
  - whois AS1853
- **Filter skalieren nur bei kleinen und mittel-großen Netzen**
- RPKI (Resourse Public Key Infrastructure): RFC6480, 6481, 6482, 6810, 6811
- **zentralistischer Ansatz steht im Gegensatz zum dezentralen BGP**
- BGPsec: RFC8205, 8206, 8207, 8208, 8209
- **ist recht neu und daher gibt es noch keine Software**

Weiterentwicklungen bei DNS

- DoT (DNS over TLS) Port 853 (TCP)

Weiterentwicklungen bei DNS

- DoT (DNS over TLS) Port 853 (TCP)
- DoH (DNS over HTTPS) Port 443 (TCP)

Weiterentwicklungen bei DNS

- DoT (DNS over TLS) Port 853 (TCP)
- DoH (DNS over HTTPS) Port 443 (TCP)
- DoQ (DNS over QUIC) Port 853 (UDP)
- **Confidentiality**: Kann mitgelesen werden?
- **Integrity**: Wurde der Inhalt verändert?
- **Availability**: Verbesserte Erreichbarkeit/Antwortverhalten

Weiterentwicklungen bei DNS

- DoT (DNS over TLS) Port 853 (TCP)
- DoH (DNS over HTTPS) Port 443 (TCP)
- DoQ (DNS over QUIC) Port 853 (UDP)
- **Confidentiality**: Kann mitgelesen werden?
- **Integrity**: Wurde der Inhalt verändert?

Praktische Beispiele

https://homepage.univie.ac.at/arsen.stasic/Linux_LV/2.pdf

Praktisches Beispiel: validierende DNS Recursor

- Seit BIND 9.5 wird validiert **dnssec-validation auto;**
- dnssec-enable ist default auf yes **dnssec-enable yes;**
- `https://etherpad.mit.edu/p/Linux-LV`
- ssh student@linux-X.ai.wu.ac.at
- aeXamael7eiqu5sahjaish4K
- dig aco.net +dnssec | grep ";; flags:"

Praktisches Beispiel: validierende DNS Recursor

- Seit BIND 9.5 wird validiert **dnssec-validation auto;**
- dnssec-enable ist default auf yes **dnssec-enable yes;**
- `https://etherpad.mit.edu/p/Linux-LV`
- ssh student@linux-X.ai.wu.ac.at
- aeXamael7eiqu5sahjaish4K
- dig aco.net +dnssec | grep ";; flags:"
- sudo su -
- apt update
- apt install bind9 dnsutils
- nano /etc/resolv.conf
- nameserver 127.0.0.1
- rndc managed-keys status *(ab BIND 9.11)*
- dig aco.net +dnssec | grep ";; flags:"

Praktisches Beispiel: auth DNS DNSSEC 1/3

- apt install apparmor-utils *(ubuntu)*
- aa-complain /usr/sbin/named *(ubuntu)*
- cd /etc/bind/
- nano named.conf.local

Bind Config

```
zone "dnsX.test.ac.at" {
  type master;
  file "/etc/bind/pri/dnsX.test.ac.at";
  key-directory "/etc/bind/keys";
  auto-dnssec maintain;
  inline-signing yes;
};
```

Praktisches Beispiel: auth DNS DNSSEC 2/3

- export ZONE=dnsX.test.ac.at *(bash)*
- mkdir -p /etc/bind/pri/
- chgrp bind /etc/bind/pri/
- chmod g+rw /etc/bind/pri/
- nano /etc/bind/pri/$ZONE

Zonefile

```
$TTL 60 ;  minutes
$ORIGIN dnsX.test.ac.at.
@ IN SOA dnsX.test.ac.at. mosthamster.dnssec.at. (
    1 ; serial
   1h ; refresh (1 hour)
  30m ; retry (30 minutes)
   1w ; expire (1 week)
  10m ; minimum (10 minutes)
)
@ IN NS linux-X.ai.wu.ac.at
@ IN A  137.208.107.75
```

Praktisches Beispiel: auth DNS DNSSEC 3/3

- mkdir -p /etc/bind/keys/
- cd /etc/bind/keys/
- dnssec-keygen -a ECDSAP256SHA256 -f KSK -n zone $ZONE *(ab BIND 9.16 ohne -r)*
- dnssec-keygen -a ECDSAP256SHA256 -n zone $ZONE *(ab BIND 9.16 ohne -r)*
- chmod g+r /etc/bind/keys/
- chmod g+r /etc/bind/keys/*
- export SALT=$(openssl rand -hex 8)
- rndc reconfig
- rndc signing -nsec3param 1 0 5 $SALT $ZONE
- rndc signing -list $ZONE
- dnssec-dsfromkey -2 $(grep -l key-signing K*)
- `https://etherpad.mit.edu/p/Linux-LV`

Praktisches Beispiel: auth DNS DNSSEC 3/3

- mkdir -p /etc/bind/keys/
- cd /etc/bind/keys/
- dnssec-keygen -a ECDSAP256SHA256 -f KSK -n zone $ZONE *(ab BIND 9.16 ohne -r)*
- dnssec-keygen -a ECDSAP256SHA256 -n zone $ZONE *(ab BIND 9.16 ohne -r)*
- chmod g+r /etc/bind/keys/
- chmod g+r /etc/bind/keys/*
- export SALT=$(openssl rand -hex 8)
- rndc reconfig
- rndc signing -nsec3param 1 0 5 $SALT $ZONE
- rndc signing -list $ZONE
- dnssec-dsfromkey -2 $(grep -I key-signing K*)
- `https://etherpad.mit.edu/p/Linux-LV`
- rndc zonestatus $ZONE *(ab BIND 9.10)*
- systemctl status bind9

Praktisches Beispiel: auth DNS RRL

Shell

```
for i in $(seq 1 25) ; do dig @127.0.0.1 $ZONE soa +short; done
```

nano /etc/bind/named.conf.options

Config (innerhalb vom options-Block)

```
 rate-limit {
    responses-per-second 5;
    window 5;
    log-only no;
    IPv4-prefix-length 24;
};
```

rndc reconfig

Web-Tools/Info zu DNSSEC?

- wget -q -O - http://ipv4.icanhazip.com/
- curl http://ipv4.icanhazip.com/
- https://etherpad.mit.edu/p/Linux-LV
- http://dnssec-or-not.com/
- http://www.dnssec-tools.org/
- http://dnssec.vs.uni-due.de/
- http://dnssectest.sidnlabs.nl/test.php
- http://dnsviz.net/d/dns10.test.ac.at/dnssec/
- http://dnssec-debugger.verisignlabs.com/dns10.test.ac.at
- http://stats.research.icann.org/dns/tld_report/

Fragen

arsen.stasic@univie.ac.at

https://homepage.univie.ac.at/arsen.stasic/Linux_LV/2.pdf