

DNSSEC – demo

Martin Stanek

Department of Computer Science
Comenius University
`stanek@dcs.fmph.uniba.sk`

Security of IT infrastructure (2016/17)

Setup

- ▶ DNS server (bind9 (9.10.3), Ubuntu 16.04): 192.168.56.103
- ▶ DNSSEC validating resolver:
 - ▶ import KSK for the root zone (include “/etc/bind/bind.keys”):

```
managed-keys {  
    . initial-key 257 3 8 "AwEAAg...ihz0=";  
};
```

...provided by the distribution
 - ▶ configure DNSSEC validation and support in options section of the configuration file
 - ▶ ...and test, e.g.:

```
dig @192.168.56.103 www.icann.org +dnssec
```

Flags for dig

AA = Authoritative Answer

TC = Truncation

RD = Recursion Desired

RA = Recursion Available

AD = Authenticated Data (DNSSEC only: authenticated data)

dig @192.168.56.103 www.icann.org +dnssec

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> @192.168.56.103 www.icann.org +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 12353
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.icann.org. IN A

;; ANSWER SECTION:
www.icann.org. 2577 IN CNAME www.vip.icann.org.
www.icann.org. 2577 IN RRSIG CNAME 7 3 3600 20170503112644 20170411230432 64337
    icann.org. ZhF+Q9...dE=
www.vip.icann.org. 30 IN A 192.0.32.7
www.vip.icann.org. 30 IN RRSIG A 7 4 30 20170428151309 20170421151309 7439
    vip.icann.org. BidBKx...Q=

;; Query time: 118 msec
;; SERVER: 192.168.56.103#53(192.168.56.103)
;; WHEN: Sun Apr 23 22:51:49 CEST 2017
;; MSG SIZE rcvd: 425
```

Authoritative server for TLD zone biti

- ▶ `/etc/bind/named.conf.local:`

```
zone "biti" {  
    type master;  
    file "/etc/bind/db.bit";  
};
```

- ▶ ...and test, e.g.:

```
dig @192.68.56.103 biti. MX  
dig @192.68.56.103 tango.bit.
```

```
; Zona bitl.
$TTL 604800
$ORIGIN bitl.
```

```
@      IN      SOA      ns1.bitl.   admin.bitl. (
                        2 ; Serial
                        28800 ; Refresh
                        7200 ; Retry
                        864000 ; Expire
                        86400 ) ; Negative Cache TTL
```

```
;
```

```
NS      ns1.bitl.
```

```
NS      ns2.bitl.
```

```
MX      10 mail.bitl.
```

```
MX      20 mail2.bitl.
```

```
ns1     IN     A       192.168.56.103
```

```
ns2     IN     A       192.168.56.103
```

```
mail    IN     A       192.168.56.200
```

```
mail2   IN     A       192.168.56.201
```

```
tango   IN     A       192.168.56.210
```

```
waltz   IN     A       192.168.56.211
```

```
samba   IN     A       192.168.56.212
```

```
rumba   IN     A       192.168.56.213
```

DNSSEC in zone biti

- ▶ generate KSK a ZSK:

```
dnssec-keygen
```

```
-a RSASHA256 -3 -b 4096 -r /dev/urandom -f KSK biti
```

```
dnssec-keygen
```

```
-a RSASHA256 -3 -b 2048 -r /dev/urandom biti
```

- ▶ public keys: .key
- ▶ private keys: .private

- ▶ signing the zone (incl. NSEC3):

```
dnssec-signzone -3 abcdef00 -S -o biti db.biti
```

- ▶ signed zone: db.biti.signed

DNSSEC in zone biti (2)

- ▶ replacing zone file with the signed one in `/etc/bind/named.conf.local`:

```
zone "biti" {  
    type master;  
    file "/etc/bind/db.bit signed";  
};
```

- ▶ ...and we can test, e.g.:

```
dig @192.168.56.103 biti. MX +dnssec  
dig @192.168.56.103 tango.bit. +dnssec  
dig @192.168.56.103 tangooo.bit. +dnssec  
...
```

notice the missing ad flag in responses (authoritative server do not set ad flag)

Other necessary actions

- ▶ regular signing of zone (the signatures have limited validity)
- ▶ managing the serial number of zone file
- ▶ inclusion of DS record for KSK into parent zone
 - ▶ file (`dsset-bit1.`) is generated automatically
- ▶ regular change of cryptographic keys
- ...