What's so hard about DNSSEC?

Paul Ebersman – Paul_Ebersman@cable.comcast.com
23-27 May 2016
RIPE72 – Copenhagen
Why use DNSSEC
What does it solve?

• Helps against cache poisoning
• Identifies DNS “lying”
• Enables DANE and other PKIs
Naysayers’ story

• It’s “hard”

• It only breaks things

• It doesn’t solve anything

• We’re trusting ICANN/root servers
My experience

• Automate or it is hard

• It does help prevent cache poisoning

• We are using DANE already for email

• We’re already trusting ICANN/root servers

• Customers starting to expect security of DNSSEC
How to start?
The two halves

• Validation

• Zone signing
Validation

• Easy to enable

• But you pay (a little) for others’ mistakes

• All major open sources packages support this.
Signing

- Automation is not an option
- Automation ease and quality varies widely
- Setting up isn’t trivial
- Beware of key rollovers
Validation issues
“But it’s an ISP support nightmare”

• Other folks screw up, you get the call
• “Why are you blocking site ‘X’?”
• It’s your resolver, you fix it!
Dunno… I sleep at night.

• Comcast & Google validate (20% of public resolvers)

• Comcast validates and signs

• 2 dozen failures a month is a bad month and this is improving (even .GOV…)

• NTAs (RFC 7646) single digits a month
What do we see?

• Expired signatures
• Incorrect removal of signing
• Inadvertent signing
• Bad key rollovers (KSK)
Signing issues
What do we see?

• Initial signing works but rollovers don’t

• Mis-matches of DS in parent and KSK in child

• Forget to put DS in parent
How do we deal with failures?
Education

- Training 1st tier
- Teach customers as we explain outage
- dnsviz.net invaluable
Outreach

• Get .mil/.gov and other large NOC contacts in advance

• Get contacts at large hosting/registries serving auth zones

• Explain to your mgmt why this is important
Negative trust anchors

- Follow the RFC (7646)
- Try to get the zone owner to fix the problem
- Educate them in how to avoid this
- NTA should be last resort
Q & A
Thank you!
Appendix A: further reading

- http://www.internetsociety.org/deploy360/dnssec/
Appendix B: example configs

• To enable DNSSEC validation in BIND

// In named.conf, add:

managed-keys {
    "." 257 3 8 "AwEAAagAIKIVZrpC6la7gEzahOR+9W29euXhJhVVLOyQbSEW0O8gcCjF
    FVQUTf6v58fLjwBd0Y10EzrAcQqBGCzh/RStioO8g0NfnfL2MTJRkxoX
    bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
    X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
    W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzugul0sGlcGOYi7OyQdXfZ57reIS Qageu
    +ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=";
};

// in options section, add:

dnssec-enable yes;
dnssec-validation yes;
Appendix B: example configs

• To enable DNSSEC signing of example.com in BIND

```bash
# create dir with permissions for bind to rwx by group
cd <YOUR-ZONE-FILE-DIR>
mkdir example.com
chmod 2775 example.com
chown bind:bind example.com

cd example.com
# create ksk
dnssec-keygen -a NSEC3RSASHA1 -b 2048 -f KSK example.com
# create zsk
dnssec-keygen -a NSEC3RSASHA1 -b 1024 example.com
# create DS records
grep key-s *.key
dnssec-dsfromkey Kexample.com.+007+42963.key > ds-records
# add DNSKEY records to zone file
# edit named.conf & reload zone
rndc reload example.com
# sign zone
rndc sign example.com
# set to NSEC3 (assuming you want that)
rndc signing -nsec3param 1 0 10 auto example.com
rndc reload example.com
# update registrar w/DS records or DNSKEY per your registrar instructions
```
Appendix B: example configs

• Sample zone statement in named.conf

zone "example.com" {
    type master;
    file "dynamic/example.com";
    key-directory "keys/example.com";
    auto-dnssec maintain;
    allow-query { any; };
    allow-transfer { key example-slave-key; 192.168.1.1; };
};
Appendix B: example configs

• To enable DNSSEC validation in Knot resolver:
  

• To enable DNSSEC validation in Unbound:
  
  - [https://www.unbound.net/documentation/howto_anchor.html](https://www.unbound.net/documentation/howto_anchor.html)
Appendix B: example configs

• To DNSSEC sign zones in Knot:

• To DNSSEC sign zones in Unbound:
  - (manually) http://www.nlnetlabs.nl/publications/dnssec_howto/
  - (automated) https://www.opendnssec.org/