DNSSEC
Is the Juice Worth the Squeeze

Paul Ebersman – Paul_Ebersman@pae-associates.com
08-09 Sep 2016
UKNOF 35 - Glasgow

The Juice

So what do you get with DNSSEC

- Cache protection
- Data integrity
- Secure certificates without CAs

Cache protection

- DNS is primarily UDP
- Easily spoofed
- Cache poisoning quite easy (Kaminsky)
- Cache poisoning very effective MitM (Man in the Middle) attack, even remotely

Data Integrity

- Important to know you got the answer the zone owner wants you to get.
- Important to be able to prove ***non-existence*** of records too
- Lets you validate that the whole delegation chain is valid.

Certificate Authorities

- Popular browser have 1300 CAs
- CAs can sign any domain
- How trustworthy are all CAs

How trustworthy are CAs

- DNSSEC: family reunion
- CA: old room-mate's dealer

Self-signed certificates

- You're already trusting the A record
- Trusting the certificate same leap of trust

Tech enabled by DNSSEC

- DANE (DNS-Based Authentication of Named Entities):
  - Email (TLS certs)
  - Alternate to CA (Certificate Authority) certs for web
  - Jabber/XMPP
  - SIP
- Other applications will get developed. API to make this all easier to use:
  - https://getdnsapi.net/

The Squeeze

What is required

- Clean up your current DNS
- Authoritative server issues
- Recursive server issues

DNS Cleanliness & DNSSEC

DNS cleanliness

- Most DNS servers very forgiving.

- We've gotten away with things that were never legal or recommended:
  - Dotted hosts (label foo.bar in zone example.com)
  - Mismatches in parent/child delegations
  - Being authoritative for zones on recursive servers
  - Views
  - NX Domain rewriting and other DNS lying
  - RPZ zones

DNS cleanliness

- DNSSEC == Wonder Woman Golden Lasso

We aren’t allowed to lie!

DNS cleanliness

- “We aren’t allowed to lie!”
- Well, not exactly. More like with our parents/spouses. We have to be much more careful when we lie and we need a really good reason…

Authoritative server choices & issues

DNSSEC auth server choices

- Key sizes for ZSK/KSK
- Expirations for ZSK/KSK
- Algorithm
- TTLs
- Rollover method
- NSEC vs NSEC3

Real secret to DNSSEC for auth

Automate!!!

Auth server issues

- Use in DNS Amplification attacks
- Key rollovers
- Complications with zone transfers and dynamic updates
- System capacity issues

Use in DNS Amplification attacks

- Use algorithms with smaller hashes/keys (like ECDSA)
- Use rate limiting, particularly on RRs like ANY
- Set “minimal responses”
- Log as much as you can

Key rollovers

- Automate!!!
- Monitor to check validation

Zone transfers and dynamic updates

- Sign on a hidden master, have all listed servers in the zone be secondary servers
- Doing multi-master and DNSSEC is hard…
- Sign in only one place

System Capacity Issues

- Faster CPU for signing host
- Need good source of randomness on signing host. Hard on VMs
- Signed zones much larger (3-10x), so more disk and more AXFR time

DNSSEC issues for validating servers

Validating server issues

- Use in amplification/DDOS attacks
- Someone else's mistake gets you support calls
- It's not your zone so you can't fix it
- Lots of user training
- Lots of staff training

Amplification/DDOS

- Do whatever BCP38/84 filtering you can to limit packet spoofing.
- Use ACLs to limit who can use your server
- Use response rate limiting for zones under attack
- Set “minimal responses” on your server
- Log everything you can

Not your mistake

- Most common problems seen are:
  - Someone turns on DNSSEC by mistake and wrong
  - Key rollovers done wrong
  - Expired keys or signatures due to bad automation
  - Someone deletes DS or DNSKEY by mistake
- Try to reach the zone owner, but this can be hard
- Explain to them that they will be unreachable with anyone using google DNS or anyone who validates.
- When all else fails, use an NTA (Negative Trust Anchor, RFC 7646)

Not your zone…

- Keep a file/DB of contacts for large registrars and service providers' NOC
- DNSVIZ output saved and sent to person complaining can help
- DNSVIZ output can also convince skeptical zone owners that it really is them that is broken

User training

- DNSVIZ output is good
- Have a reference page like deploy360 for folks that want more information
- Have pre-done files that your NOC staff can cut and paste explaining DNSSEC, what it is, why you do it, how it works

Staff training

- The more your first tier knows, the less you get called in the middle of the night

- The more material and tools you give your staff, the better it looks to the customer

Is it worth it?

Is it worth it?

- You should clean your DNS anyway
- DDoS vectors available anyway
- Cache poisoning is bad
- If you automate and train, not much extra work

Q & A

Thank you!