Your world. Our domain.
Current State and Development of DNS Security and Privacy (part 1: DNSSEC)

Marco Davids

2 October 2019
DNSSEC – adding a security layer to DNS

- DNS was developed in 1983
- Still a key component in the core of the internet
- Critical shortcoming: vulnerable to manipulation and forgery
  - Kaminsky attack / cache pollution / cache poisoning / DNS spoofing
DNSSEC

- Answers from the DNS are digitally signed
  - Public-key cryptography
- Answers can be authenticated by (validating) resolver
- Provides data integrity (and origin authentication)
  - But not confidentiality / privacy (but wait for it, there’s more in this session)
DNSSEC

- Enabler to make existing protocols better/more secure
  - DKIM, SPF, DMARC
  - CERT-records (RFC4398), SSHFP (RFC5255), IPSECKEY (RFC4025)
  - CAA (RFC6844)
  - DANE / TLSA (RFC6698 and RFC7672)
    - TLS trust anchors
DNSSEC

• Enabled in the root zone since 2010
  • Also enabled in .nl zone since 2010
• Good support in software and services
  • BIND, Unbound, PowerDNS, Knot, Microsoft, Secure64, InfoBlox, etc.
  • Also, Public DNS resolvers offer support (1.1.1.1, 8.8.8.8, 9.9.9.9 etc.)
• Signing is popular in .nl zone¹
  • Only 0.08% bogus
  • Not so much elsewhere...
  • Validation also still a bit of a challenge in many places²
• Check it on https://en.internet.nl/

Questions ?
Thanks!