# The Impact of a Signed Root on Network Infrastructure


- Suzanne Woolf
- Internet Systems Consortium

- NANOG 48, Austin, 24 Feb. 2010

# What Does it All Mean?

- We've seen that DNSSEC represents a significant change in how “DNS is done” in the public Internet
- We know how a signed root is being done, and what that means for the provisioning of the root
- What does it mean for other DNS operators?

# Possible Side-Effects: response sizes

- Responses from root servers for "." will include signatures, so will become larger:
  - greater than 512-byte UDP limit
  - Original specification says this results in fallback to TCP
- EDNS0 allows up to 4096-byte responses via UDP over IP fragments

# Response sizes (2)

- EDNS0 is now widely implemented in DNS software
- But not so well understood by middleware devices
  - Firewalls
  - CPE
- Results could be:
  - Dropped responses
  - Fallback to TCP

# Testing Side-Effects

- Testing tool provided by OARC at:
  - https://www.dns-oarc.net/oarc/services/replysizetest
- If you see issues, best to address them on your network now, or there will likely be performance issues when you turn on DNSSEC validation
- Note that much modern DNS software indicates acceptance of DNSSEC data by default ("DO=1")

# Possible Side Effects: Misconfigured keys

- What happens if a previously valid key stops working?
  - This can happen when key rollover is done....
  - If the validating resolver isn't updated with new keys, either automatically or manually
- Fielded software (BIND and others) can be very aggressive in recovery

# Misconfigured keys (2)

- A bad key looks like a validation failure caused by a MITM
- The obvious recovery strategy is brute force
  - Ask all the authoritative servers for the zone for validation data
  - ....All the way up the chain of trust
- This can be a lot of packets

# Misconfigured keys (3)

- Low probability scenario
  - But mistakes happen
  - The Internet has lots of DNS resolvers. A low percentage can still be a lot of traffic
- TLDs and root servers drastically over-provision, but scalability is still nice
- Future software will be less aggressive

# Why are we here, again?

- DNSSEC helps with certain Bad Things
- But: you can't change a system as complex as the global Internet without side effects
- Side effects to DNSSEC deployment need to be managed.

# The Bottom Line

- In many networks, DNS is not a focus
  - Not that hard to provide basic service
  - Configurations tend not to change
- DNSSEC changes this
  - Legacy devices and assumptions may not prevail
- ***KNOW YOUR NETWORK***