DNSSEC

Patrik Fältström
Distinguished Consulting Engineer
Office of the CTO

What was asked

- Does your operating system take advantage of DNSSEC in any way currently or in future, as a key component or otherwise?
- What do you see is the most challenging aspect of doing DNSSEC in the environment you provide?
- What are your plans for DNSSEC in your technical development roadmap?
- Do you see DNSSEC validation on the desktop as a good choice to make?
- What are your plans for your server software for performing DNSSEC validation?

Is DNSSEC important?

- DNSSEC is one of many security components that together make Internet more stable and secure
- Robustness, resilience and predictability

- That said, DNSSEC imply changes

Why is DNSSEC important for Cisco?

- Many of our products transport DNS traffic
- Many of our products look up DNS records
- We take stability and security seriously

Most challenging thing

- The problems I see with deployment is a mix of
  - Bad network design
  - Misconfiguration of boxes
  - Bugs in software in boxes
- Sometimes it is very hard to understand what the problem really is
  - Often detected by a “delay in DNS lookups”
  - Hard to detect while deployment level is low
  - People debugging do not yet know how to debug

Example

- Customers to broadband provider complain that webpages *sometimes* are not reachable – but that reload in browser helps
- No errors logged anywhere in the network
- By pure luck a domain name was found that in fact do sometimes fail, and they look at DNS lookups
- Responses for queries for that specific domain name where so large that it was in a fragmented UDP packet, that did not reach the resolver due to misconfiguration of the device

Where will we see problems?

- Misconfigurations, or correct configurations
  - Both related to EDNS0 and UDP fragmentation
- In transition to IPv6, synthesizing of responses
  - Transition techniques should be selected that minimize the amount of synthesizing needed
- In content delivery networks, synthesizing
  - RRSets must be pre-synthesized and signed
  - Alternatively, more HTTP redirect and less DNS tricks
- Validation in the client will because of this be difficult in many deployment scenarios, although it could often be preferred

What are we doing?

- Educating customers on how to configure
  - EDNS0
  - Fragmented IP packets
  - Content delivery networks
- Fixing bugs
- Consistent client behaviour
- More intelligent (hierarchal) CDN's
- Ultimately:
  - Produce products and services that works


CISCO