DNSSEC Tutorial: Status “Today”

Phil Regnauld
Hervey Allen

DNSSEC: Current Status

Who's signed their zones?

- .bg (Bulgaria)
- .br (Brazil)
- .pt (Portugal)
- .cz (Czech Republic)
- .gov (is close)
- .museum
- .org (signed 2 June 2009)
- .pr (Puerto Rico)
- .se (Sweden)
- Several IDN-based TLDs
- https://itar.iana.org/

DNSSEC: Current Status

Who's signed their zones?

- .uk (March 2010)
- .tm (Turkmenistan)
- .com (2011)
- … more to come

DNSSEC: Current Status cont.

Who's signed their zones?

- Anyone else?

Lots of second-level domains (.org.br, etc.). *Islands of trust*. Their *trust anchors* are their TLD (if signed), else a DLV, other signed zone, etc...

DNSSEC: Current Status
US Government NOI

The US Government's National Telecom- munications and Information Administration (NTIA) asked for Public Comments Regarding the Deployment of DNSSEC (i.e. *signing the root!*):

- http://www.ntia.doc.gov/DNS/dnssec.html
  - Press release went out 9 October 2008 with comments due by 24 November 2008.
  - See the "NOI Supporting Material" section for the various DNSSEC proposals under consideration.
  - Read the comments. Interesting and from many parties, including many "Internet and DNSSEC Celebrities".
  - By November 24, there were 55 comments (many *very* long) received.
  - Was "under consideration" by the US Government.

DNSSEC: Signing the Root

3 June 2009:

Press releases by ICANN and NIST stating that the U.S. Department of Commerce, ICANN and VeriSign agreed to work together to sign the root by the end of 2009:

- http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
- http://www.nist.gov/public_affairs/releases/dnssec_060309.html

DNSSEC: Signing the Root

October 6th, 2009:

Announcement at RIPE 59 that the root would be signed by July 1st 2010

- Each root nameserver will deploy in turn a signed root zone, at one month intervals, starting 1st Dec 2009
- During deployment, root zone will include a dummy key, with unverifiable signatures
- This is the Deliberately-Unvalidatable Root Zone (DURZ), intended to test impact of deploying a DNSSEC enabled zone
- The proper KSK and ZSK are published 1st July 2010

See http://www.root-dnssec.org/

http://www.root-dnssec.org/documentation/

DNSSEC: Signing the Root

Initial observations on the deployment (impact):

- http://labs.ripe.net/content/measuring-dns-transfer-sizes-first-results
- https://www.dns-oarc.net/node/240

An increase in query size, TCP retransmissions has been observed, but the conclusion from RIPE Labs:

"The vast majority of measurements are from resolvers that are ready and will continue to function when K-root starts providing DNSSEC answers to resolvers that request it. There are some resolvers that could experience time-outs and delays due to misconfigurations and middleware."

DNSSEC Status Conclusion

- The root will be signed within 6 months
- However, this does not mean your TLD will be...
- Multiple methods currently available to use DNSSEC if your parent zone hasn't deployed DNSSEC
- TLDs can use IANA's ITAR.
- Second-Level domains can use their ccTLD, if signed, or ISC's DLV, or manual trust anchors.
- An open question: how to roll the root key in an emergency ?...