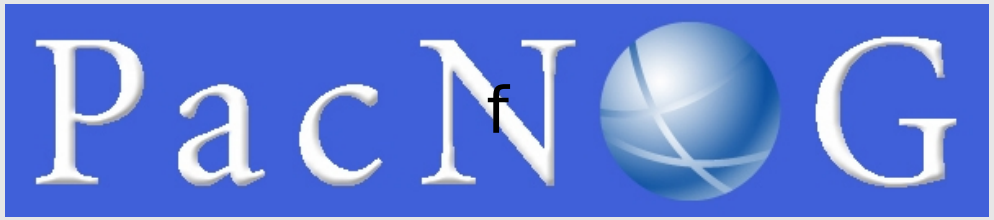
DNSSEC Tutorial: Status "Today"



Phil Regnauld
Hervey Allen

15 June 2009
Papeete, French Polynesia

http://nsrc.org/workshops/2009/pacnog5/dnssec/

DNSSEC: Current Status

Who's signed their zones?

- .bg (Bulgaria)
- .br (Brazil)
- .com ("by 2011" according to Verisign)
- .cz (Czech Republic)
- .gov
- .museum
- .org (signed 2 June 2009)
- .pr (Puerto Rico)
- .se (Sweden)
- Serveral IDN-based TLDs
  - https://itar.iana.org/

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 Telecommunications 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 Status Conclusion

- Multiple methods currently available to use DNSSEC, but nothing is optimal until the *root* (.) is signed.
- TLDs can use IANA's ITAR.
- Second-Level domains can use their ccTLD, if signed, or ISC's DLV, or other trust anchors.

Kaminsky exploit makes DNSSEC deployment inevitable... Critical...