Internet2 DNSSEC Pilot - A Reverse Tree for the Holidays?

Larry Blunk ljb@merit.edu
Shumon Huque shuque@isc.upenn.edu
Allison Mankin mankin@psg.com
Bill Owens owens@nysernet.org

Description of the Pilot

- Goal: Deploy DNSSEC and gain operational experience
  - including: does it catch anything?
- Participants sign at least one of their zones;
- Exchange keys (trust anchors) that will allow them to mutually validate DNS data
- Setup security-aware resolvers
  - Configured with the trust anchors

- Coordination - Internet2, Shinkuro
  - http://www.dnssec-deployment.org

DNSSEC Deployments so far

- MAGPI GigaPoP
  - All zones: magpi.{net,org} & 15 reverse zones
  - https://rosetta.upenn.edu/magpi/dnssec.html
- MERIT
  - radb.net, nanog.org, 169.35.192.in-addr.arpa
  - http://www.merit.edu/nrd/projects/dnssec.html
- NYSERNet - test zone
  - nyserlab.org

Deployments in the pipeline..

- University of Pennsylvania
- University of California - Berkeley
- University of California - Los Angeles
- University of Massachusetts - Amherst
- MIT
- Internet2

Why Internet2

- Internet2 connectors (universities, GigaPops) have a DNS environment with risks. They also have sensitized and skilled security administrators
- Internet2 provides secondaries and international DNS support widely, so there are some "hot" target servers
- Campus DNS groups develop their own Unix DNS tools and environments and many are prepared to adapt these to DNSSEC

Why Do We Want Signed Reverse Zones?

- Note magpi GigaPoP's signing of 15 reverse zones
- Other pilot members will soon add reverse zones
- Reverse mappings are not strong identifiers, but they have many operational uses

State of Reverse Tree DNSSEC in World

- IANA has stated it's intent to sign the .arpa and .int zones by the end of the year
- RIPE has signed its zones, both in-addr.arpa, and ip6.arpa
- https://www.ripe.net/projects/disi/keys/
- It started a delegation signing service and some dozens are signed
- Daily data and trends: http://wwwneu.iks-jena.de/leistungen/dnssec.php

Reverse Zone Signing by ARIN?

- ARIN has discussed signing their zones for several years
- Email and informal statements state that resources not applied because it is not in demand
- The Internet2 pilot expects to need as many signed delegations as RIPE's community, and more
- Can work with ARIN/RIPE on tools
- A signed reverse tree would be a nice Winter Break present