Deploying DNSSEC.
Pulling yourself up by your bootstraps
João Damas
ISC
DNSSEC status

- Standard is complete and usable
  - Minor nits with regards to some privacy issues in some contexts (nsec3, online signing)
- There are at least 2 implementations of servers (BIND and NSD)
- There is at least 1 implementation of a DNSSEC aware resolver (BIND 9.3.2 and later)
Bootstrapping

- DNSSEC follows a hierarchical model for signatures
  - Sign the root zone
  - Get the root zone to delegation-sign TLDs
  - Get TLDs to delegation-sign SLDs
  - …..
Unsigned root and TLDs

- Today the root zone remains unsigned
  - Likely this way for some time
- Very few TLDs have signed their zones and offer delegation signatures
  - .se, .ru, .org
But I want my zone signed

- DNSSEC provides for local implementations to be able to insert local trust anchors, entry points into the secure system
  - E.g. Trust-anchors clause in BIND
- Problem: If you have too many it becomes a nightmare to maintain, so it doesn’t get used
DLV

- Enter DLV, Domain Lookaside Validation
  - Is an implementation feature, not a change to the protocol. A matter of local policy.
  - It enables access to a remote, signed, repository of trust anchors, via the DNS
- Implemented in BIND’s resolver so far. More to follow?
DLV lookup

• A DLV enabled resolver will try to find a secure entry point using regular DNSSEC processes and **IF IT FAILS**, and has DLV configured, will issue a search on the specified DLV tree
DLV lookup

End user client

Asks for www.isc.org

Root servers

Return no DNSSEC info

isc.org servers

Return RRSIG with the A RR

TLD servers

Return no DNSSEC info

Validate the response

Look for trust anchors
Follow normal DNSSEC checks, if possible
Use DLV if above fails and we have a trust anchor for it
Look for more specific match (www.isc.org.dlv.isc.org)
Go up until a match is found
Enabling DLV

• On the resolver (thus far BIND)
  – Add to named.conf
    • In the options section:
      // DNSSEC configuration
      dnssec-enable yes;
      dnssec-lookaside . trust-anchor dlv.isc.org.;
    • By itself
      trusted-keys {
          dlv.isc.org. 257 3 5
          "AQPap3+2+itqZpuujLA/j/eIeyls9HG09W8rm1uVpW0zZX4viyFQyGL91
          YkGUA2uTQ1ZHWrkJ36KYJpt8ZZ+tuIismJw9/AUnNzlPgwCfq5C2MOG
          Vh33nF60k67ppiapMYsOaDFbAQf5Vcc3L+BwfJjkXsZK73nD3gBEcdcm
          uJejeQ==",
      };
  • Get the Key from ISC’s web (http://www.isc.org/ops/dlv)
DLV registries

- ISC is operating a DLV registry free of charge for anyone who wants to secure their DNS.
- Likely some closed organisations will use their own (e.g. .mil)
- Have a look and use it!
Questions?