INTERNET SYSTEMS CONSORTIUM

Easying DNSSEC deployment New features in BIND

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 are at least 2 implementations of a DNSSEC aware resolver (BIND 9.3.2 and later and unbound)

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, .br, .bg, .pr.
  - .org in final stages of deployment process

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 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)

DLV Futures

- Current DLV model as implemented in BIND allows for only one DLV registry at a time
- Roy Arends has a good idea for an extension allowing multiple repositories, specified by the zone owner
- If idea moves forward ISC will implement it in BIND 9

NSEC3

- Addition to DNSSECbis to try to avoid zone walking
- ISC did some early implementations for workshops during protocol development
- Now working on production implementation
  - To become available in BIND 9.6 (later in 2008)

Online re-signing

- Re-sign expired signatures if key is online
- Incremental signing-as-we-go
- Adding support for crypto hardware devices

Improved tools

- Turnkey DNSSEC
  - Medium term future
  - Make it easier to set things up
    - Less steps
    - More automated actions
    - Automatic DS/DLV registration

Questions?