OTDR to RS.NET

Changes to the System

bill manning

bmanning@ep.net

History

- 1997 – IETF adds three standards track DNS “features”
  - IDN – IPv6 – DNS Security
- 1998 – A sub-group of the Root Ops build a testbed to evaluate feature impact
- 2000 – Augment the testbed with TLDs
- 2002 – Project changed names

Questions

- Sound Software Engineering practice discourages “rebuilding the airplane in flight”
- Is the code stable?
- Is the spec stable?
- Will there be infrastructure “issues”?

Rough Draft

- 2003, Testbed has root, INT, ARPA, MIL, GOV, COM, NET, JP, FR, KR, NL, SE, DE, CN, MY, and CH tlds.
- Some information at http://www.rs.net

First pass (IPv6) lessons

- IPv6 RRs can be added to nearly all deployed DNS nodes (not DJBDNS, ULTRA, yet)
- IPv6 transit triggers infrastructure issues
- Registry code needs to be able to IPv6 addresses for “glue”
- Most OS’es have IPv6 stacks that “mostly” work

Moving targets

- Min UDP packet size differences – 512 vs 1280
- EDNS0 support in the servers
- UDP fragmentation and TCP rollover
- Source Address selection

Bad Things

- thinking locally (local optimizations)
  - hardcoding IPv4 assumptions in:
    - firewalls – e.g. PIX
    - proxies
    - load balancers
    - layer 2 fabric (MAC/IP tables)
    - buffering
- Tree consistency / Dual Stack
- Mapped addresses / LinkLocal addresses

Testbed Interoperability (not always v6…)

- RFC 2535 vs DS (which one… :)
- Supported RR type behaviour – Type Code Roll
- Slaves and Caching

And the winner is:

- Most IPv6 issues appear to be known.
- IPv6 spec is mostly stable
- fast, edns0 capable code is becoming available.
- a draft recommendation to ICANN/DoC for formally augmenting the roots with IPv6 transport is being circulated.
- Many TLDs are already running IPv6 enabled servers

Mind the gap

- Registration Software not broadly capable for v6 registration
- DNS evolution has embraced/accommodated IPv6
- deployed infrastructure is non-IPv6 “friendly”
- IPv6 DNS will appear sporadic, less stable due to local optimizations for IPv4, common case capabilities, e.g. firewalls, proxy DNS servers, load balancers.
- These “landmines” must be eradicated for seamless integration of IPv6.

DNSSEC

- Primary drivers
- Current Weaknesses
- Lessons learned

Primary Drivers

- Opportunistic Encryption
  - Seed for dynamic IPSEC VPNs
- ENUM
  - preserving the integrity of the telephone number/name lookup
- Others are emerging

Weaknesses

- Key Strengths
- Key Management
  - Storage
  - Publication
- Algorithm (ab)use
- Misperception of DNSSEC use
  - PKI? yes or No?

Lessons

- UNIX file system
- Key Rollover
- DNS spec clarification
- Better Checking for operational integrity
- This is not quite ready for primetime
  - Tests are useful

IDNs

- Several TLDs have added IDN code-points
  - JP
  - CN
  - KR
- All have IETF/nameprep/punycode entries, legacy and local encodings are also possible
- Some have been digitally signed!

Questions?