Autonomica

IETF report on DNS

Lars-Johan Liman
Autonomica AB

Autonomica

DNS – isn't it dead yet?

... or "The Boatsmen of Volga",
volume 4711.

Autonomica

Jakob’s bug

- The new and the old versions of DNSSEC.
  - Delegation Signer (DS) stored at parent – "wrong" place!
  - Old resolvers don’t grok, but don't get the data.
  - Semi-old resolvers think they understand ...
- A client talking to new server through semi-old relay looses badly.

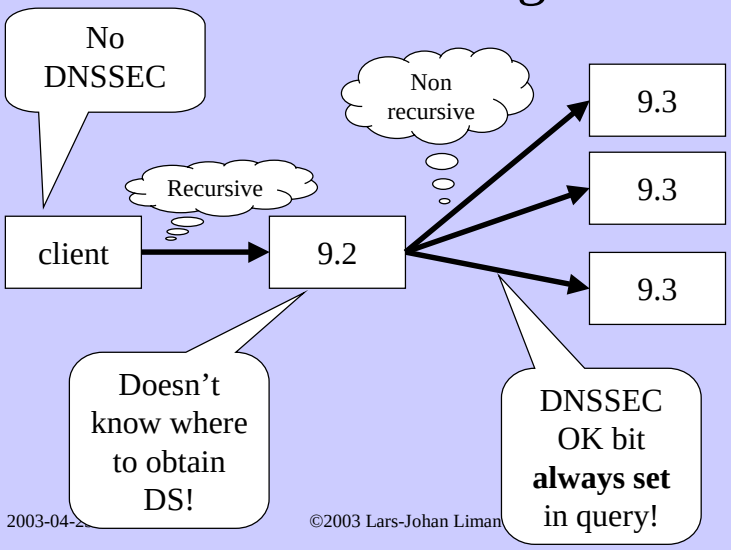
Autonomica

BIND 9.2 vs. 9.3

- BIND v9.2:
  - Uses DNSSEC according to RFC 2535.
  - Is not DS aware.
  - Does always set DNSSEC OK bit.
- BIND v9.3:
  - Uses DNSSEC with delegation signer (DS).

Autonomica

Jakob's bug



Autonomica

How solve?

1. Roll type codes for RRs?
   - KEY, SIG, and NXT.
2. New EDNS(x) version?
3. New DNSSEC OK bit?

- Versioning problem.
- Answer = f(*name, class, type, x, y, z, ...*)

Autonomica

Why rotate mnemonic?

- Need to change not only type code, but also mnemonic for RRs.
- Suppose:
  1. Save zone as a file on new server.
  2. Move it to old server.
  3. Load file on old server.
  4. Wrong type code used!

Autonomica

IPv6 support in the root?

- Name space fragmentation.
  - IPv6-only host can possibly reach IPv4 only servers. Ugly "NAT like" gatewaying.
  - IPv4-only host cannot reach IPv6 only servers.
- Pedagogic problem.
  - All zones must be served by both IPv4 and IPv6.
  - Not all need dual stack.
  - DNS entrepreneurs can sell the service you don't have yourself.
- Migrate root at early stage.

Autonomica

LLMNR

- LLMNR - Link Local Multicast Name Resolution a.k.a Multicast DNS (mDNS).
- Unqualified Names?
  - How are they resolved?
  - Not running on port 53 anymore because invalid queries were escaping to the root servers.
- TTL=255 on send, check on receive
  - TTL=255 came out of concern for spoofed responses. Is there an alternative?
- If a host has both routable and LL addrs ... ?

Autonomica

Wildcards

- Wildcard Clarify
- Clarify wild cards. Expand on wording in 1034.
- Authenticated Denial of Existence in DNSSEC
  - FUD: wild cards are a problem for DNSSEC
  - How many NXTs are needed, one per label depth?
  - Should we optimize the proof?
  - Why do all 'correct' examples have only one or two NXTs in the negative answer proof?

Autonomica

Wildcards

- Code vs Spec:
  - Almost no one gets it right
  - Why not change spec to reflect implementations?
  - Pandora's box!
  - Different code bases differ on how handled.
- "Perverse" name cases
  - "*.*.example.org" is syntactically valid and causes no problems.

Autonomica

6DNAR

(IPv6 Domain Name Auto-Registration)

Why:

- Small networks like home network should be able to use IPv6 to easily auto-configure without DNS and DHCP servers
- My comment: Much can be replaced with DHCP.
  - DHCP is not hard.

Autonomica

DNSSEC docs

Open Questions

- Unknown RR type name compression in rdata is a **MUST NOT**.
  - case closed
- Algorithm requirements (RSA/SHA1 mandatory and DSA as optional)
- Dropping KEY RR in additional section of response

Autonomica

DNSSEC docs

- Should security aware resolvers cache known bad data, where sig RRs can't be verified?

Autonomica

DS changes

- Added clarification text
- Never add KEY RR to additional.
- Eliminate NULL KEY definition from 2535
- References fixed

Autonomica

dnssec-2535-compat

- Another semantics change (the last one?)
- 2535 only sent NXTs as part of NXDOMAIN answers
- Silent on the issue of sending NXTs in positive answers?
  - Never tells you to send it
  - Never tells you **NOT** to send it.

Autonomica

dnssec-2535-compat

Why we have to fix it:

- 2535-aware resolvers don't see insecure delegations
  - Strong incentive to not sign zones
  - To get deployment, have to fix it

Good news:

- Several possible solutions
  - replace the DO bit
  - roll type codes and mnemonics for SIG/KEY/NXT
  - roll just NXT

Autonomica

dnssec-2535-compat

- Case with unknown types because of type code roll much simpler
  - no chance of them being rewritten
  - no dependency on them not being rewritten
  - unknown RRs get clearly passed through or they don't

Autonomica

DNSOP

- After 4 years: I and Ray have resigned as chairs.
  - New chairs: Rob Austein & Dave Meyer
- 6to4 delegations. Problematic. Doesn't follow IPv6 delegation trees and their ISPs.
- Problem: population.
  Solutions:
  - wildcard? No! Please not!
  - synthesis?
  - dynamic DNS?

Autonomica

.local zones

- Many bogus queries.
  - repetitive.
  - invalid TLDs.
- Stop queries with invalid TLDs
  - Process locally as much as possible.
  - Reduce load high up in server tree (esp. root).
- Stats
  - at university DNS: 49 % root queries are .local
  - at ISP DNS: 24 % root queries are .local
  - M.root local: 5th, 1.8%

Autonomica

.local zones

- Suggestion for DNS operators:
  - provide a template config
- Suggestion for DNS opmplementors:
  - encourage a temlate config in dist.
- Suggestion for NAT implementors:
  - filter och process the DNS pack for "local" zonest
- Suggestion for IANA/ICANN:
  - delegate .local to AS112 project, like 10.in-addr.arpa et. al. (Hmmm ...)

Autonomica

Response size

- Recommend TLD holders to use "same name" hack to compress better.
  - No longer optional to return query again. Long query, less room. IDN.
  - Useless with repsonse, unless at least two glues in additional.

Autonomica

Contact info

http://www.autonomica.se/liman/
presentations/ripe/ripe45-dns.pdf

liman@autonomica.se