DNS Hacktivities during Hackathon, IETF121 Dublin

Philip Homburg Stéphane Bortzmeyer Shumon Huque Ondřej Súry Johan Stenstam

November 3, 2024

Implementation of CHAIN Query Requests in DNS (RFC 7901)

Philip Homburg

- **What:** allow a stub resolver to request all DNS records needed for validation in one go (as opposed to sending many queries for DS and DNSKEY records)
- **Why:** 8 year old experimental RFC, no implementations (that I'm aware off) Test the flexibility of our Rust library (Domain crate)
- **Result:**
  - Very hacky server part
  - Hacky incomplete client part
  - But, it works!

More stuff

Stéphane Bortzmeyer and Shumon Huque

- Ossification of the DNS : hard to introduce new features
- Greasing, like in TLS and QUIC
- Implementation in an authoritative name server
- Issues raised : is it acceptable to risk breaking ?

And of course, disagreement about an existing RFC.

Tamás Csillag

- DNSKEY ksk rollover - successfully tested a new idea to do a roll between two providers will follow up with some kind of summary or rfc draft

DELEG implementation in BIND 9

Ondřej Surý

- Proof of Concept DELEG implementation in authoritative answers. **done for signed zones**
- Proof of Concept for using DELEG instead of NS records. **partly done**

The Multi-Signer, Generalized Notify, DSYNC, DNS UPDATE, etc, Project

Lars-Johan Liman, Tomas Agard, Johan Stenstam

- In the multi-signer work we needed a "`NOTIFY(DNSKEY)`" when new DNSKEYs are introduced.
- That led to the work on Generalized Notify and `NOTIFY(CDS)` and `NOTIFY(CSYNC)`. **DONE**
- That triggered the work on delegation sync via DNS UPDATE. **MOSTLY DONE**
- Now we're circling back to multi-signer and the `NOTIFY(DNSKEY)`. **DONE**
- . . . and multi-signer is becoming distributed: The zone designates the "signers" via the experimental `MSIGNER` RRset. **DONE**
- . . . then the so-called "multi-signer sidecars" (next to each signer) locate each other via the `MSIGNER` RRset and establish authenticated communication. **ONGOING**

Experiments with MTL Mode in DNS Resolvers

Joe Harvey (jsharvey@verisign.com)
Swapneel Sheth (ssheth@verisign.com)
Willem Toorop (willem@nlnetlabs.nl)

IETF Hackathon Efforts

- IETF-118
  - Introduced MTL mode open source library
- IETF-120
  - Demonstrated SLH-DSA-MTL signatures on zone file
- IETF-121
  - Implemented draft-fregly-dnsop-slh-dsa-mtl-dnssec
    - NSD providing full and condensed signatures based on EDNS option flag
    - Unbound providing verification of SLH-DSA-MTL signatures
      - Verifies condensed signatures from cached ladders
      - Requests full signatures for records that do not have a cached ladder

IETF-121 NSD & Unbound Testing Results

SUCCESS!

Unbound Config

```
server:
    trust-anchor: ". DS 20326 8 2
e06d44b80b8f1d39a95c0b0d7c65d08458e880409
bbc683457104237c7f8ec8d"
    trust-anchor: "example.com. DS 42788 248 2
d66cf16674c72d32341e0d0781a20819352be3e57
7d8082d2df2bcc2a8394a61"


stub-zone:
    name: example.com
    stub-host: stub.example
    stub-addr: 206.189.116.190
```

Unbound Log

```
libunbound[178913:0] info: MTL signature (248) - Full Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification FAILED!
libunbound[178913:0] info: MTL signature (248) - Full Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com has address 192.0.2.1
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com has IPv6 address 2001:db8::1
libunbound[178913:0] info: MTL signature (248) - No Full Signature
libunbound[178913:0] info: MTL signature (248) - Condensed Signature Verification SUCCESS!
example.com mail is handled by 10 mail.example.net.
```