Domain crate update: developments, plans; what would you like to see?

Philip Homburg
philip@nlnetlabs.nl

About domain

Presented here at FOSDEM two years ago by Martin Hoffmann:

`https://archive.fosdem.org/2024/schedule/event/fosdem-2024-2853-domain-a-modular-rust-dns-toolkit/`

Goals (my personal opinion):

- most complete DNS library
- supports low-level primitives for high performance and high-level primitives for ease of use
- foundation of our Rust-based DNS applications

Timeline

- 2024 — STF grant for development of Domain
- 2025 — Work on Cascade, a new DNSSEC signer

2024 — STF grant

- Client transports
- Server transports
- DNSSEC
- dnsi
- dnst

Client transports

- `dgram` Generic over datagram transports such as UDP.
- `stream` Generic over stream transports such as TCP and TLS. Also supports AXFR and IXFR.
- `multi_stream` automatically sets up a new stream when the old one doesn't work anymore. `dgram_stream` fallbacks to `multi_stream` when `dgram` receives a reply with the TC flag set.
- `cache` for caching replies of an upstream transport
- `redundant` for using the best upstream among multiple alternatives and `load_balancer` to distribute load over multiple upstreams.
- `tsig` Sign requests and verify that replies are correctly signed (using TSIG).

Server transports

- Transports for UDP, TCP, and TLS.
- Middleware for COOKIES, NOTIFY, TSIG, AXFR and IXFR.
- Very simple query routing based on QNAME.

DNSSEC

- DNSSEC validation for reply messages returns Secure, Insecure, Indeterminate, or Bogus.
- `validator` is a DNSSEC validating client transport. It turns Bogus into SERVFAIL (except when CD is set) and sets AD when secure, etc.
- DNSSEC signing. NSEC and NSEC3 chain generation and signing of a zone.
- A generic DNSSEC key manager that knows about key rolls. This part doesn't do any signing but directs the application what the sign and when.
- Supprt for two crypto backends at the moment: Ring crate and the Rust bindings for OpenSSL. We could add more, such as Graviola.

dnsi and dnst

- dnsi is a program querying the DNS. We didn't get as far as we wanted so now it has funtionaly similar to dig. We did try to make the output more friendly to non-experts.
- dnst is a program that meant to replace the ldns utilities. We currently have emulation of ldns-key2ds, ldns-keygen, ldns-notify, ldns-nsec3-hash, ldns-signzone, and ldns-update.
- We also added native dnst versions that have improved command line syntax, some extra features.
- We added one new utility called `keyset` that implements a DNSSEC key manager. This can be used as a building block for a DNSSEC signer.

2025 — Cascade

- bump-in-the-wire signer
- review hooks for signed and unsigned zones
- external key manager
- uses KMIP to talk to ~~kmip2pkcs11~~ morfen to avoid loading an untrusted binary blob into the main Rust application

New-base

- Octets abstraction causes too much complexity

```
Octs: FromBuilder
        + From<&'static [u8]>
        + OctetsFrom<Vec<u8>>
        + Default
        + Clone
        + Send,
Octs::Builder: EmptyBuilder + Truncate + AsRef<[u8]> + AsMut<[u8]>,
<Octs::Builder as OctetsBuilder>::AppendError: Debug,
```

- Server middleware layer is too complex

```
impl<RequestOctets, NextSvc, RequestMeta>
    CookiesMiddlewareSvc<RequestOctets, NextSvc, RequestMeta>
where
    NextSvc: Service<RequestOctets, RequestMeta>,
    NextSvc::Future: Unpin,
    RequestOctets: Octets + Send + Sync + 'static + Unpin + Clone,
    RequestMeta: Clone + Default + Send + Sync + 'static,
```

- Changing the interface allows for efficiency gains

Plan

- release Cascade (end of Q2 2026)
- work on transition to new-base
  - new zonefile
  - new zone storage
- work on dnsi/dnsi/mimir

What would you like to see

Where should we go?

- more complete stub resolver
- mDNS
- UPDATE/SIG(0)
- sample applications / servers