Dnstap Updates

Chris Mikkelson

OARC 35

May 7, 2021

FARSIGHT SECURITY

Dnstap Recap

Dnstap Recap

- Flexible, structured, binary log format for DNS software
- Supports both realtime stream and file-based processing
- Minimal overhead on instrumented software, non-blocking

Dnstap Recap

- Binary format: protobuf definition
  - https://github.com/dnstap/dnstap.pb
- Stream / File format: Frame Streams
  - Lightweight streaming protocol; file is unidirectional stream
  - https://github.com/farsightsec/fstrm (C reference implementation)
  - https://github.com/farsightsec/golang-framestream (pure go package)

Dnstap Recap

- Exports DNS messages as seen by instrumented server
- Exports relevant context along with raw message
- “Relevant”, as expected, evolves over time.
- Discussion on mailing list: see https://dnstap.info for info.

Update 1: Added Protocols

Update 1: Added Protocols

- Context includes protocol info
  - SocketFamily (INET, INET6)
  - Ports (query_port, response_port)
  - SocketProtocol (UDP, TCP)
- DNS over TLS, DNS over HTTPS?
- Added DoT, DoH values to SocketProtocol

Update 1: Additional Protocols - Open Issues

- Blurring protocol layers: DoH is not a trivial TCP transport.
- HTTP/2 stream ID replaces DNS message ID, augments port info.
- DNS over HTTP/2 vs. HTTP/3 (QUIC/UDP)?
- May need more fields to capture these details.

Update 1: Additional Protocols - Open Issues

- Other protocols:
  - DNS over QUIC
  - DNSCrypt

Update 2: Policy Reporting

Update 2: Policy Reporting

- Policy enforcement mechanisms have advanced since the days of empty zones on resolvers (e.g., Response Policy Zones)
- Policy enforcement a nontrivial part of message processing. Need visibility.
- Added “policy” field earlier this year:
  - What rule was triggered
  - What identifier matched the rule (client IP, qname, etc.)
  - What action was taken (drop, NXDOMAIN, etc.)

Update 2: Policy Reporting

- Written with RPZ in mind
  - Actions: NXDOMAIN, empty or replace answer, force TCP, or drop
  - Identifiers: query name, client IP, rdata address, NS IP or name.
- RPZ is well-known with rich functionality, covers many (if not most) use cases
- Other mechanisms supported through policy “type” string.
  - New actions needed? Suggestions welcome.
  - New identifiers? Multiple identifiers? Same.

Housekeeping

Housekeeping

- Open issues on dnstap.pb:
  - Cache Status
  - Message Tag
- Many years old, multiple proposals for each, no clear consensus which to adopt, if any

Housekeeping

- JSON Format
  - Protobuf (binary) format a barrier to entry
  - Ad-hoc JSON output added to dnstap tools
  - Standard JSON binding needed for tool-independent workflows.
- Interested? Let's talk
  - http://lists.redbarn.org/mailman/listinfo/dnstap

Questions?