DNS Zone Transfer-over-TLS
(XoT)

draft-hzpa-dprive-xfr-over-tls

Han Zhang
Pallavi Aras
Willem Toorop
Sara Dickinson
Allison Mankin
XoT - Background

Why XoT?

- Zone data can be collected via passive monitoring on-the-wire
- The main motivation for XoT is to prevent zone data collection
- TSIG provides data and source integrity but not data privacy

What is XoT?

- Encryption of DNS zone transfer (IXFR & AXFR) using DNS-over-TLS [RFC7858]
XoT Draft Timeline

- **MARCH 2019: draft-hzpa-dprive-xfr-over-tls-00 & -01:**
  - First placeholder versions published just before IETF 104 (Prague)
  - IETF 104 Hackathon: Secondary-side AXFR-over-TLS was implemented in Unbound (Unbound already supported TLS and also AXFR for RFC7706).

- **JULY 2019: draft-hzpa-dprive-xfr-over-tls-02:**
  - More detailed, outlined in following slides
Use cases

- **Confidentiality**: Encrypting zone transfers will defeat zone content leakage that can occur via passive surveillance

- **Authentication**: Use of single or mutual TLS authentication (in combination with ACLs) can complement and potentially be an alternative to TSIG

- **Performance**:
  - Existing XFR implementation must be backwards compatible [RFC1034]/[RFC1035]
  - Current usage of TCP for IXFR is sub-optimal in some cases e.g. TCP connections are frequently closed after a single IXFR
AXFR: Existing mechanism vs AXoT

Existing

UDP

NOTIFY

NOTIFY Response

SCA Request

SOA Request

AXFR Request

AXFR Response 1 (Zone Data)

AXFR Response 2 (Zone Data)

AXFR Response 3 (Zone Data)

TCP session

Primary

Secondary

XoT-Based AXFR

UDP

NOTIFY

NOTIFY Response

SCA Request

SOA Request

AXFR Request

AXFR Response 1 (Zone Data)

AXFR Response 2 (Zone Data)

AXFR Response 3 (Zone Data)

UDP (or part of TCP session)

Primary

Secondary

TLS session
AXFR: Existing mechanism vs AXoT

Existing

- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- AXFR Request
- AXFR Response 1 (Zone Data)
- AXFR Response 2 (Zone Data)
- AXFR Response 3 (Zone Data)

XoT-Based AXFR

- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- AXFR Request
- AXFR Response 1 (Zone Data)
- AXFR Response 2 (Zone Data)
- AXFR Response 3 (Zone Data)
- TCP session
- TLS session
IXFR: Existing mechanisms vs IXoT

**Existing IXFR**
- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request
- IXFR Response (Zone Data)
- IXFR Request
- IXFR Response (Zone Data)
- Retry over TCP if required.

**XOT-Based IXFR**
- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request 1
- IXFR Response 1 (Zone Data)
- IXFR Request 2
- IXFR Response 2 (Zone Data)
- UDP
- UDP or TCP
- UDP or TCP
- UDP (or part of TLS session)
- TLS session
IXFR: Existing mechanisms vs IXoT

**Existing**

- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request
- IXFR Response (Zone Data)

**XOT-Based IXFR**

- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request 1
- IXFR Response 1 (Zone Data)
- IXFR Request 2
- IXFR Response 2 (Zone Data)

- UDP
- UDP or TCP
- UDP (or part of TLS session)
- TLS session

**Retry over TCP if required.**

**High rates possible**
IXFR: Existing mechanisms vs IXoT

**Existing**

- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request
- IXFR Response (Zone Data)

**XOT-Based IXFR**

- NOTIFY
- NOTIFY Response
- SOA Request
- SOA Response
- IXFR Request 1
- IXFR Response 1 (Zone Data)
- IXFR Request 2
- IXFR Response 2 (Zone Data)

Primary

- UDP
- UDP or TCP

Secondary

- UDP
- UDP or TCP

Retry over TCP if required.

TLS session

Primary

- UDP (or part of TLS session)
XoT - Authentication mechanisms

<table>
<thead>
<tr>
<th>Method</th>
<th>Secondary</th>
<th></th>
<th>Primary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Auth</td>
<td>Channel Conf</td>
<td>Data Auth</td>
<td>Channel Conf</td>
</tr>
<tr>
<td>TSIG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppo</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Strict</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Mutual</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>ACL on master</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conclusion:** Using TSIG, Strict TLS and an ACL on the primary provides all 3 properties for both parties with reasonable overhead.
XoT - Authentication mechanisms

**Conclusion:** Using TSIG, Strict TLS and an ACL on the primary provides all 3 properties for both parties with reasonable overhead.
Policy Management for XoT

- ‘Transfer Group’ - entire group of servers involved in transfers of a given zone (all primaries, all secondaries)

- The entire transfer group SHOULD have the same policy wrt (no weak point):
  - TSIG, TLS (O, S or m), IP ACL

- CHALLENGE: How to configure, enforce and test policy implementation?
  - Often involves different operators, different software, hidden servers
  - Feedback please 😊
Current & future work

- **Latest implementation**
  - Unbound release 1.9.2 includes secondary-side AXoT
  - Server side AXoT can be deployed using a TLS proxy
  - IETF 105 Hackathon began work to add XOT support to dnsjava library (work in progress).

- **Open questions in the draft**
  - SHOULD/MUST SOA query be on a TLS connection?
  - Specify MUST use TLS 1.3?
  - Padding?

- **Next steps**
  - Review please & Adoption?