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

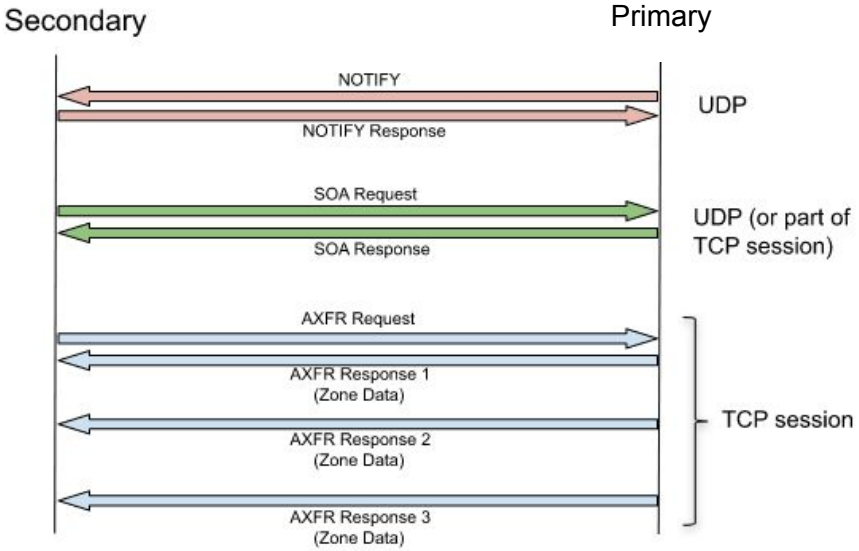
- **MARCH 2019: draft-hzpa-dprive-xfr-over-tls-00 & -01:**
  - First placeholder versions published just before IETF 104 (Prague)
  - IETF 104 Hackathon: Secondary-side AXFR-over-TLS was implemented in Unbound (Unbound already supported TLS and also AXFR for RFC7706).

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

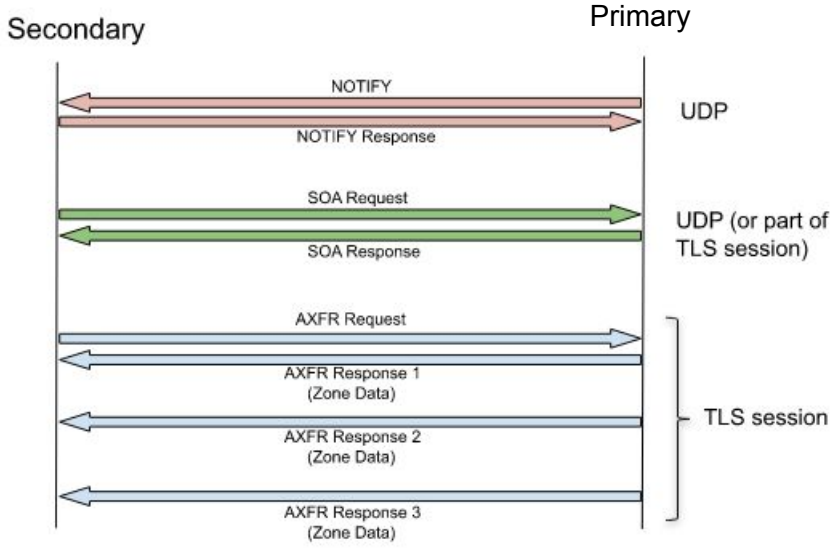
Use cases

- **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

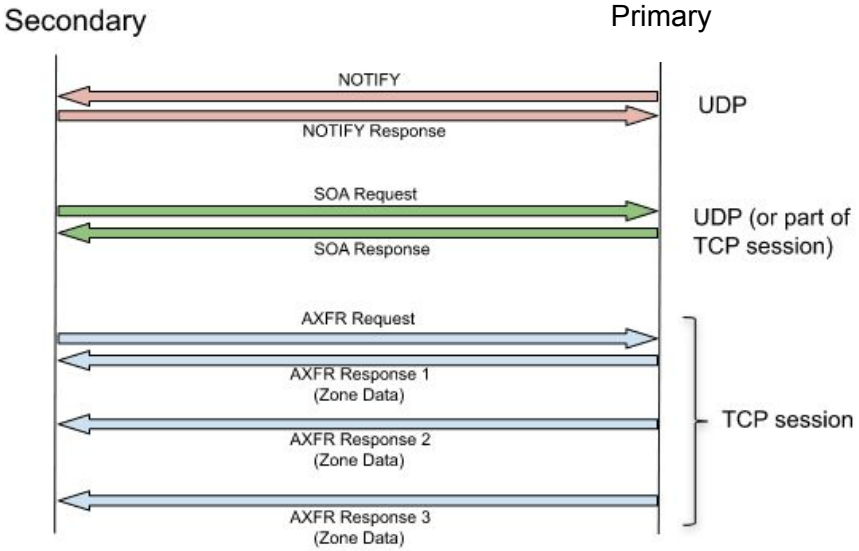


Existing

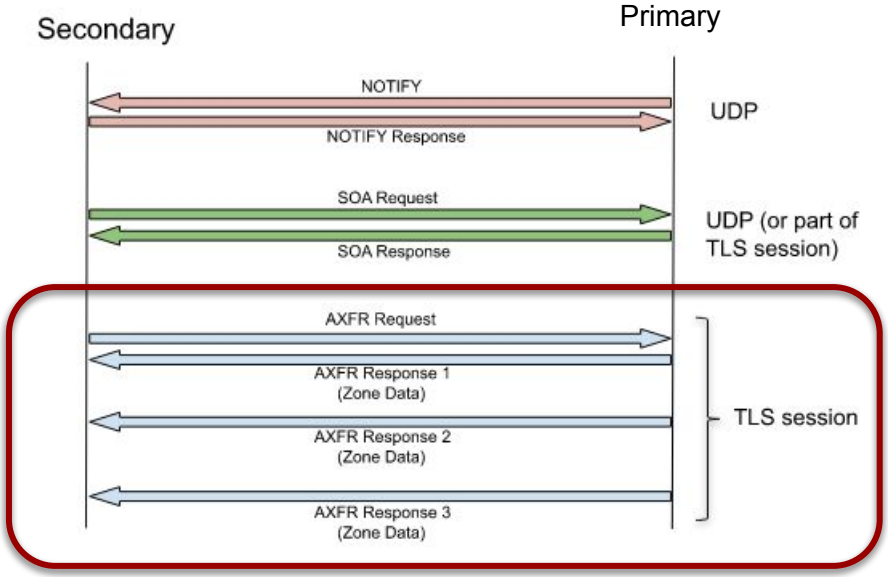


XoT-Based AXFR

AXFR: Existing mechanism vs AXoT

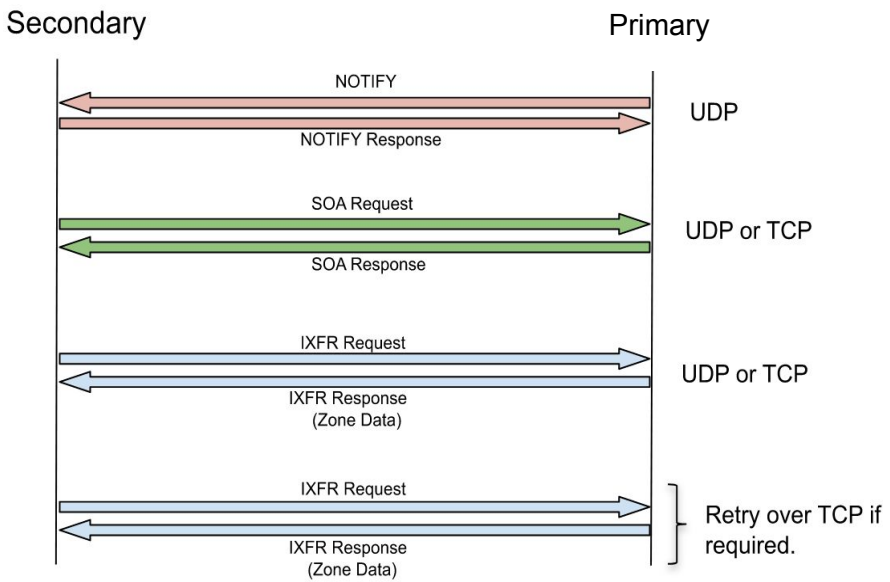


Existing

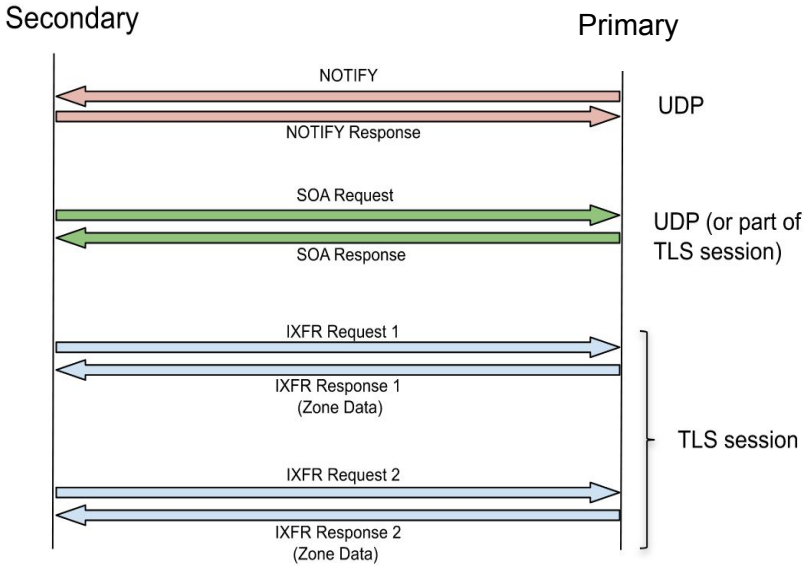


XoT-Based AXFR

IXFR : Existing mechanisms vs IXoT

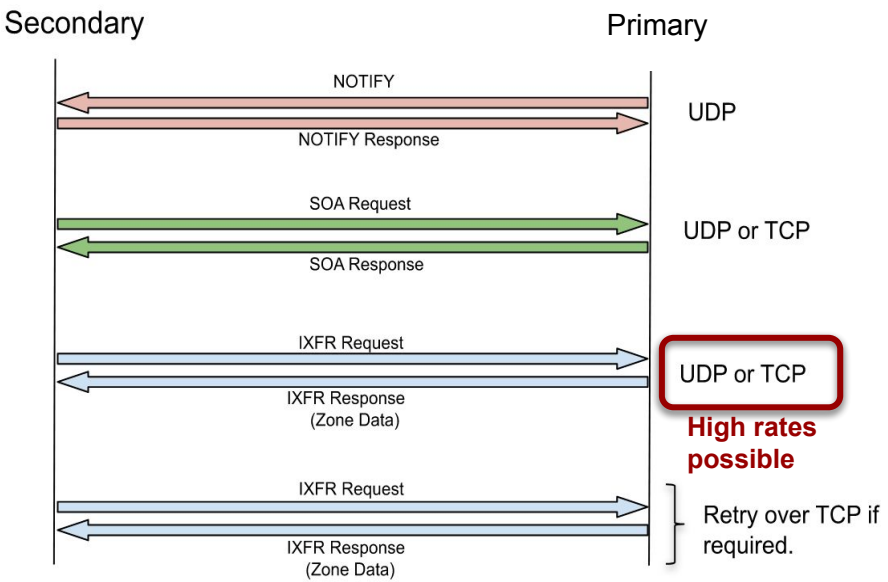


Existing

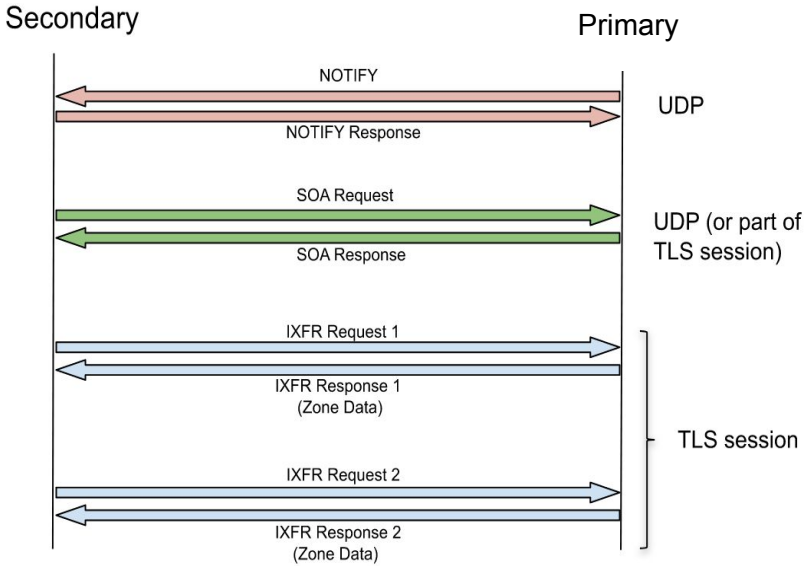


XOT-Based IXFR

IXFR : Existing mechanisms vs IXoT

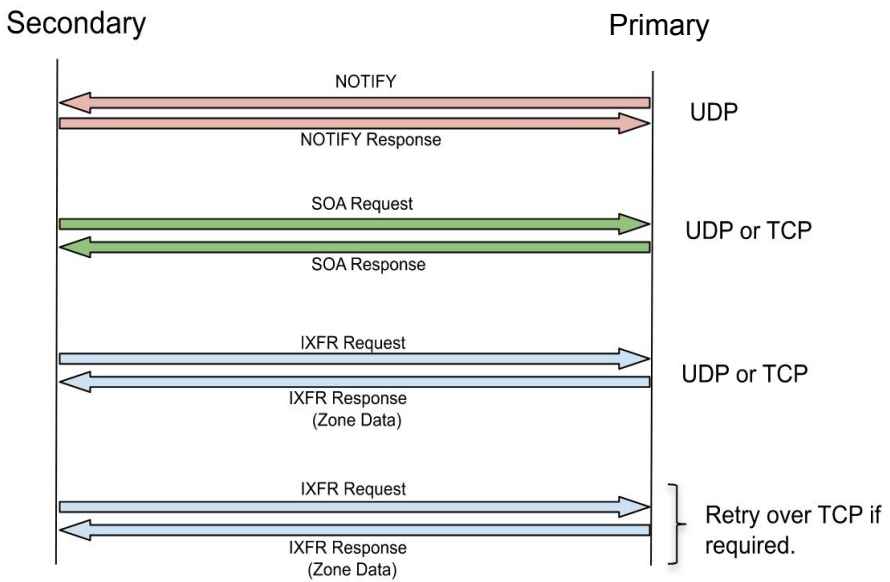


Existing

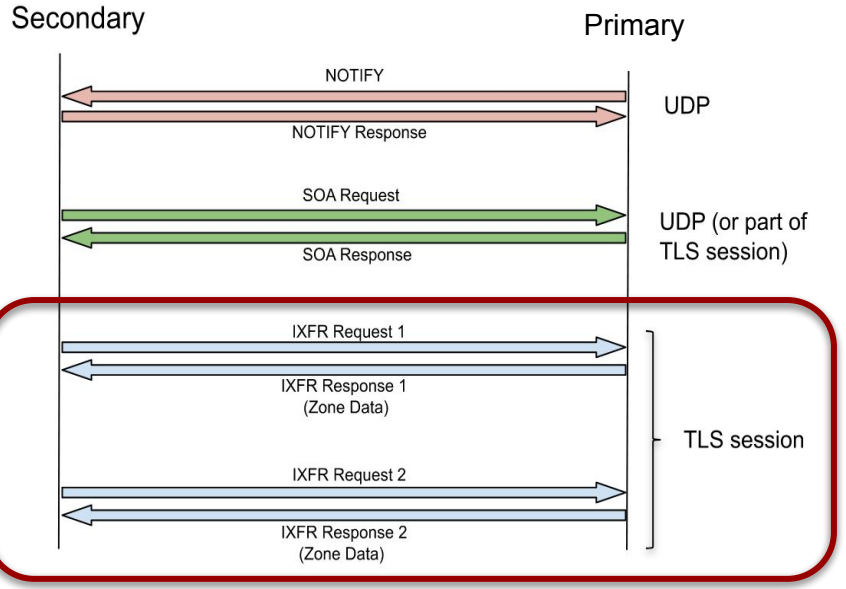


XOT-Based IXFR

IXFR : Existing mechanisms vs IXoT



Existing



XOT-Based IXFR

XoT - Authentication mechanisms

Method		Secondary			Primary		
		Data Auth	Channel Conf	Channel Auth	Data Auth	Channel Conf	Channel Auth
TSIG		■			■		
TLS	Oppo		■			■	
	Strict		■	■		■	
	Mutual		■	■		■	■
ACL on master							■

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

XoT - Authentication mechanisms

Method		Secondary			Primary		
		Data Auth	Channel Conf	Channel Auth	Data Auth	Channel Conf	Channel Auth
TSIG		●			●		
TLS	Oppo						
	Strict		●	●		●	
	Mutual						
ACL on master							●

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?