XFR over TLS

Encrypting DNS zone transfers

Shivan Kaul Sahib
Sara Dickinson
Allison Mankin
Willem Toorop
Pallavi Aras

What is the problem?

DNS zone transfers happen in plain text

DNS zone transfers happen in plain text => passive surveillance.

DNS zone transfers happen in plain text => passive surveillance.

TSIG doesn’t provide data privacy.

DNS zone transfers happen in plain text => passive surveillance.

TSIG doesn’t provide data privacy.

NSEC3/NSEC5 prevent zone enumeration, but not leakage through zone transfer.

Why should we care?

Contents of zone can contain sensitive corporate information.

Contents of zone can contain sensitive corporate information.

Regulatory or policy reasons why the zone contents must be kept private.

Solution!

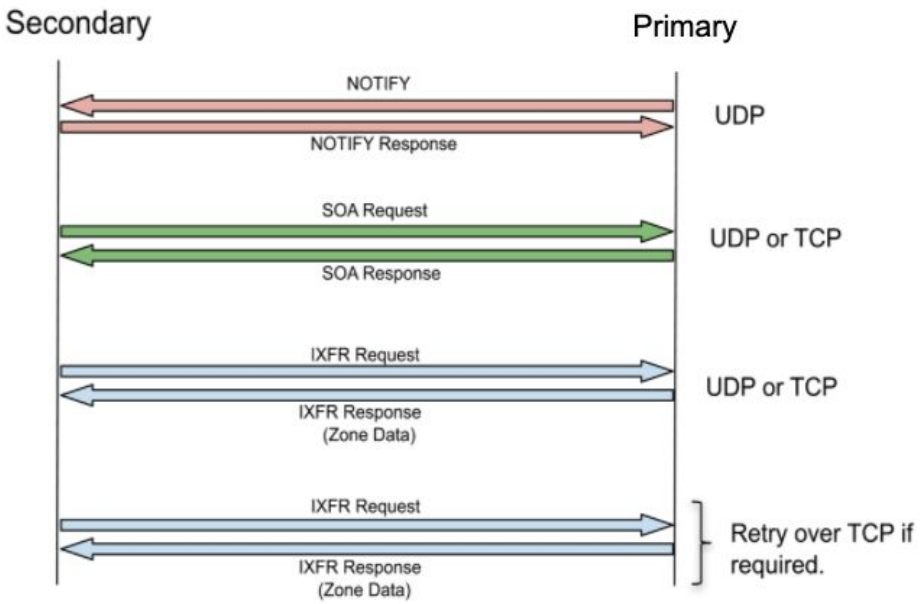
Encrypt AXFRs (full) and IXFRs (incremental) using TLS as a transport.

XoT: XFR-over-TLS

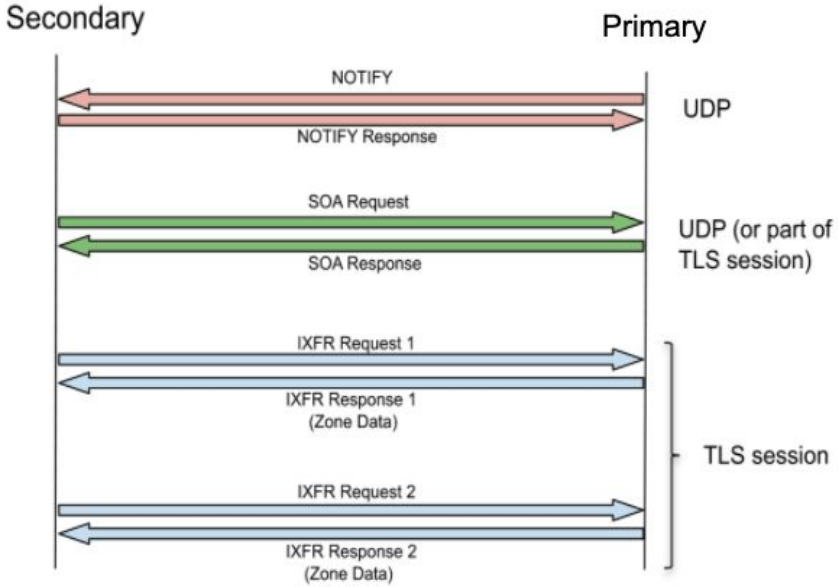
Current status

Adopted draft by IETF DNS Privacy Working Group

Working on setting up testbed to answer some open questions



Existing



XOT-Based IXFR

Open Questions

Open Questions

Threat model

Open Questions

Threat model

Padding recommendations

Threat Model

1. Difference between leakage addressed by XoT and NSEC3/NSEC5?

Threat Model

1. Difference between leakage addressed by XoT and NSEC3/NSEC5?
2. Would developing a DNS zone-specific threat model be of use?

Threat Model

1. Difference between leakage addressed by XoT and NSEC3/NSEC5?
2. Would developing a DNS zone-specific threat model be of use?
3. Documented cases of passive surveillance on DNS zone transfers?

Padding

How should padding be done for

1. AXFR, to minimize leakage of zone size

Padding

How should padding be done for

1. AXFR, to minimize leakage of zone size
2. IXFR, to minimize leakage of update rates, DNSSEC resigning

Padding

How should padding be done for

1. AXFR, to minimize leakage of zone size
2. IXFR, to minimize leakage of update rates, DNSSEC resigning

Is this a worthwhile goal? Arguments either way?

Padding experiments

Unsigned zone, regular updates

Large DNSSEC NSEC3 signed zone, no updates

Large DNSSEC NSEC3 signed zone, with updates

Thank you!

Shivan Kaul Sahib | @shivan_kaul | ssahib@salesforce.com
Sara Dickinson | @SinodunCom | sara@sinodun.com

Summary: Questions for Discussion

Threat Model

1. NSEC3 vs XFR threat?
2. General DNS zone threat model?
3. Cases of passive surveillance on zones?

Padding

1. Experiment design for padding measurements
2. Is this worthwhile?

Extra Slides

Padding Policy

- **Requirements could be context specific**

- Packet sizes and timings vary depending on several factors:
  - Frequency of updates (manual reload vs steady dynamic updates vs batch dynamic)
  - ‘Condensation’ of changes
  - DNSSEC signed (NSEC/NSEC3)
    - Ongoing resigning of records as signatures expire (spikes or jittered)
    - Updates trigger resigning -> new RRSIGs

- Next slides present two extremes of patterns/packet sizes

Takeaways

1. Unsigned zones can directly leak number of record updates even when encrypted.

Takeaways

1. Unsigned zones can directly leak number of record updates even when encrypted.
2. Re-using a single connection for multiple zones would disguise the update pattern (+ performance gain)

Takeaways

1. Unsigned zones can directly leak number of record updates even when encrypted.
2. Re-using a single connection for multiple zones would disguise the update pattern (+ performance gain)
3. DNSSEC signing with jitter disguises the actual updates, but pattern varies with zone size and signing details

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							●

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

NSEC3 usage

Nominet UK (operates .co.uk) and uses NSEC3 as the default. We know of research data that shows the majority of DNSSEC signed SLDs do use NSEC3