Hands on DNS Resilience

Online for NOMINET
20-24 September 2021

The material in these slides is based on Karst Koymans' CIA course material, see: https://www.os3.nl/2020-2021/courses/cia/start

Required!

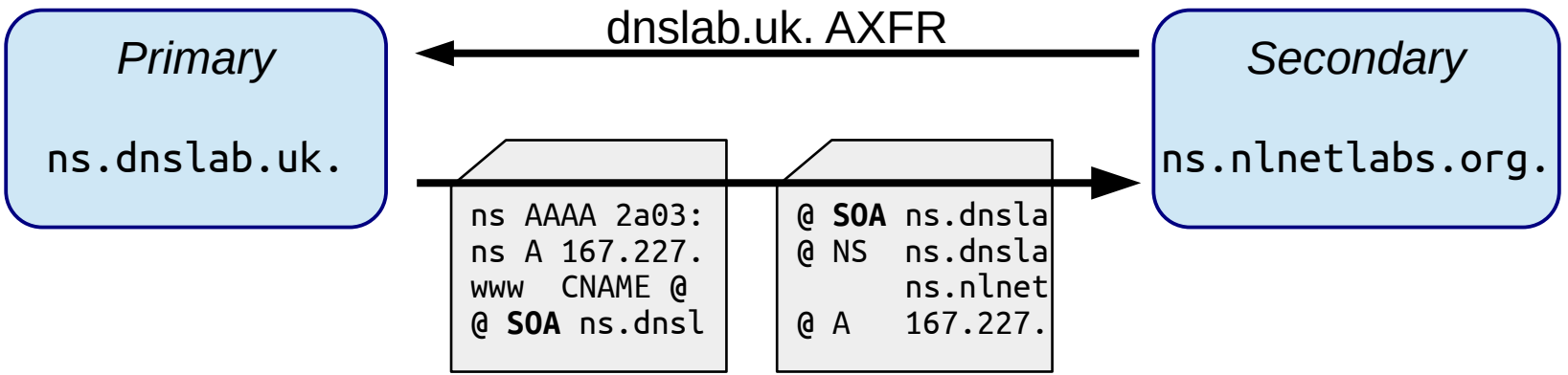
- RFC2182:

  “The DNS requires that multiple servers exist for every zone”

- Why?
  - Resilience
  - Spread the Load
- How?

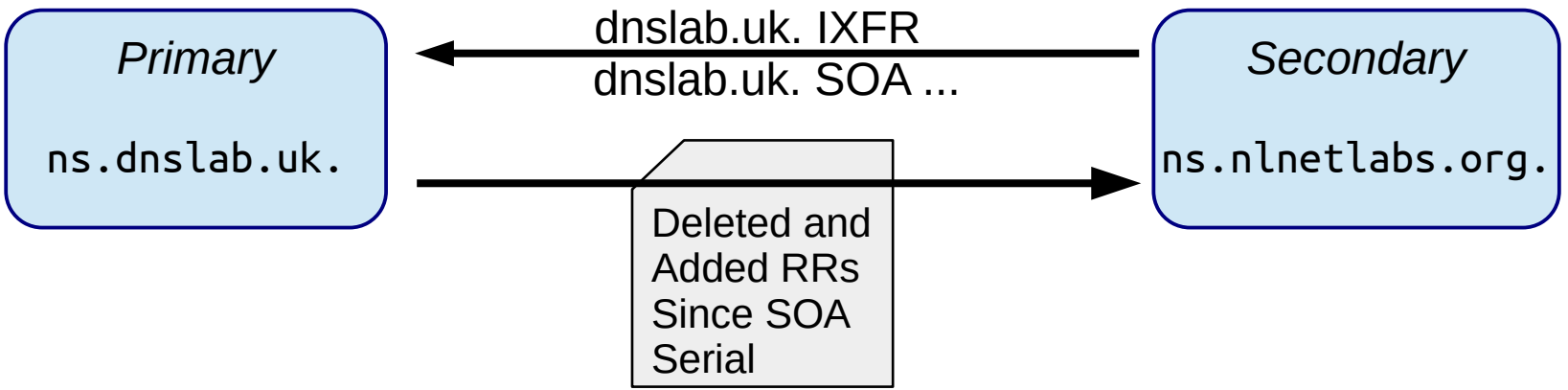
Zone transfers

- Pull
  - When Secondary starts without data
  - Query Type `AXFR` (Authoritative Transfer)



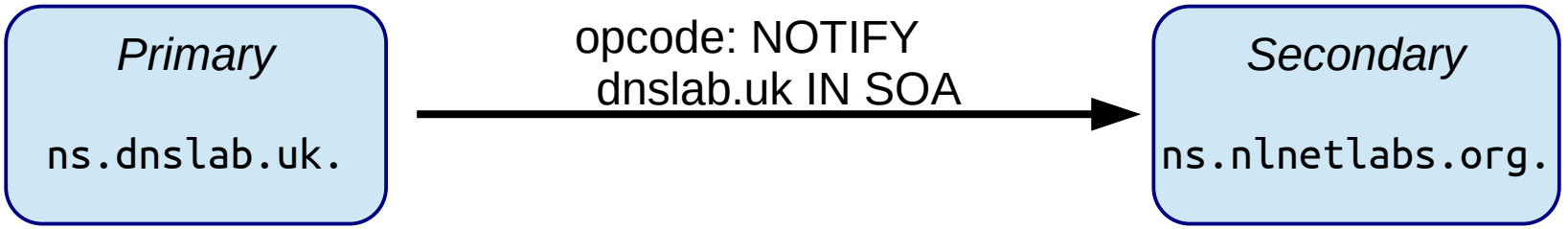
Zone transfers

- Pull
  - When data changed
    - Slave checks after SOA refresh time
  - Query Type `IXFR` (Incremental Transfer)
    - Include known SOA in authority section



Zone transfers

- Push
  - Special opcode (4) NOTIFY
- Slave behaves as if SOA refresh timed out



Zone transfers

- Push
  - Special opcode (4) NOTIFY

Network Working Group
Request for Comments: 1996
Updates: 1035
Category: Standards Track

P. Vixie
ISC
August 1996

A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)

Status of this Memo

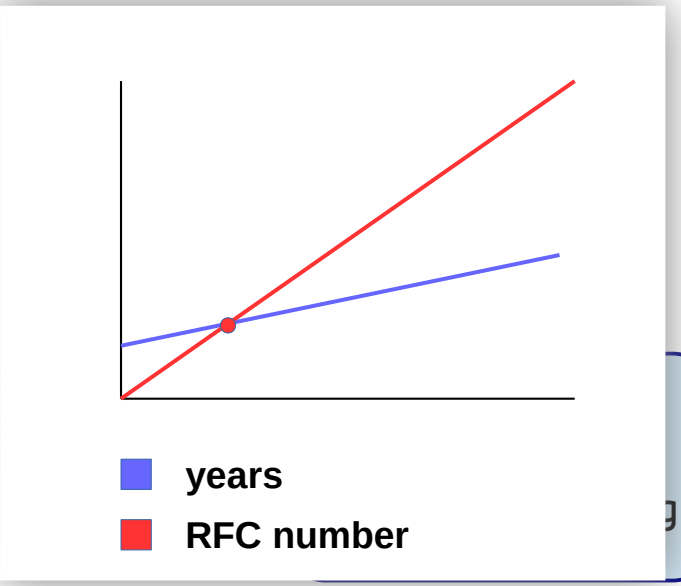
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This memo describes the NOTIFY opcode for DNS, by which a master server advises a set of slave servers that the master's data has been changed and that a query should be initiated to discover the new data.

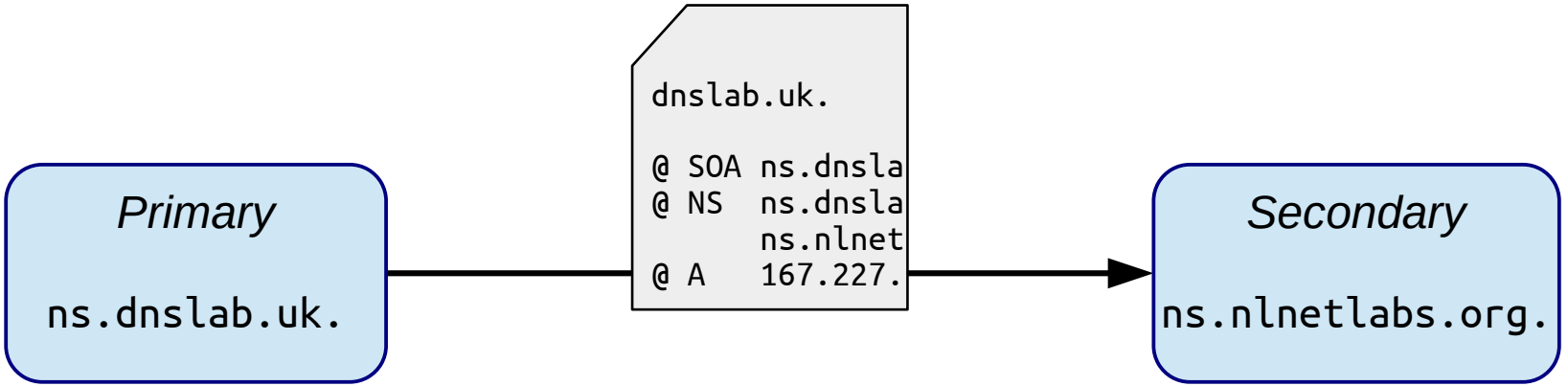
1. Rationale and Scope

1.1. Slow propagation of new and changed data in a DNS zone can be due to a zone's relatively long refresh times. Longer refresh times



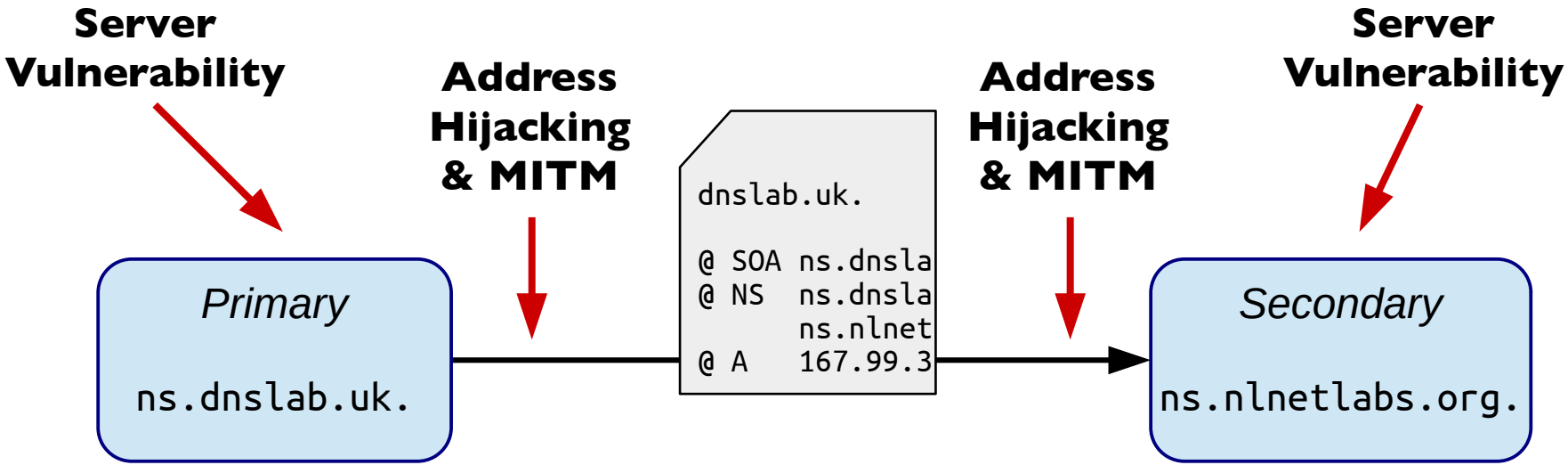
Zone transfers

- Zone transfers are often limited to slave servers
  - DNS data: public or semipublic?
  - IP level ACL… safe enough?



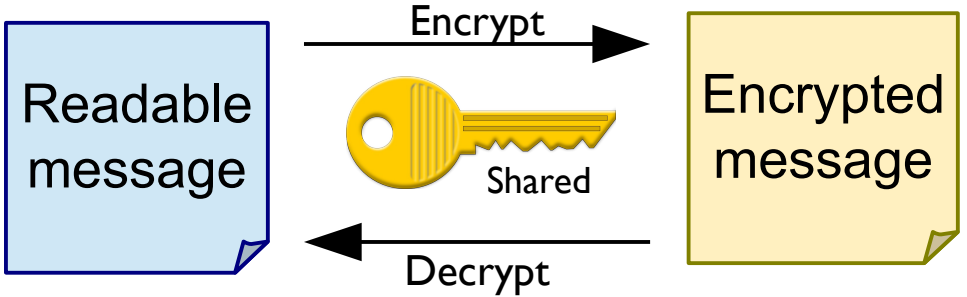
Zone transfers

- Zone transfers are often limited to secondaries
  - DNS data: public or semipublic?
  - IP level ACL… safe enough?



Transaction Signature: TSIG

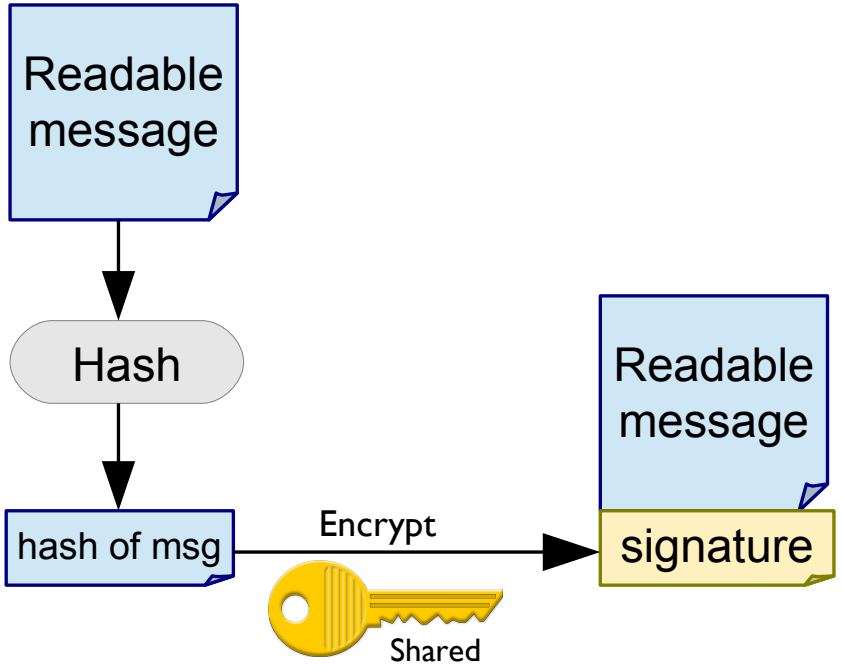
- TSIG (RFC2845)
- Shared secret

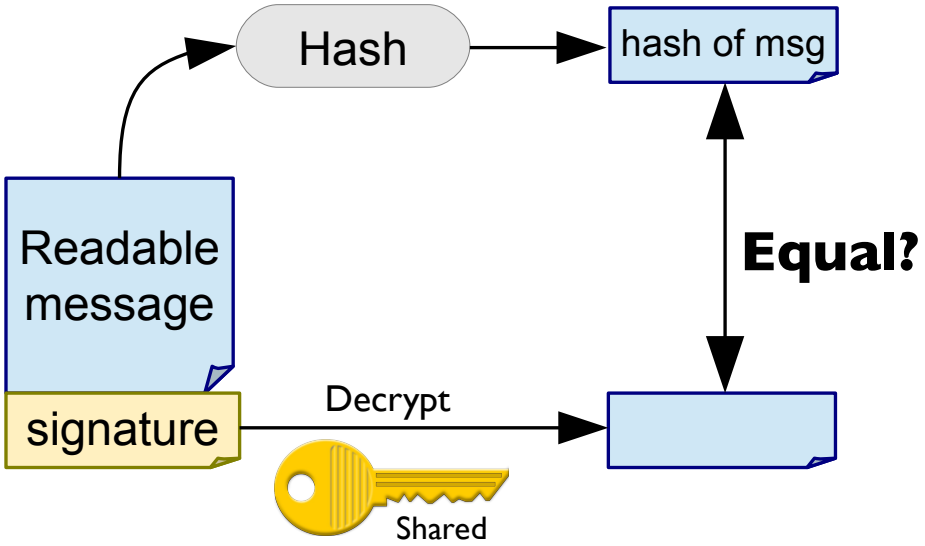


- Symmetric encryption

Transaction security with TSIG

- Hash based Message Authentication Code (HMAC)





- Create signature
- Verify signature

Transaction security with TSIG

- TSIG (RFC2845)
- Shared secret
  - Communicated out of band
  - Secret in configuration, **NOT** in zone data!
- Hash based Message Authentication Code (HMAC)
  - Provides mutual Authenticity & Integrity
  - Does not provide confidentiality

Channel privacy with XoT

- XoT (RFC9103)

Stream: Internet Engineering Task Force (IETF)
RFC: 9103
Updates: 1995, 5936, 7766
Category: Standards Track
Published: August 2021
ISSN: 2070-1721

Authors: W. Toorop, *NLnet Labs*; S. Dickinson, *Sinodun IT*; S. Sahib, *Brave Software*; P. Aras, *Salesforce*; A. Mankin, *Salesforce*

RFC 9103
DNS Zone Transfer over TLS

Abstract

DNS zone transfers are transmitted in cleartext, which gives attackers the opportunity to collect the content of a zone by eavesdropping on network connections. The DNS Transaction Signature (TSIG) mechanism is specified to restrict direct zone transfer to authorized clients only, but it does not add confidentiality. This document specifies the use of TLS, rather than cleartext, to prevent zone content collection via passive monitoring of zone transfers: XFR over TLS (XoT). Additionally, this specification updates RFC 1995 and RFC 5936 with respect to efficient use of TCP connections and RFC 7766 with respect to the recommended number of connections between a client and server for each transport.

NSD 3.7

Lab time!

- Hands on: https://dnslab.uk/
- 4. Setup a redundant authoritative name server for your domain

Photo by Alex Kondratiev on Unsplash