DNS Zone Transfers-over-TLS (abstract)

Sara Dickinson, Sinodun IT - sara@sinodun.com
Shivan Kaul Sahib, Salesforce - ssahib@salesforce.com
Allison Mankin, Salesforce - amankin@salesforce.com
Willem Toorop, NLnet Labs - willem@nlnetlabs.nl

DNS zones today often contain data that the zone owner has good reason to want to keep private. For example, the contents of the zone could include sensitive corporate information or names of persons used in names of hosts. There may also be regulatory, policy or other reasons why the zone contents in full must be treated as private.
Currently, DNS zone transfers (both full zone transfer i.e. AXFR [RFC 1035] and incremental zone transfer i.e. IXFR [RFC 1995]) occur in clear text, which gives an eavesdropper the opportunity to collect the contents of a zone by passively surveilling the network connection.

Effort has been expended to develop NSEC3 (RFC 5155) and, more recently, NSEC5 which are techniques for authenticated denial of existence which also directly mitigate zone enumeration. However they do not address the issue of surveillance of zone transfers. While DNS Transaction Signatures (TSIG) (RFC 2845) can enable authenticated zone transfers (RFC 5936), they do not provide confidentiality.

DNS zone transfers-over-TLS (XoT) is proposed and specifies the use of TLS to prevent zone content collection via passive monitoring. An Internet Draft describing XoT has been adopted by the DPRIVE (DNS Privacy) Working Group at the Internet Engineering Task Force (IETF). However, some questions still remain around this solution.

1. There is a need to establish padding recommendations for XoT, in an analogous manner to that proposed for stub to recursive DoT (RFC8467) . How should padding be done for
    a. Full zone transfer i.e. AXFR in order to minimise leakage of zone size
    b. Incremental zone transfer i.e. IXFR responses to minimise the information leakage about e.g. update rates, DNSSEC resigning
    c. We plan to submit a new Internet-Draft discussing padding for XoT - have some initial ideas around measurements
2. Has the threat model for zone transfers and data leakage from zones been fully understood?
    a. Would developing a DNS-specific threat model be of use?
    b. What are the distinctions (if any) between the information leakage addressed by XoT and the information leakage addressed by NSEC3 and NSEC5 against zone-walking to obtain a zone?
    c. We would also be interested in hearing of any documented cases of actual attacks involving passive surveillance on DNS zone transfers.