Domain Name System (DNS) Resource Record types for transferring covert information from primary to secondaries

Witold Kręcicki, ISC

23 July 2019
IETF105
Montreal

Idea

- In-band transfer of 'covert' data with the zone
- Generic - can be used for virtually anything
- Examples: NOTE RR, DHCP timeout, NSEC5 keys, ZSK for inline signing
- Recommends encryption/XFR security, it can be mandated on a per-RR basis
  - Not needed for NSEC5, definitely required for ZSK
  - Should it mandate a form of security? (impossible to enforce IPSEC or a VPN)
  - Should it mandate a specific form of security? (XoT)

Details

- Special range in currently reserved RR TYPEs - 0xF000 - 0xF0FF (is private range needed?)
- Mechanisms to disallow zone transfer to secondaries not understanding COVERT semantics - EDNS0 option in XFR request
- Server MUST NOT serve COVERT records without an explicit ACL allowing it
- Update to RFC3597 to disallow loading of zone with unknown COVERT RRs (COVERTNNNNN instead of TYPENNNNN), recommendation to do the same for binary formats (e.g. BIND mapfile) (not in -00)
- First usage - "A DNS Resource Record for Confidential Comments, E. Hunt, D. Mahoney"

Adoption?

Adoption for NOTE RR?