DoT For insecure delegations

draft-bretelle-dprive-dot-for-insecure-delegations

Manu Bretelle

IETF 104, Prague, 29 March 2019

DNSSEC/DoT

- DNSSEC
  - origin authentication/data integrity
  - payload not modified in transit end-to-end
  - no encryption/no privacy
- DoT
  - authentication of remote peer
  - payload not modified in transit with peer
  - encryption/privacy

DANE

- draft-bortzmeyer-dprive-resolver-to-auth-01
  - DANE authentication through TLS
    - TLSA records [RFC6698]
      - _853._tcp.ns1.example.net
        - Full certificate
        - SubjectPublicKeyInfo

DANE

- Authentication stays within DNS
- Works for Cloud provider (out-of-bailiwick)
- Each name server handle its own secret
- DNSSEC is required at name server level
- Extra queries

X509

- Uses client CA store
- Validate against hostname
- Works for Cloud Providers case
- Each name server handle its own secret
- DNSSEC not required
- No extra queries
- No signal that DoT is supported
- Reliance on Web PKI

DSPKI

Like DS... but for SPKI

DSPKI RR type

- Parent zone host and sign DSPKI record
- recursive server can validate DSPKI using DNSSEC
- recursive server can validate name server cert against SPKI hash

DSPKI

- Does not works for Cloud Providers case
- 1 DSPKI for all nameservers
- DNSSEC required at parent
- No extra queries
- Signal that DoT is supported
- Requires change to the TLDs
- Requires support for new RR type

DS overload

Use a new "algorithm" for SPKI hash

- Does not works for Cloud Providers case
- 1 DS for all nameservers
- DNSSEC required at parent
- No extra queries
- Signal that DoT is supported
- Sync between zone owner and name servers

DS with X509
Do9 (because why not another Do*)

Use a new "algorithm" for NS name hash.

- works for Cloud Providers case
- 1 DS per nameserver
- DNSSEC required at parent
- No extra queries
- Signal that DoT is supported
- Sync between zone owner only once to enable

SPKI in NS target

Like DNSCurve but for TLS

SPKI encoded in NS target

- Target left-most label encoding:
  dot-$(base32(pin_sha256, padding=False))
- no new RR type
- no extra round-trip
- NS is not signed: can't validate target was not modified
- parent involved

	DNSEC not required	DoT signalling	Cloud Provider support	No Zone owner involved	No Parent change	No Extra queries	Not downgradable
TLSA	name server	over 53					
X509							
DSPKI	parent				new type		
DS	parent				new algo		
Do9	parent			once	new algo		
SPKI in name							