Certificate Transparency for Domain Name System Security Extensions

draft-zhang-ct-dnssec-trans-00

Dacheng Zhang

Use Cases (1)

- Detection of misissurance of DNSSEC keys
  - If the owner of foo.example.com finds that its parent zone (example.com) publish a DS RR for its zone which however does not point to any legal zone signing keys or key signing keys, the owner can claim that a mississuance event occurs.

Use Cases (2)

- Detection of MITM Attackers who has compromised a key for signing DNS data
  - A forged DNS RR signed with the compromised key will not be adopted if it does not have a valid SCT
  - If the attacker tries to publish the RR to the log, the owner of the zone may detect the problem
- DNSSEC works well if the keys are securely protected and the zone owners work properly. CT can benefit when this assumption is broken

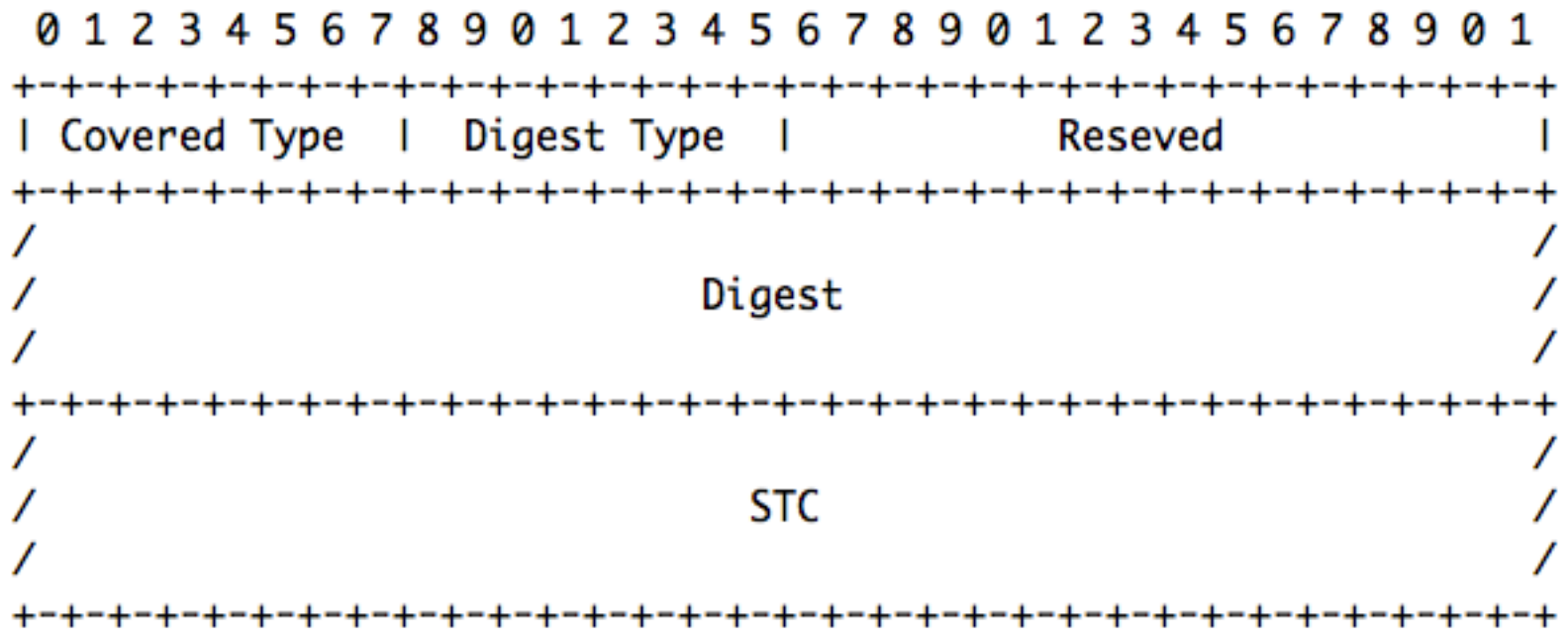
Log Operations on Publishing NDSSEC RRs

- When generating a new DNSKEY / DS / NSEC RR a zone owner will publish the RR to the CT logs.
- The RR and the associated authentication chain need to be provided
- After validating the RR, the log MUST immediately return a Signed Certificate Timestamp (SCT)
- The SCT is maintained in a SCT RR
- DNS clients MUST NOT trust a key that does not have a valid SCT.

Authentication Chain

- A typical authentication chain is
  - Public Key->[DS->(DNSKEY)*->DNSKEY]*->RRset, where "*" denotes zero or more sub-chains
  - Each DS/DNSKEY RR in the chains vouching for the next one with a RRSIG RR
  - In practice, a RRSIG RR may be used to sign a DS/DNSKEY RRset rather than a single RR. In this case, not only the DS/DNSKEY RR on the authentication chain but also other records in the RRset SHOULD be provided to the log to perform the verification

SCT RR



- The SCT RR needs to be signed with a proper public key

Open Questions

- Do we also need to also publish the RRs defined in [RFC1035] into the logs.
- Should we encapsulate RRs into certificates or deliver them directly to the logs?
- When publishing a RR to a log, do we really need to provide additional RRs constructing an authentication chain?
  - The log could find the associated chain from DNS
- When a resolver verify an authentication chain, does it need to check every SCT of each RR on the chain?

END