trans: Name Redaction & RFC6962-bis

Eran Messeri, Google, eranm@google.com

Definition: Name Redaction

The ability to avoid publishing domain names, in whole or partially, in Certificate Transparency logs.

Name redaction: Solution #1

Irreversible redaction of labels.

Precertificate contains:

- SAN-like extension with ?.?.example.com
- Number of labels to redact for each dNSName

Final certificate contains:

- SAN extension with top.secret.example.com

Client:

- MUST match the redacted labels with the actual hostname
- Cannot know if that’s the host name intended in the precertificate.

Name Redaction: Solution #2

Reversibility, for clients and monitors in-the-know, of redacted labels.

Precertificate:

- SAN-like extension with HASH(top).HASH(secret).example.com or HASH(salt || top).HASH(salt || secret).example.com.
- Salt in Precertificate.

Final certificate:

- The same SAN-like extension.
- SAN extension with top.secret.example.com.

Client:

- Removes SAN extension to verify SCT.
- Hashes labels to verify hostname matches one in precertificate.

Name redaction: Solution #3

Solve problem with solution #1 while maintaining irreversibility.

Precertificate:

- Same as in Solution #2, except Salt is not included.

Final Certificate:

- Same as in Solution #2, containing the Salt.

Client:

- The same as in Solution #2.

Redaction: state of things

- Have we over-engineered the solution ?
  - Spent a lot of the group's (and individuals') time engineering a solution.
  - Complicates clients, monitors, increases protocol complexity.
- Still lacking clear requirements
  - Particularly around threats redaction is trying to solve.
- No agreement re what is implementable, CAs and Browsers both unhappy.
- Would like to ask the community for scenarios that require redaction.
  - Come talk to us over lunch?
  - We'll channel the feedback to the mailing list.

6962-bis open issues

- Relaxing Section 5.1 discussion (what should logs accept):
- Privacy concerns of personal certificates and legal requirements.
- Historic STHs fetching for 6962bis.

6962-bis open issue

Relaxing Section 5.1:

“**Logs MUST accept** certificates and precertificates that are fully valid according to RFC 5280 [RFC5280] verification rules and are submitted with such a chain.”

Proposed compromise: change MUST -> SHOULD.

6962-bis open issue

Ability to retrieve old Signed Tree Heads

Proposal is to add (optional) API for getting an STH at a given time.

(There are a few optional, similar lookup APIs in 6962-bis)

Position: Looking for support from the WG to put it in a monitoring API

- Replies from this API can’t be trusted (have to monitor logs anyway).
- There’s other, monitoring-related API that we could move there.

6962-bis open issue: Privacy concerns

What to do when:

- “Private” certificates appear in logs.
- Logs are required to remove data.

Goal:

- Agree that this is not a redaction problem.
- Get consensus to solve this under trans WG
- Build a solution on top of 6962-bis.
- … but do not block 6962-bis

6962-bis reference implementation(s)

https://github.com/eranmes/certificate-transparency/tree/py_6962_bis

- Very raw (not merged upstream yet)
- Only supports add-chain, get-sth (does not validate chain).
  - But returns valid TransItems
- Plans:
  - Implement get-sth-consistency, get-proof-by-hash
  - Implement CMS decoding for precerts

Looking for Python reviewers

Other Work

- Emily Stark is presenting an Expect-CT draft at httpbis (Thursday).
- There'll be a chance to discuss CT policies, check the Chromium ct-policy@chromium.org group for details.