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: Missing goals

- We started with vague requirements, e.g. top.secret.example.com.
- First technical solution was to allow irreversible redaction of labels.
  - ?.?.example.com
- Second solution was hashing of the redacted labels:
  - HASH(top).HASH(secret).example.com
  - HASH(salt || top).HASH(salt || secret).example.com, salt in precertificate.
  - HASH(salt || top).HASH(salt || secret).example.com, salt in final cert.
- 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 issue

- Relaxing Section 5.1 discussion (what should logs accept):
  Proposed compromise: change MUST -> SHOULD.
- Privacy concerns of personal certificates and legal requirements Goal: Is there consensus for solving this problem under the trans WG? (not block bis)
- Historic STHs fetching for 6962bis:
  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.

Privacy concerns

What to do when:

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

Goal:

- 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
- Already caught some spec issues
- Plans:
  - Implement get-sth-consistency, get-proof-by-hash
  - Implement CMS decoding for precerts

Other Work

- Emily Stark is working on an Expect-CT draft at httpbis (Thursday).