Certificate Transparency

Ben Laurie <benl@google.com>

What between now and last call?

- Resolve open issues.
- Specify gossip protocol.
- Specify DNS inclusion proof retrieval.
- Log migration.
- Implementation?

Gossip

- Problem: How do we know that everyone sees the same log?
- Solution: gossip Signed Tree Heads.
- If I see STH_A and STH_B ($A < B$) from some log, I can demand ConsistencyProof(STH_A, STH_B).
- Once that is seen, I can discard STH_A.

How do clients Gossip?

- Proposal: on every handshake, the server sends a few STHs and so does the client.

- Servers and clients get consistency proofs and discard old STHs.

- Some servers (e.g. logs) could send/receive all cached STHs. Most probably should not.

Which STHs?

- Open question. Oldest? Newest? Stalest? Freshest?

- Certainly: STHs you have been unable to get consistency proofs for.

- Will resolve this with simulation.

Should we gossip anything else?

- Recent consistency proofs?
- Popular inclusion proofs?
- Something else?
- Again, simulation will help.

DNS Inclusion Proof

- Checking an SCT for inclusion in a log reveals which site was visited.

- Retrieving the inclusion proof via DNS reveals the site to the DNS provider (which it already knew), but only reveals to the log that someone behind that caching resolver visited it.

- Prototype exists in open source code.

Private Domain Labels

- CAs issue certs for “internal” domains.
- Their customers would rather not reveal the domain names, but would like EV to continue to work.
- Allow “(PRIVATE).example.com” to be logged instead of “top.secret.example.com”.
- An extension specifies how many labels have been redacted from CN/SANs.
- (Name constrained intermediates also achieve this).

Client Behaviour

- UI? We're not qualified. And not up to us.
- Hard/soft/no fail on no log/verification fail/whatever? Not up to us.
- Which logs to trust? Not up to us.
- Check for inclusion? Not up to us.
- I-D specifies **how** to do these things. Vendors/users decide **what** to do.

Client Behaviour

- That said, we can make suggestions (SHOULD or MAY).

Google's Plans

- Google will require all EV certificates to be registered in the appropriate number of logs by Jan 2015.

- EV certificates not accompanied by an SCT will lose the EV indicator.

- Google is implementing RFC 6962, plus private domain labels backported from 6962-bis.