Balancing Customer Privacy with Transparency

Certificate Transparency: RFC 6962

The CT log (public database) contains either a copy of the full certificate or a “pre-certificate” which contains all the elements of the certificate except embedded CT information.

Client support

- Mozilla Firefox – 2017
- Apple – iOS 10 and macOS Sierra allows applications to require CT
- Chrome – EV since 2015, all new certs starting Oct 2017
- OpenSSL 1.0.2 (no validation, just parsing)

Mozilla and Apple have not yet published information on which logs they trust or policy on accepting logs

Information Disclosure

- Fully Qualified Domain Names
  - secret.projects.example.com
- Subject Attributes
  - Individual names
  - Addresses
  - Company affiliation
- Other?

RFC 6962-bis

(bis is French for again or encore)

Calls out two options for privacy

1. Use wildcards (allows privacy for left most label)
2. Use Name Constrained subordinate CAs

Separate Draft proposes a third option

3. Pre-certificates with some subject information omitted

Choosing a certificate profile with less subject information is also an option.

Use cases for privacy

- Binding of domain name to corporate entity (domain name uses proxy registration)
- PII in certain certificate types (Qualified?)
- Overly descriptive labels in FQDNs (provides a blueprint of network topology)
- Disclosure of confidential projects (e.g. newthing.example.com or fordacquisition.gm.com) – may become public at a future point

Technical Implementations of DNS Privacy

- Private DNS subtree (e.g. corp.example.com subtree is permanently private)
- Split Horizon DNS (e.g. two copies of the DNS zone)

- DNSSEC added NSEC3 to avoid disclosure of record names to address similar concerns

IETF Public Notary Transparency (“trans”) WG

https://datatracker.ietf.org/wg/trans/charter/

https://www.ietf.org/mailman/listinfo/trans