Certificate Transparency Root Explorer

Nikita Korzhitskii
Niklas Carlsson
Web Public Key Infrastructure (WebPKI)

Root certificates of trusted Certificate Authorities
e.g. GlobalSign Root CA, Amazon Root CA, GoDaddy Root CA
Web Public Key Infrastructure (WebPKI)

Root CAs issue Intermediate certificates to themselves or other organizations.
Web Public Key Infrastructure (WebPKI)

Client w/ Root Store 1: google.com, liu.se, fb.me, mozilla.org
Client w/ Root Store 2: google.com, liu.se, fb.me, mozilla.org, xkcd.com, github.io, kth.se, mit.edu
Client w/ Root Store 3: github.io, kth.se, mit.edu, *.linkoping.se
Certificate Transparency

- An internet standard, RFC 6962
- Append-only logging of issued certificates
Certificate Transparency

- An internet standard, RFC 6962
- Append-only logging of issued certificates
Certificate Transparency

• A *CT log* is a signed binary append-only Merkle tree of certificate chains
• Any party can submit certificates
• Logs can be checked for consistency

• Initially developed and adopted by Google
• Recently adopted by Apple
• Most CAs log their certificates upon issuance
• CT extends beyond WebPKI to RPKI
Applications of Certificate Transparency

- Connection verification
- Detection of misissued certificates
- Detection of active, phishing, other domains (privacy issues)
- Representation of the Internet structure
- Many more...

We are interested in end-to-end security applications of CT
Certificate Transparency Root Explorer

...is a tool for exploring certificate stores.
One can visualize intersections, compare, parse, search and export certificate information.
An SQLite database of logs and roots could be imported and exported.
CT logs could be scanned online.

Available root stores (Snapshot from 27th December, 2018):
Mozilla, Microsoft, Apple and multiple Certificate Transparency Logs.

Requirements:
Chrome or Chromium Browser.

By default, only logs by Google are available for live log scanning. The rest of the logs have not explicitly configured response headers related to the CORS policy.

GitHub: nikita-kun/certificate-transparency-root-explorer
# Certificate Transparency Root Explorer

This tool allows you to explore and analyze certificate transparency logs from various sources. It provides a comprehensive view of certificate transparency root logs, including link to GitHub repository for further exploration.

## Online Logs
- DigitalCert Log Server (2022) - 17496 entries
- Google Argon2021' (2222)
- Google Argon2020' (2222)
- Google Argon2019' (2222)
- Google Argon2018' (2222)
- Cloudflare 'Miniburn2023' (2222)
- Cloudflare 'Miniburn2022' (2222)
- Cloudflare 'Miniburn2021' (2222)
- Cloudflare 'Miniburn2020' (2222)
- Cloudflare 'Miniburn2019' (2222)
- Cloudflare 'Miniburn2018' (2222)
- Cloudflare 'Miniburn2017' (2222)
- Mozilla Inclusion CA Certificate List (2018-12) (532)
- Mozilla Inclusion CA Certificate List (2016-12) (532)
- Microsoft Trusted Root Program (2018-10) (532)
- Apple Trust Store Version 20.80.1400 (111)

## Root Stores
- Mozilla Included CA Certificate List (2018-12) (532)
- Mozilla Included CA Certificate List (2016-12) (532)
- Microsoft Trusted Root Program (2018-10) (532)

## Certificate Transparency Logs

The tool also allows you to view detailed information about individual certificates, including their issuers, dates, and other relevant details. This information can be used to identify potential security risks and to improve overall certificate transparency.

GitHub: nikita-kun/certificate-transparency-root-explorer
The dataset

- Collected on December 27th, 2018
- 56 CT logs (54 were mentioned in Google’s list of known logs)
- 3 Vendor Root Stores
- 802 Root/Intermediate Certificate
In order to enable attribution of each logged certificate to its issuer, the log SHALL publish a list of acceptable root certificates (this list might usefully be the union of root certificates trusted by major browser vendors).

RFC 6962
In order to enable attribution of each logged certificate to its issuer, the log SHALL publish a list of acceptable root certificates
(this list might usefully be the union of root certificates trusted by major browser vendors).

RFC 6962
Conclusion

• Certificate Transparency is rapidly developing
• As of January 2019, CT logs contained 3 billion entries
• CT is already in your Chrome browser and Apple OSes
• Many potential applications

However:
• Internet is not fully covered by CT
• Google and Apple rely on logs maintained by 4 operators
  → Cloudflare, DigiCert, Google and Sectigo

Intersection of root stores by Mozilla, Microsoft and Apple (top); Argon2019, Nimbus2019 and Nessie/Yeti2019 logs (bottom)
Thank you!

www.liu.se