Certificate Transparency in 2024

Pass the SALT 2024, Lille

July 2024

Philippe Boneff
phboneff@

Engineer @ Google Open Source Security, TrustFabric
Certificate Transparency Tech Lead

Deter bad behaviour by making it discoverable.

Table of Contents - Certificate Transparency in 2024

Value proposition 01

CT ecosystem 02

Current CT dynamics 03

Future of CT 04

01

Value proposition

What problems CT solves

Premise

User contacts a domain over HTTPS and wants to ensure they are connected with the authentic domain owner

Requisite

User gets a certificate for this domain **that proves ownership** of this domain

Problem

How does the user know this proof of ownership is **authentic**?

Solution

Convince the user that domain owners would be aware of any mis-issued certificate, and would react

Why would a certificate be mis-issued?

NEGLIGENCE

TARGETED ATTACK

How CT delivers that solution

Convince the user that domain owners would be aware of any mis-issued certificate and would react

01 | Provides an infrastructure to log all certificates

02 | Builds the incentive to log every certificate

03 | Enables domain owners to discover all certificates

04 | Keep CAs accountable, including for mis-issued certs

What CT enables tangentially

List all HTTPS certs

- Find expiring certificates
- Research on the HTTPS ecosystem

xyz.com g00.gl

abc.co.uk

Monitor all domains

- Know what is public
- Find malware
- Help attackers

02

CT ecosystem

CT actors

What are they?

g00.gl

xyz.com

abc.co.uk

Domain owners
Google, BBC, usa.gov

CAs
Google, Let's Encrypt, DigiCert

User Agents
iOS, Safari, Chrome

Log operators
Cloudflare, Let's Encrypt, Google, Sectigo, TrustAsia, Digicert

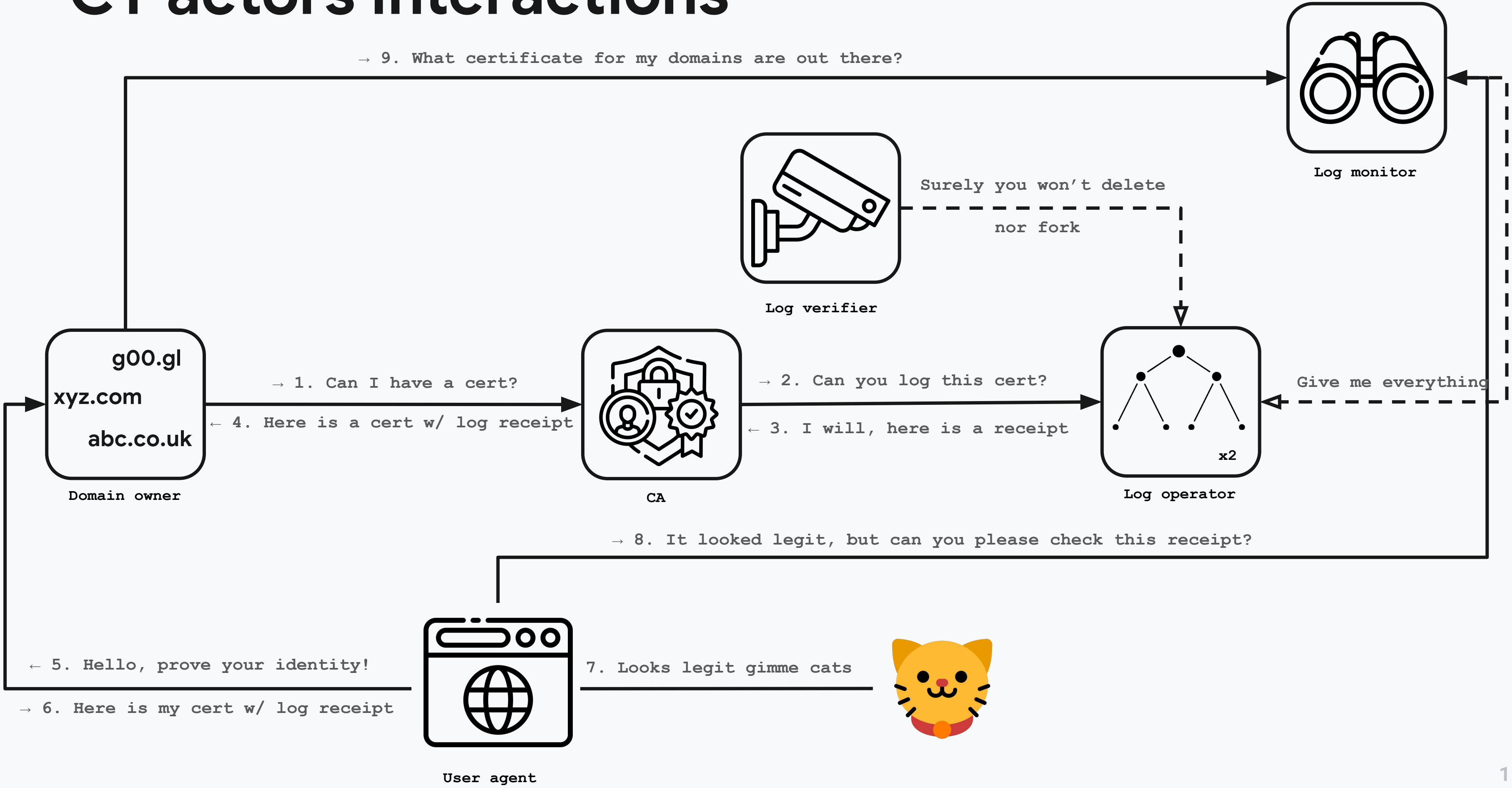
Log monitors
Facebook, crt.sh, Google, certstream

Log verifiers
Cloudflare, SSLMate, Google

Researchers
Universities

images: Flaticon.com

CT actors interactions



→ 9. What certificate for my domains are out there?

Log monitor

Surely you won’t delete nor fork

Log verifier

g00.gl
xyz.com
abc.co.uk

Domain owner

→ 1. Can I have a cert?

← 4. Here is a cert w/ log receipt

CA

→ 2. Can you log this cert?

← 3. I will, here is a receipt

x2

Log operator

Give me everything

→ 8. It looked legit, but can you please check this receipt?

← 5. Hello, prove your identity!

→ 6. Here is my cert w/ log receipt

7. Looks legit gimme cats

User agent

How can domain owners benefit from CT

Mis-issuance protection

ACTIVE

Monitor certificates issued for your domains. If you don't, a certificate might be mis-issued and you won't know.

Verify that SCT have been integrated. If you don't, you might use a certificate that was not logged, and incentivize certificates not to be logged. Chrome does this for you, to some extent.

PASSIVE

Tamper-evident logs allow you to monitor certificates issued for your domain **later**.

Halo effect: most CAs log all certificates they issue by default. Though some offer not to for money.

Other use cases

Visibility into the HTTPS ecosystem

List domain names (serving HTTPS)

03

Current CT dynamics

Usage patterns

6 Log operators

Cloudflare, Let’s Encrypt, Trustasia, Digicert, Sectigo, Google

Would be nice to have more!

~2-4 Billion certs / year*

Growth starting to be exponential

*Google logs

Temporal logs

Many log monitors

Make sure log behave correctly & watch for certificates

SSLMate, Cloudflare, Facebook, crt.sh, certstream, ...

How do you know the monitor doesn’t hide anything?

3 main user agents, 2 policies

Chrome, Brave, Apple (Safari + platforms)

More to come soon?

Researchers

Want to download data at scale

How to interact with CT logs: RFC6962

`https://datatracker.ietf.org/doc/html/rfc6962`

IETF standard

Written in 2011

paved the way for other transparency implementations

13 years old

Log implementation: Trillian

Used by ~all rfc6962 CT log operators

Dynamic get-entries

`get-entries?start=X&end=Y`

log operators can return less than Y entries

```
get-proof-by-hash
get-sth-consistency
```

24 MMD

- A CT log returns a promise to include a cert: SCT
- An entry MUST appear in the log within 24h
- Where are the entries I care about?

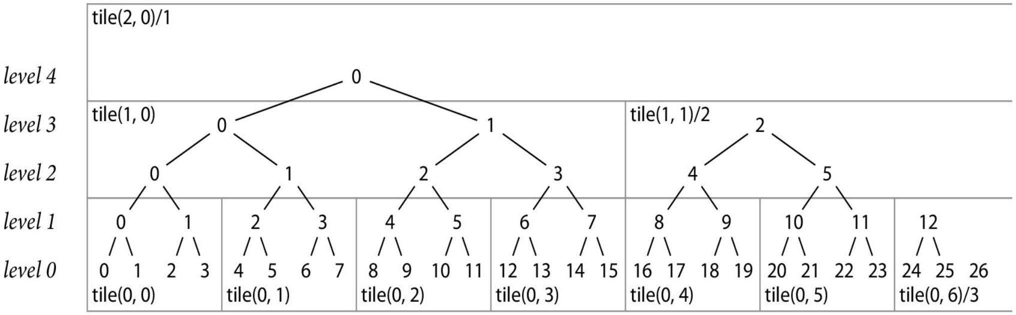
04

Future of CT

ct-static-api specs

Tiles

- Standard, static tiles format to publish log data
- Enables using bucket storage systems (S3, GCS)
- Cacheable



research.swtch.com/tlog

Checkpoint format

- Standard* "checkpoint" format to publish a log root

*with custom CT behaviour for backward compatibility

Synchronous SCT

- A log response includes the assigned index
- Enables inclusion proof to be built without the need for an online index

Issuer bundles

- Entries contain hashes of issuer certs, not the certs
- Issuer certs can be fetched on a different endpoint

Why are we doing this?

Reduce cost of operations

- Easier to spin up logs: no need to design APIs follow specs
- Easier to serve logs: cacheability, static responses

Transparency boom!

- Let's align all the ecosystems: Sigstore, Sigsum, Go module Checksum database, Key Transparency, Pixel binary transparency, Armory Drive Firmware Transparency
- C2SP specs: https://github.com/C2SP/C2SP

Cross-ecosystem projects

- Witnessing
- Protects against split view attacks

Sunlight log

First implementation of ct-static-api

$4k per year

CT log only

- Static serving via S3 buckets style
- Can be deployed with any S3-like system

Synchronous SCT

- A log response includes the index at which an entry
- <1s sequencing + integration

sunlight.dev
filippo.io
Filippo Valsorda

Trillian Tessera

Next generation of Trillian

General purpose tiled log

- Using tiles and checkpoint format
- Multiple storage systems: little abstraction, as simple as possible
- Multi cloud
- Also works for ct-static-api

Fast async integration

- The entry at index will be integrated within seconds
- add-entry returns an SCT with an index

Multi node architecture

- Increased reliability
- Brings interesting global consensus challenges

More soon on github.com/transparency-dev

More log operators?!

Why would I run a log?

- 6 log operators is not a lot
- Support a critical part of the internet: no log, no HTTPS
- Geographical, jurisdictional, implementation diversity: **there's no EU log today**
- Reduce number of external dependencies if you're a CA
- Get engaged in a vibrant community

How do I get in touch?

- Slack
- transparency.dev
- certificate-transparency.org
- github.com/transparency-dev
- github.com/google/trillian
- github.com/google/certificate-transparency-go

05

Questions