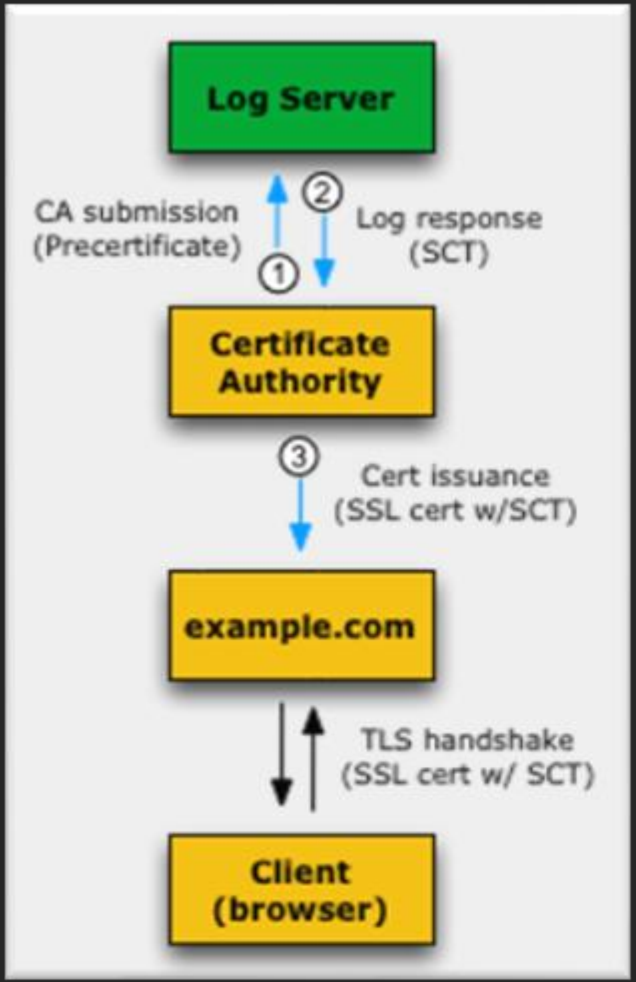
DNS Transparency Logs

RAFFAELE SOMMESE -
MATTIJS JONKER
UNIVERSITY OF TWENTE

DINR 2021

Introduction

- Access to zone files has been subject to confidentiality requirements by TLDs operators.
- ICANN created the Centralized Zone Data Service (CZDS), a service for requesting and obtaining access to zone files of different TLDs in a quick and standardized way.
- Unfortunately, the zone files are published in CZDS once per day.
- This granularity is sufficient for long-term trend analysis but has limits when it comes to intraday events.
- We need more fine-grained timing information.


Log Server
CA submission (Precertificate)
1
2
Log response (SCT)
Certificate Authority
3
Cert issuance (SSL cert w/SCT)
example.com
TLS handshake (SSL cert w/ SCT)
Client (browser)

Certificate Transparency Logs?

- A system of public logs that record all certificates issued by publicly trusted certificate authorities.
- Defined in RFC6962
- Originally designed with the goal of auditing possible fraudulent certificate issuance.
- Nowadays, a fundamental resource for operators and researchers, which enabled numerous studies on the X.509 certificate ecosystem.

The DNS Transparency Logs

The “DNS Transparency Logs” would provide near real-time insights into changes inside a zone file (e.g. insert of a new domain, nameserver, or glue records).

Can be enriched with the information provided via RDAP (or WHOIS).

Use Cases

- Detection of DNS hijacking events
- Behavioral analysis of newly registered domains
- Operators' behavior for infrastructure under attack
- Other suggestions?

DNS Transparency Logs Infrastructure

- An Extensible Provisioning Protocol (EPP) fork!
- The main challenge to address is how to create a bridge to share the “non-sensitive” content with the third parties interested.
- Protect information that could be subject to privacy concerns, such as registrant personal data.
- Trademark protection? Business? Hiding market share of registrars?
- Other concerns?

Let's discuss

- Why?
- Why not?
- Which challenge are there to implement it?