Documentation

What is Certificate Transparency?
How Certificate Transparency Works
How Log Proofs Work
Benefits and Advantages
Comparison with Other Technologies
Getting Started
Extended Validation in Chrome
Known Logs
General Transparency

Developer Resources

Open Source Project
Certificate Transparency Forum
Certificate Transparency hack days
Certificate Transparency in Chrome
Certificate Transparency in OpenSSL
Resources for site owners
Mailing Lists
Open Source Libraries

Additional Information

FAQ
Certificate Transparency RFC
IETF Working Group
NIST Workshop Presentation I (4/2013)
NIST Workshop Presentation II (4/2013)
Nature (12/2012)

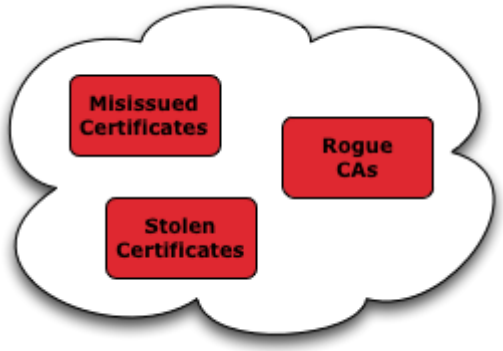
Newsletters

August 2015 Newsletter

What is Certificate Transparency?

Thanks to modern cryptography, browsers can usually detect malicious websites that are provisioned with forged or fake SSL certificates. However, current cryptographic mechanisms aren't so good at detecting malicious websites if they're provisioned with mistakenly issued certificates or certificates that have been issued by a certificate authority (CA) that's been compromised or gone rogue. In these cases, browsers see nothing wrong with the certificates because the CA appears to be in good standing, giving users the impression that the website they're visiting is authentic and their connection is secure. One of the problems is that there is currently no easy or effective way to audit or monitor SSL certificates in real time, so when these missteps happen (malicious or otherwise), the suspect certificates aren't usually detected and revoked for weeks or even months. What's more, these types of SSL missteps are occurring with increasing frequency. Over the past few years there have been numerous instances of misissued certificates being used to spoof legitimate sites, and, in some case, install malicious software or spy on unsuspecting users.

In one case, a prominent Dutch CA



(DigiNotar) was compromised and the hackers were able to use the CA's system to issue fake SSL certificates. The certificates were used to impersonate numerous sites in Iran, such as Gmail and Facebook, which enabled the operators of the fake sites to spy on unsuspecting site users. In another case, a Malaysian subordinate certificate authority (DigiCert Sdn. Bhd.), mistakenly issued 22 weak SSL certificates, which could be used to impersonate websites and sign malicious software. As a result, major browsers had to revoke their trust in all certificates issued

by DigiCert Sdn. Bhd. (Note: DigiCert Sdn. Bhd. is not affiliated with the U.S.-based corporation DigiCert, Inc.)

More recently, a large U.S.-based CA (TrustWave) admitted that it issued subordinate root certificates to one of its customers so the customer could monitor traffic on their internal network. Subordinate root certificates can be used to create SSL certificates for nearly any domain on the Internet. Although Trustwave has revoked the certificate and stated that it will no longer issue subordinate root certificates to customers, it illustrates just how easy it is for CAs to make missteps and just how severe the consequences of those missteps might be.

In many cases, mistakenly issued certificates have been used by hackers for malicious attacks that have dire consequences, but the fallout after mitigation can be far ranging and harmful, too. Eventually, the Dutch CA's certificates were revoked and the CA was shut down. The revocation and closure caused a ripple effect throughout the Netherlands as people were denied access to government and private sites that were provisioned with the CA's SSL certificates.

Certificate Transparency to the Rescue

Certificate Transparency aims to remedy these certificate-based threats by making the issuance and existence of SSL certificates open to scrutiny by domain owners, CAs, and domain users. Specifically, Certificate Transparency has three main goals:

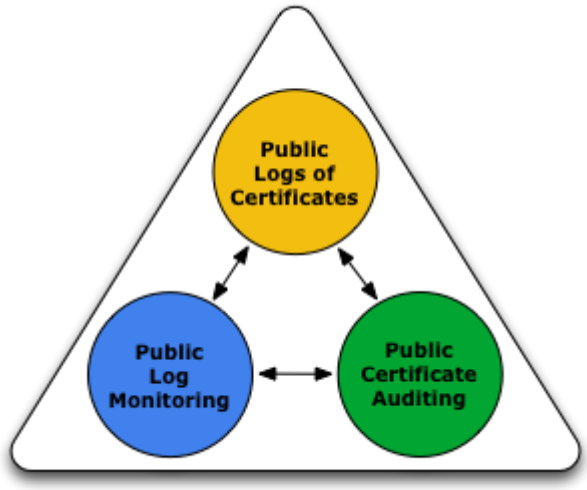
- Make it impossible (or at least very difficult) for a CA to issue a SSL certificate for a domain without the certificate being visible to the owner of that domain.
- Provide an open auditing and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly or maliciously issued.
- Protect users (as much as possible) from being duped by certificates that were mistakenly or maliciously issued.

Certificate Transparency satisfies these goals by creating an open framework for monitoring the TLS/SSL certificate system and auditing specific TLS/SSL certificates. This open framework consists of three main components, which are described below.

Certificate Logs

Certificate logs are simple network services that maintain cryptographically assured, publicly auditable, append-only records of certificates. Anyone can submit certificates to a log, although certificate authorities will likely be the foremost submitters. Likewise, anyone can query a log for a cryptographic proof, which can be used to verify that the log is behaving properly or verify that a particular certificate has been logged. The number of log servers doesn't have to be large (say, much less than a thousand

worldwide), and each could be operated independently by a CA, an ISP, or any other interested party.



Monitors

Monitors are publicly run servers that periodically contact all of the log servers and watch for suspicious certificates. For example, monitors can tell if an illegitimate or unauthorized certificate has been issued for a domain, and they can watch for certificates that have unusual certificate extensions or strange permissions, such as certificates that have CA capabilities.

A monitor acts much the same way as a credit-reporting alert, which tells you whenever someone applies for a loan or credit card in your name. Some monitors will be run by companies and organizations, such as Google, or a bank, or a government. Others will be run as subscription services that domain owners and certificate authorities can buy into. Tech-savvy individuals can run their own monitors.

Auditors

Auditors are lightweight software components that typically perform two functions. First, they can verify that logs are behaving correctly and are cryptographically consistent. If a log is not behaving properly, then the log will need to explain itself or risk being shut down. Second, they can verify that a particular certificate appears in a log. This is a particularly important auditing function because the Certificate Transparency framework requires that all SSL certificates be registered in a log. If a certificate has not been registered in a log, it's a sign that the certificate is suspect, and TLS clients may refuse to connect to sites that have suspect certificates.

An auditor could be an integral component of a browser's TLS client, a standalone service, or a secondary function of a monitor. Anyone can create an auditor, although it's likely that CAs will run the bulk of all auditors because they are an efficient way to gain insight into the operational integrity of all CAs.

Altogether, these components create an open framework

that lets anyone observe and verify newly issued and existing SSL certificates in nearly real time.

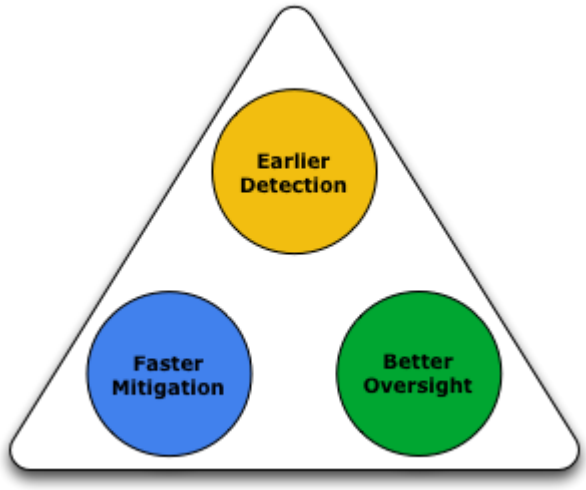
Note: Auditors and monitors also communicate with each other to exchange information about logs. This communication path, known as gossip, helps auditors and monitors detect forked logs.

Fewer Missteps, Safer Browsing

When implemented, Certificate Transparency helps guard against several types of certificate-based threats, including misissued certificates, maliciously acquired certificates, and rogue CAs. These threats can increase financial liabilities for domain owners, tarnish the reputation of legitimate CAs, and expose Internet users to a wide range of attacks such as a website spoofing, server impersonation, and man-in-the-middle attacks.

The Certificate Transparency framework aims to curb these certificate-based threats by bringing public scrutiny and openness to the SSL certificate system. Through its open framework of publicly run monitors and auditors, Certificate Transparency provides several benefits that are lacking or absent in the current SSL certificate system:

- **Early detection of misissued certificates, malicious certificates, and rogue CAs.**



  In most cases, the Certificate Transparency system can detect suspect certificates or CAs in a few hours instead of a few days, a few weeks, or a few months.

- **Faster mitigation after suspect certificates or CAs are detected.**

  Although Certificate Transparency relies on existing mitigation mechanisms to address harmful certificates and CAs--for example, certificate revocation--the shortened detection time will speed up the overall mitigation process when harmful certificates or CAs are discovered.

- **Better oversight of the entire TLS/SSL system.**

  Certificate Transparency is founded on an open framework that supports public observation and verification of newly issued and existing TLS/SSL certificates, which gives any interested party the opportunity to observe and verify the health and integrity of the TLS/SSL system--domain owners, CAs, and users alike.

As a focused solution, Certificate Transparency strengthens the chains of trust that extend from CAs all the way down to individual servers, making HTTPS connections more reliable and less vulnerable to interception or impersonation. But what's more, as a general security measure, Certificate Transparency helps guard against broader Internet security attacks, making browsing safer for all users.