NIST Workshop on Improving Trust in the Online Marketplace, April 10-11, 2013
Abstract submission

Certificate Transparency - protocol design and implementation

Emilia Kasper, Adam Langley, Ben Laurie - Google
{ekasper, agl, benl}@google.com

The TLS protocol offers several mechanisms for revoking compromised certificates as well as certificates mistakenly issued to an entity that is not the rightful owner of the domain. However, revocation can only take effect after the compromise has been detected. Recent incidents of rogue certificates used in man-in-the-middle (MitM) attacks against high-value domains including google.com have shown that the delay between the initial breach in Certificate Authority (CA) security and the response to an attack in the wild can stretch to several weeks if not months.

The Certificate Transparency (CT) protocol aims to minimize the window of compromise - thus increasing the cost of an attack - by making all TLS certificates public knowledge through public certificate logs. CT logs are publicly auditable, “untrusted” third parties whose correct operation is fully cryptographically verifiable. In this talk, we describe the cryptographic setup of a CT log, and re-evaluate the MitM threat model in the new world where CT has been deployed.

Note that the publishing of all certificates can only be mandated if TLS clients are instructed to reject certificates that have not been logged. To make world-wide deployment of such a hard-fail protocol feasible, CT proposes a mechanism that allows servers to start participating immediately, without losing backwards compatibility.

The protocol is also extremely lightweight on participating TLS clients. Existence of a certificate in the log can be verified without inspecting the entire log: CT only adds a few hundred bytes of verification data to the TLS handshake. If (and only if) this initial verification succeeds, an asynchronous exchange of a few kilobytes of “gossip” data once per observed certificate is sufficient to verify the correct operation of CT logs.

The second part of this talk shall thus cover the deployment strategy of CT, and Google’s experience in building a robust and efficient CT log service.