DigiCert-Google Abstract – Certificate Transparency
Submitted for NIST Workshop to be held April 10-11, 2013
Submitted – February 15, 2013

Category: Transparency and alternative certification, distribution or confirmation of key information

Title: A Window of Opportunity: How Certificate Transparency Increases Online Trust Accountability and Security: A Browser-CA Perspective

Submitted by authors: Google, DigiCert

Abstract

Recent events involving certificate authorities, such as the DigiNotar compromise and Comodo-hacker breach, illustrate the need for mechanisms that ensure a certification authority's (CA) knowledge of issued certificates and permit domain holders to easily detect certificate mis-issuance. A faster knowledge of improperly issued certificates is vital in detecting compromise and remediating fraudulently used certificates.

Google's Certificate Transparency (CT) proposal solves both problems by requiring all public end-entity certificates to be accompanied by a proof of incorporation in a public log. Certificates without a proof are considered untrusted and rejected by browsers during the SSL handshake, while certificate logs themselves are untrusted entities whose correct operation is publicly verified. Requiring public logging to activate a certificate provides easy detection of certificates containing problematic extensions, certificates not authorized by the subscriber, and certificates inadvertently issued by the CA. Further, CT permits older TLS clients to continue operating without log proofs, and begins providing industry-wide benefits with adoption by a single major browser without significantly delaying issuance times.

The strongest argument for CT is that its implementation would have prevented, or effectively remediated, each of the events that occurred during the past few years by minimizing the window between the incident and response, and alerting domain owners about the issuance of illegitimate certificates.

To facilitate adoption by servers, CT offers a mechanism for CAs to embed log proofs in the certificate itself. Several CAs, including DigiCert, have worked closely with Google on creating a proof-of-concept system that all CAs will eventually want to incorporate into their operations. At the NIST workshop, Google and DigiCert will present their development of CT from the perspective of a log operator, browser and CA. The presentation will focus on how CT increases security throughout the Internet and the practical issues surrounding implementation.