Abstract Title: Failures of Trust in the Online PKI Marketplace Cannot be Fixed by "Raising the Bar" on Certificate Authority Security

Author: Brad Hill, PayPal Inc.

Technology Space: Preventative Measures, Detection Measures

Abstract Body:

A majority of efforts today to improve trust in the online PKI marketplace focus on preventative measures, attempting to "raise the bar" against successful exploitation of a Certificate Authority through measures like improved network security controls. Though a necessary stopgap, these efforts simply perpetuate an arms race in which defenders suffer severe and structural disadvantages relative to attackers:

1. Attackers can choose among many points of attack in the CA infrastructure

2. Attackers can target inconsistencies between issuing and accepting systems in the PKI

3. Attackers can target legitimate certificates with cryptographic attacks

4. Attackers can compromise the data CAs rely upon, such as the DNS or Whois

5. CAs or their employees may be subject to corruption or coercion

6. The value at stake for attackers and relying parties far exceeds the resources available to defenders

Solutions to the current crisis of trust in the online PKI marketplace must focus instead on improving our ability to rapidly detect problems and initiate incident response such that the amount of trust relying parties must place in the system is reduced, the ability of all stakeholders to transparently verify the system's correctness is improved, and so that the expected value to an attacker of any successful compromise is greatly reduced. Among several current proposals, we believe the Certificate Transparency (CT) system proposed by Laurie, et al. at Google, augmented with DNS Certification Authority Authorization (CAA) records, best satisfies the needs of a detection-oriented approach to the problem.