Overview of the Attack Model document (draft-ietf-trans-threat-analysis-01)

Steve Kent
BBN Technologies

Purpose

- The goals of this document are
  - Provide an introduction to CT (more appropriate for an architecture document, but …)
  - Define “mis-issuance”
  - Establish a taxonomy of attacks in the CT context, by examining scenarios based on benign and malicious CAs, as well as benign and mis-behaving logs and Monitors
  - Examine the impact of various classes of attacks, in various scenarios, in terms of CT goals

Document Outline

- Introduction
- Semantic mis-issuance
- Syntactic mis-issuance
- Issues applicable to Sections 2 & 3

Concise CT Goals Statement

- Certificate transparency (CT) is a set of mechanisms designed to detect, deter, and facilitate remediation of certificate mis-issuance
  - Monitoring of logs provides detection
  - Logging provides deterrence
  - Certificate revocation, triggered by Monitoring, effects remediation

Semantic Mis-issuance

- The fundamental semantic constraint for a certificate is that it was issued to an entity that is authorized to represent the Subject (or Subject AlternativeName) identified by the certificate.
- It is also assumed that the entity requested the certificate from the CA
- Semantic mis-issuance yields a “bogus” certificate

Syntactic Mis-issuance

- A certificate is characterized as syntactically mis-issued if it violates syntax constraints associated with the type of certificate that it purports to represent.
- Syntax constraints for certificates are established by certificate profiles, and typically are application-specific.
- Examples: EV & DV certificates, S/MIME IPsec, …

CT Beneficiaries

- Subjects – benefit by having bogus (logged) certificates detected and revoked, thus preventing prolonged spoofing of the Subject's web identity
- RPs (browsers) – benefit by rejecting bogus certificates, relying on a revocation mechanism (CRL, OCSP, or browser-vendor blacklists), after a bogus certificate has been detected

Herd Immunity?

- All Subjects may benefit from CT, even Subjects that do not have SCTs for their certificates, if the Subjects' names and public keys are monitored
- All RPs may benefit, even if they do not discriminate against certificates w/o SCTs, because they are protected against bogus certificates via revocation

Monitors

- Two types: self monitoring or 3rd party
- Provisioned with reference information for the set of Subjects being protected
  - List of Subject names (or SANs)
  - List of public keys associated with each name
- Acquires log entries and looks for conflicts with Subject reference info
- Rely on the Audit function to detect misbehaving logs

Attack Taxonomy

- Semantic & Syntactic mis-issuance
  - Benign vs. malicious CAs
  - Certificate logged vs. not logged
  - Benign vs. misbehaving logs
  - Self-monitoring and benign 3rd party Monitors vs. misbehaving Monitors
  - “Careful” browsers vs. vanilla browsers

The Role of Auditing

- The primary purpose of auditing is to detect misbehaving logs, so that Monitors will not rely on them
- A log misbehaves if it
  - Fails to meet its published MMD
  - Fails to log a certificate for which it has issued an SCT
  - Provides different Merkle tree data to different clients (e.g., to hide log entries from Monitors)

Section 4 Topics

- Subject selection of Monitors to ensure “adequate” coverage of logs
- Monitor discovery & selection of logs, especially for self-Monitors
- Browser behavior: incremental deployment vs. missing SCT hard failure
- Remediation for malicious CA behavior
- Auditing issues

Auditing Challenges

- To preserve privacy, the Audit function must not disclose information about which sites a browser visits, except to entities trusted by the browser user
- To detect log misbehavior an Auditor needs access to log replies sent to different clients, while preserving privacy
- The audit mechanism must support potentially tens of millions of (self) Monitors

Going Forward

- I’ve received comments from only a few individuals; I’ve made changes in response to those comments
- We need WG agreement (via the list) on
  - CT goals
  - Definitions of mis-issuance
  - Functional characterization of Monitors and Auditing
  - Details of the attack model & implications for CT secruity

QUESTIONS ?