Update on the Attack/Threat Model
(draft-ietf-trans-threat-analysis-01)

and 2 slides on the Architecture Document

Steve Kent
BBN Technologies

Changes in version -03

- The introduction is mostly the same, with some refinements to the description of Auditing
- A brief, new section was added to discuss threats, as requested at the prior meeting
- There were some minor edits throughout, e.g., changing “careful browser” to “CT-aware” browser
- A normative reference was added to point to the CT architecture document

Comments?

- I have received NO comments on the list or privately for this version of the document, which is why I elected to not get up at 1 AM to present this briefing ☺
- Based on the lack of requested changes to this document, I assume we're ready for WGLC ;-)
- The next few slides ask some simple questions, in hopes of stimulating discussion …

Do we agree on the Goals?

- 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
  - Auditors deter mis-issuance and alert Monitors to log misbehavior

How About this definition?

- 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

How About this One?

- 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, …

Monitor Characteristics?

- 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
- Relies on the Audit function to detect misbehaving logs

Characterization 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
  - Exceeds STH frequency count
  - Fails to log a certificate for which it has issued an SCT
  - Provides different Merkle tree data to different clients (motivating a gossip mechanism)

Architecture Document (1)

- As discussed at the prior meeting, I believe that much of the text from the introduction belongs in an architecture document. So, I generated one using some of that text
- As I tried to complete that document it became apparent that it should provide only a high level view of CT, and refer to other documents that provide details for CT elements: log, CT-aware CA, Monitor, Auditor, and CT-aware browser
- 6962-bis is mostly a log specification, and it could shrink to become just that, making it easier to read

Architecture Document (2)

- We published a first cut at the architecture document (draft-kent-trans-architecture-00.txt) but plan to shrink it, and point to 4 CT element documents:
  - Log specification (based on 6962-bis)
  - CT-aware client specification
  - CT-aware CA/Subject specification
  - Monitor/Auditor specification
- Each of these documents will be small and focused and thus easier to read than the architecture document (or 6269-bis)
- We will streamline the architecture document, and have it refer to these specs

Post-Prague Vacation Photo