A Threat Analysis for TRANS

Stephen Kent
BBN Technologies

Presentation Outline

- Why, What & How
- Analysis structure
- Analysis Outline
- What’s Missing

Terminology

- A vulnerability is a security flaw in a protocol or system
- An attack is a means to exploit a vulnerability
- A countermeasure is a procedure or mechanism that attempts to thwart a class of attacks
- A threat is a motivated capable adversary
  - A capable adversary that is not motivated to attack a system is not a threat
  - A motivated adversary not capable of mounting a class of attack is not a threat

What is a Threat Analysis

- A threat analysis examines attacks and consequences thereof in the context of a system (paraphrased from RFC 4949)
  - Provides a taxonomy of threat actors and classes of attacks
  - Characterizes the major elements of a system, to understand how they may be attacked or how they may serve as countermeasures
  - Examines how attacks are addressed by the system
    - attacks that are thwarted by countermeasures in the system
    - un-remedied vulnerabilities
- The analysis requires that the security functionality or security goals of the system are clearly articulated

When is it Needed

- Most IETF protocols are not security protocols, and so the Security Considerations section of a RFC suffices
- IETF protocols that are security-focused may merit generation of a separate threat analysis document or an extensive Security Considerations section
- BGPsec is an example of a system for which a threat model (RFC 7132) was required
- CT is a complex, security-focused system with a number of elements (logs, TLS clients, Monitors, audit function) and thus it seems to merit a threat analysis

What Good is It?

- Before a design is complete, a threat analysis can help guide system designers to address un-remedied vulnerabilities
- After a design is complete, a threat analysis helps prospective users understand what security the system offers and what residual vulnerabilities exist
- A threat analysis makes clear to readers what types of threats and attacks the system design envisions, and also what is out of scope

The Current CT Analysis Text

- Characterizes mis-issuance as either
  - Syntactic mis-issuance (relative to a certificate profile)
  - Semantic mis-issuance (issued to an entity not authorized to represent the Subject name in the certificate)
- Defines and examines a taxonomy of scenarios
  - Non-malicious CAs vs. malicious CAs
  - Errors vs. attacks
  - Certificates that are logged vs. non-logged certificates
  - Benign vs. conspiring logs
  - Self-monitoring vs. benign or conspiring Monitors

Attack Analysis Outline

- 1.1. Non-malicious CA
- 1.1.1. Error
- 1.1.2. Attack victim
- 1.1.2.1. Certificate logged
- 1.1.2.1.1. Benign log
- 1.1.2.1.1.1. Self-monitor
- 1.1.2.1.1.2. Benign 3rd party Monitor
- 1.1.2.1.1.3. Conspiring 3rd party Monitor
- 1.1.2.1.2. Conspiring log
- 1.1.2.2. Certificate not logged
- 1.2. Malicious CA
- 1.2.1. Certificate logged
- 1.2.1.1. Benign log
- 1.2.1.1.1. Self-monitor
- 1.2.1.1.2. Benign 3rd party Monitor
- 1.2.1.1.3. Conspiring 3rd party Monitor
- 1.2.1.2. Conspiring log
- 1.2.2. Certificate not logged

What's Missing?

- I originally envisioned a threat model, but focused on attacks because of lack of feedback on the adversary section
- Some threats are implicitly identified, because the analysis considers malicious CAs, plus conspiring logs and conspiring Monitors
- A concise statement of CT security goals is needed, either here or in 6962-bis, e.g.,
  - The goal of CT is to deter, detect, and help mitigate certificate mis-issuance.

Separate or Part of 69-bis?

- Absent specifications for log clients, the analysis identifies many un-remedied vulnerabilities
- Because 69-bis defers specification of client behavior, we can't be sure if the log interfaces it defines suffice to address the security goals
- If we complete client behavior specifications before progressing 6962-bis, then the threat analysis will be more positive, whether it is part of 6962-bis or a separate document

QUESTIONS ?