What is Trusted Computing?

Ariel Segall

Day 1

Approved for Public Release: 12-2749.
Distribution unlimited
What is Trust?

According to the Trusted Computing Group\textsuperscript{1}:

\begin{quote}
A trusted component is one which is predictable.
\end{quote}

- Trusted is not the same as good!
  - But it gives us a foundation to build on
- Two broad reasons to trust:
  - Reliable evidence
  - Out-of-band assumptions/No choice!

\textsuperscript{1}We’ll get to them shortly
What is Trust?

According to the Trusted Computing Group\(^1\):

*A trusted component is one which is predictable.*

- Trusted is not the same as good!
  - But it gives us a foundation to build on

- Two broad reasons to trust:
  - Reliable evidence *Attestation*
  - Out-of-band assumptions/No choice! *Root of Trust*

\(^1\)We’ll get to them shortly
What is Trusted Computing?

- Not a precise term
- Generally, refers to systems that use hardware to provide security support to software
  - Today: Trusted Platform Modules (TPMs); processors with secure modes (TXT, SVM)
  - Future: Mobile Trusted Modules (MTMs)
- Also covers infrastructure relying on above
  - Software applications
  - Network Access Control (NAC)
  - Secure storage devices
  - etc...

Goal: build trust in entire system for some purpose
The Grand Trusted Computing Vision

- Before logging into a computer, I know it’s good.
- Machines that aren’t up-to-date are routed to a DMZ to perform updates before connecting to the network.
- Servers can confirm exactly which machines they’re talking to and whether they’re running good software before providing sensitive data.
- All of my data, including secret keys, are protected by hardware and cannot be stolen over the network.

We’re not there yet, but we’re moving in the right direction.
A High-Level Workstation View

Operating System

Apps

TPM
CPU
TXT/SVM

What is Trusted Computing?
Trusted NAC From 50,000 Feet

Client Machines Wishing to Connect

Gateway

Network

Integrity Report

STOP

What is Trusted Computing?
The Trusted Computing Group (TCG)

- Industry (mostly) consortium
- Defining standards for trusted computing
- Layered vision: starting from hardware, moving up to applications
- Workgroups focused on particular subsets of the problem; e.g:
  - Technological: TPM, Mobile Solutions
  - Interoperability: Infrastructure, Trusted Network Connect
  - Use cases: Server, Trusted Multi-Tenant Infrastructure
- www.trustedcomputinggroup.org
- Formerly the Trusted Computing Platform Alliance (TCPA)

Most technologies in this area are defined by or with the TCG.
Why the TCG Matters

Sometimes we trust because we have no choice!

- TCG standards help define which components we must trust
- Standards can be evaluated to determine if we should trust
- TCG has compliance programs
  - Not government CA, but better than nothing
- Give us a foundation on which to build

Unfortunately, not very good at communicating with users.
Trusted Computing Topics in This Class

- Trusted Platform Modules
  - The foundation most of the rest is built on
  - Most of the technical meat of this class

- Roots of Trust for Measurement
  - With the TPM, what allow us to verify machine state
  - Two kinds: static (BIOS) and dynamic (CPU)

- Trusted Network Connect
  - NAC protocol with trusted computing support

- Not covered in detail:
  - Storage: Too specialized
  - Most infrastructure protocols: Too many!