Do I know you? Can I trust you?
Building Trustworthy Systems

Overview

Stacy Cannady – Cisco - scannady@cisco.com
TCG Board of Directors

May 2014
Agenda

Challenge

How Does TCG Define Trusted Systems?

Designs and Architectures

Gazing into the Crystal Ball
Challenge: Why are Trustworthy Systems Needed?

Bottom line: When all you have is an IP address, how do you answer these two questions about what is on the other end:

- Do I know you?
- Can I trust you?
In the uncertain world of software, how does one create trust?

- A standard business practice is to reduce risk by building relationships with suppliers and customers
  - Meet each other – establish proof of identity
  - Get to know each other – establish knowledge of character

- How does this map to the digital world?
  - Establish proof of identity – exchange of digital certificates
  - Establish knowledge of character – measure integrity of the software inventory on the platform – is that inventory what you expect to find?
  - Perform these exchanges with the assistance of dedicated security hardware

……..“Dedicated security hardware”? Like what?
The Trusted Platform Module (TPM) – a standards-based hardware security module – the foundation of platform security

- The TPM is a hardware security module that protects keys, integrity measurements, digital certificates and other small secrets.
- It potentially can be used in any computing device that requires these functions.
- It is assembled onto the motherboard of the platform, or can run as software in a secure operational context.
- TPMs are now shipped in almost all enterprise end point computers.
- TPMs are also found in several tablets and in a handful of other platforms such as smartphones, ATMs, servers and gaming machines.
A little more specificity – What does a TPM get me?

- Provides a hardware foundation for trusted platforms

- Provides interoperable interfaces that support trusted services
  - Authentication – Answer the question of who this platform is with a HW-protected digital signature
  - Access control – Protect secrets against software-based attack
  - Platform/application integrity – Provide HW-protected evidence that the software has not been tampered with
  - Cryptographic services – signing and encryption, symmetric and asymmetric crypto

- Secure repository for cryptographic keys
- Secure storage and reporting of measured state of resident software
Sold!

Where do I get TPMs and How do I Use/Manage Them?
A High Security use case on PCs
Enhancing Visibility and Control over where work is done in the Cloud
Intel Trusted eXecution Technology (TXT) on PCs and Servers

TXT – What does it do?
• The Sysadmin selects and configures a BIOS for the platform
• He uses Intel tools to measure and sign the BIOS
• The configured BIOS is installed on the platform, along with Golden Measurements
• Repeat this for the Hypervisor
• At power on, TXT HW and FW validate the BIOS and Hypervisor before they are booted

The integrity of blue components is validated Intel HW and the TPM.
Applying the SecureView Model to Cloud Servers

- SecureView uses Intel TXT and the TPM to validate BIOS and the Hypervisor at start
  - You always know you started a trusted Hypervisor and all of its services
  - If one of those services continuously validates runtime integrity, you know the hypervisor remains trusted

- If VMs are also integrity checked at start, then the VM is also trusted
  - Same deal – if one of the services in a VM validates runtime integrity, you know the VM remains trusted

- Defense against zero-day attack: Integrity validation is focused only on detecting ANY uncontrolled change – not any specific change
Example Cloud Stack at System Start

Integrity of VM measured at start and runtime integrity validated as for hypervisor

Runtime integrity validated by Trapezoid or the like

TXT and TPM validate integrity of Hypervisor
Protection of the Cloud Stack in Execution

Runtime integrity validation monitors uncontrolled changes to processes in execution – any change is seen, therefore we have (limited) Zero-Day defense

- Continuous integrity validation gives no insight into the nature of the change.
- Operationally, that is generally unimportant.
- The rapid discovery that uncontrolled change occurred, IS important.

The HW is mostly out of the loop during runtime (until TCG’s DRTM spec is implemented)
Intel Trusted Compute Pools
Teaching Embedded Systems About Stranger Danger

Design:
- Authentication protocol enhanced to require
  - Certificate exchange
  - Integrity report exchange
- At session start, each side
  - Signs a nonce and their integrity report using a HW protected key
  - Validates the provided report
- No match, no session
  - No session, no hack

GPU includes a TPM

Unknown operator

No key and no valid integrity report

Central ICS console
Questions?

www.trustedcomputinggroup.org

scannady@cisco.com