SESSION ID: TECH-F03

TRUSTED SUPPLY CHAIN & REMOTE PROVISIONING WITH THE TRUSTED PLATFORM MODULE

Tom Dodson
Supply Chain Security Architect
Intel Corporation/Business Client Products

Monty Wiseman
Security Architecture
GE/Global Research
Trusted Supply Chain Introduction

- **Problem**
  - Assurance of a device’s origin in today’s diverse manufacturing, logistics, and just in time inventory.
  - Remote deployment and provisioning requires assurance in the Supply Chain.
    - Reduce reliance on physically tracking devices through the Supply Chain
    - Reduces cost, decreases service time, ...

- **Solution**
  - Use a Root of Trust to provide assurance of a device’s origin
  - This Root of Trust establishes the foundation for a Trusted Supply Chain

- We will explain the use of a hardware Root of Trust to establish a Trusted Supply Chain
Trusted Supply Chain – Value Proposition

Platform Manufacturer

- Counterfeit and substitution detection
- Inventory Tracking
- Reduced cost with
- Increase trust

Installer

- Reduced in situ installation and replacement cost
- Remote proof allow remote key provisioning
- Keys allows trusted remote configuration
- Trusted channels using keys allows multiplexing connections reducing cabling costs

Plant Operator

- Attestation increases trust and capabilities of analytics
“cyber security officials are concerned that computers and handheld devices could introduce compromised hardware into the Defense Department supply chain, posing cyber espionage risks, said officials familiar with the report.”

DFAR 252.246
Contractor Counterfeit Electronic Part Detection and Avoidance System:
Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
TPM General Architecture

- **Endorsement Key (EK)**
  - Permanent* Key proves this is the expected TPM
  - Provides assertions about the TPM...
    - but no assertions about the platform
- **EK “certifies” other TPM / Platform keys**
  - Created by the owner or users

* Some exceptions apply
Trusting the Chain of Trust

- Value of the Measurements are proportional to the trust in the RTM
- Provided by the Platform Manufacturer
TPM General Architecture

- **TPM**
  - EK Cert signed by TPM Vendor
- **Platform Manufacturer (PM) attaches TPM to platform**
  - EK is bound to the Platform
  - Provides a platform-specific key
- **Platform Certificate**
  - Attributes assert information about the platform
    - As built data (components)
    - RTM binding to TPM
- **Supply chain obtains proof of assertions**
  - Verify Platform and EK Certificate signatures
  - Verify EK Certificate bound to *that* platform

* RTM: Root of Trust for Measurement
Trusted Supply Chain

TPM Manufacturer
- TPM Manu Cert
- EK Certificate
  - TPM Attributes
- Platform Manufacturer
  - Plat Manu Cert
  - Platform Certificate
    - Reference
    - Platform Attributes
- Platform Owner
  - Owner CA
  - EK Certificate
  - Platform Certificate
    - Reference
    - Platform Attributes
  - Owner Key
    - 1. Verify Plat Cert signature
    - 2. Verify EK Cert signature
    - 3. Verify EK Cert == Plat Cert
    - 4. Verify EK == EK Cert

EK verifies Owner Key is TPM resident
Generating the Chain of Trust

**Trusted Platform Module**
- Creates Endorsement Key (EK) for each Trusted Platform Module (TPM)
- Establishes hardware root of trust

**Endorsement Key Certificate**

**Platform**
- Platform Manufacturer
  - Permanently mounts TPM onto the platform
  - Creates platform certificate and binds it to the EK

**Platform Certificate**
- Signing Service
  -Platform Certificate cryptographically binds the platform to the EK

**Appliance Certificate**
- System Integrator
  - Creates appliance certificate; binds it to the platform certificate

**End User**
- System Integrator
  - Establishes technology provider accountability
  - Creates transparency

Chain of Trust Built Up by Multiple Parties in System Lifecycle

Ability to trace appliance to credible hardware root of trust

• Establishes technology provider accountability
• Creates transparency
Trusted Supply Chain Overview

• Enables **component-level traceability** for platforms and systems:
  • *Mitigates risk* of counterfeit electronic parts
  • *Conforms to DFARs* Supplement 246.870-2

• Traceability based on a hardware root of trust for each system:
  • Root of trust provided by **Trusted Platform Module** (TPM) 2.0 on motherboard
  • Associates *platform* with the TPM public Endorsement Key (EK)

• Trusted Supply Chain also provides an end-user **Auto Verify tool**:
  • *Identifies certain system changes* from the time of manufacturing to the time of first boot

• “As-Built” data report and Auto Verify tool offer customers *confidence in the authenticity of their systems*
Trusted Supply Chain Components

- Trusted Supply Chain provides traceability for customer platforms
- The following are the traceability components

<table>
<thead>
<tr>
<th>TSC COMPONENT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-Level Traceability</td>
<td>• Supported by <em>signed platform certificates</em></td>
</tr>
<tr>
<td></td>
<td>• Linked to discrete <em>Trusted Platform Module</em> on motherboard</td>
</tr>
<tr>
<td>Component-Level Traceability</td>
<td>• Supported by <em>“as-built” report</em> from ODM</td>
</tr>
<tr>
<td></td>
<td>• <em>ODM partnerships</em> are vital to two-level traceability</td>
</tr>
<tr>
<td>Statement of Conformance</td>
<td>• Attests to <em>authenticity of system</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Signed by Platform Manufacturer</em></td>
</tr>
<tr>
<td>Customer Web Portal</td>
<td>• Provides <em>customer access</em> to signed files</td>
</tr>
<tr>
<td></td>
<td>• Files available for <em>download</em></td>
</tr>
</tbody>
</table>
Trusted Supply Chain Process

1. Component and Platform Data Captured at ODM
   - "As-Built" Data File
     - Component Data (vendor, part #, serial #, validation history, ...)
   - Direct Platform Data File
     - Platform Snapshot Data (e.g., model #, PCR data, processor, memory, disk, ...)
   - TPM Platform Certificate Data File
     - Certificate Data (Endorsement Key, Endorsement Key serial #, ...)

2. Data Transmitted to Intel Key Generation Services
   - "As-Built" Data File
   - Direct Platform Data File
   - TPM Platform Certificate Data File

3. Signed Certificates Created & Stored on Intel Database
   - Signed "As-Built" Data
   - Signed Platform Certificate
   - Signed Statement of Conformance

4. Signed Certificates Available for Download, View, and Data Analytics

5. Auto Verify Tool (Web Download)
Direct Platform Data snapshots

- Is the platform that arrived at the customer that same platform that shipped out of the ODM Factory?
- The Auto Verify tool uses “SnapShots” to compare the contents of the Direct Platform Data
- Any changes in the Direct Platform Data from the ODM to the Customer will be flagged!

**Diagram:**

1. **ODM “Snap Shot”**
   - Motherboard
   - TPM
   - EK Certificate
   - ODM MANUFACTURING

2. **“Direct Platform Data File”**

3. **End Customer**
   - First Power On

4. **OOB “Snap Shot”**
   - TPM
   - Platform Certificate
   - Motherboard
   - END CUSTOMER FIRST POWER ON
System-Level Traceability

- Traceability based on a hardware root of trust for each system:
  - Root of trust provided by Trusted Platform Module (TPM) 2.0 on motherboard
  - Associates platform serial # with TPM serial # and public Endorsement Key (EK)

- Software tools deployed during the manufacturing flow at the ODM:
  - Capture system information
  - Capture TPM Certificate (Including public EK)

- Unique X.509 Platform Certificate for each system:
  - Generated and signed using Platform Manufacturer Certificate Authority
  - Attest that the purchased system is the specific system built by expected manufacturer
Auto Verify Tool

- **Platform Certificate Validation:**
  - Verifies that the platform TPM matches the signed platform certificate downloaded from the Customer Web Portal
  - Platform Attestation is confirmed by comparing the TPM module’s Endorsement Key against the Endorsement Key stored in the platform certificate

- **Direct Platform Components Validation:**
  - The Auto Verify tool compares the “snapshot” of the platform component data taken during manufacturing with a “snapshot” of the platform components taken at first boot
  - Any changes in system will be flagged and reported out to the customer in the tool
  - Additional platform “snapshots” can be used throughout the Platform life cycle
Auto Verify tool Identifies Changes

Changes in the Platform Data between snapshots are Identified

Identified changes are displayed
Summary

- A Trusted Supply Chain is based on a hardware Root of Trust
  - TPM provides this hardware Root of Trust
- End-user verifiable component authenticity backs up the hardware Root of Trust
- Auto-Verify tool validates the system component
- Platform Certificate Verification for TPM/Platform authentication
- Intel® Transparent Supply Chain provides a Trusted Supply Chain for Multiple OEMs
Apply What You Have Learned Today

- Next week you should:
  - Consider your companies IT Components supply chains

- In the first three months following this presentation you should:
  - Identify IT Components that have supply chain risk
  - Determine if there is an opportunity to incorporate TSC supply chain

- Within six months you should:
  - Implement a secure supply chain based upon the TPM Module
  - Consider platforms that incorporate TSC and the TPM Module
References

- **Contacts:**
  - Monty Wiseman: monty.wiseman@ge.com
  - Tom Dodson: tom.dodson@intel.com

- **Trusted Computing Group**
  - [https://trustedcomputinggroup.org/](https://trustedcomputinggroup.org/)
  - Infrastructure Work Group documents:
    - [https://trustedcomputinggroup.org/work-groups/infrastructure/](https://trustedcomputinggroup.org/work-groups/infrastructure/)

- **Software Stacks**
  - [https://github.com/tpm2-software](https://github.com/tpm2-software)
  - [https://sourceforge.net/projects/ibmtpm20tss/](https://sourceforge.net/projects/ibmtpm20tss/)

- **A Practical Guide to TPM 2.0**