Building hardware-based security with a Trusted Platform Module (TPM)

Tony Mangefeste
Senior Program Manager
Microsoft Corporation
Agenda

- Security goals for Windows 8
- Trusted Platform Module basics
- Improving security during boot with TPMs
- TPM-enabled features in Windows 8
- Provisioning and control
- TPM hardware evolution and guidance

You will leave understanding

- How TPMs are used by Windows 8 and apps
- What kind of TPM hardware to expect on Windows 8 systems
Our world today

- Cyber crime focuses on stealing data for monetary gain
- Worrying about cybercrime is universal
  - Ranging from governments to your mom
  - And everyone in between
- Socially engineered attacks are particularly successful on machines used with administrator accounts
- Bootkit and rootkit attacks can infect anti-malware software and alter boot logs to avoid detection
Security goals for Windows 8

• Windows 8 is a trusted platform for consumers, businesses and financial institutions

• Hardware helps anti-malware products reduce persistent malware
  • System compromise by malware reduced
  • Sophisticated malware can be reliably detected and removed
  • New tools, APIs, and hardware capabilities for anti-malware products

• Customers benefit from easy-to-use hardware-based security
Trusted Platform Module basics
Trusted Platform Module basics

- TPMs are passive security devices that provide hardware-based security and cryptographic functions
- Specs are published by the Trusted Computing Group
- Business laptops often have a TPM 1.2 used for BitLocker
TPM basics

- System firmware and the TPM work together
- Firmware records boot measurements in the TPM
- TPM measurements are not reset until the next power cycle
- TPM created keys can be bound to boot measurements
Improving security during boot with TPMs
Secured boot: Improving malware resistance during boot

- Secure boot: Using Firmware Policy to validate the OS loader
- Early launch anti-malware: Starting anti-malware products first before other 3rd party code
- Measured boot: Recording the start state of the system as evidence for external verification
**UEFI secure boot**

### Existing Boot Processes

- BIOS
- **Any OS Loader Code**
- OS Start

- The BIOS starts any OS loader, even malware
- Now firmware enforces policy, only starting trusted OS loaders
- OS loader enforces signature verification of later components

### Secure Boot with Windows 8

- Native UEFI 2.3.1
- **verified OS Loader Only**
- OS Start

- UEFI will only launch a verified OS loader – such as Windows 8
- Essentially malware cannot replace the boot loader
Early launch anti-malware (ELAM)

- The Anti-Malware boot driver is specially signed
- Windows starts ELAM software before any other 3rd party boot drivers
- ELAM driver can enforce policy even for boot start drivers
- Rootkit malware can no longer bypass anti-malware inspection
Post-boot clients can use signed TPM measurements to prove initial system state and ELAM software.

ELAM software can invalidate client health assertions if the client stops enforcing policy (i.e. providing no signature updates or running unknown software).
Secured boot architecture

1. Secure Boot prevents running an unknown OS loader
2. ELAM starts first and enforces its policy
3. Boot measurements were recorded during boot
4. Signed TPM boot measurements can be sent to an off-box service for analysis
TPM-enabled features in Windows 8
BitLocker network unlock for Windows 8

1. TPM + PIN (Windows 7)
   - TPM
   - PIN
   - Encrypted OS Volume

2. BitLocker Network Unlock
   - Windows 8 WDS Server
   - Key Request
   - Client Key
   - TPM
   - Encrypted OS Volume
   - Native UEFI Boot
   - UEFI DHCP 4 or 6

1. Continued investment in BitLocker Drive Encryption™ and TPM
2. No user PIN required when booting on a physically secured network (a PIN is still required when roaming)
TPM based certificate storage

- Certificates have many uses such as e-mail/document signing and authentication with or without a user supplied PIN
- The certificate template can be configured to specify the TPM is used to store the private key
  - Software can never discover the private key
  - The TPM protects the PIN with its dictionary attack logic
  - These protections are malware resistant
- Your apps can use the new Platform Crypto Provider KSP to create and store keys
TPM based Virtual Smart Card

- Windows 8 enables a TPM to act like a permanently-inserted Smart Card
- Scenarios include logging onto Windows, simplified use of Direct Access
- Enables enterprises to extend existing investments in physical smart cards
TPM provisioning and control
TPM Auto Provisioning

<table>
<thead>
<tr>
<th>Windows State</th>
<th>Out of Box</th>
<th>After Reboot</th>
<th>Later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Ready</td>
<td>Not Ready</td>
<td>Ready</td>
<td>User in Control</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>The user chooses to use the TPM by turning on a TPM-enabled feature or running a TPM-based application</td>
</tr>
<tr>
<td>Deactivated</td>
<td>Activated</td>
<td>Activated</td>
<td></td>
</tr>
<tr>
<td>Ownership Not Taken</td>
<td>Ownership Not Taken</td>
<td>Ownership Taken</td>
<td></td>
</tr>
</tbody>
</table>

- Windows prepares the TPM for use without physical presence
- New TCG Physical Presence Interface Specification 1.2
TPM Based App Runs

Is TPM State Ready?

No

App Launches OS Wizard

Administrator Interaction

Clear TPM (If necessary)

Yes

App Uses the TPM

Windows 8 TPM Wizard

Older hardware or system state may prevent auto-provisioning. The app may be ready to use the TPM before it is provisioned. New Windows 8 wizard for preparing the TPM. Applications do not need their own TPM provisioning logic.
TPM hardware evolution and guidance
Windows 8 supports TPM 1.2 & TPM 2.0*

- Microsoft is working with partners to support discrete and integrated TPMs for different form factors and market segments
- Build your apps using new Windows 8 APIs so it works with TPM 1.2 or TPM 2.0

Microsoft refers to the TCG “TPM Next” as “TPM 2.0”
Summary

- There are many compelling TPM scenarios
- Expect TPM 1.2 and TPM 2.0 on a wide array of platforms
- TPMs are useful for apps with familiar programming models like smart cards, certificates and a key storage provider
- Windows 8 has a bunch of new TPM-enabled features
Further reading and documentation

- [Trusted Computing Group](#)
- Links to MSDN
  - [Windows Hardware Dev Center](#)
  - [Windows Dev Center](#)