Deploying Secure Boot: Key Creation and Management

UEFI Summer Summit – July 16-20, 2012
Presented by Arie van der Hoeven (Microsoft Corporation)
Agenda

- Introduction
- Secure Boot Basics
- Secure Boot Keys
- Key Deployment
- Key Creation and Management
- Checklist
Introduction

• Today partners are testing Secure Boot using WHCK tools and Microsoft provided certificates
  – But passing Windows requirements is just a start
• OEMs and ODMs need to have a plan for securely creating and managing their own keys
  – Customers will increasingly ask about this
  – What is your story?
• Reputations are on the line
In the news...

Los Angeles Times
Microsoft warns of phone-call security scam targeting PC users
By Nathan Okwara-Giles, June 17, 2011
Microsoft is warning its customers of a new scam that employs "criminals posing as computer security engineers and people at home to tell them their computer security

eWeek.com
Researchers Discover Link Between TDSS Rootkit and DNSChanger Trojan
By Nick Bilott, May 2, 2011
TDSS rootkit, the hard-to-remove malware behind numerous sophisticated attacks, appears to have spread the DNSChanger Trojan.

eWeek.com
Microsoft Recommends Reinstalling Windows to Remove Nasty Trojan
By Fahmita Y. Rashid, June 28, 2011
A new variant of the Trojan Popureb burrows deep enough into the Windows operating system to make removing the malware almost impossible.

COMPUTERWORLD
Expect targeted attacks after massive Epsilon email breach, say experts
By Gregg Keizer, April 4, 2011
Database of stolen addresses is a gold mine for hackers and scammers.

COMPUTERWORLD
HIGH-PROFILE DATA BREACH Epsilon Interactive reported April 1 caused widespread fear among companies. The company noted on its website that the breach was a "targeted attack" and that it was not using the stolen data.

PCWorld
Microsoft Exposes Scope of Botnet Threat
By Tony Bradley, October 15, 2010
Microsoft's latest Security Intelligence Report focuses on the expanding threat posed by bots and botnets.

PCWorld
Me broot: The Stealthiest Rootkit in the Wild?
By Nick Wingfield, March 18, 2011
In a detailed examination of the stealthiest of all rootkits, Microsoft this week unveiled the ninth volume of its Security Intelligence Report (SIR). The semi-annual assessment of the state of computer security

THE WALL STREET JOURNAL
Hack attack spills web security firm's confidential data
By Dan Goodin in San Francisco. Posted in Security, 11th April 2011
Try this for irony: The website of web application security provider Barracuda Networks has sustained an attack that the company claims to have exposed the company's own web application.
Secure Boot prevents malicious Boot code and OS loader

AM software is started before all 3rd party software

Secure Boot

BitLocker Unlocks Disk if TPM and Secure Boot Integrity in place

AM Policy

Windows Kernel and Drivers

Windows Logon

UEFI Boot

AM Policy

Windows Logon

Client

Attestation Service

TPM

Client retrieves TPM measurements of client state on demand

Measurements of components including AM software are stored in the TPM

UEFI Summer Summit – July 2012
UEFI Secure Boot Keys

- **Platform Key (PK)**
  - One only
  - Allows modification of KEK database

- **Key Exchange Key (KEK)**
  - Can be multiple
  - Allows modification of db and dbx

- **Authorized Database (db)**
  - CA, Key, or image hash to allow

- **Forbidden Database (dbx)**
  - CA, Key, or image hash to block
# Keys Required for Secure Boot

<table>
<thead>
<tr>
<th>Key/db Name</th>
<th>Variable</th>
<th>Owner</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKpub</td>
<td>PK</td>
<td>OEM</td>
<td>PK – 1 only. Must be RSA 2048 or stronger</td>
</tr>
<tr>
<td>Microsoft KEK CA</td>
<td>KEK</td>
<td>Microsoft</td>
<td>Allows updates to db and dbx:</td>
</tr>
<tr>
<td>Microsoft Windows Production CA</td>
<td>db</td>
<td>Microsoft</td>
<td>This CA in the Signature Database (db) allows Windows 8 to boot</td>
</tr>
<tr>
<td>Forbidden Signature Database</td>
<td>dbx</td>
<td>Microsoft</td>
<td>List of known bad Keys, CAs or images from Microsoft</td>
</tr>
</tbody>
</table>

**+ Required for Secure Firmware Updates**

<table>
<thead>
<tr>
<th>Key/db Name</th>
<th>Owner</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure firmware update key</td>
<td>OEM</td>
<td>Recommendation is to have this key be different from PK. Must be RSA 2048 or stronger</td>
</tr>
</tbody>
</table>
### Optional Keys for Secure Boot (non WinRT only)

#### Recommended for non WinRT Systems

<table>
<thead>
<tr>
<th>Key/db Name</th>
<th>Variable</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft UEFI driver signing CA</td>
<td>db</td>
<td>Microsoft</td>
<td>Microsoft signer for 3’rd party UEFI binaries via DevCenter program</td>
</tr>
</tbody>
</table>

#### Optional for Customization

<table>
<thead>
<tr>
<th>Key/db Name</th>
<th>Variable</th>
<th>Owner</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OEM or 3’rd party KEKpub</td>
<td>KEK</td>
<td>OEM/3’rd party</td>
<td>Allows db/dbx updates e.g. for an alternate OS or Trusted 3’rd party</td>
</tr>
<tr>
<td>OEM or 3’rd party CA</td>
<td>db</td>
<td>OEM/3’rd party</td>
<td>Allows 3’rd party OS or drivers signed by a trusted 3’rd party</td>
</tr>
<tr>
<td>Image Hashes</td>
<td>db</td>
<td>OEM</td>
<td>Hashes of images on PC that are allowed to execute even if not signed</td>
</tr>
<tr>
<td>Forbidden Signature Database (dbx)</td>
<td>dbx</td>
<td>OEM/3’rd party</td>
<td>List of known bad Keys, CAs or images from OEM or partner</td>
</tr>
</tbody>
</table>
Key Deployment Process

1. Create Platform Key (PK) and Secure FW Update Key
2. Create PK Backup (Recommended)
3. Add KEK (w/db, dbx) and sign with PKpri
4. Add Secure Update Key (pub)
5. Enroll PKpub
6. Protect PKpri and Secure Update (pri)
7. Ensure Network and Physical Security
8. Manage and refine security practices
9. Done? (Never really)
Hardware Security Modules

• Microsoft strongly recommends using a Hardware Security Module (HSM) for key creation
• Most HSMs have Federal Information Processing Standard (FIPS) Publication 140-2 level 3 compliance
  – Requires that keys are not exported or imported from the HSM.
• HSMs support multiple key storage options
  – Local on the HSM itself
  – On the server attached to the HSM - for solutions which requires lots of keys
• The cryptographic module security policy shall specify a physical security policy, including:
  – Tamper-evident seals, locks, tamper response and zeroization switches, and alarms
  – Policy includes actions required by the operator(s) to ensure that physical security is maintained such as periodic inspections
Other Key Creation Options

• Trusted Platform Modules (TPM) or Smart Cards
  – Crypto processors slow for manufacturing environment
  – Not suitable for storing large number of keys
  – May not be compliant to FIPS 140-2 level 3

• Software / Crypto API generated keys
  – Can use encrypted drives, VMs and other security options
  – Not as secure as using an HSM

• Makecert
  – Intended for testing purposes only
  – Discouraged by Microsoft
Checklist

- Define your security strategy
  - Identify roles
  - Procure server and hardware for key management
    - Recommended solution – network or standalone HSM
    - Consider whether you will need one or several HSM’s for high availability and also your key back up strategy
  - Set policy for how frequently will you be rekeying keys
  - Have a contingency plan for Secure Boot Key compromise
  - Identify how many PK and other keys will you be generating
- Use HSM to pre-generate secure boot related keys and certificates
- Get the Microsoft KEK and other Secure Boot related keys and certificates
- Sign UEFI drivers
- Update firmware with Secure Boot keys based on the system type
- Run tests including WHCK Secure Boot tests
- Deploy > Refine > Deploy > Refine...
Resources

- Microsoft Connect  http://connect.microsoft.com/
- MSDN:  http://msdn.microsoft.com/
  – Search on keyword “Secure Boot”
- http://www.microsoft.com/security
- UEFI 2.3.1. Specification errata C:  http://www.uefi.org/
- Trusted Computing Group:  http://www.trustedcomputinggroup.org/
- Tianocore:  http://www.tianocore.sourceforge.net
- Beyond BIOS:  http://www.intel.com/intelpress/sum_efi.htm
Thanks for attending the UEFI Summer Summit 2012

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

Microsoft