Hacking Measured Boot and UEFI

Dan Griffin
JW Secure, Inc.
WWJBD?

Don’t let h@xors keep you from getting the girl…
Introduction

• What is UEFI?
• What is a TPM?
• What is “secure boot”?
• What is “measured boot”?
• What is “remote attestation”?
Hardware Landscape

- BYOD
- Capability standards
  - Phones
  - Tablets
  - PCs
Why the UEFI lock down?

- OEM & ISV revenue streams
- Importance of app store based user experience
- Defense against rootkits & bad drivers
- Screw the Linux community
State of UEFI

- Not new
- Full featured – can even include a network stack (yikes!)
- Software dev kits are available (Intel TianoCore)
- Test hardware is available (Intel; BeagleBoard)
UEFI secure boot

• Usually can be disabled/modified by user
  o Behavior varies by implementation
  o Complicated, even for power users
• But not on Windows 8 ARM. Options:
  o Buy a $99 signing certificate from VeriSign
  o Use a different ARM platform
  o Use x86
Measured Boot + Remote Attestation
What is measured boot?

- BIOS
- Boot Loader
- Kernel
- Early Drivers
- Hash of next item(s)
- TPM
- [PCR data]
- [AIK pub]
- [Signature]
- Boot Log
What is remote attestation?

Client Device
TPM

Signed Boot Log

Attestation Server

some token…
Demo

Measured Boot Tool
(http://mbt.codeplex.com/)
Part 1: What’s in the boot log?
c:\CodePlex\MeasuredBootTool\x64\Debug
>MeasuredBootTool.exe
Bitlocker <TPM> = True
Integrity services = True

Early boot binaries:
\Windows\system32\winload.exe -- SIGNED
\Boot\en-US\bootmgr.EEX.MUI -- SIGNED
\Windows\System32\Drivers\Keeepkg.sys -- SIGNED
\Windows\System32\drivers\Wdf\B0000.sys -- SIGNED
\Windows\boot\resources\en-US\bootres.dll.mui -- SIGNED
\Windows\System32\drivers\msemc.sys -- SIGNED
\Windows\System32\drivers\vdrroot.sys -- SIGNED
\Windows\System32\drivers\storahci.sys -- SIGNED
\Windows\System32\drivers\VMMEMIB.sys -- SIGNED
\Windows\System32\drivers\stpm.sys -- SIGNED
\Windows\System32\drivers\pei.sys -- SIGNED
\Windows\System32\drivers\scng.sys -- SIGNED
\Windows\System32\drivers\WalBoot.sys (ELAM) -- SIGNED
\Windows\System32\drivers\upv.sys -- SIGNED
\Windows\System32\drivers\xEnStorClass.sys -- SIGNED
\Windows\System32\drivers\rbdyboost.sys -- SIGNED
\Windows\System32\drivers\disk.sys -- SIGNED
\Windows\System32\drivers\wanetap.sys -- SIGNED
\Windows\System32\drivers\filtngr.sys -- SIGNED
\Windows\System32\drivers\WMFilter.sys -- SIGNED
\Windows\System32\drivers\msisadrv.sys -- SIGNED
\Windows\System32\CI.dll -- SIGNED
\Windows\System32\Drivers\Fp\Rec\sys -- SIGNED
\Windows\System32\drivers\tn.sys -- SIGNED
\Windows\System32\Drivers\fwvol1.sys -- SIGNED
\Windows\System32\drivers\ntds.sys -- SIGNED
\Windows\System32\drivers\partmgr.sys -- SIGNED
\Windows\System32\Drivers\WDFLDR.sys -- SIGNED
\Windows\system32\BOOTVID.dll -- SIGNED
\Windows\system32\mcupdate_GenuineIntel.dll -- SIGNED
\Windows\System32\drivers\spaceport.sys -- SIGNED
\Windows\System32\Drivers\Wmp\sys -- SIGNED
\Windows\System32\Drivers\MfIsr.sys -- SIGNED
\Windows\System32\drivers\storport.sys -- SIGNED
\Windows\System32\drivers\ACPI.sys -- SIGNED
\Windows\System32\Drivers\HpdVladesh.sys -- SIGNED
\Windows\boot\resources\bootres.dll -- SIGNED
\Windows\System32\Drivers\KsEdd.sys -- SIGNED
\Windows\System32\drivers\CLFS.SYS -- SIGNED
\Windows\System32\en-US\winload.exe.MUI -- SIGNED
\Windows\System32\ApiSetSchema.dll -- SIGNED
\Windows\System32\drivers\pdc.sys -- SIGNED
\Windows\System32\drivers\ntmst.sys -- SIGNED
\Windows\System32\drivers\nrutmr.sys -- SIGNED
\Windows\System32\drivers\NETTIO.SYS -- SIGNED
\Windows\System32\drivers\tcpip.sys -- SIGNED
\Windows\System32\Drivers\WppRecorder.sys -- SIGNED
\Windows\System32\drivers\upolicy.sys -- SIGNED
\Windows\System32\Drivers\acplex.sys -- SIGNED
\Windows\System32\Drivers\wplufs.sys -- SIGNED
\Windows\System32\ntoskrnl.exe -- SIGNED
\Windows\System32\hal.dll -- SIGNED
\Windows\System32\PSHDR.dll -- SIGNED
\Windows\System32\drivers\fupckint.sys -- SIGNED
\Windows\System32\drivers\wlngr.sys -- SIGNED
\Windows\System32\kd.dll -- SIGNED
\Windows\System32\drivers\wlngrx.sys -- SIGNED
\Windows\System32\drivers\fillinfo.sys -- SIGNED
\Windows\System32\drivers\CLASSPMP.SYS -- SIGNED
Demo

Measured Boot Tool

(http://mbt.codeplex.com/)

Part 2: How do you do remote attestation?
Client Device

C: Get AIK creation nonce
S: Nonce

C: Get challenge (EK pub, AIK pub)
S: Challenge

C: Get attestation nonce
S: Nonce

C: Signed boot log
S: Token

Attestation Service
Demo

Sample application #1: reduce fraud, protect the bank from h@xors, get the girl
Cloud Services Demand ID

• Enterprise: BYOD
• Consumer
  – Targeted advertising
  – eCommerce, mobile banking, etc.
• But most user IDs are static & cached on device
  – That only works for low-value purchases
  – How to improve ID for high-value purchases?
Low Friction Authentication

• Each additional screen requiring user input
  – Slows down the process while user reorients
  – Causes more users to abandon the web site

• In contrast, Progressive Authentication:
  – Let users investigate a site using just cookies
  – Defers questions until information is needed
  – Reduces user drop out from frustration
Splash Screen

- The screen a user sees when app launched
- With similar data in the launch tile
User Sign in

- User name can be taken from cookie
- But account details are hidden until the user enters a password
Enrollment - 1

- The first time the app is used the user must activate the app.
- When this button is pressed an SMS message is sent to the phone # on file.
Enrollment - 2

- After the user gets the pin from the SMS message, it is entered.
- After this the user proceeds as with a normal sign-in procedure.
After Sign-in

- The user sees all account information

Checking (7657435)
- Balance: $8,433.22
- Available: $8,433.22

Savings Account
- Balance: $431,100
- Available: $431,100

Interest Rate Change to 0.998% (0.94% APY) Oct 21, 2011
User tries to move money

- When user goes to move $ out of account
- The health of the device is checked
Remediation Needed

- If the device is not healthy enough to allow money transfer
- The user is directed to a site to fix the problem
Demo

Sample application #2: reduce fraud, protect MI6 from h@xors, get the girl
Secure Purchase Order System

Windows Security

Microsoft Smart Card Provider
Please enter your PIN.

PIN

Click here for more information

OK  Cancel

feedback@jwsecure.com
## Secure Purchase Order System

**Welcome, Dan!**

**Make a new purchase order**

### Current Purchase Orders

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Supplies</td>
<td>$1344.33</td>
</tr>
<tr>
<td>Computers</td>
<td>$22444</td>
</tr>
<tr>
<td>Desk</td>
<td>$3000.00</td>
</tr>
</tbody>
</table>

**Approved / Confirmed?**

- Office Supplies: Yes
- Computers: Yes
- Desk: Yes

---

[feedback@jwsecure.com](mailto:feedback@jwsecure.com)
Secure Purchase Order System

Signing you in...

Make a new purchase order

Current Purchase Orders

Approved / Confirmed?

feedback@jwsecure.com
Error Initializing Workflow

Error creating workflow

The key hash 66B248A036EA0433FD2299E72529E779438368CC for client W8A is not trusted.

at SecurePO.POWorkflow.SignOn()
at SecurePO.Window1.InitWorkflow()
Pseudo-Demo

Sample application #3: protect the data from h@xors, etc…
Policy-Enforced File Access

• BYOD
• Download sensitive files from document repository
• Leave laptop in back of taxi
Weaknesses

- UEFI toolkits evolving rapidly
- Provisioning; TPM EK database
- Integrity of the TPM hardware
- Hibernate file is unprotected
- Trend of migration from hardware to firmware
- Patching delay & whitelist maintenance
Conclusion

• Likelihood of mainstream adoption?
• What the consumerization trend means for hackers
• Opportunities in this space
Questions?

dan@jwsecure.com
206-683-6551
@JWSdan

JW Secure provides custom security software development services.