



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

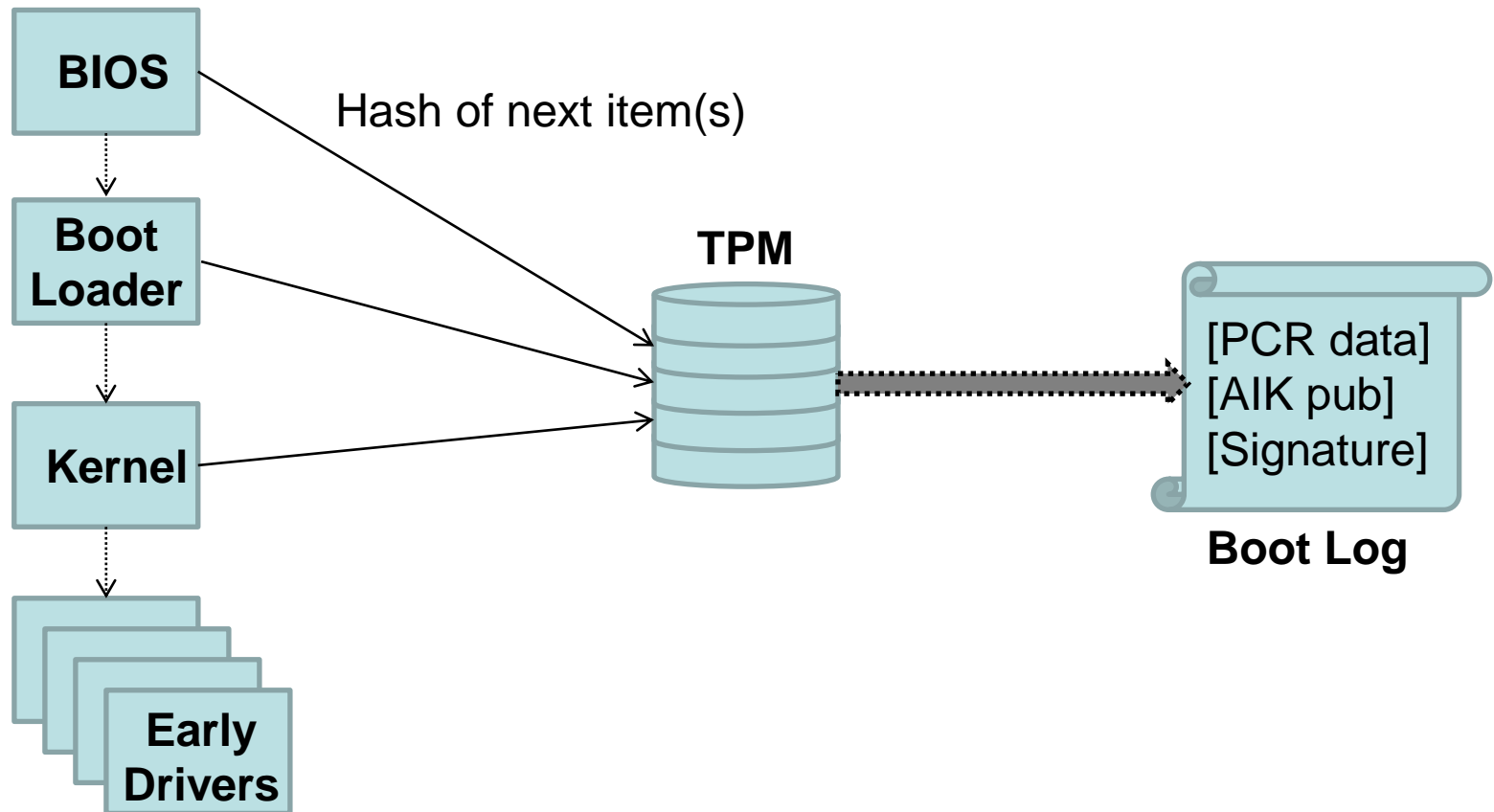
- Usually can be disabled/modified by user
 - Behavior varies by implementation
 - Complicated, even for power users
- But not on Windows 8 ARM. Options:
 - Buy a \$99 signing certificate from VeriSign
 - Use a different ARM platform
 - Use x86



Measured Boot + Remote Attestation

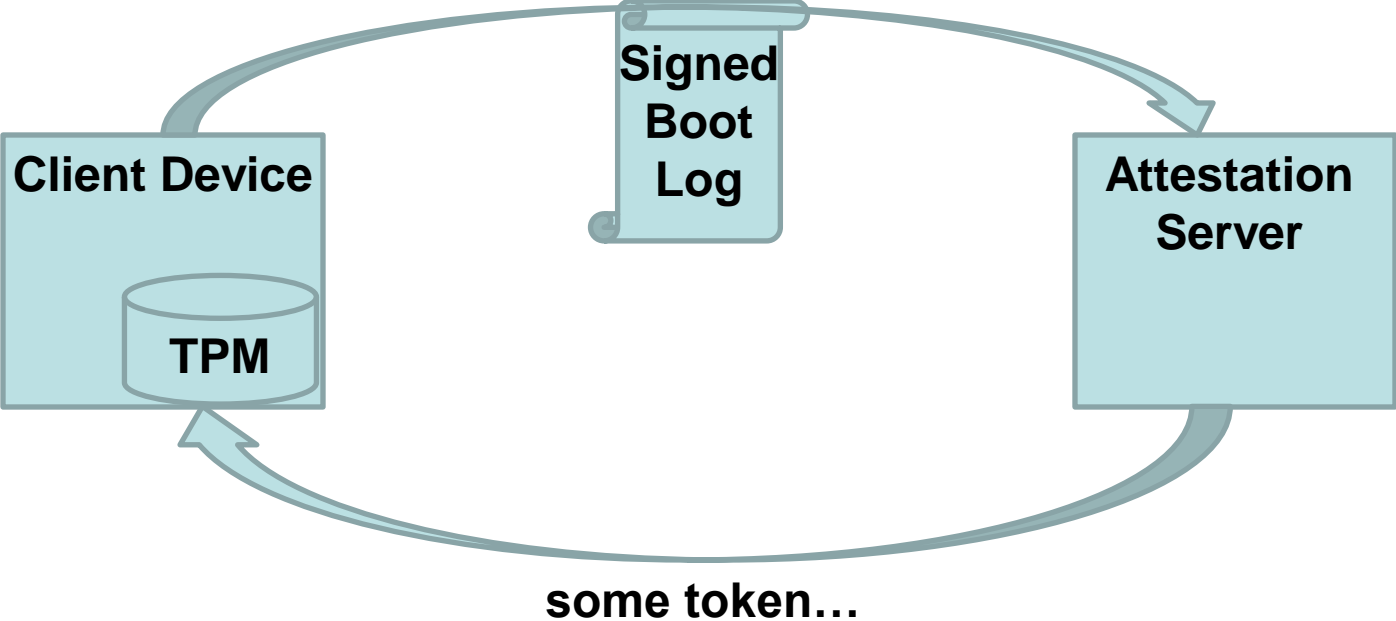


What is measured boot?





What is remote attestation?





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.EXE.MUI -- SIGNED
\Windows\System32\Drivers\ksecpkg.sys -- SIGNED
\Windows\system32\drivers\Wdf01000.sys -- SIGNED
\Windows\boot\resources\en-US\bootres.dll.mui -- SIGNED
\Windows\System32\drivers\msrpc.sys -- SIGNED
\Windows\System32\drivers\vdrvroot.sys -- SIGNED
\Windows\System32\drivers\storahci.sys -- SIGNED
\Windows\System32\drivers\WMILIB.SYS -- SIGNED
\Windows\system32\drivers\tpm.sys -- SIGNED
\Windows\System32\drivers\pci.sys -- SIGNED
\Windows\System32\Drivers\cng.sys -- SIGNED
\Windows\system32\drivers\WdBoot.sys (ELAM) -- SIGNED
\Windows\System32\drivers\pcw.sys -- SIGNED
\Windows\System32\drivers\EhStorClass.sys -- SIGNED
\Windows\System32\drivers\rdyboost.sys -- SIGNED
\Windows\System32\drivers\disk.sys -- SIGNED
\Windows\System32\drivers\volsnap.sys -- SIGNED
\Windows\system32\drivers\fltmgr.sys -- SIGNED
\Windows\system32\drivers\WdFilter.sys -- SIGNED
\Windows\System32\drivers\msisadrv.sys -- SIGNED
\Windows\system32\CI.dll -- SIGNED
\Windows\System32\Drivers\Fs_Rec.sys -- SIGNED
\Windows\System32\drivers\tm.sys -- SIGNED
\Windows\System32\DRIVERS\fuelvol.sys -- SIGNED
\Windows\system32\drivers\ndis.sys -- SIGNED
\Windows\System32\drivers\partmgr.sys -- SIGNED
\Windows\system32\drivers\WDFLDR.SYS -- SIGNED
\Windows\system32\BOOTUID.dll -- SIGNED
\Windows\system32\mcupdate_GenuineIntel.dll -- SIGNED
\Windows\System32\drivers\spaceport.sys -- SIGNED
\Windows\System32\Drivers\mup.sys -- SIGNED
\Windows\System32\Drivers\Ntfs.sys -- SIGNED
\Windows\System32\drivers\storport.sys -- SIGNED
\Windows\System32\drivers\ACPI.sys -- SIGNED
\Windows\system32\DRIVERS\hpdskflt.sys -- SIGNED
\Windows\boot\resources\bootres.dll -- SIGNED
\Windows\System32\Drivers\ksecdd.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\mountmgr.sys -- SIGNED
\Windows\system32\drivers\NETIO.SYS -- SIGNED
\Windows\System32\drivers\tcpip.sys -- SIGNED
\Windows\System32\Drivers\WppRecorder.sys -- SIGNED
\Windows\System32\drivers\hwpolicy.sys -- SIGNED
\Windows\System32\Drivers\acpiex.sys -- SIGNED
\Windows\system32\DRIVERS\wfpwfs.sys -- SIGNED
\Windows\system32\ntoskrnl.exe -- SIGNED
\Windows\system32\hal.dll -- SIGNED
\Windows\system32\PSHED.dll -- SIGNED
\Windows\System32\drivers\fwpkclnt.sys -- SIGNED
\Windows\System32\drivers\volmgr.sys -- SIGNED
\Windows\system32\kd.dll -- SIGNED
\Windows\System32\drivers\volmgrx.sys -- SIGNED
\Windows\System32\drivers\fileinfo.sys -- SIGNED
\Windows\System32\drivers\CLASSPNP.SYS -- SIGNED
```

```
c:\CodePlex\MeasuredBootTool\x64\Debug
```




Demo

Measured Boot Tool

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

Part 2: How do you do remote attestation?



Client Device

Attestation Service





Demo

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



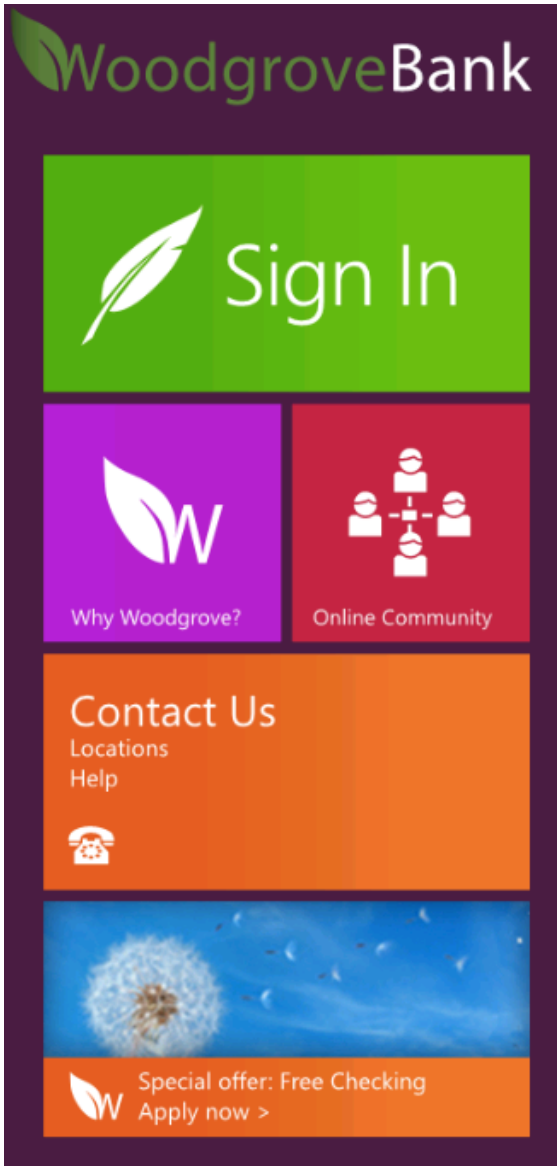
Cloud Services Demand ID

- 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



WoodgroveBank

Sign in

Enter your username and password below to view your account information.

[Sign up for a new account.](#)

[Forget your password?](#)

User Sign in

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



WoodgroveBank

Activate

Your device must be activated before it can be used to access account data. To receive an activation PIN text message, hit activate.

Cancel

Activate

[Manage your devices](#)

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



 WoodgroveBank

Sign in

Enter your username and password below to view your account information.

[Sign up for a new account.](#)

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



WoodgroveBank

Account balance

Hello Tom.
tom@jwsecure.com
[Update this information.](#)

Transfer

New Account

Contact

Checking (7657435)

Balance	\$8433.22
Available	\$8433.22

Savings Account

Balance	\$4311.00
Available	\$4311.00

History

Interest Rate Change to
0.998% (0.94% APY) Oct 21, 2011

After Sign-in

- The user sees all account information



User tries to move money

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

WoodgroveBank

Transfer money

Please select a source and destination account for your money transfer.

- Balance
- New Account
- Contact

\$222

1102768 Savings (\$4311.00)

7657435 Checking (\$8433.22)

tuesday

Transfer Money



Remediation Needed

The device does not appear to be updated with the latest firmware.

Please visit our website at <http://www.woodgrovebank.com/mobile> to find out how to solve the problem.

ok

Contact

\$222

1102768 Savings (\$3534.00)

7657435 Checking (\$9210.22)

Memo (optional)

Transfer Money

- 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

Secure Purchase Order System

Signing you in...

Make a new purchase order



Current Purchase Orders

Approved / Confirmed?

feedback@jwsecure.com

The main interface is a dark blue window titled 'Secure Purchase Order System'. On the left side, there is a vertical navigation bar with a blue background. It contains the text 'Signing you in...' and a prominent button labeled 'Make a new purchase order'. Below the button is a 3D illustration of a cardboard box with a green arrow pointing to the right, a laptop, and a document with a green checkmark. The main content area on the right is a table with a dark blue background and a light blue header. The header contains the text 'Secure Purchase Order System' and two column headers: 'Current Purchase Orders' and 'Approved / Confirmed?'. The table body is currently empty. At the bottom left of the window, the email address 'feedback@jwsecure.com' is displayed.



Secure Purchase Order System

Secure Purchase Order System

Signing you in

Make a new


Approved / Confirmed?

Windows Security

Microsoft Smart Card Provider

Please enter your PIN.

PIN

 PIN

[Click here for more information](#)

OK Cancel

feedback@jwsecure.com

The image shows a screenshot of a web application titled "Secure Purchase Order System" with a Windows Security dialog box overlaid. The dialog box is titled "Microsoft Smart Card Provider" and prompts the user to "Please enter your PIN." It features a text input field labeled "PIN" and a "Click here for more information" link. The background application has a dark blue theme and includes a "Make a new" button with a box icon and a "feedback@jwsecure.com" link at the bottom left.



Secure Purchase Order System



Secure Purchase Order System

Welcome, Dan!

Make a new purchase order



Current Purchase Orders

Approved / Confirmed?

Office Supplies - \$1344.33

Paper, printer cartridges
sally fuller 27/2/2012



Computers - \$22444

Computer for lab
joe smith 27/2/2012



Desk - \$3000.00

Ergo Desk for new hire
nirin rama 27/2/2012






Secure Purchase Order System

Secure Purchase Order System

Signing you in...

Make a new purchase order



Current Purchase Orders

Approved / Confirmed?

feedback@jwsecure.com

The main interface is a dark blue window titled 'Secure Purchase Order System'. On the left side, there is a vertical navigation bar with a blue background. It contains the text 'Signing you in...' and a prominent button labeled 'Make a new purchase order'. Below the button is a 3D illustration of a brown cardboard box with a green arrow pointing to the right, a laptop, and a document with a green checkmark. The main content area on the right is a table with a dark blue background and a light blue header. The header contains the text 'Secure Purchase Order System' and two column titles: 'Current Purchase Orders' and 'Approved / Confirmed?'. The table body is currently empty. At the bottom left of the window, the email address 'feedback@jwsecure.com' is displayed.



Secure Purchase Order System

Secure Purchase Order System

Signing you in...

Make a new purchase order

Current Purchase Orders

Approved / Confirmed?

Error Initializing Workflow

Error creating workflow

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

at SecurePO.POWorkflow.SignOn()
at SecurePO.Window1.InitWorkflow()

OK

feedback@jwsecure.com



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.