Security in knowledge

Windows 8 Security - The Unsung Hero!

Chris Hallum

Microsoft Corporation

Session ID: SPO1-T18

Session Classification: General Interest

Agenda

- Windows 8 Investment Areas
- Enhancing Security with Modern Hardware
- Malware Resistance
- Protecting Data with Encryption
- Access Control
- Windows Editions, Devices, and Security

Security in the news…

Phone-call security scam targeting PC users

Microsoft is warning customers about a new threat where criminals acting as computer security engineers call people …nce to warn them about a security threat

Microsoft Work Exposes Magnitude of Botnet Threat

Microsoft's Security Intelligence Report sheds light on the expanding threat that bots…

Lost Devices Cost Companies Billions

Last month, an oil giant announced an unencrypted laptop containing sensitive information on 13,000 individuals. The incident may cost

Michigan firm about to determine 200,000 account passwords in under an hour

The most popular passwords among 400,000 exposed by the Gawker hack "123456" and "password" according analysis done by a Michigan security

RSA warns customers after company is hacked

SecurID tokens from EMC's RSA Security division, which are used for two-factor authentication, have been compromised after a sophisticated cyber-attack…

Researchers Discover Link Between a Series of Trojans

A difficult to remove rootkit behind numerous sophisticated attacks, appears to have helped spread yet another Trojan.

The Stealthiest Rootkit in the Wild?

…eds launched the raids against individuals who have allegedly been managing the Rustock botnet," a vast network of computers

Security firm's confidential data is exposed after successful hack

A web application security provider has just revealed that a …

The road to Windows 8

1995

Key Threats

- Internet was just growing
- Mail was on the verge

Windows 95

2001

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

2004

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Exploit buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

2007

Key Threats

- Zotob (2005)
- Summer of Office 0-day)
- Rootkits
- Exploit Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure "by default" configuration (Windows features and IE)

2009

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

2012

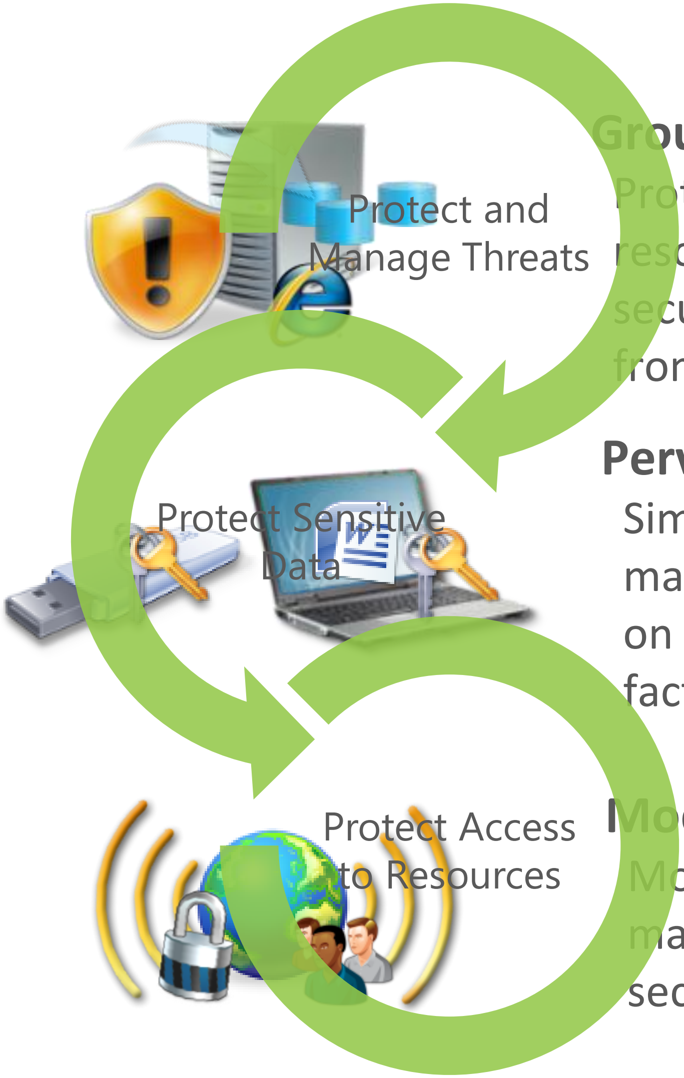
Key Threats

- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)

Windows 8

- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (w/ELAM)
- Measured Boot and Remote Attestation Support
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Picture Password, PIN
- Dynamic Access Control
- Built-in Anti-Virus

Windows 8 investments in client security



Groundbreaking Malware Resistance

Protects the client, data, and corporate resources by making the client inherently secure and less vulnerable from the effects from malware.

Pervasive Device Encryption

Simplifies provisioning and compliance management the of encrypted drives on the widest variety of PC form factors and storage technologies

Modernized Access Control

Modernizes access control and data management while increasing data security within the enterprise.

Malware Resistance

Security in knowledge

Challenges That We Face In Combatting Malware

Vulnerabilities can be minimized but not completely eliminated

Malware can compromise PC before starting Windows

Malware can compromise Anti-Malware software by tampering or starting

Malware can hide from Anti-Malware software

Anti-Virus is always playing catch-up with latest malware

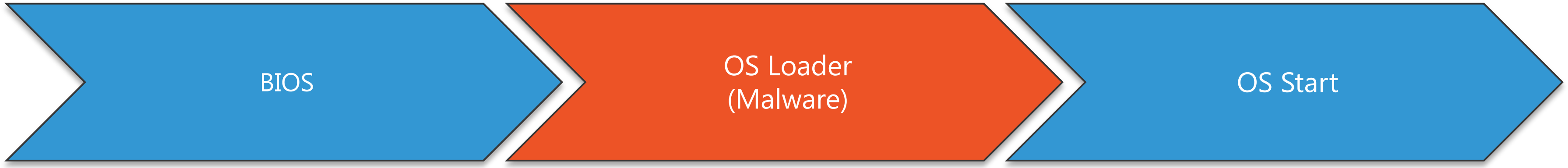
Secure Hardware

Why UEFI?

- What is UEFI?
  - An interface built on top of and replaces some aspects of traditional BIOS
  - Like BIOS it hands control of the pre-boot environment to an OS
- Key Benefits
  - architecture-independent
  - enables device initialization and operation (mouse, pre-os apps, menus)
- Key Security Benefits:
  - Secure Boot - Open capability supported by Windows 8, Linux, …
  - Encrypted Drive support for BitLocker
  - Network unlock support for BitLocker
- A Windows Certification Requirement (UEFI 2.3.1)

UEFI Secure Boot: Legacy vs. Modern

Legacy Boot



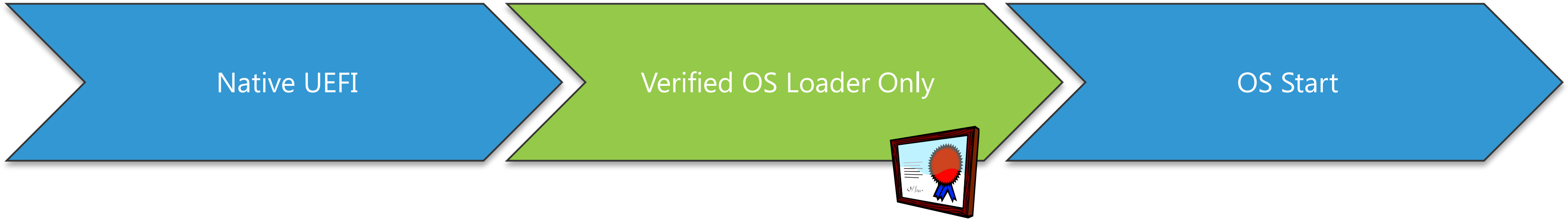
BIOS

OS Loader
(Malware)

OS Start

- BIOS Starts any OS Loader, even malware
- Malware may starts before Windows

Modern Boot



Native UEFI

Verified OS Loader Only

OS Start

- The firmware enforces policy, only starts signed OS loaders
- OS loader enforces signature verification of Windows components. If fails Trusted Boot triggers remediation.
- Result - Malware unable to change boot and OS components

- UEFI is Secure by Design
  - UEFI Firmware, Drivers, Applications, and Loaders must be trusted (i.e.: signed)
  - UEFI Database lists trusted and untrusted Keys, CA's, and Image Hashes
  - Secured RollBack feature prevents rollback to insecure version
  - Untrusted (unsigned) Option ROMs (containing firmware) can not run
- Maintaining UEFI with Windows Update
  - Updates to UEFI Firmware, Drivers, Applications, and Loaders
  - Revocation process for signatures and image hashes
- UEFI Remediation
  - UEFI able to execute UEFI firmware integrity check and self-remediate
  - UEFI able recover Windows boot manager if integrity checks fail

- TPM Value Proposition
  - Enables commercial-grade security via physical and virtual key isolation from OS
  - TPM 1.2 spec: mature standard, years of deployment and hardening
  - Improvements in TPM provisioning lowers deployment barriers
- TCG Standard evolution: TPM 2.0*
  - Algorithm extensibility allows for implementation and deployment in additional countries
  - Security scenarios are compatible with TPM 1.2 or 2.0
- Windows 8: TPM 2.0 support enables implementation choice
  - Discrete TPM
  - Firmware-based (ARM TrustZone® ; Intel's Platform Trust Technology (PTT))
  - Windows Logo Requirement for AOAC Only

* Microsoft refers to the TCG TPM.Next as "TPM 2.0".

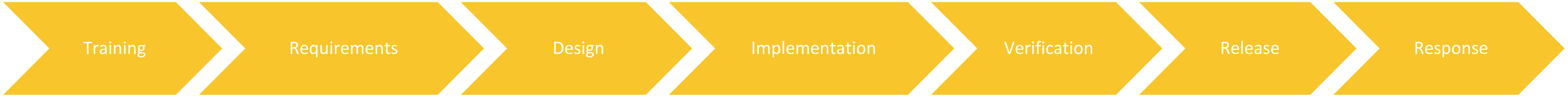
Hardware Requirement and Feature Usage

#	Feature	TPM 1.2/2.0	UEFI 2.3.1
1	BitLocker: Volume Encryption	X	
2	BitLocker: Volume Network Unlock	X	X
3	Trusted Boot: Secure Boot		X
4	Trusted Boot: ELAM		X
5	Measured Boot	X	
6	Virtual Smart Cards	X	
7	Certificate Storage (Hardware Bound)	X	
8	Address Space Layout Randomization (ASLR)	X	
9	Visual Studio Compiler	X	
10	More…		

Securing the Code and Core

Securing the Code and Core

- Preventing vulnerabilities before they're written
  - Security Development Lifecycle (SDL)
  - Tools - Threat Models, Code Analyzers, Fuzzers, Visual Studio, …
  - Impact - MSFT products not in Top 10 vulnerabilities list – Kaspersky (Q3 2012 Report)



- Reduce the ability to exploit vulnerabilities
  - Many exploit mitigation features vastly improved - ASLR, DEP, Windows Heap
  - Chris Valasek from a senior security researcher at Coverity said:

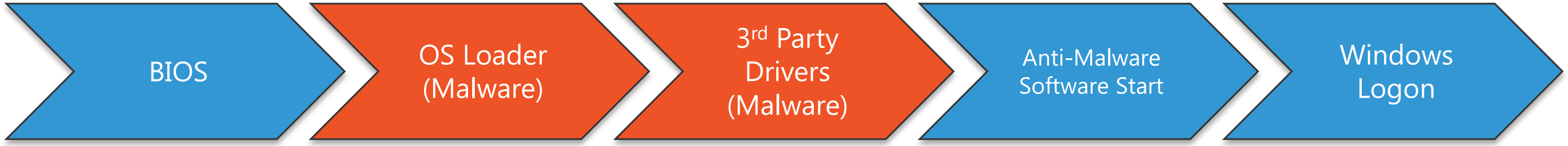
    "the security advancements from Windows XP to Windows 7 are leaps and bounds.. the advancements from version 7 to 8 are just as great."
    "I wouldn't want to be tasked with creating a heap exploit for Windows 8."

Securing the Boot

- Trusted Boot
  - End to end boot process protection:
    - Windows operating system loader
    - Windows system files and drivers
    - Anti-malware software
  - Ensures and prevents:
    - a compromised operating system from starting
    - software from starting before Windows
    - 3rd party software from starting before Anti-malware
  - Automatic remediation/self healing if compromised
- Measured Boot
  - Creates comprehensive set of measurements based on Trusted Boot execution
  - Can offer measurements to a Remote Attestation Service for analysis

Trusted Boot

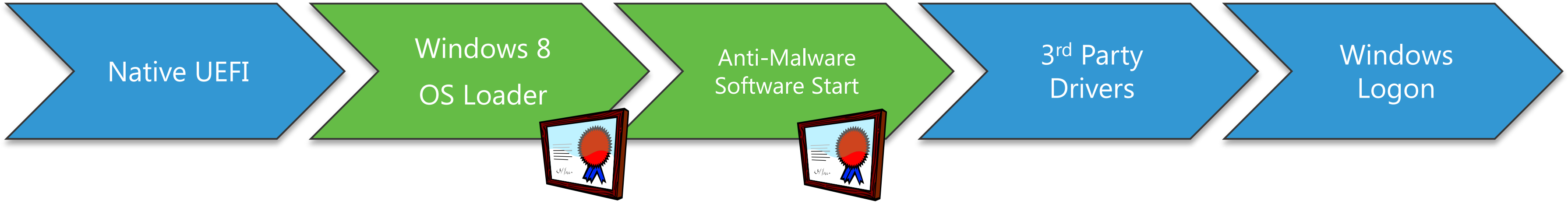
Windows 7



BIOS → OS Loader (Malware) → 3rd Party Drivers (Malware) → Anti-Malware Software Start → Windows Logon

- Malware is able to boot before Windows and Anti-malware
  - Malware able to hide and remain undetected
  - Systems can be compromised before AM starts

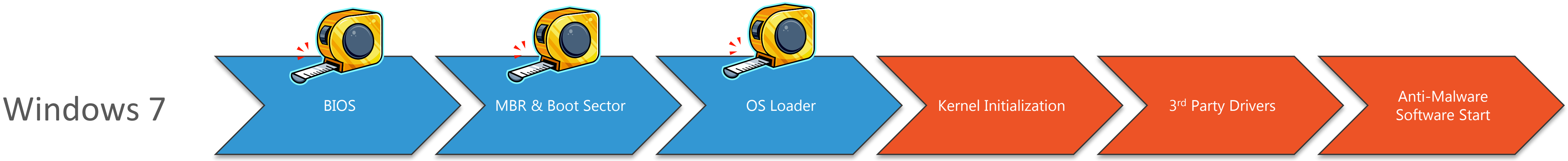
Windows 8



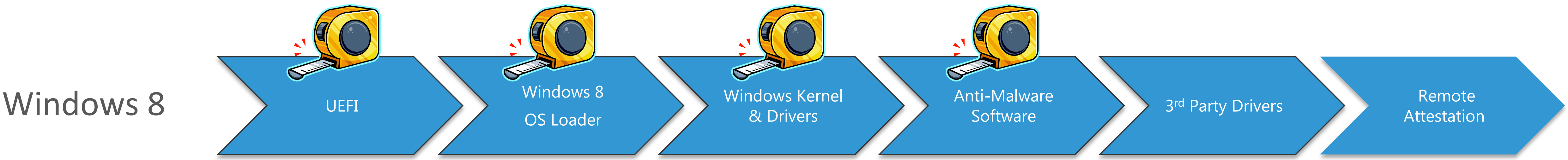
Native UEFI → Windows 8 OS Loader → Anti-Malware Software Start → 3rd Party Drivers → Windows Logon

- Trusted Boot loads Anti-Malware early in the boot process
  - Early Load Anti-Malware (ELAM) driver is specially signed by Microsoft
  - Windows starts AM software before any 3rd party boot drivers
  - Malware can no longer bypass AM inspection

Measured Boot

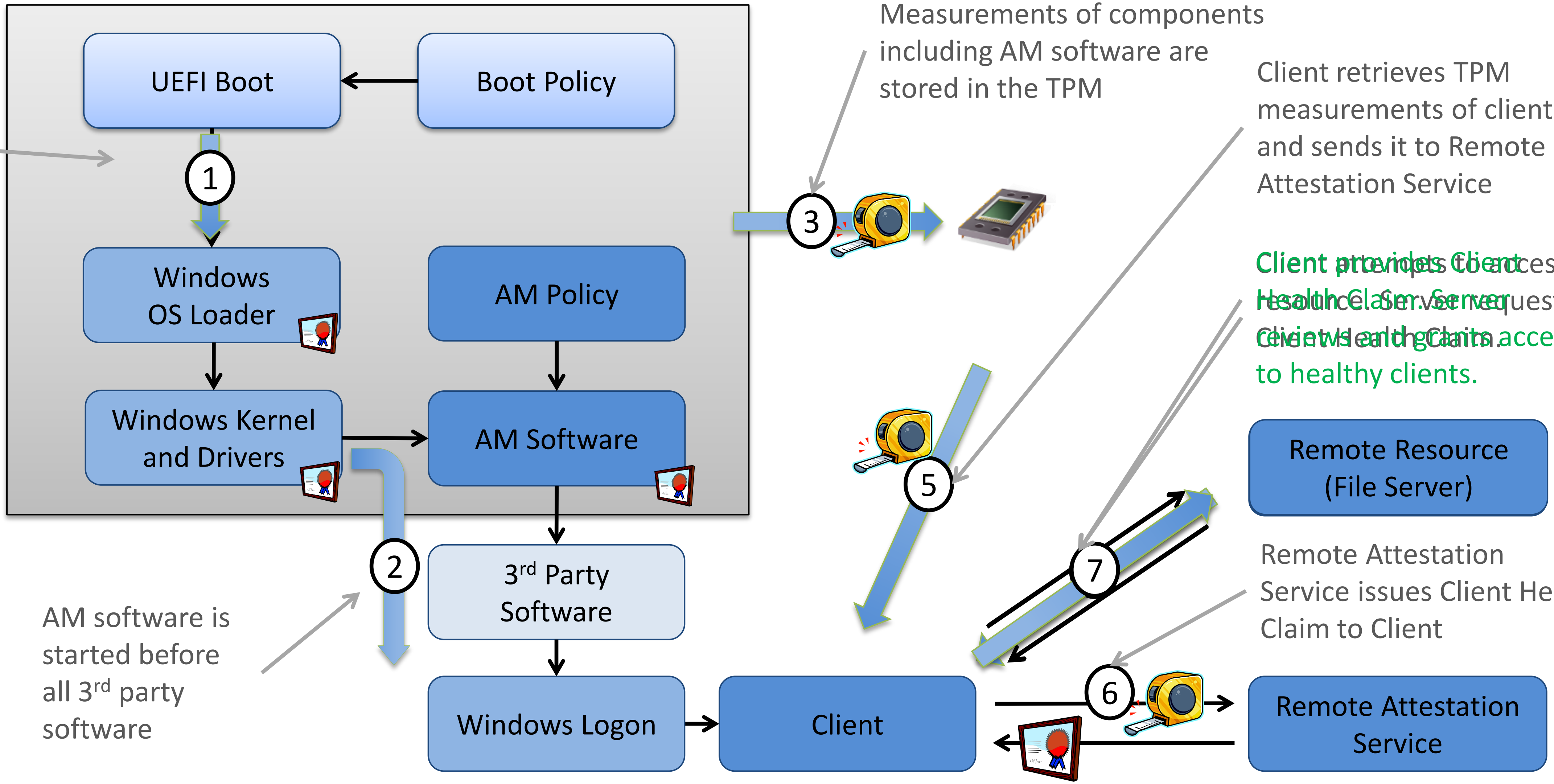


- Measurements of some boot components evaluated as part of boot
- Only enabled when BitLocker has been provisioned



- Measures all boot components
- Measurements are protected by the Trusted Platform Module (TPM)
- Remote attestation, if available, can evaluate client state
- Enabled when TPM is present. BitLocker not required

Boot Malware Resistance: Putting it all together



Secure Boot prevents malicious OS loader

AM software is started before all 3rd party software

Measurements of components including AM software are stored in the TPM

Client retrieves TPM measurements of client and sends it to Remote Attestation Service

Client attempts to access resource. Server requests Client Health Claim.

Client provides Client Health Claim. Server grants access to healthy clients.

Remote Attestation Service issues Client Health Claim to Client

Application Control

- Situation Today
  - Users can install and run non-standard applications
  - Even standard users can install some types of software
  - Unauthorized applications may:
    - Introduce malware
    - Increase helpdesk calls
    - Reduce user productivity
    - Undermine compliance efforts
- Solution: AppLocker
  - Eliminate unwanted/unknown applications in your network
  - Enforce application standardization within your organization
  - Easily create and manage flexible rules using Group Policy
  - Expression based Rules able to operate digital signatures, hashes, folder, and files
  - Updated in Windows 8 to manage Windows Store Apps

Securing After the Boot

Securing the System Post Boot

- Protecting the system and data with an anti-malware solution
  - Windows Defender, is a comprehensive Anti-Malware Solution, and.. there has been some Recent Criticism and a Response
  - System Center Endpoint Protection (SCEP) provides a manageable Microsoft solution
- Reducing the surface area of attacks with Windows Firewall
  - Provides firewalling and packet filtering functions
  - Improved to support new technologies
  - Manageable with System Center Endpoint Protection (SCEP)

Securing the System Post Boot – Applications

- Trustworthy apps from the Windows Store
  - ISV onboarding and app screening process
  - Community based ratings and reviews

- Powerful apps that are inherently more secure
  - Sandboxed apps (AppContainer); Secures system, apps, and data from malicious apps
  - Apps run with low privilege. Limited system access
  - Controlled access to other apps. Contracts and extensions provide controlled interop
  - Access to user data with user approval only

Securing the System Post Boot - Browsing

- Internet Explorer 9 – Smart Screen
  - Helps detect phishing sites and malicious downloads
  - Has blocked >1.5B malware and >150M phishing attacks
- Internet Explorer 10 – Smart Screen
  - Application Reputation has been moved into core
  - Protects users of regardless of browser, mail, IM, etc client
- Internet Explorer 10 – Enhanced Protected Mode
  - Difficult to exploit due to ASLR
  - Tabs and Process Isolation
  - Requires user interaction to gain access to user data
  - Do Not Track (DNT) capability

Protecting Sensitive Information

BitLocker and BitLocker to Go

- BitLocker
  - Prevents unauthorized access to data on lost or stolen PCs
  - Supports full volume encryption of OS and Data volumes
  - Offers variety of pre-boot authentication options:
  - TPM-only, PIN/Password, Network Unlock, USB storage
  - Supports PCs, Servers, and “Slate” form factors

- BitLocker to Go
  - Used to protect data on removable drives
  - Able to deny or grant write access to volumes by organization
  - Enables read-only access on Windows Vista & Windows XP

Windows 8 – Provisioning Enhancements

- Provisioning is the top pain point for encrypting devices:
  - Provisioning is challenging regardless of vendor
  - TPM provisioning is complex for IT and end users
  - Encryption take too much time
- Solutions in Windows 8 make BitLocker the best choice:
  - Auto Provisioning solves most TPM related provisioning issues
  - Instant on BitLocker protection with Encrypted Hard Drive
  - Fast encryption on traditional storage devices with Used Disk Space Only Encryption
  - Encrypt new devices in parallel with imaging rather than after

Windows 8 - Improved Experience & Security

- Improving the IT and End-user Experience on Windows 8
  - Eliminating the need for Pre-Boot Authentication (Connected Standby devices)
  - Fewer support issues on Windows 8 Certified devices
  - Device Encryption automatically provisioned from factory on Windows RT devices
  - Users no longer involved in the complexity of TPM provisioning process

- Improved Security with Windows BitLocker
  - Improved anti-hammering for Windows sign-in on BitLocker protected devices
  - Automatic resume of BitLocker protection when device is left in suspended mode
  - Use EAS to enforce BitLocker protection in non-domain joined and BYOD

- Support for Server and Server Class Storage Scenarios
  - Storage Area Networks (SAN) Support
  - Windows Server Cluster Support

- Multi-factor authentication works in unattended scenarios
  - Network protector leverages WDS for 2nd factor
  - Enables 2nd factor authentication in Server scenarios
  - Simplifies patching process on unattended devices

- Device Encryption – Windows RT
  - Encryption of internal fixed disk is automatic and configured out of the box
  - Protects device using TPM and 128bit encryption
  - Protection is enabled once an administrator uses a Microsoft Account to sign-in
  - Recovery Key is stored in the SkyDrive

- BitLocker and BitLocker To Go – Windows Pro, and Enterprise
  - Enables encryption of fixed disk (BitLocker) and removable disks (BitLocker to Go)
  - Protects disks using 128bit or 256 bit encryption and variety of protector options such as TPM, PIN, Password, Network Unlock, Startup Key
  - Protection is enabled through imaging, mgmt solutions (e.g.: MBAM), or end user
  - Recovery Keys can be stored in AD or mgmt solutions (e.g.: MBAM)

What is Microsoft BitLocker Administration and Monitoring?

Simplify provisioning and deployment

Provide reporting (e.g.: compliance & audit)

Reduce costs (e.g.: Simplified Recovery

"We can use MBAM v1.0 to get greater value from BitLocker. We can ensure that BitLocker is enabled and that we are compliant with corporate encryption mandates without taxing our employees or IT staff."

Bob Johnson Director of IT, BT U.S. and Canada

Improving compliance and security

Integrating with existing systems (e.g.: SCCM)

Reducing costs (e.g.: Self Service, Decreased Risk)

Modernized Access Control

New Sign-In Options / Varying Security

- Passwords, PIN, and Picture Password
  - PIN and Picture Password Both are easy to use sign in option for Touch devices
  - Picture password offers a secure (blog) personal sign-in experience, easy to remember

Length	PIN	Password (a-z)	Password (complex)	Picture Password
1	10	26	n/a	2,554
2	100	676	n/a	1,581,773
3	1,000	17,576	81,120	1,155,509,083
4	10,000	456,976	4,218,240	
5	100,000	11,881,376	182,790,400	
6	1,000,000	308,915,776	7,128,825,600	
7	10,000,000	8,031,810,176	259,489,251,840	
8	100,000,000	208,827,064,576	8,995,627,397,120	

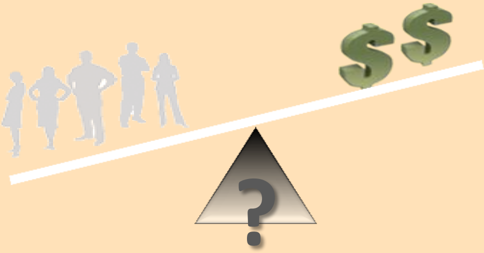
- Mitigating Attacks
  - Account Lockout Policy - "Account lockout threshold" + "Account lockout duration"
  - Security Option Policy - "Interactive logon: Machine account lockout threshold"

But how secure are these options?

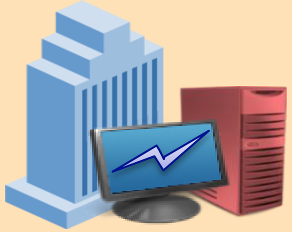
- Passwords and 1FA becoming increasingly inadequate
  - Wired - Kill the Password: Why a String of Characters Can't Protect Us Anymore – Mat Honan
  - Email addresses becoming universal usernames
  - Basic personal info is enough to trick customer service agents into revealing more sensitive information
  - Malicious users use information on one service to gain entry into another
  - Hacked email accounts enables malicious users to reset your pw on other sites (e.g.: Your investment acct)
- Need to move to Multi-Factor Authentication
  - Virtual Smartcards (VSC's) address some of the key challenges with existing MFA solutions
  - Easy to deploy and cost effective way to enable strong multi-factor auth
  - Provides a secure, seamless, and always ready experience for end users
  - Deployment at scale requires a management solution (e.g.: Intercede's MyID)

Data Management Challenges

Growth of users and data

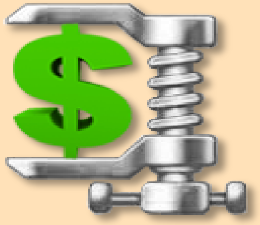


Distributed computing



Regulatory and Business Compliance

Budget Constraints



Different views of Information Governance

CSO/CIO department

"I need to have the right compliance controls to keep me out of jail"

Infrastructure Support

"I don't know what data is in my repositories and how to control it"

Content Owner

"Is my important data appropriately protected and compliant with regulations – how do I audit this"

IW

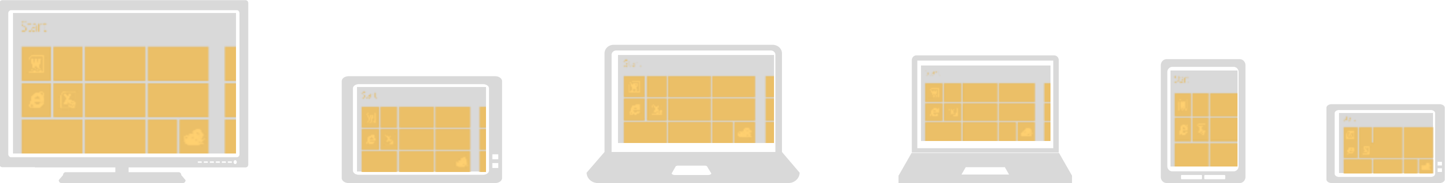
"I don't know if I am complying with my organization's polices"

Identify data	Control access	Audit access	Protect data
Manual tagging by content owners	Expression based access conditions with support for user claims, device claims and file tags	Central audit policies that can be applied across multiple file servers	Automatic RMS protection for Office documents based on file tags
Automatic classification (tagging)	Central access policies targeted based on file tags	Expression based auditing conditions with support for user claims, device claims and file tags	Near real time protection soon after the file is tagged
Application based tagging	Access denied remediation	Policy staging audits to simulate policy changes in a real environment	Extensibility for non Office RMS protectors

Editions, Devices, and Security

Security in knowledge

Windows Editions, Devices, and Security



- Windows 8 editions including Windows RT:
  - Share the same core security features (e.g.: Mitigations, Trusted and Measured Boot, VSC, etc)
  - Professional edition now includes BitLocker and BitLocker to Go
  - Enterprise edition include additional security capabilities (AppLocker, Direct Access)
- Windows RT Security related Differences
  - Windows RT, like all Connected Standby devices, includes UEFI and TPM
  - Makes use of Device Encryption powered by BitLocker technology; Encrypted OOB
  - Application platform locked down to just run Windows Store Apps, Windows OS Desktop applications, Office
  - Managed by EAS and Intune rather than through Group Policy
- Windows to Go Security related Differences
  - None, Windows to Go shares same security features as Enterprise; No compromises
  - TPM is not applicable in Windows to Go scenarios due to roaming

Breakthrough Security with Windows 8

Ground Breaking Malware Resistance

- Fundamentally resistant and resilient against attacks
- Always protected with an in-box anti-malware solution
- Protects users and data from internet based threats

Pervasive Device Encryption

- Encryption is pervasive on all devices
- Fast provisioning of encrypted devices
- Simplified user experience with single sign-in options

Modernized Access Control

- Secure always connected and always managed from anywhere
- Easy to use and deploy strong multi-factor authentication
- Access control automatically adapts to a changing environment
- Ensures connections and access are only granted to healthy and secure devices

Windows

Microsoft

Appendix

Security in knowledge