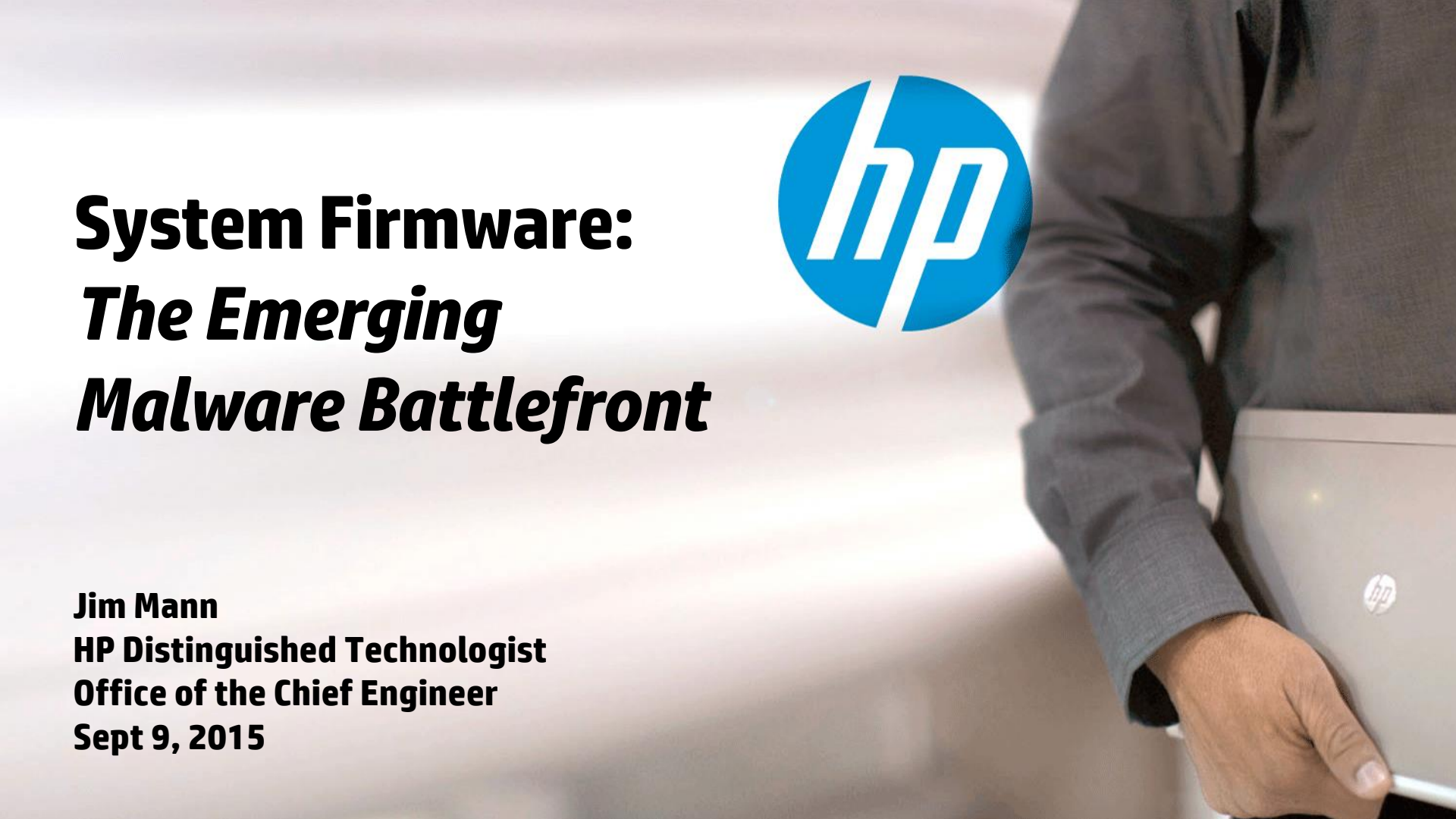


System Firmware: *The Emerging Malware Battlefront*

Jim Mann
HP Distinguished Technologist
Office of the Chief Engineer
Sept 9, 2015

Top 5 ways to know if you're in the right presentation

5

You think

Secure Boot

is a really safe piece of cowboy footwear

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Top 5 ways to know if you're in the right presentation

4

You think

Root of Trust

is something that will help a spelling bee contestant spell 'trust'

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Top 5 ways to know if you're in the right presentation

3

You think

Permanent Denial of Service

means never getting in to that greasy-spoon diner down the street

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Top 5 ways to know if you're in the right presentation

2

You think

Boot Block

is that thing that helps a cowboy remove his boots

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Top 5 ways to know if you're in the right presentation

1

You think

Firmware

is really

tight-fitting jeans

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

A Degrading Threat Landscape

The many forms of cybercrime

Professional

Hacktivism

State-sponsored

Terrorism

Cyber-physical

Today's IT platforms were designed for a friendlier Internet of the 90s

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Situation & Motivations

Going Higher & Burrowing Deeper

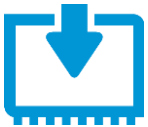
Bulk Data Collection

Cloud

Apps

Operating System

Stealth
Persistence
Disruption



System Firmware

Supply Chain

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

What is System Firmware?

Most modern computer devices contain firmware and critical data

- Embedded software
- Executed on either a microcontroller on the device or the host processor (e.g. Expansion ROMs)
- Executes before the operating system
- Provides initialization of the device
- Typically mutable (on flash memory => “semi-permanent”)
- Typically contains “critical data” (e.g. configuration information)

PC or Server BIOS/UEFI is “special” firmware (aka host processor boot firmware)

- BIOS = Basic Input/Output System (legacy)
- UEFI = Unified Extensible Firmware Interface (modern)
- Not associated with just one device or component
- First instruction executed by host processor…*but rarely the first instruction executed on the system!*

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Why is System Firmware a target for attack?

Ideal place to put malicious code

Control	Executes prior to the Operating System
Permanence	Code is in a chip on the system board or other embedded device
Detection	Very difficult; can't be done from the operating system
Recovery	Likely requires a service event that involves hardware rework/replacement

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Impacts of Firmware Attacks

Control of Device

Data Collection

Data Modification

Remote Monitoring

(Permanent) Denial of Service

Service Events

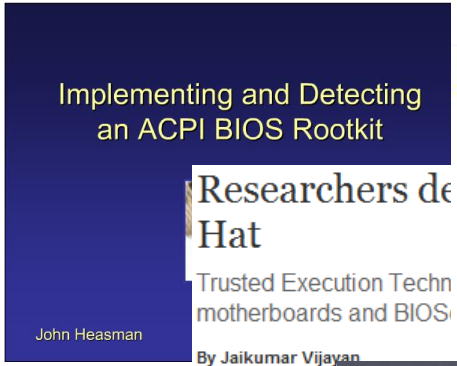
Brand Damage

Business Disruption

Are these attacks just theoretical?

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

A Little History



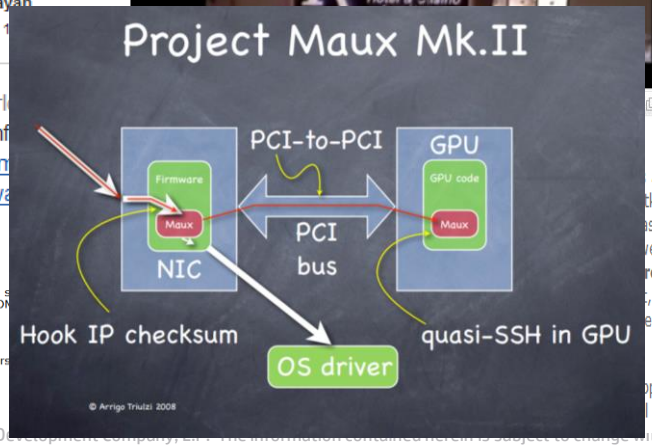
Editorial Reviews

Product Description

Explaining security vulnerabilities, possible exploitation s
used to gather information from BIOS and expansion RON
BIOS are also covered.

About the Author

Darmawan Salihun has published papers on BIOS revers
CodeBreakers Journal.



rootkit in

a Chinese security company called **Qihoo 360** blogged
tkit hitting Chinese computers. This turned to be a very
s it appears to be the first real malware targeting
ell-known proof of concept called **IceLord** in 2007. The
romi and contains a bit of everything: a BIOS rootkit
, a kernel mode rootkit, a PE file infector and a Trojan
ed to infect 64-bit operating system and it is not able to

pper that contains five crypted resource files: *hook.rom*,
l of these files will be presented later in this analysis.

application and OS patches you want, your machine still can be
compromised at the lowest level--without the use of any vulnerability.

RAM:
d

ecurity researchers from Core
on methods for infecting the
ing attempts. Anibal Sacco and
e BIOS with a small bit of code
part is, the method worked on a
ng VMware Player.

id Ortega. "We're not using a
act of this. We can reinfect the

lain,
rumelard

s, you need either root privileges
scope. But the methods are
ootkit to implement the attack.

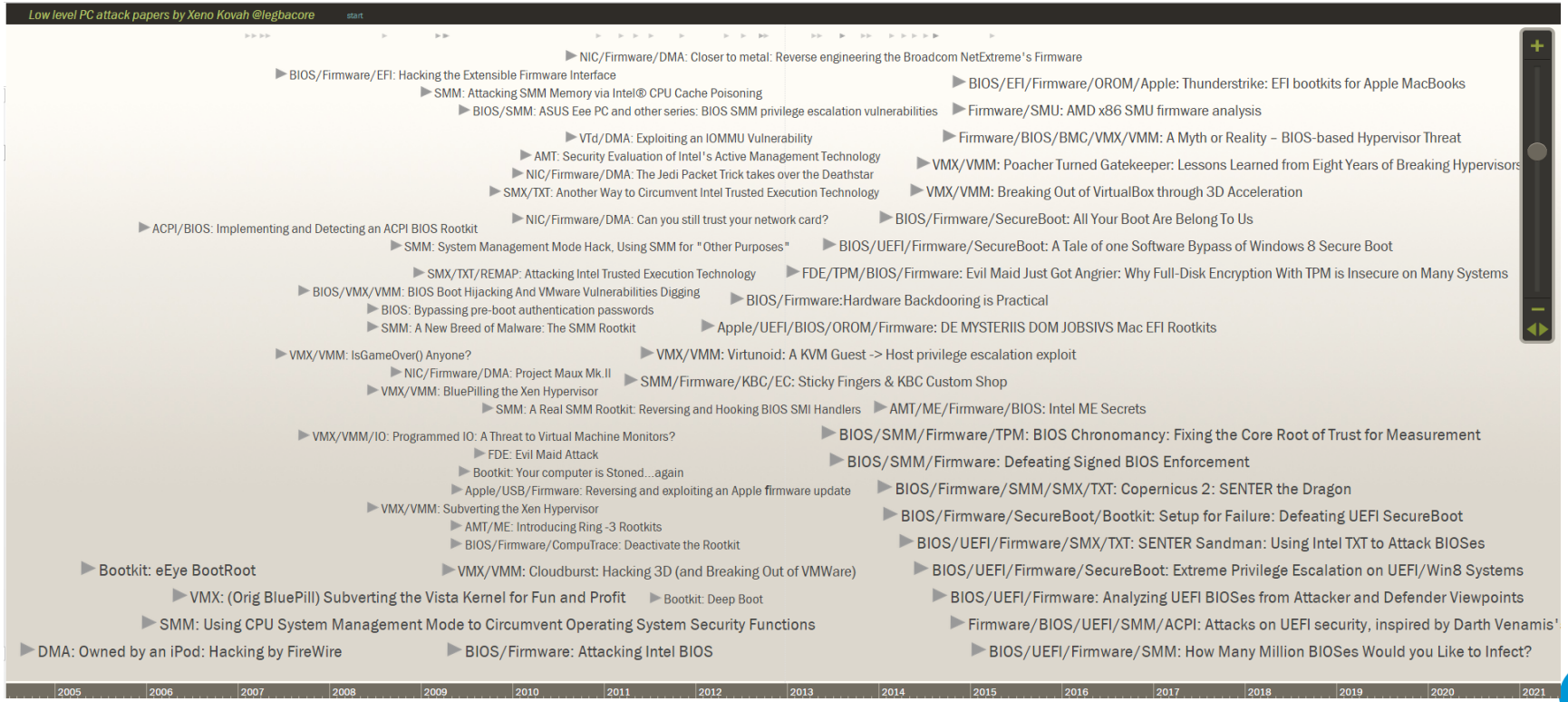
have a little code that can

rity
aubourg 75007 Paris

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Timeline of PC Firmware Attacks

Credit: Xeno Kovah (http://timeglider.com/timeline/5ca2daa6078caaf4)



© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Recent Real World Impacts

Targeted Attacks at Scale

Saudi Aramco (2012)

- 30,000 PCs and 1,000 servers
- Master Boot Record (MBR), the partition tables, files corrupted
- Weeks to get systems back up and running

South Korea ATM network attack… (2013)

- Remote access and MBRs wiped

Sony Pictures (2014)

- Data stolen, then hard drives wiped

Sands Casino (2014)

- Hard drives wiped on PCs and servers

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

The Industry Path for PC BIOS/UEFI Security

A relative timeline

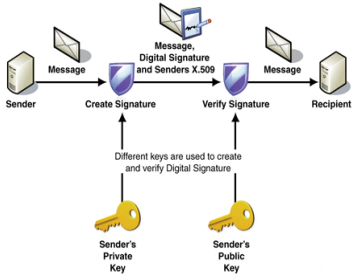
Memory Tech	ROM	Flash			
Code	**BIOS (Basic Input/Output System)**		**UEFI (Universal Extensible Firmware Interface)**		
	OEM Proprietary	IBV's	Proprietary + closed shared	Proprietary + open	
Protections	Inherent	Jumper	Flash Regions	Chipset	NIST SP 800-174(B) ISO/IEC 19678:2015
Implications	Time To Market Flexibility Cost	Mutable code Physical presence User inconvenience	Modular code Vendor unique protection Inconsistent protection	More visible code More common code Black box protections to OEMs	

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

NIST SP 800-147 (& 800-147B)

BIOS Protection Guidelines

Authenticity



Only **cryptographically signed** code can be used to update system firmware

(BIOS code from factory must be inherently trusted)

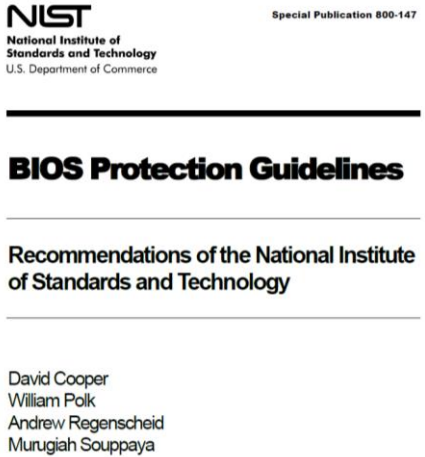
Integrity

The system must **prevent unintended or malicious modification** of BIOS code, preferably with hardware-based mechanisms

Non-bypassability

The **authenticated BIOS update process** shall be the only way to modify BIOS

April, 2011



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-147

BIOS Protection Guidelines

Recommendations of the National Institute of Standards and Technology

David Cooper
William Polk
Andrew Regenscheid
Murugiah Souppaya

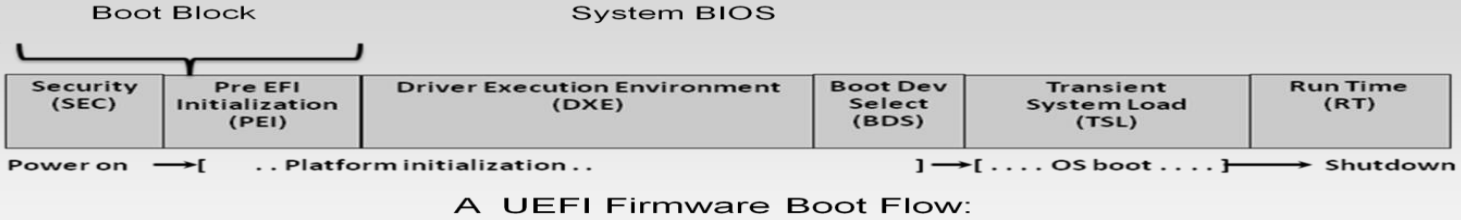
Now also ISO/IEC 19678:2015

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP BIOS Protection History

Pre-2013

Started in 2002 with HP Labs partnership



A UEFI Firmware Boot Flow:

- Separation of Boot Block, *protected by chipset*, enforcing integrity of system BIOS/UEFI
- Boot Block checks rest of system BIOS/UEFI
- Secure BIOS/UEFI Update Process
- First to implement TPM in clients
- First to use TPM to secure: BIOS/UEFI Pre-boot user authentication, DriveLock, Full Disk Encryption
- One of the first to implement NIST SP 800-147 (*BIOS Protection Guidelines*)
- One of the first to provide early support for NIST SP 800-155 (*Golden Measurements*)
- Boot Block => Root of Trust for Update (RTU) – ***assumed to be good!***

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Roots of Trust

Root of Trust

A component that forms the basis of providing one or more security-specific functions, such as measurement, storage, reporting, recovery, verification, update, etc. **A Root of Trust is trusted to always behave in the expected manner because its misbehavior cannot be detected** and because it's proper functioning is essential to providing its security-specific functions.

Examples

Root of Trust for Update (RTU)

Root of Trust for Measurement (RTM)

Root of Trust for Storage (RTS)

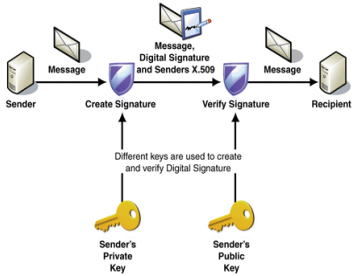
Root of Trust for Reporting (RTR)

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

NIST SP 800-147 (& 800-147B)…and beyond

Protection, Detection, Recovery

Authenticity



Only **cryptographically signed** code can be used to update system firmware

(BIOS code from factory must be inherently trusted)

Integrity

The system must **prevent unintended or malicious modification** of BIOS code, preferably with hardware-based mechanisms

Non-bypassability

The **authenticated BIOS update process** shall be the only way to modify BIOS

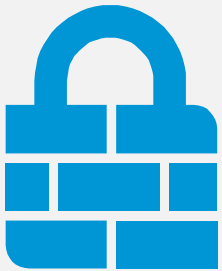
Detection & Recovery

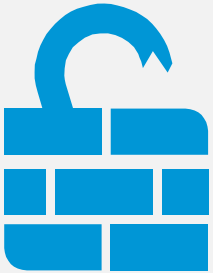
Secure automatic or manual firmware recovery from corruption or wrongful overwrite

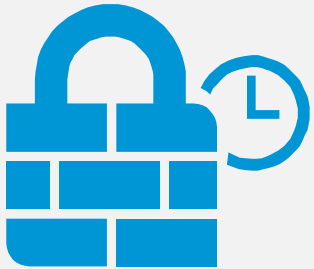
© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Platform Security Philosophy

Protection	Detection	Recovery
Build the highest walls across all levels	Quickly identify threats when they appear	Increase user productivity Lower total cost of ownership





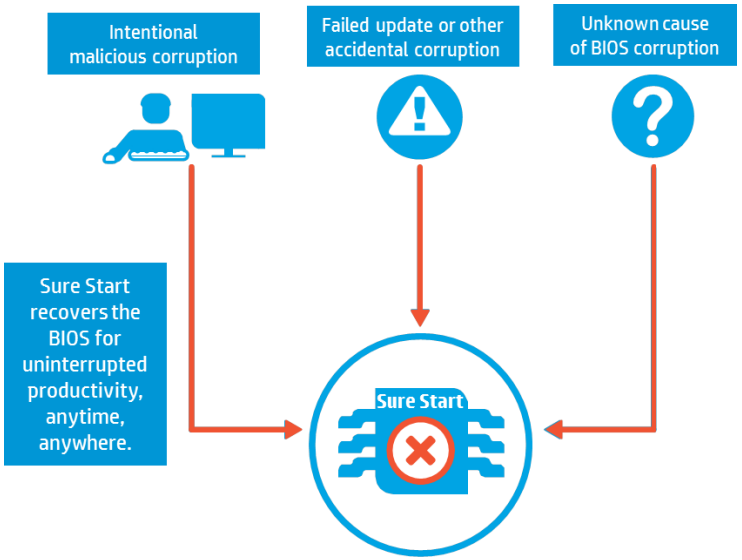


© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Sure Start

Developed with HP Labs

First and only self-healing technology solution created to protect against Malware and Security attacks aimed at the BIOS/UEFI



Features

- Self-healing: Automatic recovery from BIOS malware and security attacks[1,2]
- Firmware protection against Permanent Denial of Service (PDoS) attacks
- Detects, reports and allows auto recovery of Advance Persistent Threats (APTs) aimed at BIOS

Problems it solves

- No user downtime waiting for IT/Service ticket[2]
- Results in fewer help desk calls for crisis recovery or bricked units.
- Secure by default; safeguards machine unique data

Customer benefits

- Virtually uninterrupted Productivity
- Confidence in BIOS/UEFI Rollout
- Reduce TCO; no need to reinstall/replace hardware[3]
- Detection and recovery transparent to customer

1. 100% Automatic recovery of BIOS boot block.
2. If all copies of BIOS are compromised or deleted, a manual step for recovering BIOS is available.
3. Applicable to 2013 Elitebooks and Zbooks.

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained here

Roots of Trust

With HP Sure Start…

Root of Trust

A component that forms the basis of providing one or more security-specific functions, such as measurement, storage, reporting, recovery, verification, update, etc. A RoT is trusted to always behave in the expected manner because its misbehavior cannot be detected and because it's proper functioning is essential to providing its security-specific functions.

Examples

Root of Trust for Update (RTU)

Root of Trust for Measurement (RTM)

Root of Trust for Storage (RTS)

Root of Trust for Reporting (RTR)

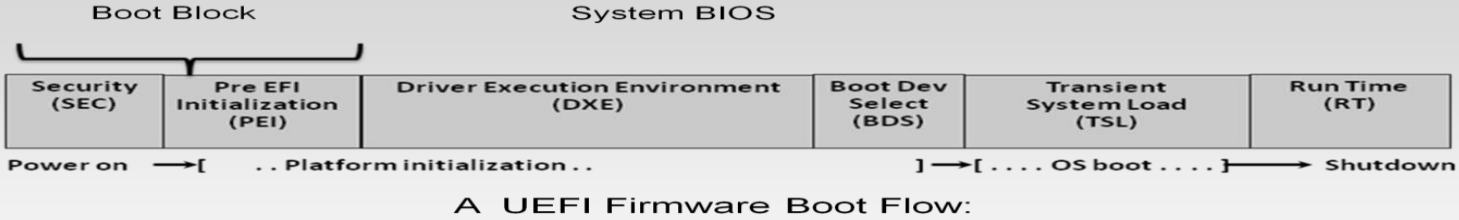
Root of Trust for Detection (RTD)

Root of Trust for Recovery (RTRec)

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP BIOS Protection History

2013 and beyond



A UEFI Firmware Boot Flow:

- **HP Sure Start** checks the Boot Block
- If Boot Block is corrupted, **HP Sure Start** recovers it from a known good image
- Boot Block checks rest of system BIOS/UEFI
- Goes beyond NIST SP 800-147 (*BIOS Protection Guidelines*)
- Boot Block => Root of Trust for Update (RTU) – ***now known to be good!***

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Sure Start and platform personality

HP Sure Start protects critical data that are intended to be immutable upon leaving HP factory / authorized service center

- Product Name
- Model
- SKU Number
- Serial Number
- System Board CT
- System Configuration ID (aka Feature Byte)
  - Estar, Touch Capable. TPM, TCM, SLP, Computrace, SoftSylus
- Warranty Start Date
- UUID
- Vt-x, Vt-d, etc default settings

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

HP Client Security

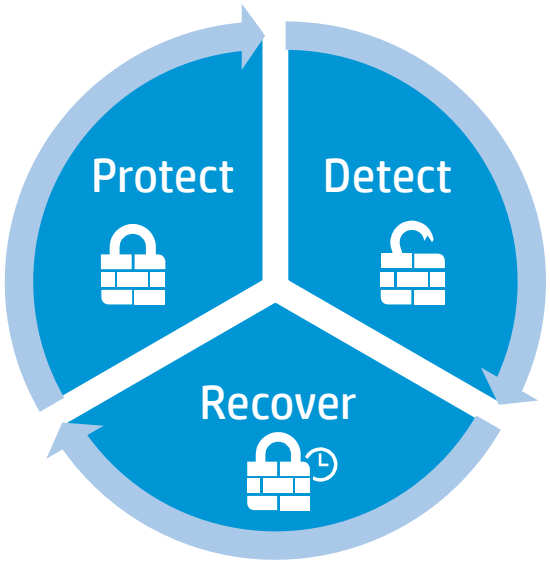
Protect

BIOS/UEFI Based
- **HP Sure Start**
- HP BIOSphere Protection
- Pre-boot Security
- Power-on Authentication

Software Based
- HP Drive Encryption
- HP Credential Manager

Hardware Based
- Physical device security
- TPM
- Self-encrypting drives
- Secure Erase

HP Touchpoint Manager
- Mobile device security policy
- Local password reset



Detect

BIOS/UEFI Based
- **HP Sure Start**
- Master Boot Record Security
- Secure Boot

Software Based
- Microsoft Security Essentials (Win 7)
- Microsoft Defender (Win8)

Hardware Based
- Smart Card Readers
- Fingerprint Reader

HP Touchpoint Manager
- Firewall policy violations
- Anti-virus policy violations

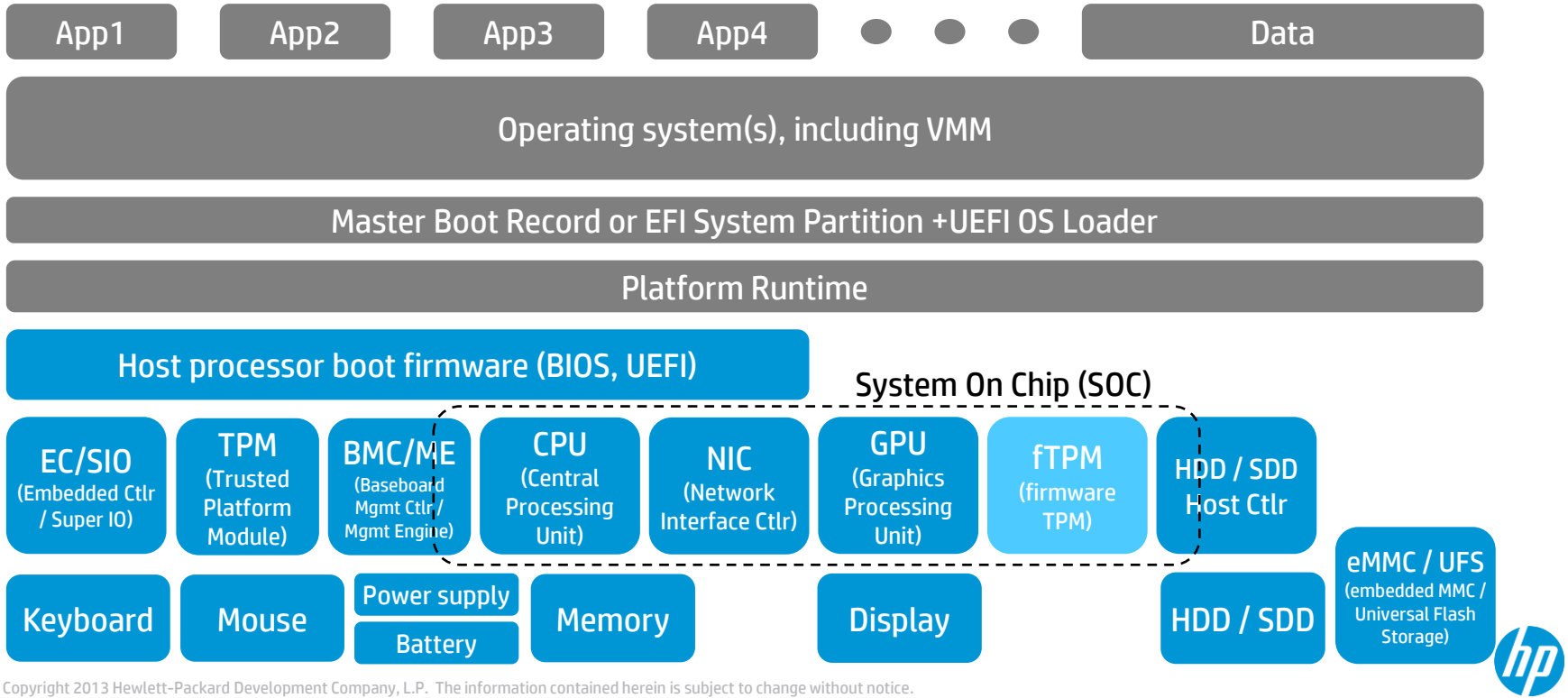
Recover

BIOS/UEFI Based
- **HP Sure Start**
- Always On Remote Management
- Master Boot Record Security

HP Touchpoint Manager
- Firewall enablement
- Anti-virus enablement
- Remote find, lock and wipe
- Boot error code reporting

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

(Over-)simplified PC/Server Functional Diagram

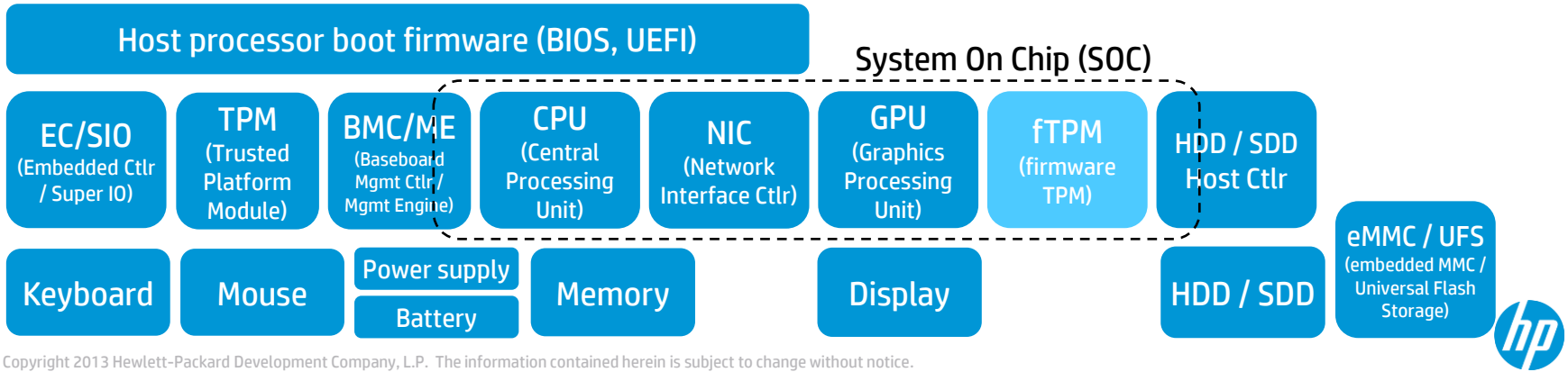


© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

(Over-)simplified PC/Server Functional Diagram

Firmware everywhere

Most modern computer devices contain mutable firmware and critical data
Focus has been almost solely on host processor boot firmware
Focus has been almost solely on protection
All firmware needs protection mechanisms
Unfortunately, protection mechanisms are not always perfect
Detection and Recovery mechanisms are also required



© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

What now?

Improving system firmware resiliency

Protection

- Ensure integrity of all firmware and critical data
- Ensure only authentic firmware and only valid critical data updates
- Ensure update mechanisms cannot be bypassed

Detection

- Must be able to reliably detect a failure of the protection mechanism
- Ideally done before firmware is executed
- Do not allow corruption of firmware or critical data to corrupt the detection mechanism

Recovery

- Secure mechanism
- State of integrity
- At scale

Founded in roots of trust

- Ideally immutable

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Firmware resiliency considerations

Cost

- Likely additional compute & storage
- Non-Recurring Engineering (NRE)

Performance

- Digital signature verification takes non-zero time

Device Cooperation

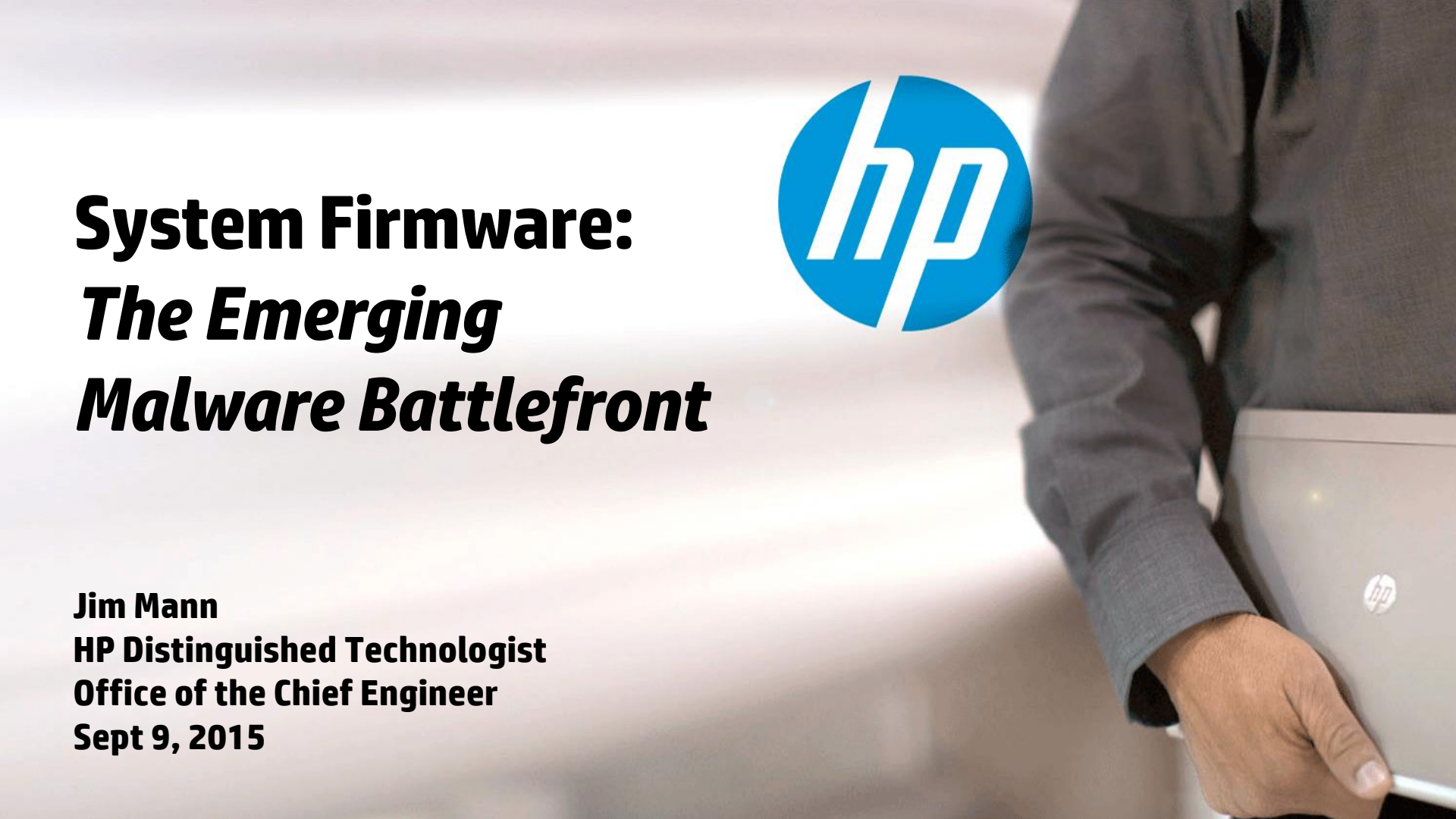
- Some devices may need help from other devices

Supplier Cooperation

- Lots of suppliers involved in any reasonably complex system

System firmware resiliency is critical to system resiliency

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



System Firmware: *The Emerging Malware Battlefront*

Jim Mann
HP Distinguished Technologist
Office of the Chief Engineer
Sept 9, 2015