BIOS Security

Andrew Regenscheid

Computer Security Division

Information Technology Lab

Federal Computer Security Program
Managers' Forum

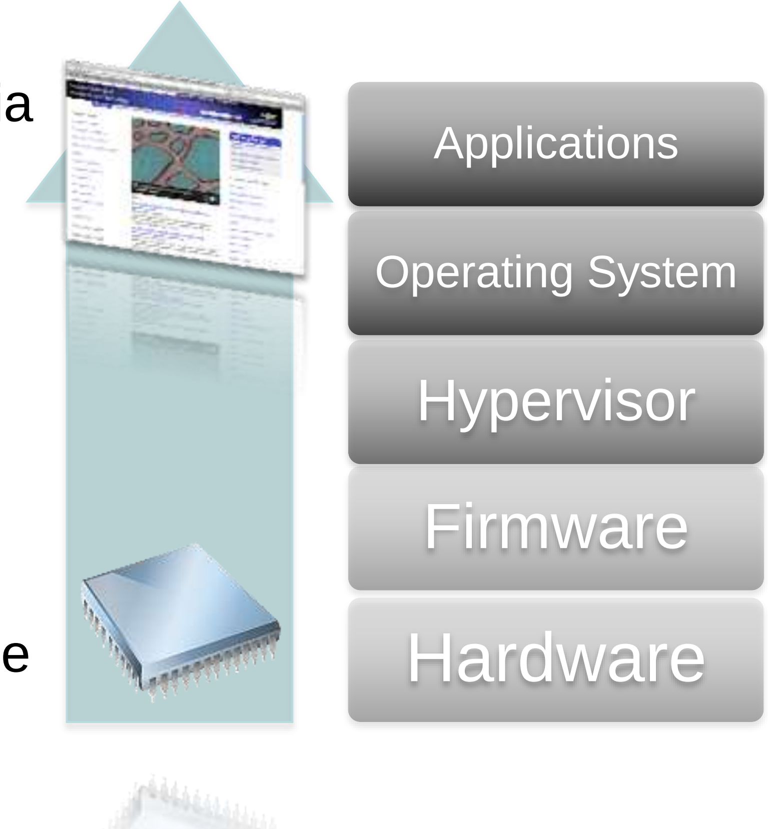
June 2012

Outline

- Motivation
- Overview of System BIOS
- Threats to System BIOS
- BIOS Security Guidelines
  - Overview of *BIOS Protection Guidelines*
  - Overview of *BIOS Integrity Measurement Guidelines*
- Adoption

Motivation

- Major malware outbreaks spread via OS vulnerabilities (e.g., Blaster, Nimda).
- Targets have moved to application layer.
  - In 2009, 49% of web-based attacks targeted PDF vulnerabilities [Sym10].
- Future attacks could move down the stack to firmware.



Applications

Operating System

Hypervisor

Firmware

Hardware

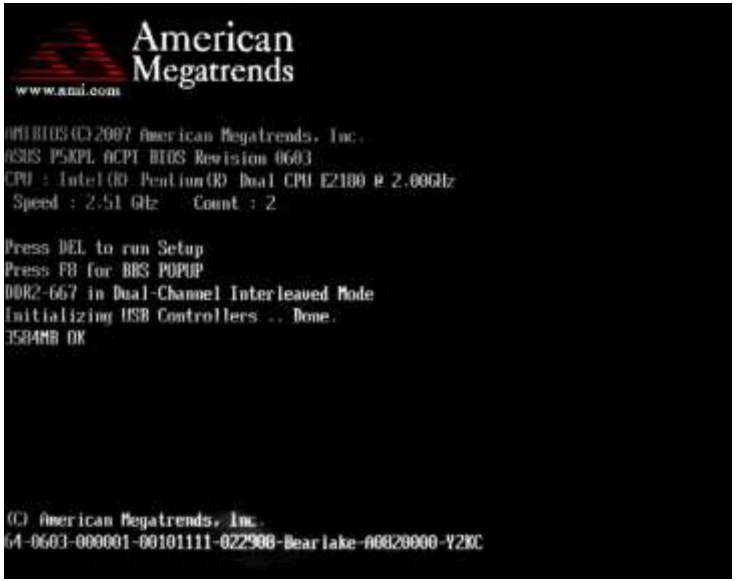
[Sym10] *Symantec Global Internet Security Threat Report- Trends for 2009*. April 2010

Status Quo

- Modern computer architectures frequently lack a firm foundation in hardware/firmware from which to build trust.
- New forms of malware inject themselves below the OS and anti-malware to bypass security mechanisms.

What is BIOS?

- BIOS- *Basic Input/Output System*
- Fundamental system firmware used to boot and initialize system.
- Types of boot firmware:
  - **System BIOS**- Stored on system flash on the motherboard.
  - **Option ROMs**- Stored on add-in cards
- BIOS specifications:
  - Conventional BIOS- legacy systems.
  - Unified Extensible Firmware Interface (UEFI) BIOS- Specification for new BIOS with additional features.

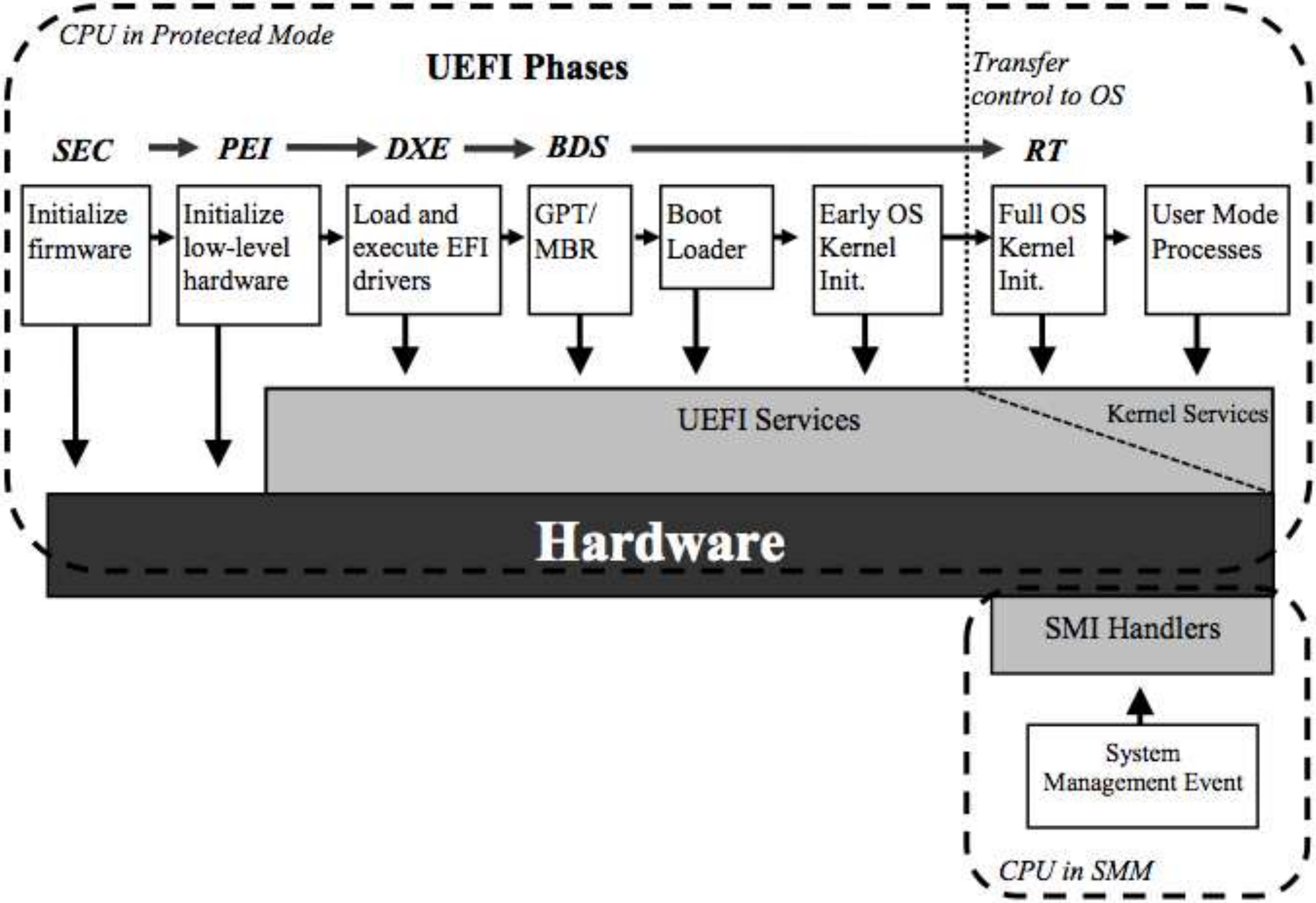


```
AMIBIOS(C)2007 American Megatrends, Inc.
ASUS P5KPL ACPI BIOS Revision 0603
CPU : Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz
 Speed : 2.51 GHz    Count : 2

Press DEL to run Setup
Press F8 for BBS POPUP
DDR2-667 in Dual-Channel Interleaved Mode
Initializing USB Controllers .. Done.
3584MB OK




(C) American Megatrends, Inc.
64-0603-000001-00101111-022908-Bearlake-A0820000-Y2KC
```

Role of System BIOS

- Historically provided the OS access to hardware.
- Primary purpose: Initialize and test hardware components and load the OS.
- Involved with system management:
  - May load CPU microcode patches.
  - Initializes ACPI tables and code for power management.
  - Loads System Management Mode code for low-level management functions.

Boot Process - UEFI



Threat Vectors

- System BIOS code is updatable.
  - No longer need to use boot disks.
  - Most BIOS is updatable from OS.
- Remote attacks are possible on modern systems.
  - Malware exploiting update mechanism to flash malicious BIOS.
  - Compromised enterprise management infrastructure could push malicious BIOS updates.
  - Rollback to a vulnerable BIOS.

Security of BIOS

- BIOS is a critical security component of systems.
- Potentially attractive target.
  - Damaging BIOS could result in denial of service.
  - Malicious BIOS could inject a rootkit.
- BIOS attacks can persist beyond reboots and reformatted/replaced hard drives.
- BIOS code executes with high-privileges on systems.

Timeline of BIOS Research

- 1998 – Chernobyl (CIH) Virus
- 2004 – NiBiTor (NVIDIA BIOS Editor)
- 2006 – ACPI BIOS Rootkit
- 2006 – Persistent BIOS Infection
- 2007 – Hacking the Extensible Firmware Interface
- 2008 – UEFI Hypervisors
- 2009 – Deactivate the Rootkit (Computrace)
- 2009 – Attacking Intel BIOS
- 2011 – Mebromi

Attacks on BIOS

- Two widely-known attacks:
  - 1998- **Chernobyl** (CIH) - Attempted to overwrite BIOS on systems with a specific chipset.
  - 2011- **Mebromi**- First BIOS-based rootkit.
- Several academic studies:
  - Proof of concept demonstrating insertion of malicious code into BIOS.
  - Vulnerabilities discovered in BIOS signing implementations.
  - Potential for low-level rootkit in SMM code.

Guidelines on BIOS Security

- Two-pronged approach:
  - – ***Protect*** System BIOS from unauthorized changes by implemented a secure BIOS update mechanism (***SP800-147***).
  - – ***Detect*** unauthorized changes to System BIOS and configuration settings using secure measurement and reporting mechanisms (***SP800-155***).

Protecting BIOS

- Covered in **NIST SP800-147, *BIOS Protection Guidelines***.
- Scope: Protecting the system BIOS in laptop and desktop systems.
- Split into 2 parts:
  - *Guidelines on BIOS Implementations:* Intended for computer manufacturers.
  - *Recommended Practices for Managing the BIOS*: Intended for system administrators.

Protection Mechanisms

- Guidelines outlining protective features that can be implemented in the system BIOS.
- Intended for computer manufacturers.
  - Manufacturers may develop their own BIOS.
  - Purchase a customized BIOS from an Independent BIOS Vendor.
- Protection mechanisms intended to lock-down BIOS update process with mechanisms already used by OS and application vendors.

Protection Mechanisms

- Key Mechanisms:
  - ***Authenticated BIOS updates*** using digital signatures.
  - ***Integrity protections*** to system flash to prevent unauthorized modifications to the BIOS.
  - ***Non-bypassability*** to ensure BIOS protections cannot be circumvented.
- Secure Local Updates
  - Unsigned updates are allowed if the operator must be physically present.
  - Intended to facilitate recovery situations.
  - Not expected, or needed, in all products.

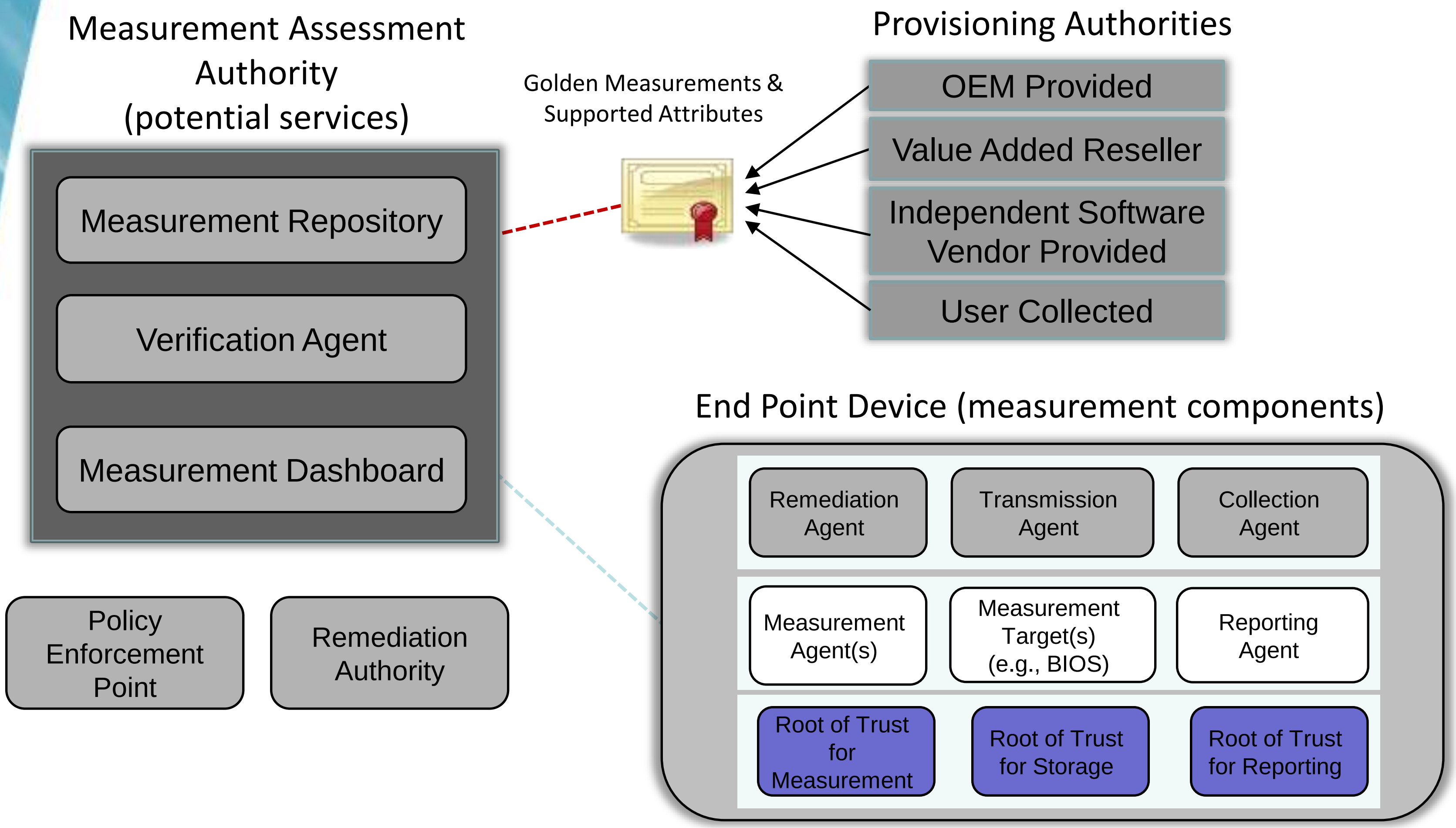
Detecting Changes to BIOS

- Secure BIOS integrity measurement and reporting provides foundation for ***detecting*** unauthorized changes to BIOS.
- BIOS protections may not be sufficient:
  - Vulnerabilities could allow malicious updates.
  - Sensitive configuration data may not be protected.
- **NIST SP 800-155** provides guidelines for OEMs, OS vendors, security software vendors, and IT infrastructure manufacturers.

BIOS Measurement

- Goal is to **detect** unauthorized changes so administrators can **react** and **remediate**.
- Roots of trust are the foundation of BIOS integrity measurement.
  - They securely measure, store, report BIOS components.
  - Measurements are usually in the form of hashes.
- Measurements are sent to the Measurement Assessment Authority (MAA), which verifies measurements.
- The MAA can instruct IT components (e.g., managed switch) to respond accordingly.
  - Devices with valid measurements can be granted access.

Integrity Measurement Architecture



Measurement Assessment Authority (potential services)

Measurement Repository

Verification Agent

Measurement Dashboard

Policy Enforcement Point

Remediation Authority

Golden Measurements & Supported Attributes

Provisioning Authorities

OEM Provided

Value Added Reseller

Independent Software Vendor Provided

User Collected

End Point Device (measurement components)

Remediation Agent

Transmission Agent

Collection Agent

Measurement Agent(s)

Measurement Target(s) (e.g., BIOS)

Reporting Agent

Root of Trust for Measurement

Root of Trust for Storage

Root of Trust for Reporting

Core Components

- **Roots of Trust:** Must be inherently trusted and secure by design to perform their function.
  - **RoT for Measurement**: Trusted to hash code and data.
  - **RoT for Storage**: Trusted to securely store hashes.
  - **RoT for Reporting**: Provides for integrity and non-repudiation of measurement reports.
- **Software Agents:** Critical, but untrusted, pieces of software that interact with the roots of trust.

Attributes and Measurements

- **Attributes:** Defined properties of a system used to assess confidence in a system and its measurements. e.g.,
  - Types of roots of trust used on a device
  - Support for BIOS protections (SP800-147)
- **Measurements:** Cryptographic hashes of code and/or configuration data.
- **Measurement Logs**: Contain actual measurements and descriptions of objects/events included in the measurements.
- **Integrity Measurement Registers**: Contain cryptographic hashes of measurements of like items
  - Reside in protected storage

Measurement Flow

Device Provisioning

- Obtain the initial set of trusted measurements (i.e., golden measurements) from OEM or generate during provisioning.

Measurement

- The device uses the RTM (or a chain of trust for measurement rooted in the RTM) to measure BIOS code and configuration data during boot.
- Measurements are protected using the RTS.

Measurement Flow (cont.)

Reporting

•Depending on the model, the MAA receives measurements from an endpoint device in one of two ways:

- The MAA could request for measurements from a device.
- The device could periodically push measurements to the MAA.

•The collection and reporting agents will generate a signed report (using the RTR).

•The transmission agent will send report to MAA.

MAA Verification

•MAA’s verification agent will verify the signed report, and the measurements within the report.

•Results are stored for administrators, and possibly used to grant/deny device access to network resources.

NIST SP800-155

- NIST SP800-155 provides guidelines on:
  - Security of roots of trust
  - Attributes and measurements
  - Security properties of measurement collection and reporting
  - Remediation strategies
- Points to industry standards and specifications for interoperability.
  - TCG’s Trusted Network Connect specifications
  - SCAP

Use Case: Comply-to-Connect

Scenario: An organization will only allow systems with secure BIOS on its network.

- Organization procures SP800-147 and SP800-155 compliant products.
- During provisioning, administrators store golden measurements of BIOS code and data for each device.
- Upon device connection, a Network Access Control (NAC) server requests BIOS measurements.
- NAC verifies device attributes include BIOS protection.
- If the measurements are also valid, the NAC server instructs the switch/AP to allow the device on the network.

What Should Organizations Do?

- Current Focus: BIOS Protections.
  - New computer purchases should include a BIOS implementing signed and protected updates.
  - Existing systems should be updated as BIOS updates become available.
- BIOS Measurement a longer-term goal.
  - Requires significant changes across organizations.
  - New computer and IT infrastructure purchases should support BIOS measurement.
- Manage BIOS as another critical software layer.
  - Ensure BIOS protections are enabled.
  - SP800-147 includes recommended practices for managing the BIOS.

Availability

- BIOS protections are quickly becoming a standard feature.
  - BIOS protections in new business-class machines from two major OEMs.
  - Many machines <2 years old have updates available.
- But, the feature is not always enabled by default:
  - Verify in BIOS configuration.
  - Some OEMs provide tools to check BIOS configuration settings.
- Ask your OEM about support for SP800-147.

Availability

- BIOS protections should become a standard feature in all PCs in 2013.

Windows 8 Hardware Certification Requirements

"*Further, it is recommended that manufacturers writing BIOS code adhere to the NIST guidelines set out in NIST SP 800-147*"

– section System.Fundamentals.Firmware.UEFISecureBoot .8

Government Adoption

- DHS Memo, March 7, 2012
  - "By October 1, 2012, departments and agencies should include the requirement for BIOS protections compliant with NIST SP800-147 [...] in new procurements of PC client systems."
- DoD CIO Memo, Sept 8, 2011
  - "To ensure the security of DoD information systems, including those designated as national security systems, specifications for PC client systems in solicitations issued after January 1, 2012 shall include a requirement for … SP 800-147."
- DoD Instruction 8500.2 (Draft), IA Implementation
  - "BIOS shall be managed in accordance with … SP 800-147 "

Upcoming Work

- Extend BIOS protections to other firmware and platforms
  - Server BIOS protections
  - Network devices
  - Option ROMs- Boot firmware in add-in cards
- Extend BIOS measurement to servers
- Roots of trust in mobile devices
- Promote adoption
  - BIOS update deployment guide

More Information

NIST BIOS Security publications available at:

csrc.nist.gov

Contact Information

Andrew Regenscheid

andrew.regenscheid@nist.gov