Protecting the Storage Platform through Measurement and Attestation

Jeff Plank and Joe Foster
Abstract

Securing the operational state of components has become an ever increasing topic amongst the industry. Much of the industry has secured the platforms upon which they operate but the subcomponents have become the next bastion of enforcing a security model. In this talk, we will cover the attack vectors and counter measures to head off the vulnerabilities that previously embedded firmware appeared safe. We will discuss recent events, industry initiatives, the notion of trusted firmware, and what storage users should look for in a secure device.

Learning Objectives:

1. Understanding the security landscape and what has ultimately changed in the industry
2. Threat modeling for the new age of protection
3. Understanding how secure trusted firmware translates into solution requirements and product guarantees
4. Learn what attestation measurements are and how they translate into proving to the platform what firmware is actually running
Agenda

- Product Landscape
- Threat model
- Secure boot for everyone
- Attestation, what happens after Secure Boot
- Platform trust establishment
- Secure Update
- Protection through Obscurity
- Secure Debug
Supply Chain

- Various Points of entry
- Where has the adapter been?
- Is it really the expected adapter?
- Was it intercepted in flight?

- Is it running altered firmware?
- Does it contain the intended components?
- Will it stay that way?

Did I get what I ordered?
Is it still running Securely?
Threat Modeling

- Global Trade, Manufacturing, and development
  - Worldwide development cites
  - Global Supply
  - Untrusted manufacturing

- Availability of Information, methods, resources (Internet)
  - Embedded Operating Systems available for download
  - Hardware Probes are easily available for purchase
  - Leaked utilities and source to the Internet

- Nation State Actors
  - China, US (NSA), Russia etc.
  - Well Funded – What would you be willing to do for $5M?
  - Research facilities
  - Production lines
  - Hacking to a whole new level (organized and legitimized)

- Sophistication of the Actor

- Repercussions of the Event (IOT)
  - Power Plants, Flight Controls, Printers, Centrifuge
Sophisticated

HOW THE NSA’S Firmware Hacking Works and Why It’s So Unsettling

One of the most shocking parts of the recently discovered spying network Equation Group is its mysterious module designed to reprogram or reflash a computer hard drive’s firmware with malicious code. The Kaspersky researchers who uncovered this said its ability to subvert hard drive firmware—the guts of any computer—"surpasses anything else" they had ever seen.

The hacking tool, believed to be a product of the NSA, is significant because subverting the firmware gives the attackers God-like control of the system in a way that is stealthy and persistent even through software updates. The module, named "nls_933w.dll", is the first of its kind found in the wild and is used with both the EquationDrug and GrayFish spy platforms Kaspersky uncovered.

It also has another capability: to create invisible storage space on the hard drive to hide data stolen from the system so the attackers can retrieve it later. This lets spies like the Equation Group bypass disk encryption by secreting documents they want to seize in areas that don’t get encrypted.

https://www.wired.com/2015/02/nsa-firmware-hacking/
Customer Concerns

- Gray Market Products infiltration into the data center
- Lost of information / IP
- Altered products (hardware and firmware)
- Continuous secure operations
- Ability to recover from exploits
- Verification of running systems
- Data Security (Encryption)
- Denial of Service Attacks (System shutdown)
Customer Requests

- Hardware Root of Trust for ASICs
- Firmware Recovery and Restoration
- Continuous Firmware Monitoring and Verification
- Encrypting Firmware
- Reduction in Attack surfaces
- Product Hardening
- Intrusion detection (PCI, Driver, UART, etc)
- Secure Manufacturing (Authorized Products)
- Ownership and Personalization
Market Demand

- IBM Announced Secured Systems
- Dell Announced Secured Portfolio
- HPE Announced Secure Server Products
- Companies are now mandating firmware security – Cerberus, Titan, Intel
- Moving from discussion to implementation and standardization – ie OCP Security Project, PCI-SIG Proposals, DMTF (PMCI)
- MCHP/MSCC is a key part of the Ecosystem of Security for storage, switches, platforms ROT and component ROT
Security Is All About Trust

- User
- Customer (Datacenter)
- Integrator (OEM)
- Board Manufacturer
- ASIC Foundry

Hardware
Software
Secure Boot In Action

- Security begins with the Root of Trust contained in the ASIC
  - Embedded Signing Keys
  - Strong Hashing Functions
  - Immutable Authenticating Boot logic in Silicon Boot ROM
- Trust is extended by verifying the authenticity and integrity of FLASH content prior to executing it
  - Digital signatures are supplied with all Firmware and Configuration Binaries
  - Validated with Embedded ASIC signing keys
  - ASIC Calculated Signatures are computed against the stored images and compared with stored signatures.
Digital Signatures to Secure Firmware

- Verifies authenticity and integrity
- Generated during FW development process
- Verified during FW boot process.
Trust Establishment (Interposers)

**Chain (Root) of Trust: example**

- **Security Chip**
  - Validates: Check for Integrity, Authenticate & Decrypt
  - Immutable Code

- **External Security Code**
  - Validates: Check for Integrity, Authenticate & Decrypt (opt)
  - Mutable Code

- **AP Boot Loader**
  - Validates: Check for Integrity, Authenticate & Decrypt (opt)
  - Trust Establishment for external processor

- **AP appl. code**
  - Running Trusted FW
Trust Establishment (Embedded)

Chain (Root) of Trust: example

- **Security of Chip**
  - Validates: Check for Integrity, Authenticate & Decrypt
  - Immutable Code

- **External Security Code**
  - Validates: Check for Integrity, Authenticate & Decrypt (opt)
  - Mutable Code

- **AP Boot Loader**
  - Validates: Check for Integrity, Authenticate & Decrypt (opt)
  - Trust Establishment for Main FW

- **External SPI Flash**
  - AP appl. code
  - Running Trusted FW

Application Processor (AP)/SOC
Boot Loader

SPI
Attestation

- Enables a third party to reliably & easily attest to the status of a platform. Specifically detect changes that have occurred in HW and FW that impact the trustworthiness of a platform.

- Examples
  - Back Dated Firmware Versions – Old with Security holes
  - Valid Firmware but meant for another platform
  - Non – Secured Part detection
  - Secure But Tampered Hardware

- Platform Roots of trust use attestation to continually monitor and validate system components
Attestation: Example Flow

- Public Attestation Key
- Response
- Passes Measurement
- Valid State
- Fails Measurement
- Take Countermeasures

Attestation Requestor

2nd Executable

1st Executable

Boot Loader

Response

Nonce

PKA Encryption Engine

PCR 3

PCR 2

PCR 1

PCR 0

Strap Values

Security Values

1st Executable Measurement

2nd Executable Measurement

Boot Loader Reset

Private Attestation Key

Public Attestation Key

Response

Passes Measurement

Valid State

Fails Measurement

Take Countermeasures

Measurement

Valid State

Fails Measurement

Take Countermeasures

Measurement

Valid State

Fails Measurement

Take Countermeasures
System of Trust

- BMC
- CPU
- SPI Flash
- ROT Security Processor
- Adapters
- Drive
- Active Component ROT
- Active Component ROT
- Active Component ROT
Manufacturing Identification and Authorization

- Authenticated Parts
- Protection from unauthorized adaptation
- ASIC Unique Identification
- ASIC Authorization / Registration to HSM
- Customer Customization with Public Key injection

Device

Verifier

Challenge/Response with Attestation Measurements
Secure Firmware Update

FW Staging Area

Decompress flash image into non-persistent staging area and validate signature

Begin Firmware Flash

FW Area 1

Program Persistent Memory Area Copy 1

Secureboot Process

Firmware Successfully Booted?

Yes

Original FW Running

No

FW Area 2

Program Persistent Memory Area Copy 2

Public Key to Revoke?

Yes

New Redundant FW Running

No

Roll Back Firmware to Original Version and Restart

Original FW Running

Revoke Public Key

Revoke Public Key
Cryptographic Obscurity

- Encrypted Firmware
- Encrypted Firmware Configuration Parameters
- Encrypted FIPS Critical Security Parameters (CSP)
- Encrypted Operational Memory (DRAM)
Secure Debug Mode

- Secure Debug Mode is the ability to place parts in a debug mode using an authenticated chip specific mechanism
- Ability to detect that a part is in secure debug mode
- Chip Specific mechanisms can not be shared among devices
- Multiple Levels of Forensic Modes
  - Access to UART (Read Only, Read/Write)
  - Access to JTAG/ETAG Debug Ports (Read / Write)
  - Ability to load unsigned firmware
  - Additional Needs and levels
Secure Debug Mode: Example Flow

1) Extract Device Specific Information

2) Request Debug Access

3) Authenticated Device Specific Debug Unlock

4) Authenticated Device Specific Debug Unlock

Private Key

Public Key

Security Officer

Engineer

ASIC
Industry Security Projects

- OCP Security Project
  https://www.opencompute.org/projects/security

- Intel PCIe Device Security Enhancements

- NIST SP800-193 – Released May 2018

- Microsoft Project Cerberus
  https://azure.microsoft.com/en-us/blog/microsofts-project-olympus-delivers-cloud-hardware-innovation-at-scale/

- DMTF PMCI Security Task Force
  https://www.dmtf.org/content/get-involved-dmtfs-pmci-security-task-force

- ...
Microchip Products

Devices With Enabled Security
- SSD Controllers
- UBM Controllers
- PCIe Switches
- SAS Expanders
- Storage Controllers

Security Devices
- SmartFusion 2
- Islogic 2
- PolarFire FPGA
Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world’s standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer’s responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided “as is,” with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

©2018 Microsemi, a wholly owned subsidiary of Microchip Technology Inc. All rights reserved. Microsemi and the Microsemi logo are registered trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.