TRAPEZOID®

Trust Data Intelligence

Cybersecurity Innovation Forum

September 2015

Outline

- Problem Space
- Issues and Attacks
- How we are trying to solve problem
- NIST Firmware Related Documents
- Demo

You can’t trust your software
if you don’t trust your hardware.

Hardware is vulnerable

Since 2008, there has been a growing awareness of the fundamental threats to enterprise hardware.

Virus on flash cards on swithes

Supplier accidentally ships Malware-riddled replacement motherboards

Microsoft finds malware on new computers in China

]HackingTeam[Data breach shows firmware tools for offense

2011 Mebromi BIOS virus discovered; infects the master boot record of a device

black hat / DEFCON

2012: "*Hardware Backdooring is Practical*"
2013: "*Bypass Secure Boot Windows 8*"
2013: "*BIOS Chronomancy: Fixing Core Root of Trust for Measurement*"
2014: *"Extreme Privilege Escalation On Windows 8/UEFI Systems"*
2014: *"Exposing Bootkits with BIOS emulation"*
2014: *"Computrace Backdoor Revisited"*
2014: *"Shadow Walker: TLB Splitting on Modern x86"*
2014: *"Lessons learned from 8 years breaking hypervisors"*
2014: *"Summary of BIOS attacks"*
2014: *"NSA Playset - DIY Hardware implant"*

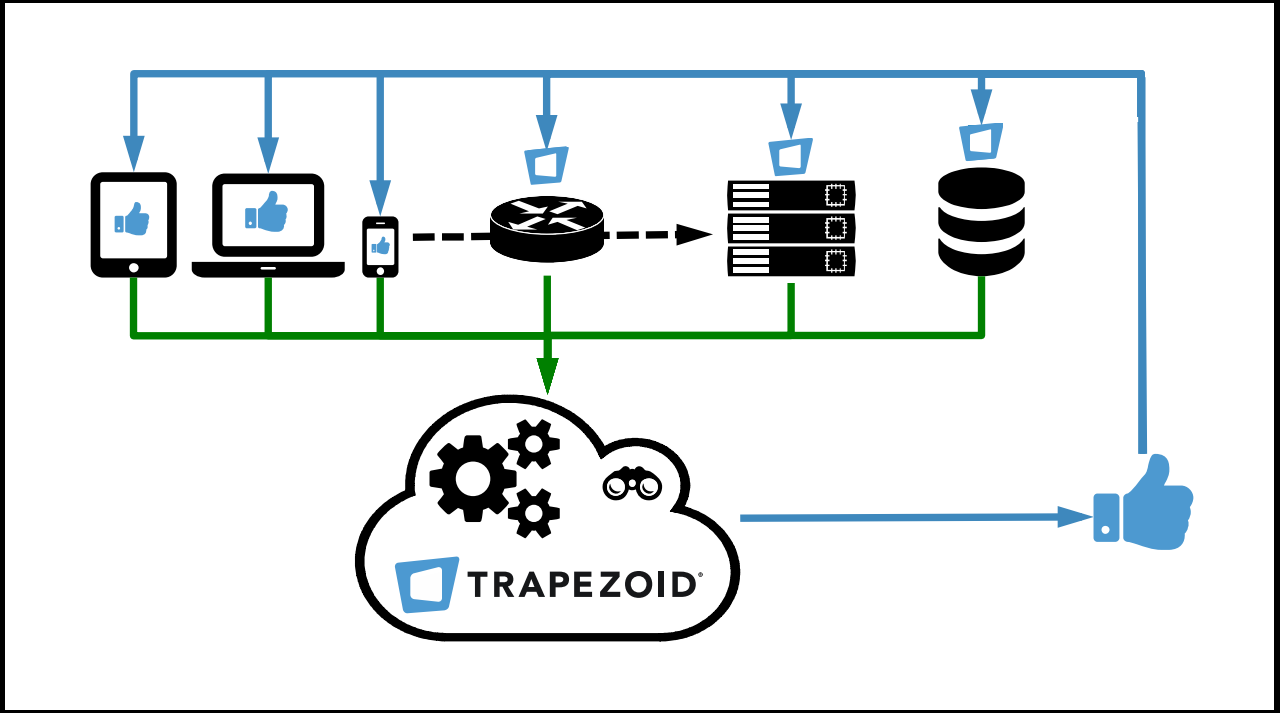
LEGBACORE Demonstrates 3 min Lighteater BIOS Takeover March 2015

2014 Leak of NSA ANT catalog

EQUATION GROUP: Kaspersky reports on sophisticated hard drive firmware capabilities.

Trapezoid Vision

"Ensure A Trusted Connection Is Established
For Every Client To Cloud Transaction"



Trapezoid's Trust Visibility Engine

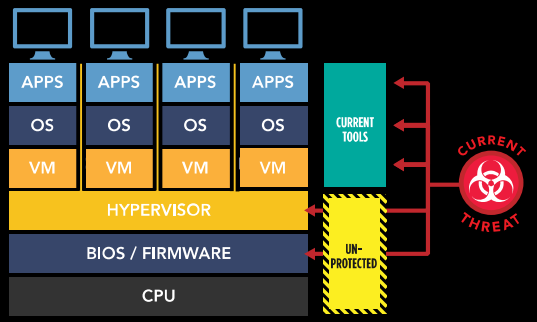
- Is an ***integrity verification tool*** to detect unauthorized changes to firmware
- Addresses ***newly identified*** vulnerabilities
- Helps organizations ***address the risk*** of this newly evolving threat
- Leverages ***hardware-based "root of trust"*** technologies for integrity and jurisdictional location
- Provides ***higher assurance*** that devices are operating as intended

Trapezoid® Marker

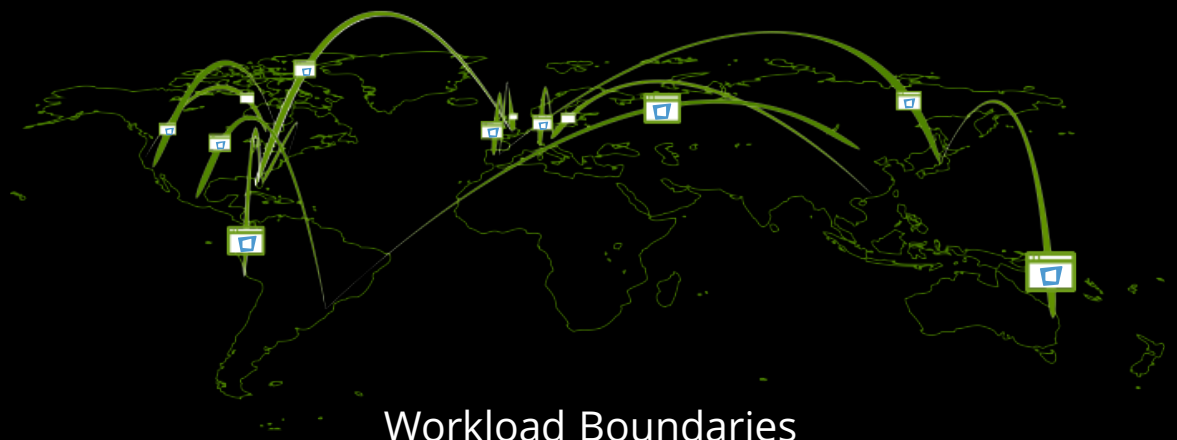
A unique, intelligent, tamper-evident seal created using our patent-pending technology.

- Unique cryptographic tag for hardware
- Forensic mapping of virtual machines to physical hardware
- Define workload and data boundaries
- OEM platform watermark for supply chain validation

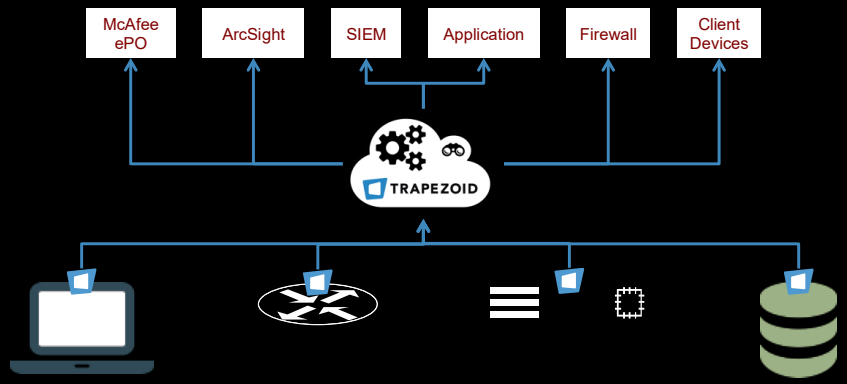
Use Cases



BIOS/Firmware Integrity



Workload Boundaries



Compliance Reporting & Integration

Applicable Compliance

FEDERAL

NIST/FISMA/FEDRAMP call for an "**integrity verification tool to detect unauthorized changes to firmware**"

ENTERPRISE

"***Framework for Improving Critical Infrastructure Cybersecurity***" PR.DS-6: **Integrity checking mechanisms are used to verify** software, **firmware**, and information integrity

"***ISO/IEC 19678 Information Technology — BIOS Protection Guidelines***": Unauthorized modification of BIOS firmware by malicious software constitutes a **significant threat**

MEDICAL

HIPAA Security Rule requires **protection against "reasonably anticipated" threats** and periodic risk assessments must take into account risks associated with **evolving threats or vulnerabilities**

FINANCIAL

PCI DSS require companies to "**identify and evaluate evolving malware threats**," and that "trends in malicious software should be included in the identification of new security vulnerabilities, and **methods to address new trends** should be incorporated into the company's configuration standards and protection mechanisms as needed."

TELECOM

NSTAC recommends Trusted Computing Platforms calling for systems to be protected by "computer-based policy and enforced by **hardware based 'roots of trust' . . .** to provide higher assurance that devices are operating as intended, and producing the desired outcome with respect to security."

SP800-147 BIOS Protection Guidelines

- “Requirements” are for vendors implementing a secure update mechanism and found in Appendix A.
- 3-C: If BIOS flash protections are not implemented, then BIOS integrity shall be verified prior to each execution, using the Verification Component of the RTU to authenticate the BIOS image.
- Trapezoid inventories platforms to find out which servers in an environment have these types of capabilities.
- Trapezoid collects and tracks integrity data over time.

NIST SP800-147B (Servers)

- August 2014
- Geared to OEM's: This guide is intended to provide server platform vendors with recommendations and guidelines for a secure BIOS update process.
- Follow on to SP800-147 (April 2011) which deals with desktop and laptop computers
- Servers may use guidelines in earlier document if they have only one BIOS update mechanism
- Discusses role of service processors
- Does not address supply chain, physical replacement of a chip, or local update (physical access)

DRAFT SP800-155 (Dec 2011)

- BIOS Integrity Measurement Guidelines
- For HW and SW vendors developing products to support BIOS integrity measurements.
- For organizations developing procurement strategies for the technologies

NIST IR 7904 Draft (Dec 2012)

- Goals
  - Improve Cloud Security
  - Speed Cloud Adoption
- Use Cases
  - Coke vs Pepsi on same cloud
  - Two countries with different data laws
- 3 Stages
  - Platform Attestation and Safe Hypervisor Launch
  - Trust Based Homogeneous Secure Migration
  - Trust+Geolocation based Homogeneous Secure Migration

Other NIST docs referencing Firmware

- General: No longer just “hardware and software” now “hardware, FIRMWARE, and software”
- 800-82: Guide to Industrial Control Systems Security, May 2015
  - Mentions Firmware in Change and configuration management
  - Overlays 800-53r4
- 800-161: April 2015 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
  - Only accept updates directly from OEM or that you deploy via centralized patch management type system
  - Points back to FIPS200 configuration management and 800-53
- 800-171: June 2015 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - Points back to FIPS200 and 800-53

NIST SP800-53Ar4 SI-7

- **Assessing Security and Privacy Controls in Federal Information Systems and Organizations**
- Software, FIRMWARE, and Information Integrity
- Previous Revisions: no mention of Firmware
- 16 Sections
- Manufacturers and OEM’s adding capabilities to address
- Trapezoid’s tool allows validation

SI-7 Sections

1. Integrity Checks
2. Automated Notification of Integrity Checks
3. Centrally Managed Integrity Tools
4. Tamper Evident Packing (MOVED)
5. Automated Response to Integrity Violations
6. Cryptographic Protection
7. Integration of Detection and Response
8. Auditing Capability for Significant Events
9. Verify Boot Process
10. Protection of Boot Process
11. Confined Environments with Limited Privilege
12. Integrity Verification
13. Code Execution in Protected Environment
14. Binary or Machine Executable Code
15. Code Authentication
16. Time Limit on Process Execution Without Supervision

TRAPEZOID®
Trust Data Intelligence

Thank you

Trapezoid, Inc.
4931 SW 75th Avenue
Miami, Florida 33155
786.621.8580
www.trapezoid.com
jgonzalez@trapezoid.com