Intel Advanced Technology in the Enterprise: Best Security Practices

Shiva R. Dasari
Senior Software Engineer, IBM
Vincent J. Zimmer
Principal Engineer, Intel

EFIS001

Sponsors of Tomorrow.

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

Trusted Computing Elements and Security Features in the platform

Shiva R. Dasari

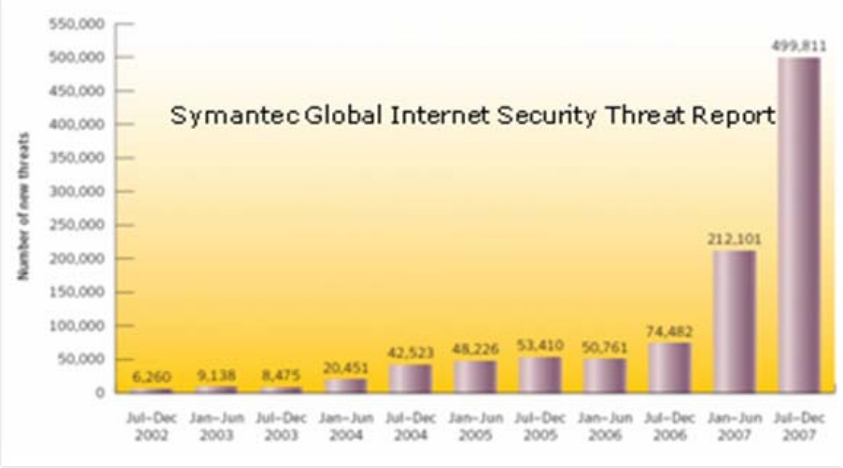
Senior Software Engineer, IBM

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

Platform Security – The Problem Statement

- **Protection Against Malicious Code**
  - Worms, patching
- **Business Process Compliance**
  - Regulatory requirements from EU Privacy, SarbOx, Basel II, HIPAA, GLB etc.
- **Internal/External Access and Data Protection**
  - Secure provisioning of Infrastructure/Users
  - Managing access/identity across disparate applications



Source: Symantec

Security isn't hype, but real market need

Dictionary Terminology

- **Trust**
  - An entity can be trusted if it always behaves in the expected manner for the intended purpose

- **Measurement**
  - The process of obtaining the identity of an entity

- **Security**
  - ". . .[1]maintenance that ensure a state of inviolability from hostile acts or influences"

Trust needs an agreed upon lexicon

[1] ***www.wikipedia.org***

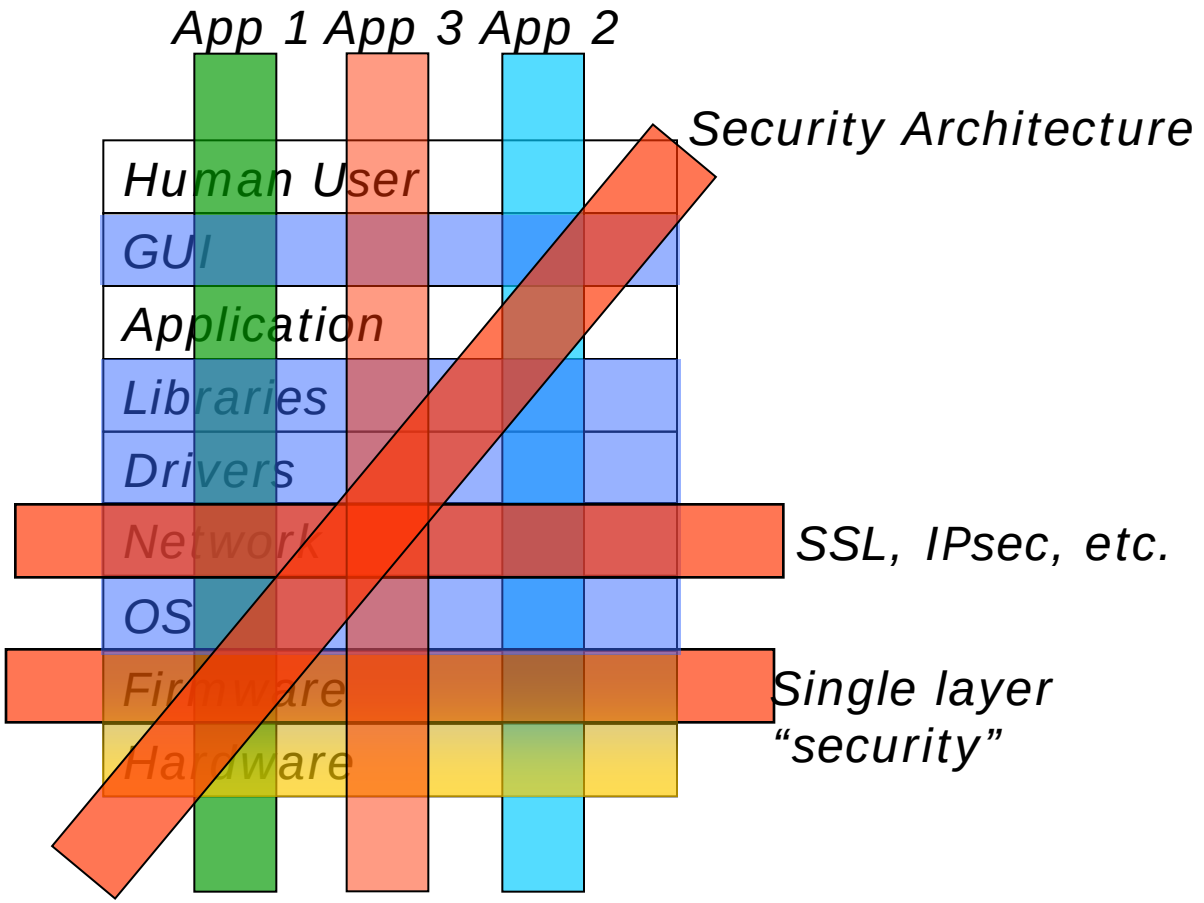
Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

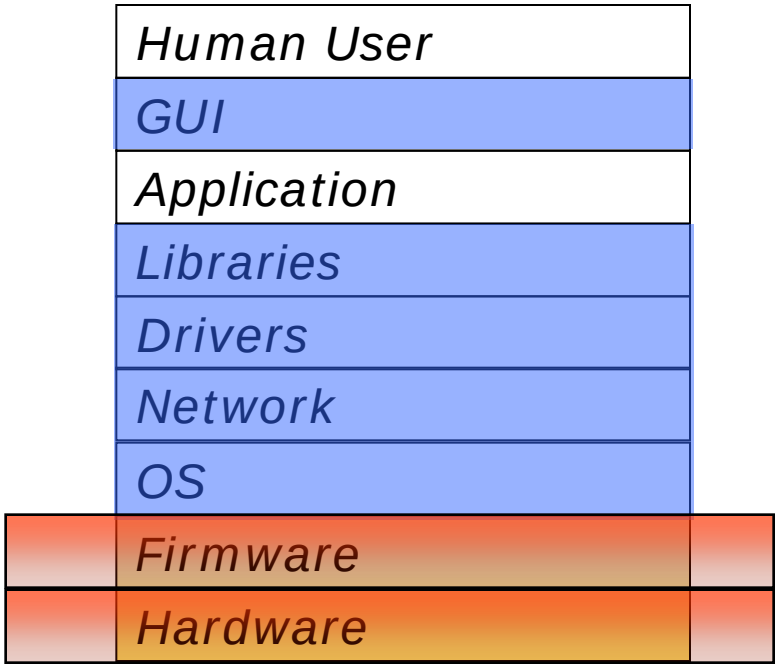
Elements of trust

Providing 'Trust'

Security architecture to deliver trust



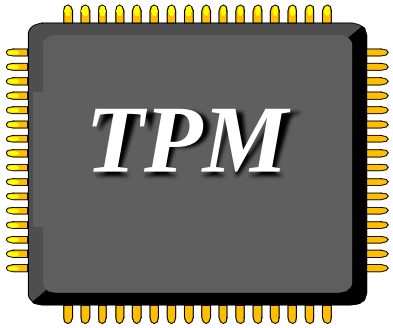
Roots of trust of security architecture



Hardware and firmware are the roots of trust

What is the heart of Trust

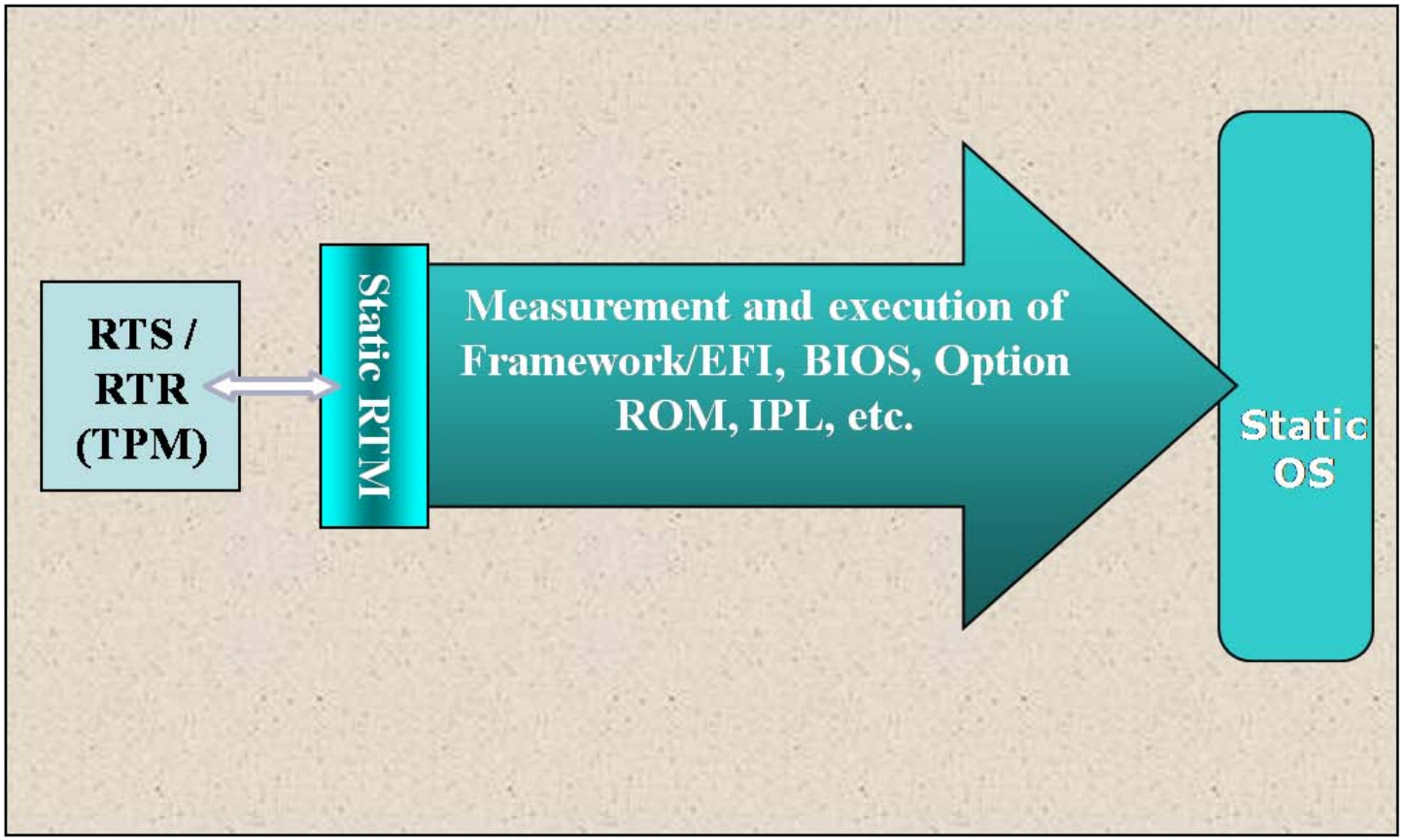
- The hardware root of trust includes
  - TPM
  - Flash
  - Binding of above into system
- TCG defines TPM's functionality
  - Protected capabilities
  - Shielded locations



- Not the implementation
  - Vendors are free to differentiate the TPM implementation
  - Must still meet the protected capabilities and shielded locations requirements

Need a hardware root of trust

SRTM[1] for Platform Firmware



Firmware use of TPM and Measurements

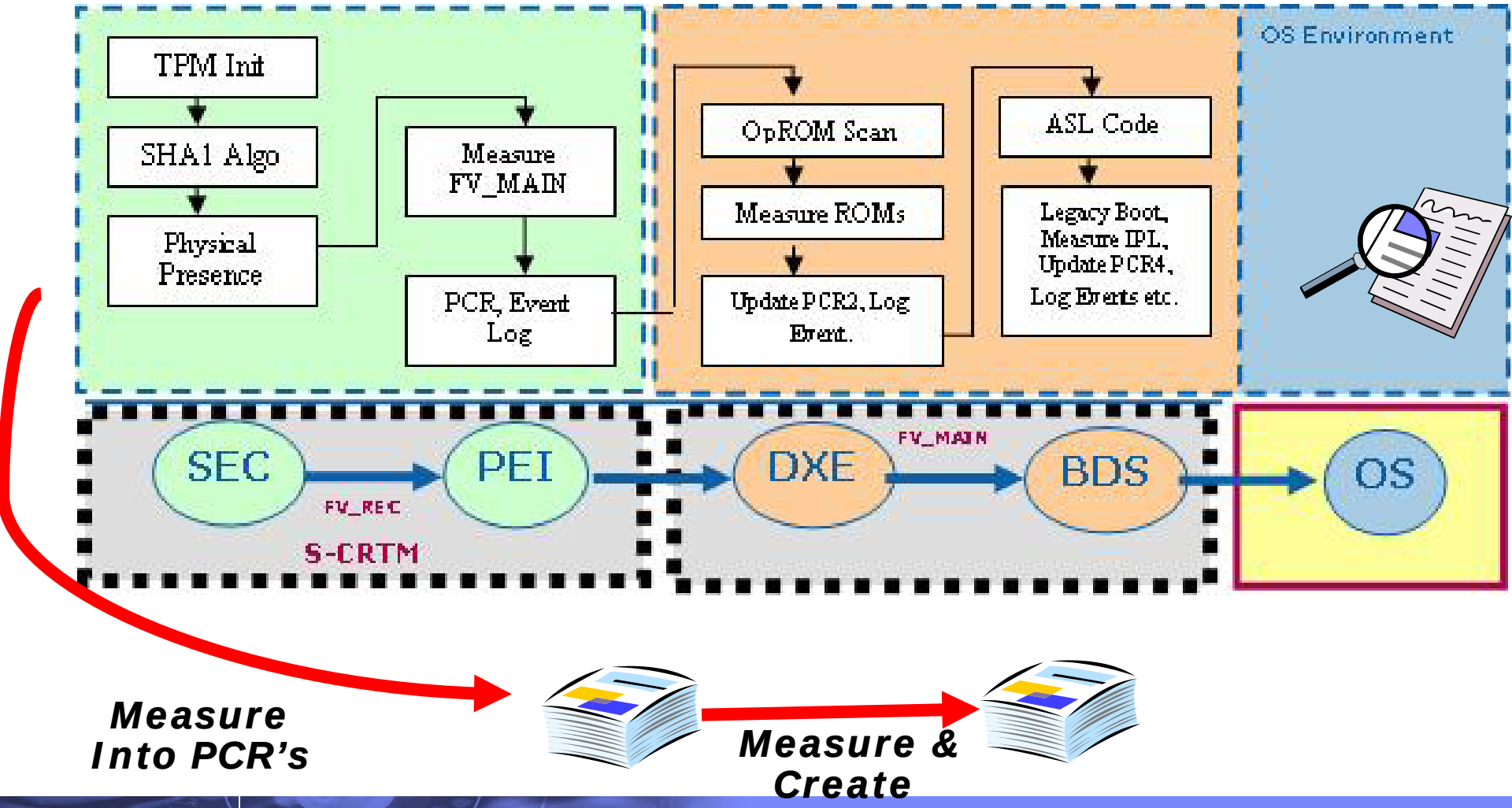
[1] Static Root of Trust for Management (SRTM)

CRTM

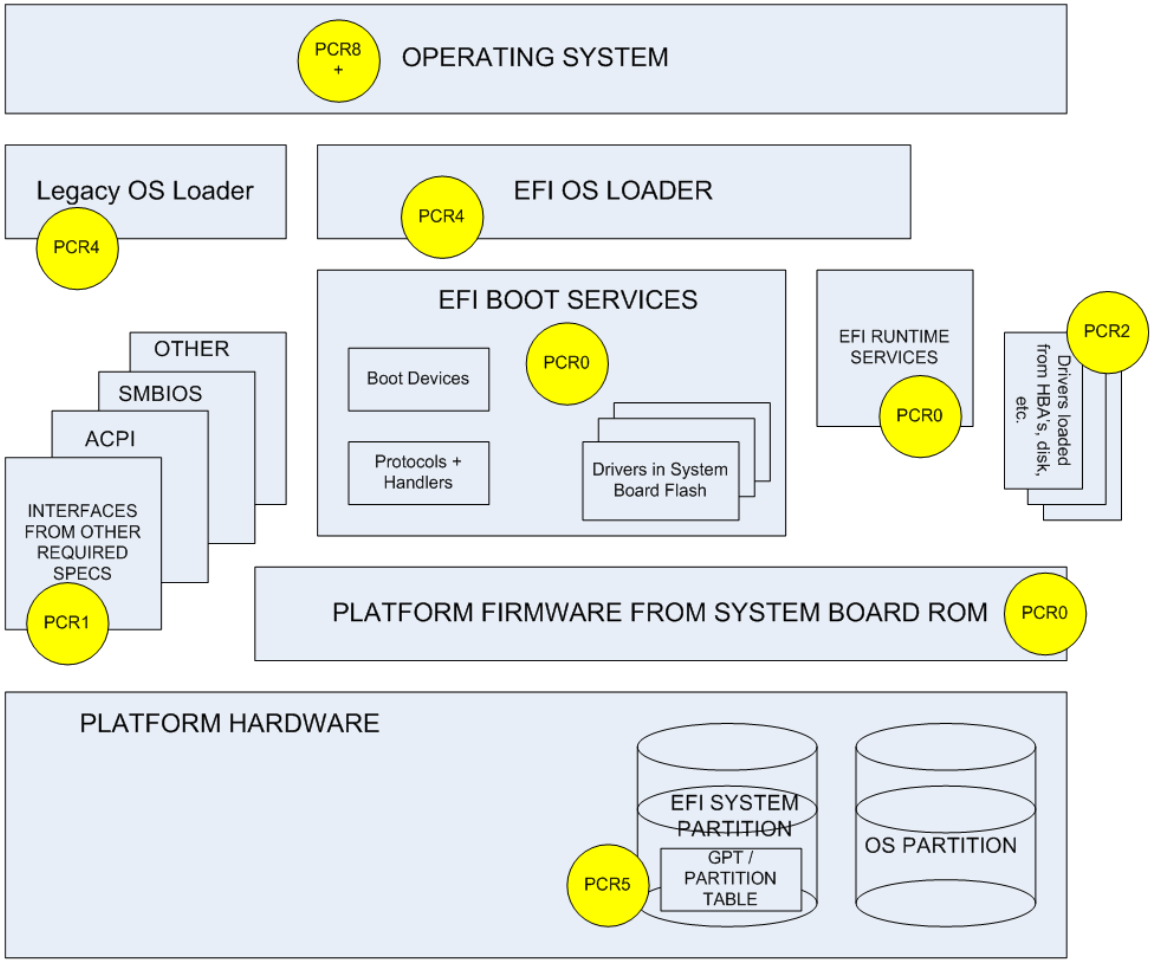
- What is CRTM
  - Core root of trust for measurement
  - Detects physical presence and initiates measurements for rest of firmware bootstrap
- Properties of CRTM
  - immutable, or never changed in the field
  - appropriate cryptographic techniques need to be employed in order to update the CRTM.
- For updatable CRTM
  - A signed capsule is one implementation path.
  - Need manufacturer-approved/secure update process

CRTM is the firmware foundation of trust

UEFI/PI Architecture Boot Flow – Create/Evaluate Integrity List



Measured items in UEFI



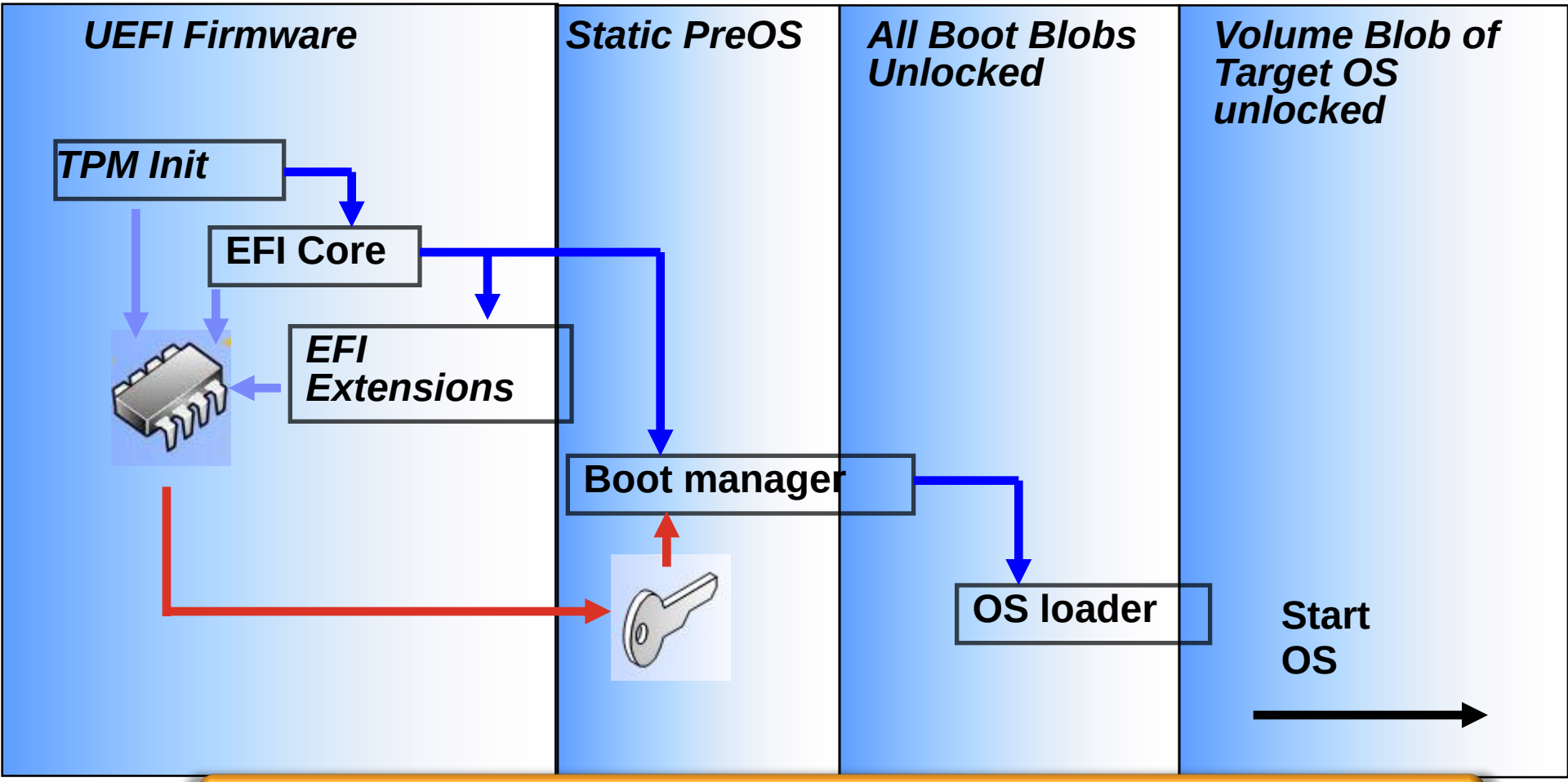
Standardized way to measure and report

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

BitLocker™ Drive Encryption

Static Root of Trust Measurement of early boot components



UEFI Windows* is using SRTM

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

IBM System x Servers

- Comprehensive System x portfolio Transition to UEFI based firmware
  - UEFI 2.1 PI 1.0 specification compliant
  - Improved management and configuration capabilities
  - Advanced "Touchless" Compatibility Support Module (CSM)
  - **Trusted Platform features: TPM enablement, TCG and Core Root of Trust for Measurement support**

Blade
- HS22

Rack-mount
- x3650 M2
- x3550 M2
- X3250 M3

Tower
- x3500 M2
- x3400 M2
- x3200 M3

Best Practices on Building Security Features using PI-based Technology

Vincent Zimmer

Principal Engineer, Intel

Sponsors of Tomorrow.™ intel

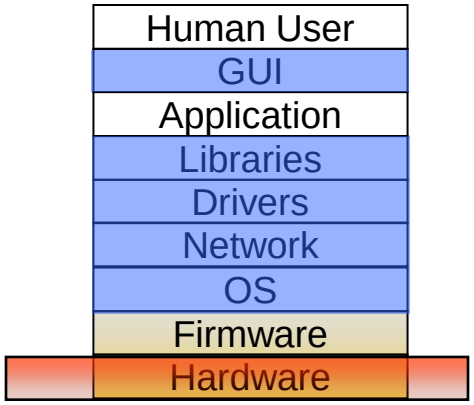
Background on Best Practices

- Many of these prescriptions covered below are already treated in various TCG documents and design guides
- The intent of this section is to provide a platform and UEFI PI-focused summary of rules and practices

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

Hardware Best Practices



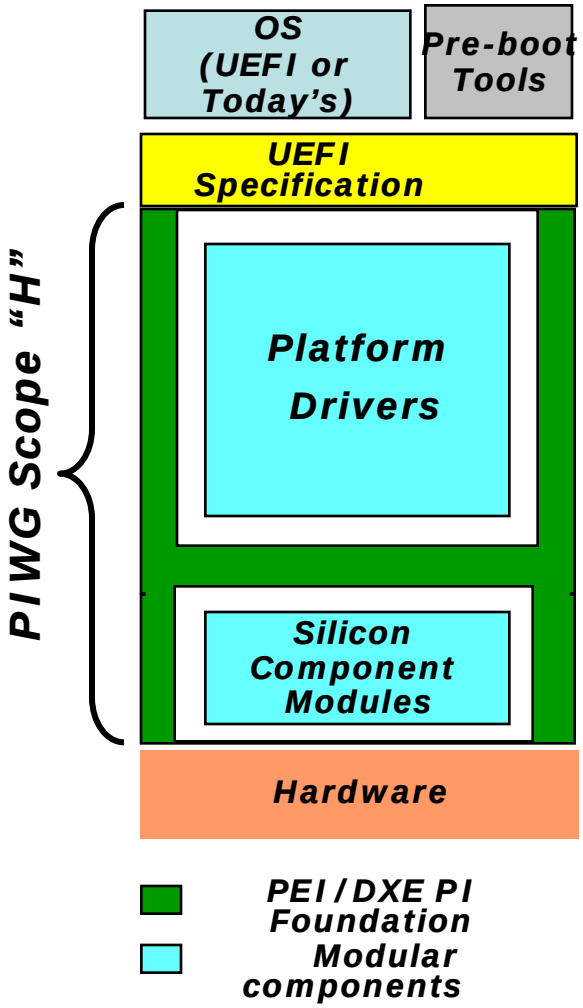
- CRTM flash protection
  - Locking must not be controlled by any un-trusted programmable entities
  - Once locked within CRTM code, it must not be un-lockable without going through a system reset
- Physical Presence
  - Physical Presence (PP) hardware must not be changeable by any un-trusted programmable entity
- Reset
  - TPM must get reset for any type of platform reset
  - No path available to manipulate reset vector in the system

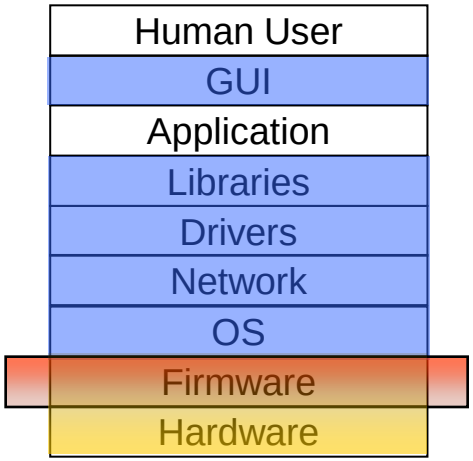
Hardware is a key part of root of trust

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

What About Firmware Practices? UEFI PI Overview





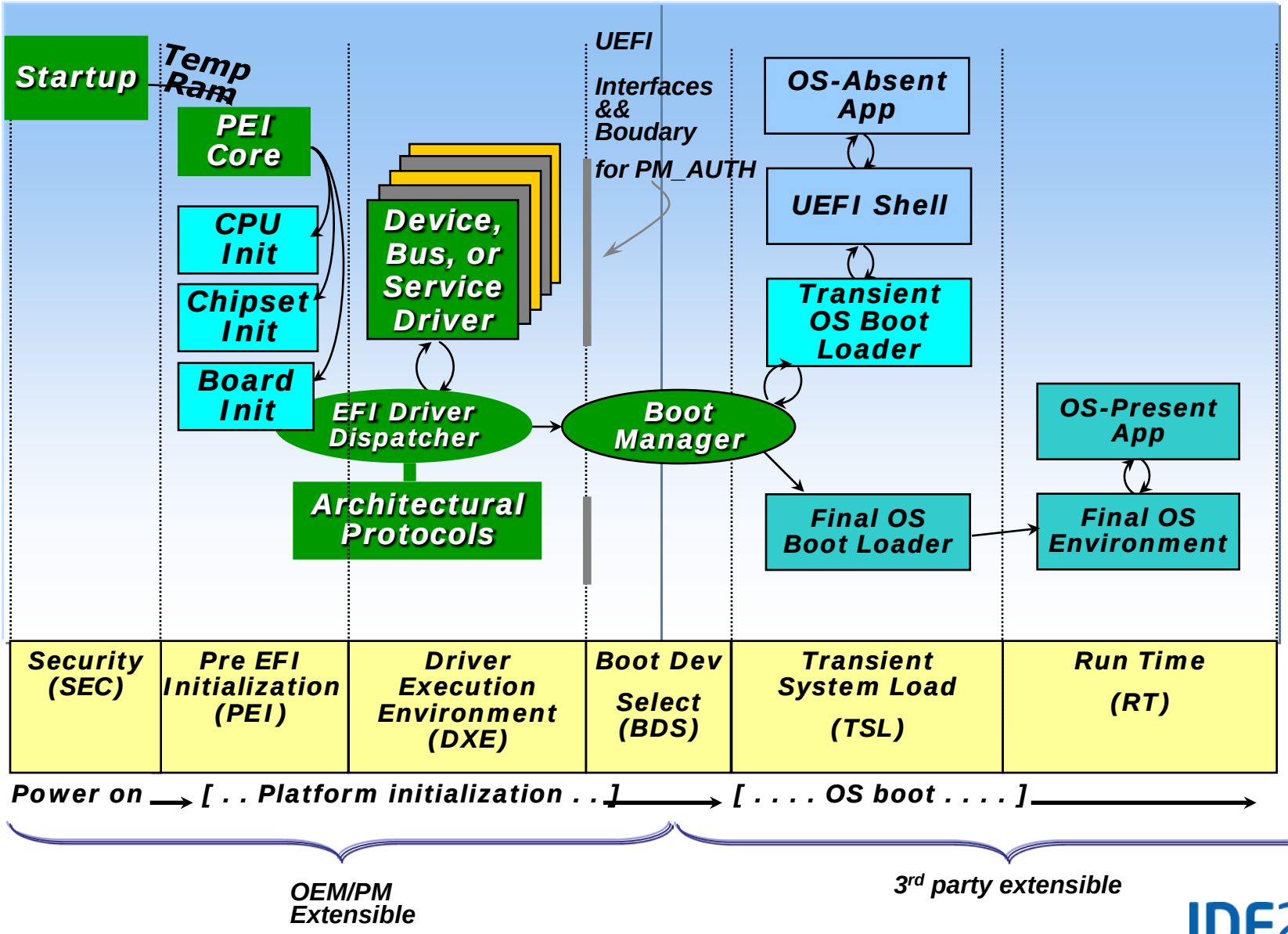
- UEFI 2.3 (published) specifies how firmware boots the OS loader
- UEFI's Platform Initialization Architecture specifies how modules initializing SI and the platform interact and provides common services for those modules
- PI DXE is the preferred UEFI Implementation
- PEIMs and DXE drivers to implement CRTM, SRTM, Update, other security features

Design Intent

- The PI phase is under control of the Platform Manufacturer (PM)
- Updates to PI phase should occur under PM authorization (PM_AUTH)
- PI phase can be decomposed into compartments
  - SEC
  - PEI
  - DXE
  - DXE SMM

Methods of building PI impacts trust

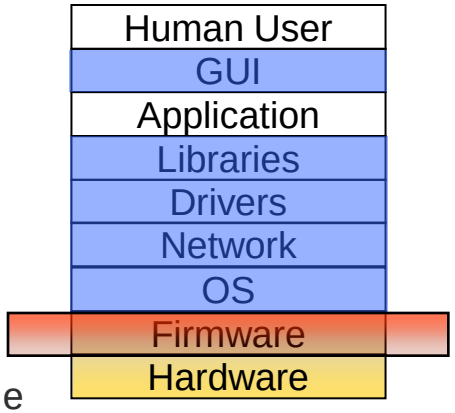
Overall View of Boot Time Line



Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

UEFI PI Best Practices



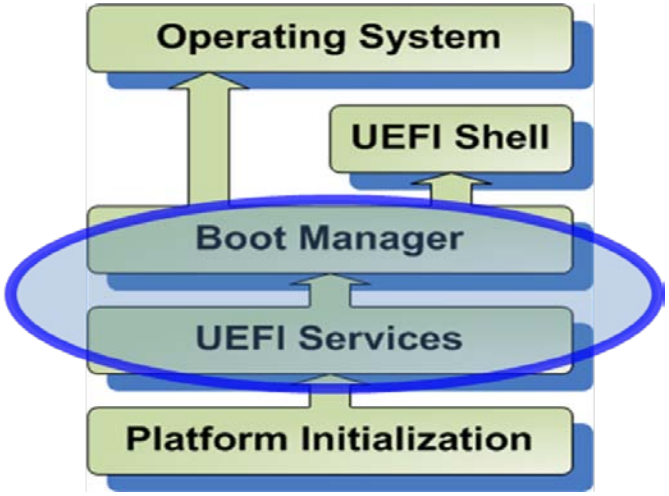
- HW mis-configuration:
  - Appropriate set locks and other hardware configuration should be set by the PM-only PI code prior to running 3rd party code, such as UEFI drivers or operating system loaders
- Callouts
  - Don't call out from PM_AUTH PI code to non-PM_AUTH code
  - Measure any code before loading
- Interface correctness
  - Pass compliance tests
  - Check & validate input, especially from non-PI PM_AUTH into PI code
- Flash protection and update security
  - Appropriate update of PI and CRTM – either immutable or cryptographic update
- Denial of service
  - Platform recovery/update strategy

Firmware completes the platform trust solution

Agenda

- Trusted Computing Elements
  - Problems to solve
  - Firmware and trusted computing
  - OS usage
  - Platform perspective
- Best practices
  - H/W rules
  - PI overview
  - Firmware rules
- Futures

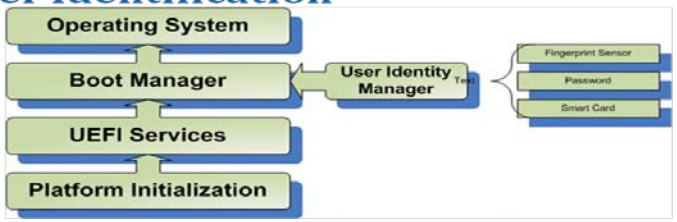
Futures - UEFI



Driver Signing

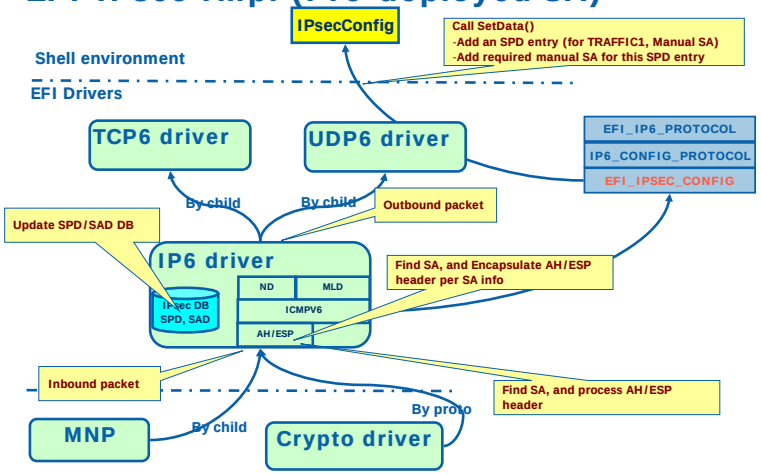
- Expands the types of signatures recognized by UEFI
  - SHA-1, SHA-256, RSA2048/SHA-1, RSA2048/SHA-256 & Authenticode
- Standard method for configuring the "known-good" and "known-bad" signature databases.
- Provides standard behavior when execution is denied to provide policy-based updates to the lists.

UEFI User Identification



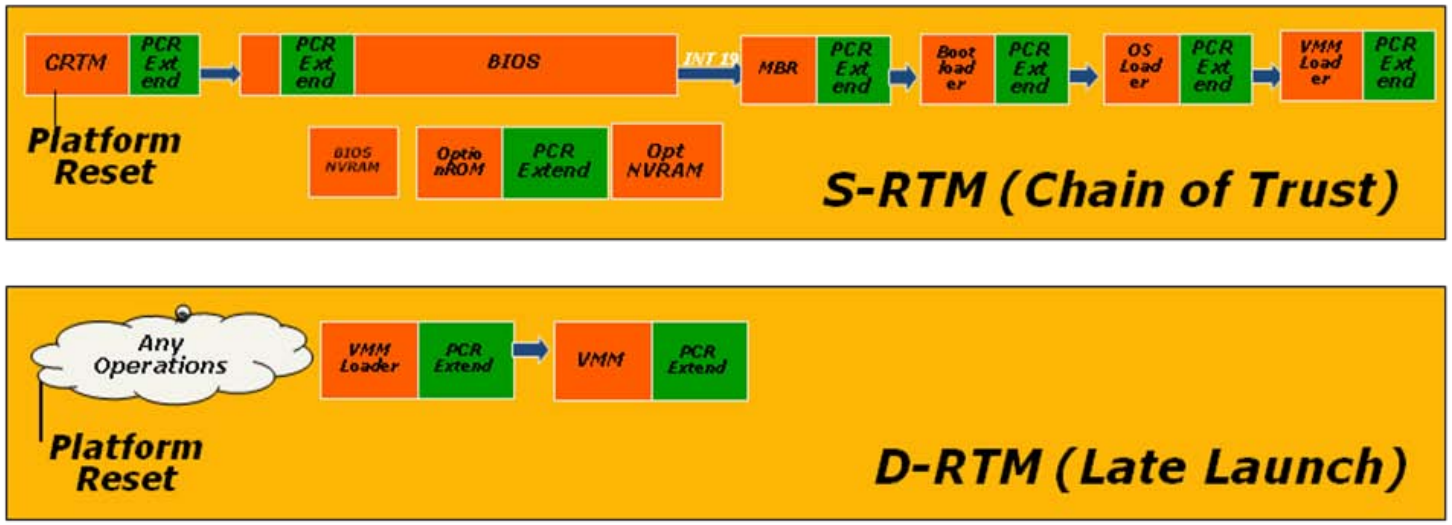
- Standard framework for user-authentication devices such as smart cards, smart tokens & fingerprint sensors.
- Uses UEFI HII to display information to the user.
- Introduces optional policy controls for connecting to devices, loading images and accessing setup pages.

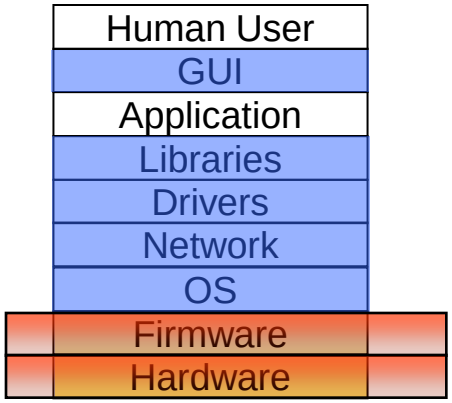
EFI IPsec Impl (Pre-deployed SA)



UEFI Security continues to evolve

Trust Models: S-RTM & D-RTM





- S-RTM measurement chain starts at reset and includes components from various sources
- D-RTM measurement chain starts with a trusted secure event trigger such as SINIT. D-RTM leads to a smaller TCB, reduced attack surface and thus a more secure system
- MLE provider must make assurances that the MLE maintains the TCB. Smaller TCB simplifies MLE design.

Firmware & Hardware security evolution

Summary

- Security problems in the industry are real
- Trust and a security architecture can address some needs, esp h/w and f/w
- UEFI f/w and TCG hardware for SRTM, BitLocker usage, IBM platforms
- Follow best practices on implementing hardware and firmware
- UEFI and hardware security evolution

Call to action- Security Requirements

- **Use the TPM**
- **Follow best practices on hardware and firmware**
- **Get involved in UEFI and TCG forums**
- **Get the white paper**
  - http://download.intel.com/technology/efi/docs/pdfs/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf

Additional resources on UEFI:

- Other Technical and UEFI Sessions – Next slide
- Intel / IBM Security Whitepaper: http://download.intel.com/technology/efi/docs/pdfs/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf
- Visit UEFI Booth #136
- More web based info:
  - Specifications and Implementation sites: www.tianocore.org, www.uefi.org, www.intel.com/technology/efi
- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress

IDF 2009 UEFI & Other Security Sessions

ECT#	Company	Description	Time	RM	D
S002 ✓	Intel, Vmware	Intel® Trusted Execution Technology (Intel® TXT): A More Secure Launch Environment for the Enterprise Cloud	11:15	2007	T

EFI#	Company	Description	Time	RM	D
P001 ✓	Dell, HP, IBM, Intel, Microsoft	Using UEFI as the Foundation for Innovation	10:10	2005	T
S001 ✓	IBM, Intel	Intel Advanced Technology in the Enterprise: Best Security Practices	16:15	2001	W
S002	Dell, Intel, Insyde SW	Secure FW Lockdown through Standardized UEFI Management Protocols	17:15	2001	W
S003	Intel, AMI	Best Technical Methods for UEFI Development -Reducing Platform Boot Times -Firmware Debugging: UEFI and USB for platform forensics	11:10	2002	Th
S004	Microsoft, Insyde SW, Intel	UEFI Boot Time Opt. Under Microsoft Windows 7	13:40	2002	Th
S005	Phoenix, Intel	Transitioning the Plug-In Industry from Legacy to UEFI: Real World Cases	14:40	2002	Th
Q001	Intel, All	Q & A session	15:40	2002	Th

✓ DONE

Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessions

Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events

Q&A

Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.
- Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
-

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the third quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel's actual results, and variances from Intel's current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation's expectations. Ongoing uncertainty in global economic conditions pose a risk to the overall economy as consumers and businesses may defer purchases in response to tighter credit and negative financial news, which could negatively affect product demand and other related matters. Consequently, demand could be different from Intel's expectations due to factors including changes in business and economic conditions, including conditions in the credit market that could affect consumer confidence; customer acceptance of Intel's and competitors' products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Additionally, Intel is in the process of transitioning to its next generation of products on 32nm process technology, and there could be execution issues associated with these changes, including product defects and errata along with lower than anticipated manufacturing yields. Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel's response to such actions; and Intel's ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; capacity utilization; start-up costs, including costs associated with the new 32nm process technology; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; product mix and pricing; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; and the timing and execution of the manufacturing ramp and associated costs. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The current financial stress affecting the banking system and financial markets and the going concern threats to investment banks and other financial institutions have resulted in a tightening in the credit markets, a reduced level of liquidity in many financial markets, and heightened volatility in fixed income, credit and equity markets. There could be a number of follow-on effects from the credit crisis on Intel's business, including insolvency of key suppliers resulting in product delays; inability of customers to obtain credit to finance purchases of our products and/or customer insolvencies; counterparty failures negatively impacting our treasury operations; increased expense or inability to obtain short-term financing of Intel's operations from the issuance of commercial paper; and increased impairments from the inability of investee companies to obtain financing. The majority of our non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management's plans with respect to our investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. A detailed discussion of these and other risk factors that could affect Intel's results is included in Intel's SEC filings, including the report on Form 10-Q for the quarter ended June 27, 2009.

Rev. 7/27/09