Unified Extensible Firmware Interface (UEFI): Best Platform Security Practices

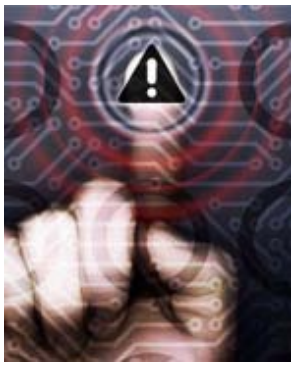
Qin Long - Senior Software Engineer, Intel
Zhan Gao - Principal Engineer, Nanjing Byosoft, Ltd

EFIS003

Sponsors of Tomorrow.™ intel

Agenda

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

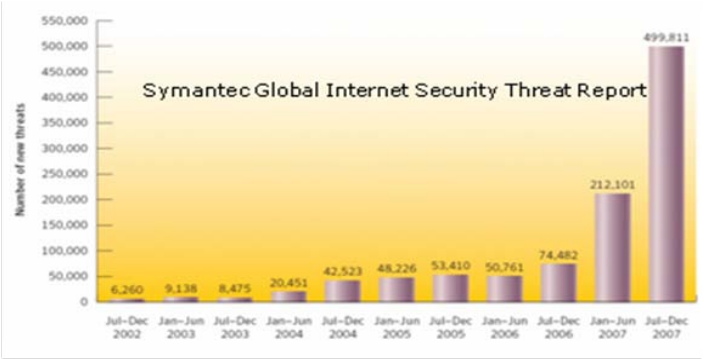


Background & Motivation

- Security is not only OS things: researchers have started to look for vulnerabilities in layers above, as well as underneath the OS.
- Real World: SMM configuration bugs, exploitable memory overflows, firmware downgrades triggered by malware, …
- Challenges
  - Firmware is an interesting attack target: Early execution, Privileges, Asset Data, SMM, etc
  - Malicious software running underneath the OS is quite powerful: Difficult to detect; Cannot be eliminated by OS reboot or re-install; Information Leak; Identify Theft; …
- Should consider more security things on Platform & Firmware now!

Platform Security – The Problem Statement

- **Protection Against Malicious Code**
  - Worms, Virus, Rootkit, Bootkit
- **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

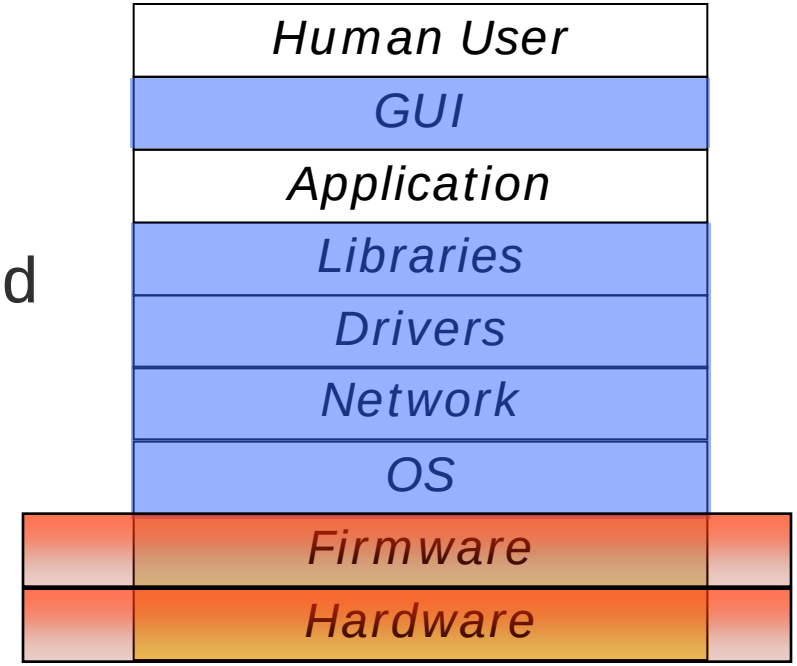
Agenda

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

Goals / Guidelines

- Potential Threats
  - ✓ Spoofing
  - ✓ Tampering
  - ✓ Repudiation
  - ✓ Information Disclosure
  - ✓ Denial of Service
  - ✓ Elevation of Privilege
- Platform and UEFI PI-focused summary of **rules** and **practices**
  - ✓ Integrity Protection
  - ✓ Data Protection
  - ✓ Verification
  - ✓ Platform Availability

Roots of Trust of Security Architecture



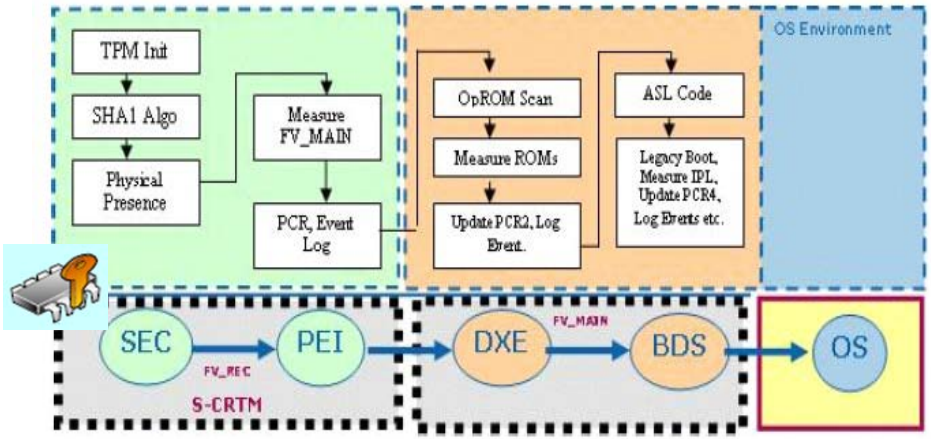
Hardware and Firmware are the Roots of Trust

Agenda

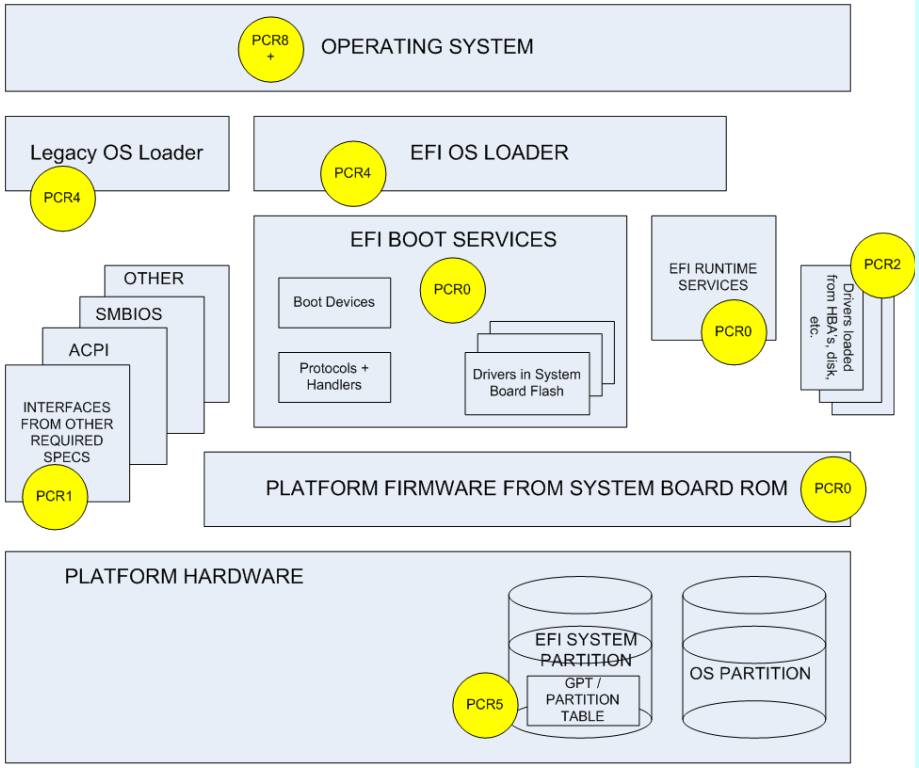
- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

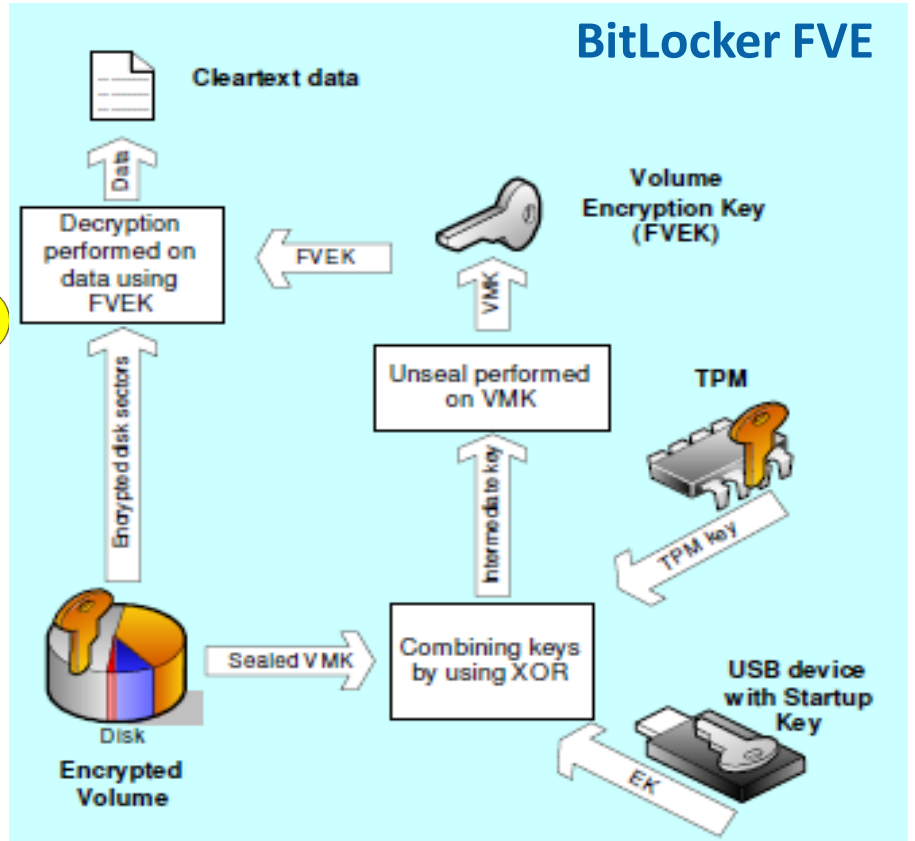
Trusted Computing & Measured Boot

- The hardware root of trust includes
  - TPM
  - Flash
  - Binding of above into system
- Measured Boot
  - Provide an end-to-end solution for the customer to be TCG conformant
  - Recording the platform state of the machine into a PCR
  - Boot Flow
- S-CRTM
  - Core Root of Trust for Measurement
  - Detects physical presence and initiates measurements for Rest of firmware bootstrap



UEFI Measurement & OS Usage





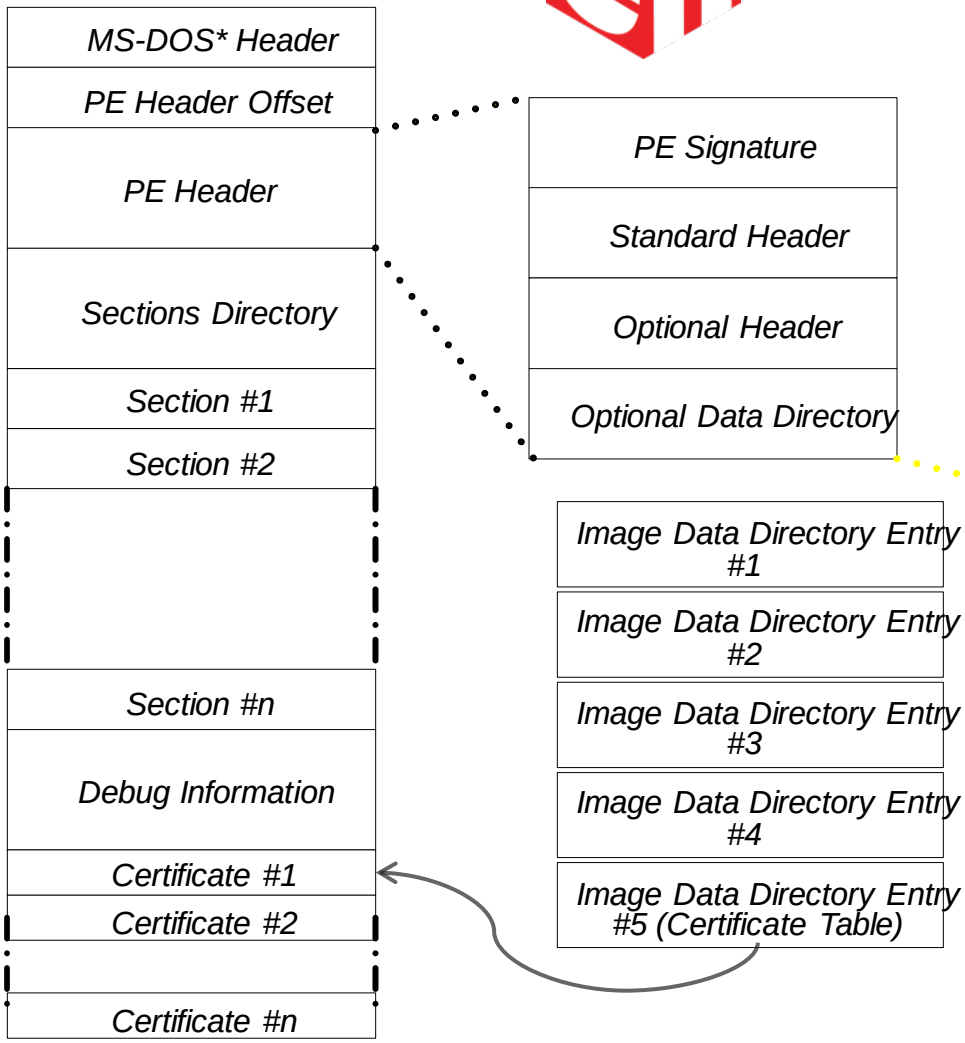
Standardized way to measure and report

Agenda

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

UEFI Driver Signing

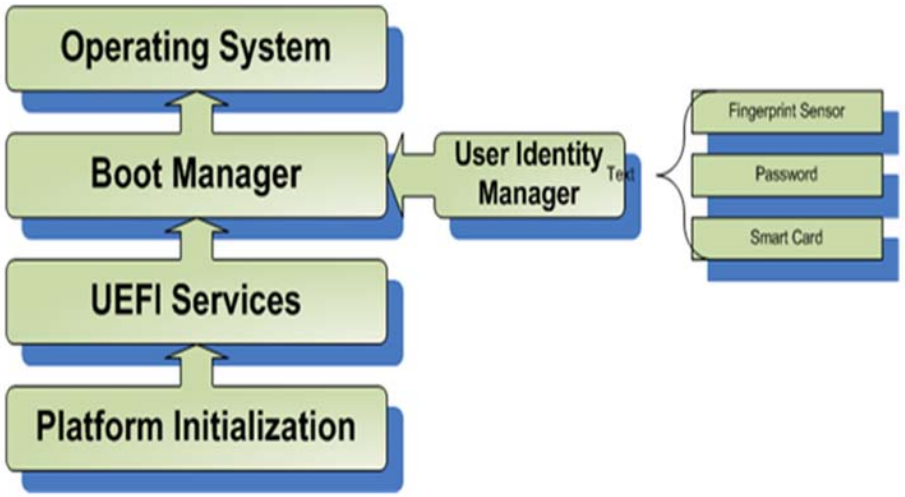
- Expand the types of signatures recognized by UEFI
  - EFI_CERT
  - Authenticode
- Core firmware verification of publisher identity and image integrity of all UEFI extensions
- Security / Trust Policy Configuration to identifies a small set of trusted root certification authorities
- Enable installation and verification of boot applications used to boot any operating system the customer selects for the platform



Embed signatures within executable

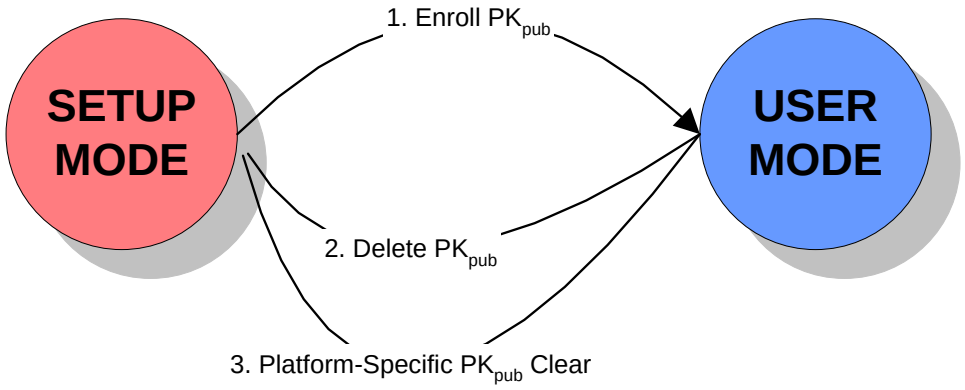
UEFI User Identification

- 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

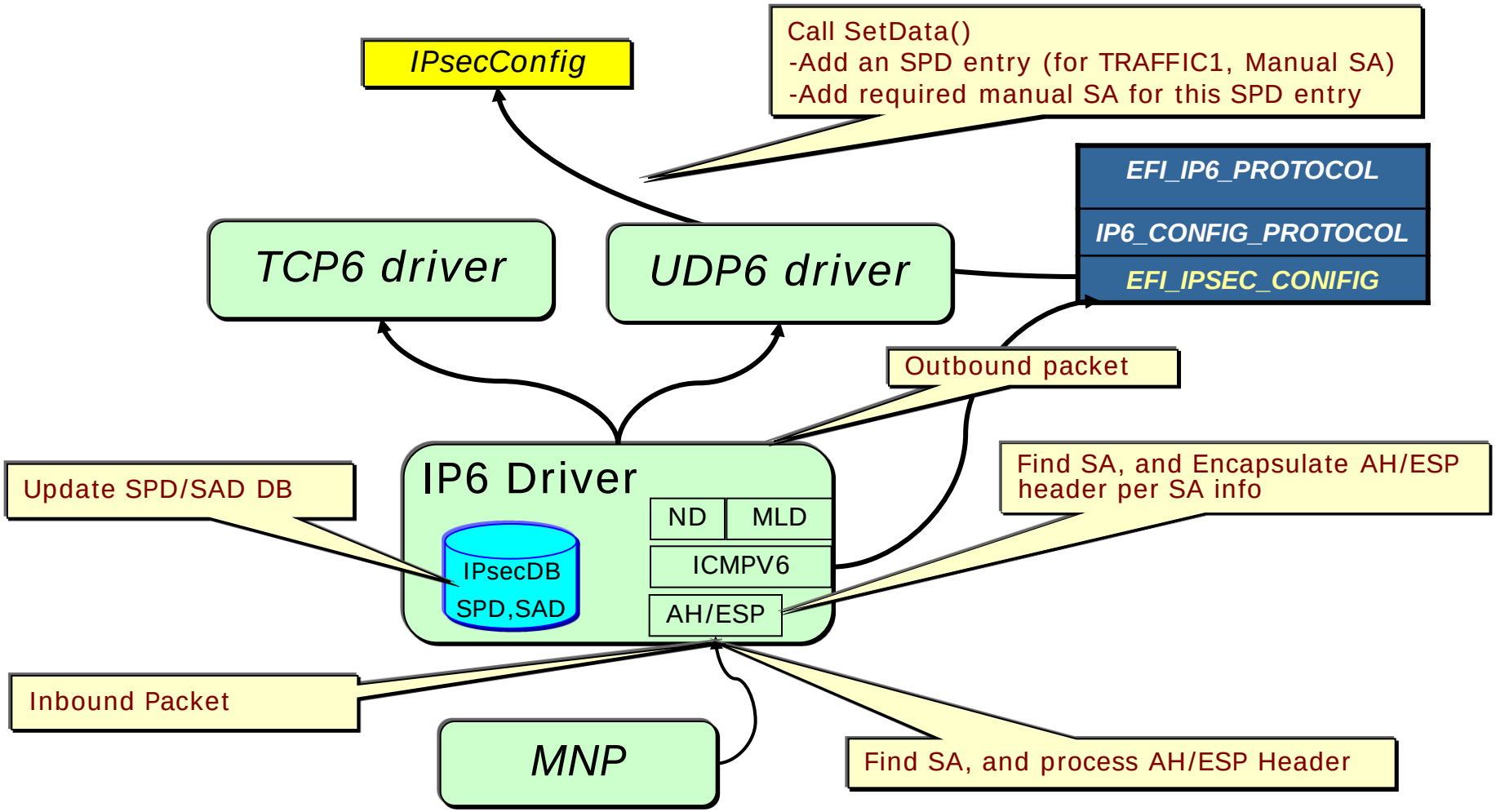


UEFI Authenticated Variable

- Variable is “valuable” information for platform
- Write-protected Variable service, based on asymmetric key technology
- Pre-defined variables for platform mode switching & key exchange between Firmware and OS



UEFI IPsec (Pre-deployed SA)

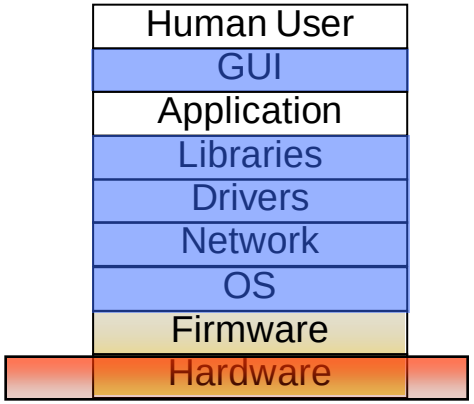


UEFI Security Continues to Evolve

Agenda

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

Hardware Best Practices



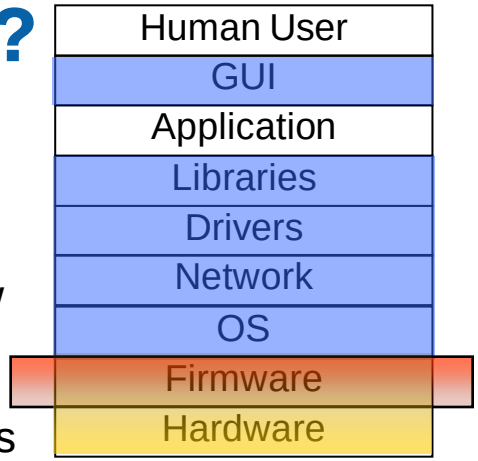
- CRTM Flash Protection
  - Locking must not be controlled by any un-trusted programmable entities
  - Once locked within CRTM code, it must not be un-lockable without going through a system reset
- Physical Presence
  - Physical Presence (PP) hardware must not be changeable by any un-trusted programmable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

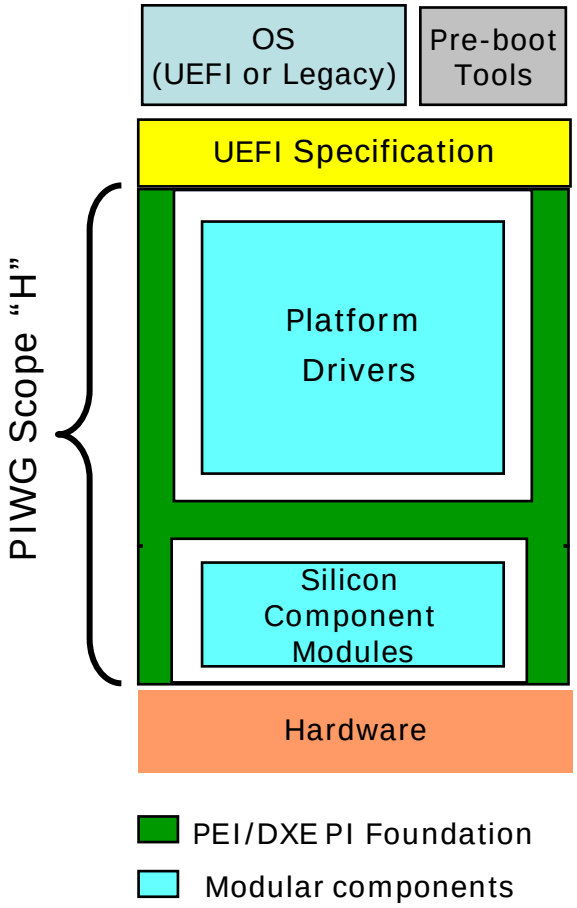
Hardware is a key part of root of trust

Agenda

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

What About Firmware Practices? UEFI PI Overview

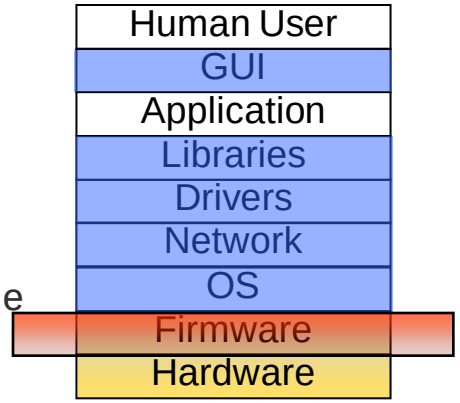




- UEFI 2.3 (published) specifies how firmware boots the OS loader
- UEFI's Platform Initialization Architecture specifies how modules initializing SI and the platform interact and provides common services for those modules
- PI DXE is the preferred UEFI Implementation
- PEIMs and DXE drivers to implement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

UEFI PI Best Practices



- Hardware 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

- Background & Motivation
- Best Practices on Platform Security
  - Trusted Computing Elements
  - UEFI Security Overview
  - Hardware Rules
  - UEFI PI & Firmware Practices
- UID & Byosoft Practices on PBA

UEFI User Identification

Authentication over platform & identifier

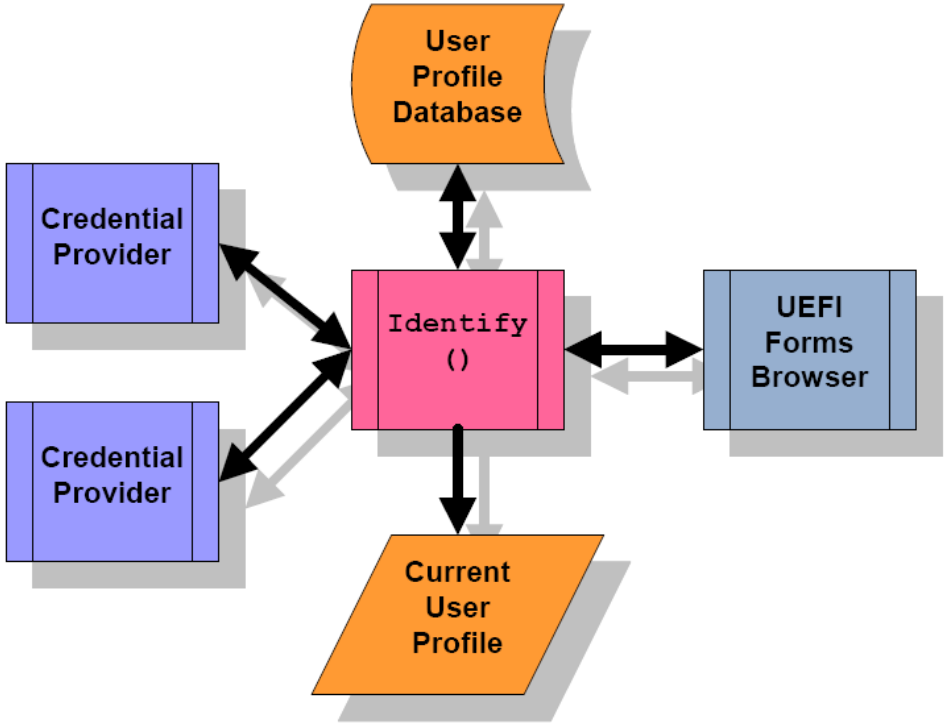
- User authentication prior to the OS loading
- Better resource control - identifier-based platform
- SSO vision
- Independent of OS and applications (push authentication into pre-boot environment)

Concepts:

- User profile
- Single-factor/Multi-factor
- Enroll
- Credential
  - What you know (Password)
  - What you have (Smart Card)
  - What you are (Fingerprint)

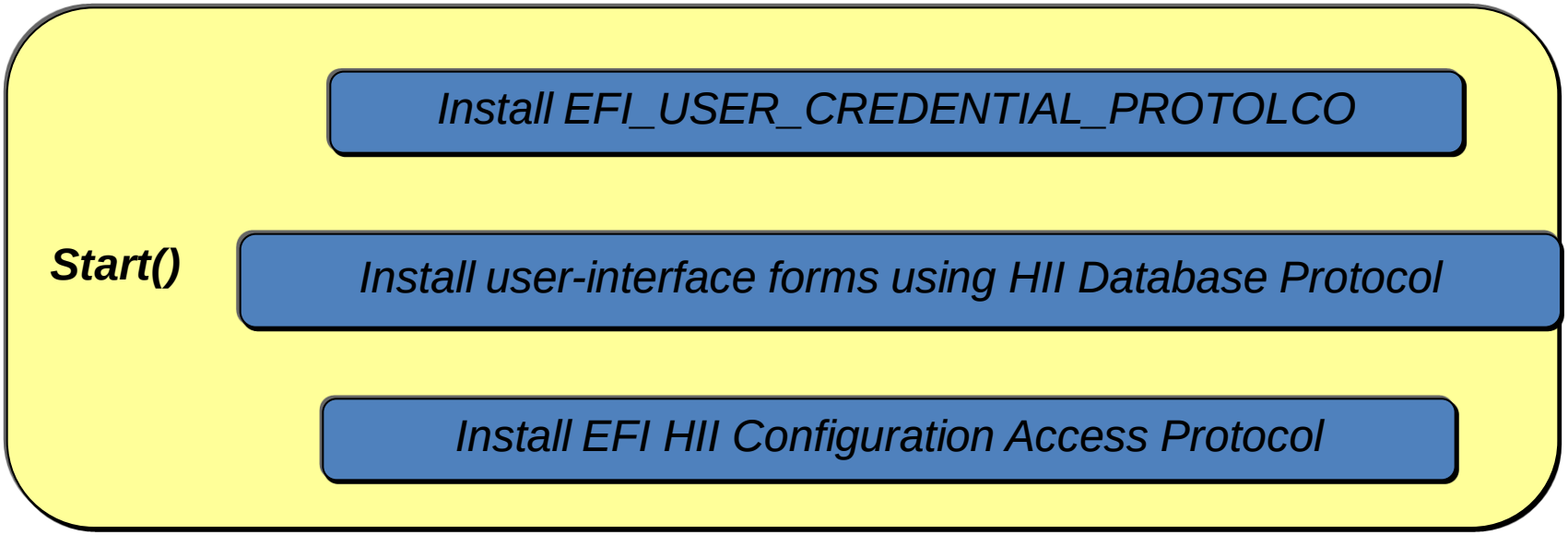
Components in UEFI UID

- User Identity Manager
  - User Information
  - User Identification Policy
  - User Privileges
- Credential Provider
  - Fingerprint sensor
  - Smart Card
  - Password
  - Network Authentication
- Access Control
  - Access Policy



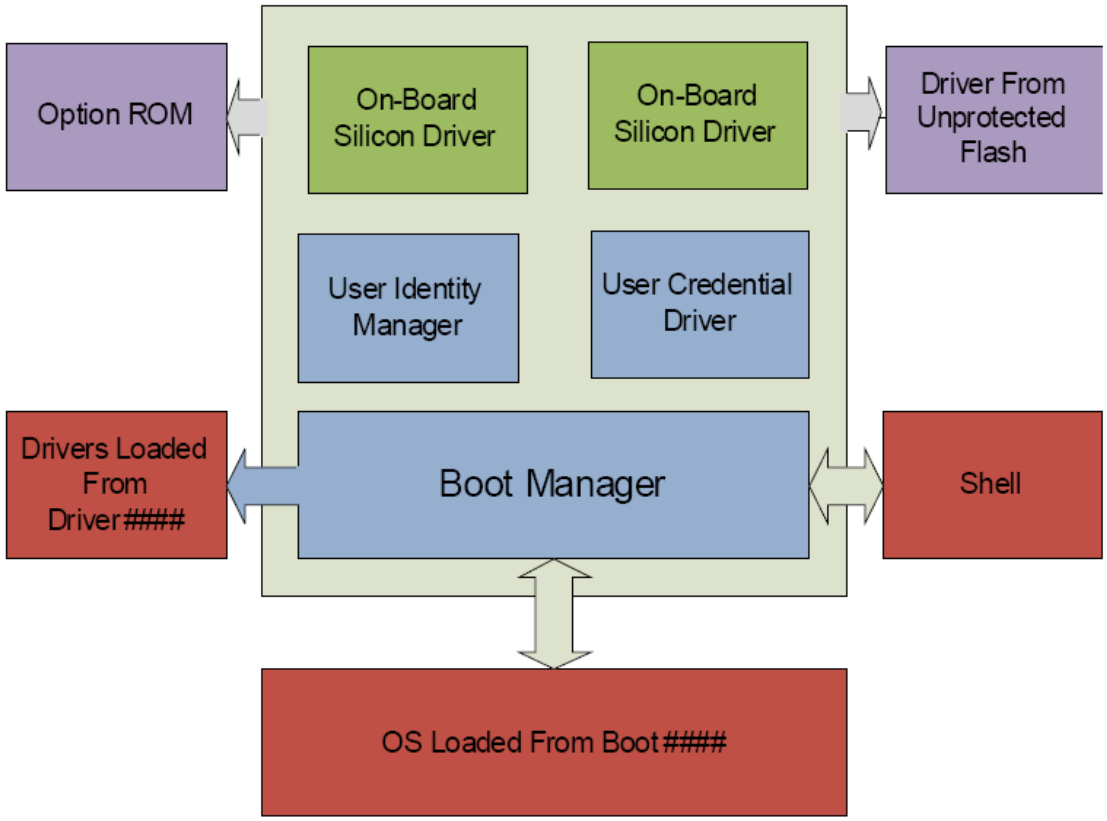
Credential Provider Driver

- Follow the UEFI Driver Model



- UEFI Spec does not explicitly support passing credential info to OS. The EFI System Configuration Table is a place to store the encrypt credential info to an OS-present driver or app.

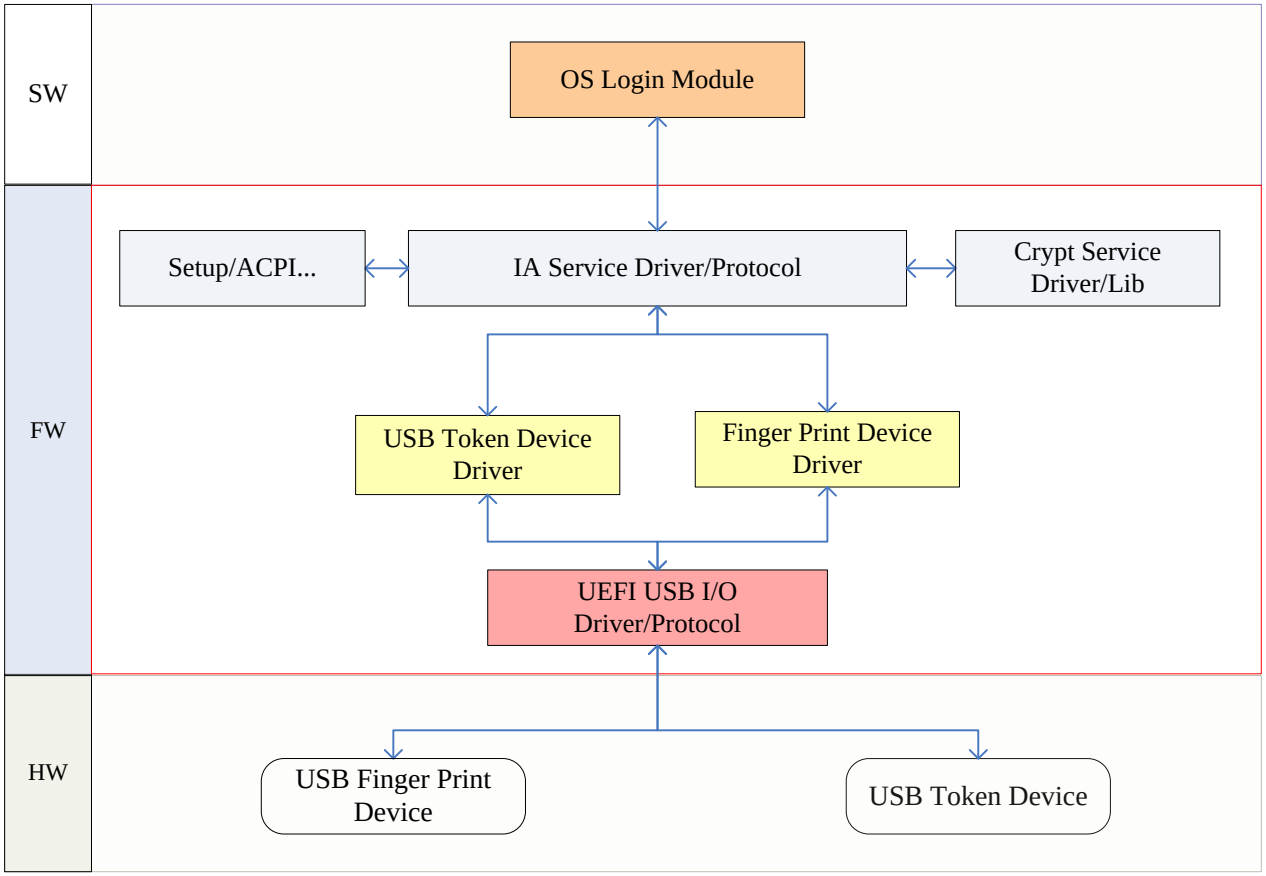
Security Considerations



The drivers which be loaded from unprotected location should be verified.

Byosoft UID Practice

- Fingerprint and USB smart card implementation using two protocols



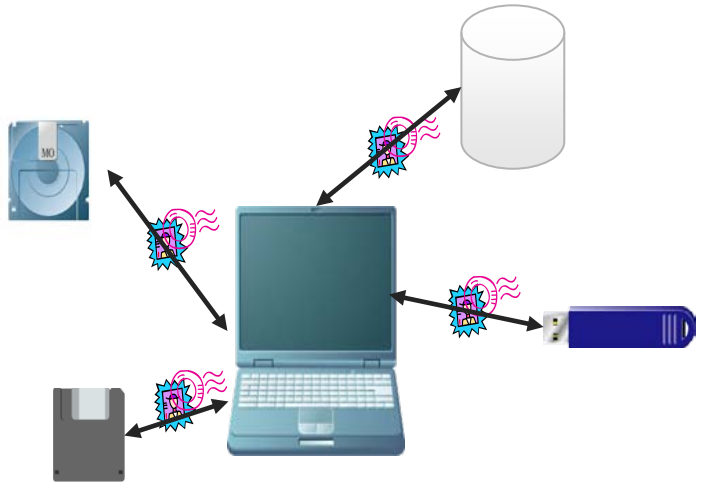
Byosoft UID Extension: Mutil-User/OS

UID is the foundation of many security functions, such as Mutil-User/OS

- **Separate storage space for individual**
- **Boot different OS from each space**
- **Feature:**
  * One machine can be used by different users
  * Combines with the UID, provides more functions

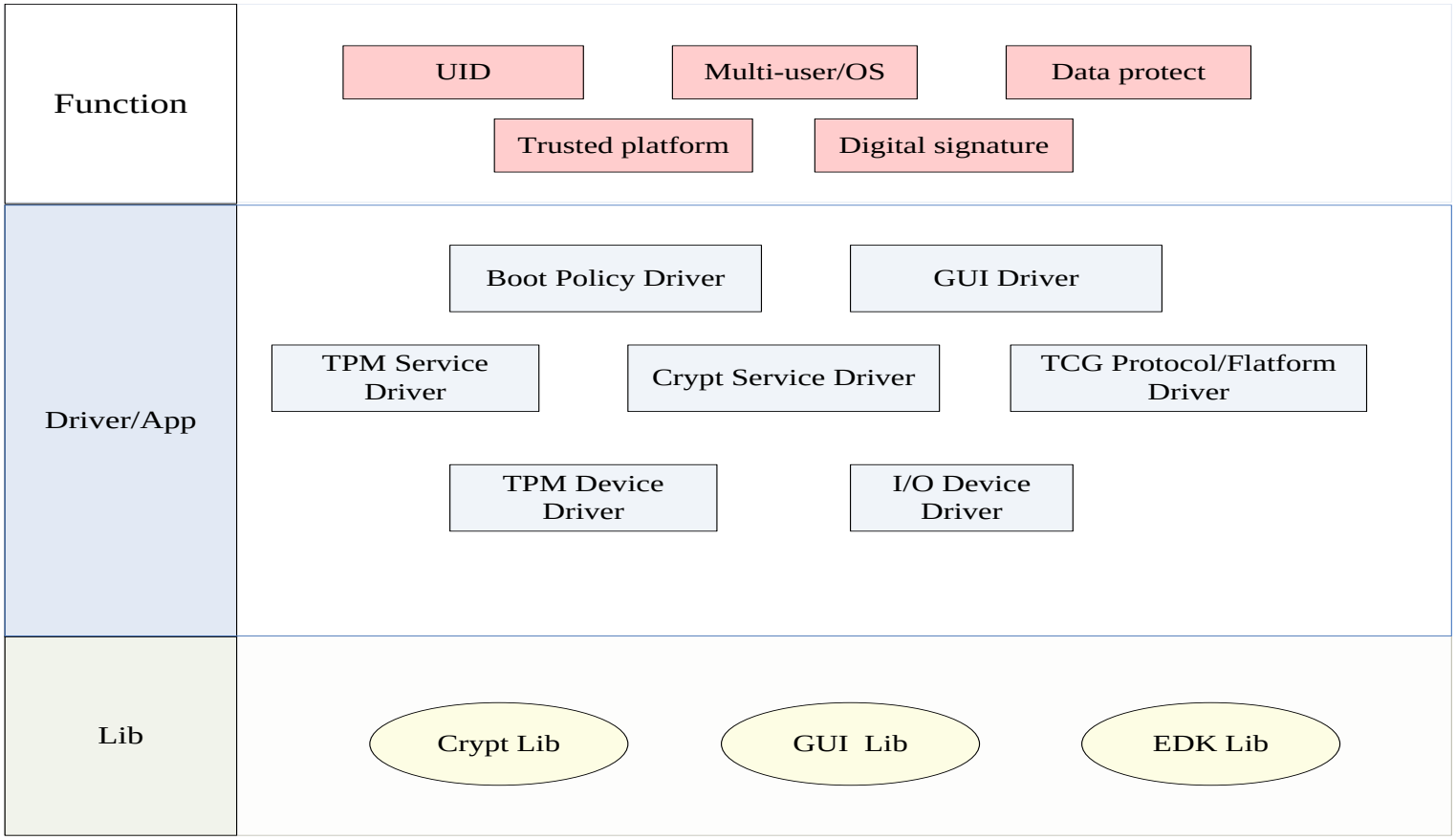
Byosoft UID Extension: Pre-boot Data Protection

- One access control mechanism for preserving confidentiality
- Two methods:
  * Pure software
  * Using 3th party hardware (TPM or other) to improve the secure level
- Features:
  * Be independent of OS
  * Binds secret data with platform
  * Simple to deploy



UID is the naturally KEY for Cryptology algorithms

Byosoft Platform Security Practices



Firmware completes the platform trust solution

Summary

- Security problems in the industry are real
- Trust and a security architecture can address some needs, especially hardware and firmware
- Follow best practices on hardware and firmware configuration and implementation
- UEFI and hardware security evolution

Next Steps – Security Requirements

- Use the trusted device
- Follow best practices on hardware and firmware
- Get involved in UEFI and Trusted Computing forums
- Download the Security white paper: http://download.intel.com/technology/efi/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications and Implementation sites: www.tianocore.org, www.uefi.org, www.intel.com/technology/efi
  - Security Whitepaper: http://download.intel.com/technology/efi/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf
  - Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress
  - UEFI Plugfest Event at Intel in Dupont Washington, June 22-25, 2010 www.uefi.org or email: laurie.jarlstrom@intel.com

IDF 2010 UEFI Spring Sessions
April 14

EFI#	Company	Description	Time	RM
S001 ✔	Intel, IBM, HP	Using the Latest EFI Development Kit (EDK II) for UEFI Advanced Development and Innovation	11:10	302AB
S002 ✔	Intel, HP, Byosoft	Notebook Advancements for Unified Extensible Firmware Interface (UEFI) for Pre-boot Productivity	13:00	302AB
S003 ✔	Intel, Byosoft	Unified Extensible Firmware Interface (UEFI): Best Platform Security Practices	14:00	302AB
S004	Intel, Microsoft, Insyde	UEFI Fast Boot for Microsoft* Windows* 7 : Fast Boot Without Compromising your BIOS	15:00	302AB
S005	Intel, Inspur, Insyde	UEFI Firmware Solutions for Enterprise Servers: A Case Study in 8-way Processor Support	16:00	302AB

✔ 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/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

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 first 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. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; 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; defects or disruptions in the supply of materials or resources; 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; product mix and pricing; 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; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; the timing and execution of the manufacturing ramp and associated costs; and capacity utilization;. 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 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 the timing of closing of acquisitions and divestitures. 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. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting our ability to design our products, or requiring other remedies such as compulsory licensing of intellectual property. 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.

Rev. 1/14/10