Secure Firmware Lockdown through Standardized (UEFI) Management Protocols

Vincent Zimmer
Principal Engineer, Intel
Anand Joshi
Sr. Developer, Dell Inc.
Marty Nicholes
Architect, Insyde Software

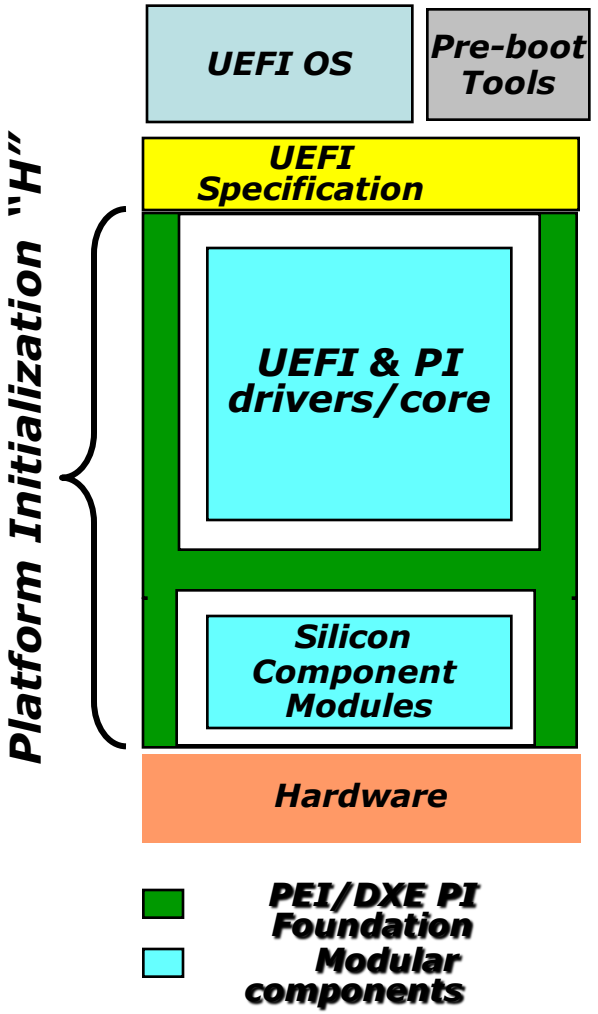
EFIS002

Sponsors of Tomorrow.™ intel

AGENDA

- Why Firmware (FW) Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

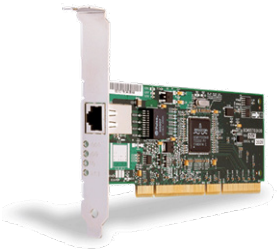
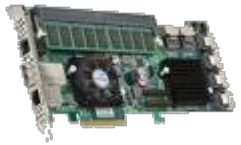
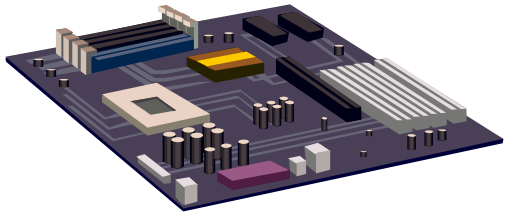
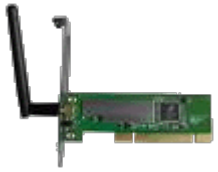
UEFI & PI Security Evolution



- UEFI 2.0
  - BIS, UEFI driver signing, Hash protocol, Authentication info
- UEFI 2.1
  - Authenticated-Write Access for UEFI Variables
- UEFI2.2
  - IPsec, Authenticode addition to driver signing, Driver / loader verification, User Identification
- UEFI2.3
  - ***Firmware Management protocol***
    - ***Assurance & interoperability around 'updates'***

What is Firmware Management

- Today's system contains number of firmware from various vendors
  - System BIOS
  - Network
  - Storage
  - Etc.
- Firmware Management is Keeping track of firmwares in the system

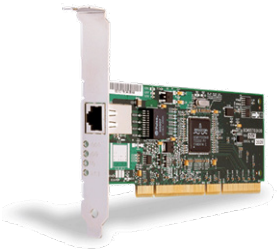
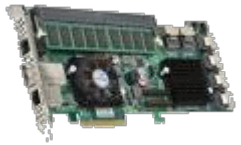
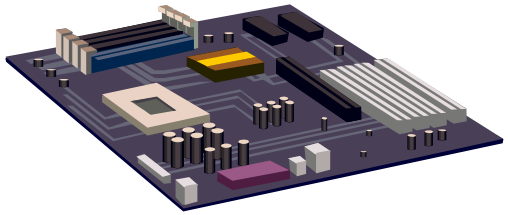
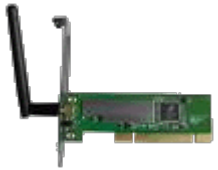






Firmware Management Lifecycle

- Having the right firmware level when the system is deployed
  - IT policy
  - The latest

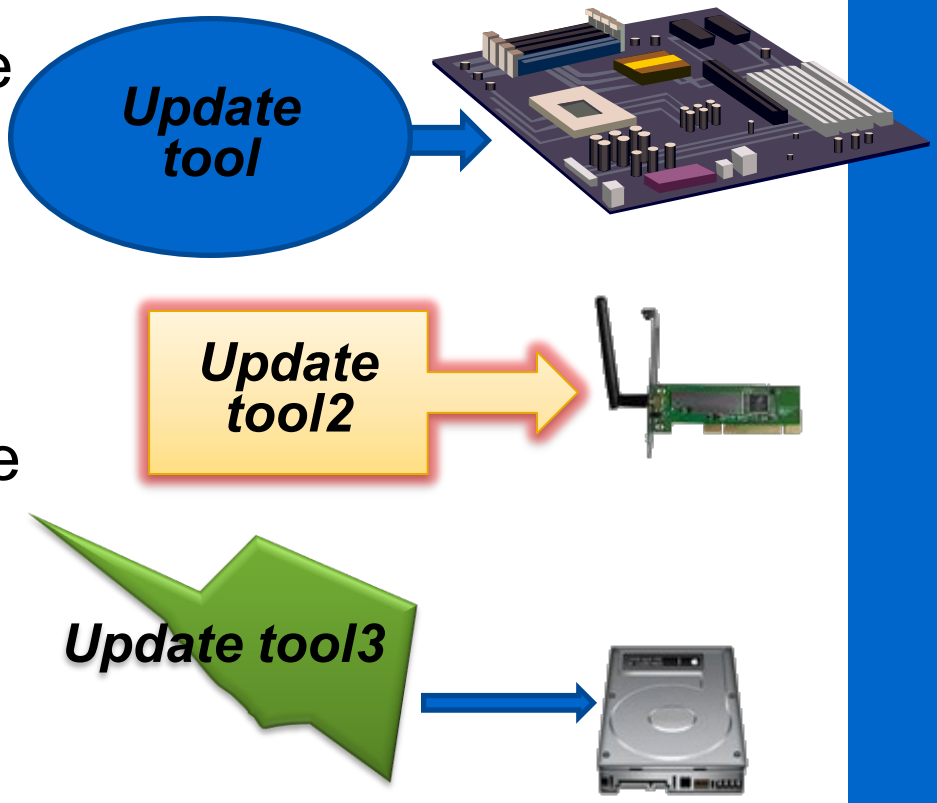
  Or

  - Goldilocks
- Maintaining firmware during the life of the system
  - Bug fixes
  - Performance improvement
  - Etc.


Why Firmware Management Protocol

- IHVs need to provide update packages for different OS
  - Windows*
  - Linux*
  - Some other flavors
- Every vendor has a separate tool
  - Different UI
  - Different scripts



Result: More complexity, more IT cost

Why Firmware Management Protocol

- At the abstract level firmware management involves common set of functionality
  - Locating the device
  - Identifying the current firmware level
  - Update the firmware image

Need for OS agnostic standardized Firmware Management

AGENDA

- Why Firmware (FW) Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

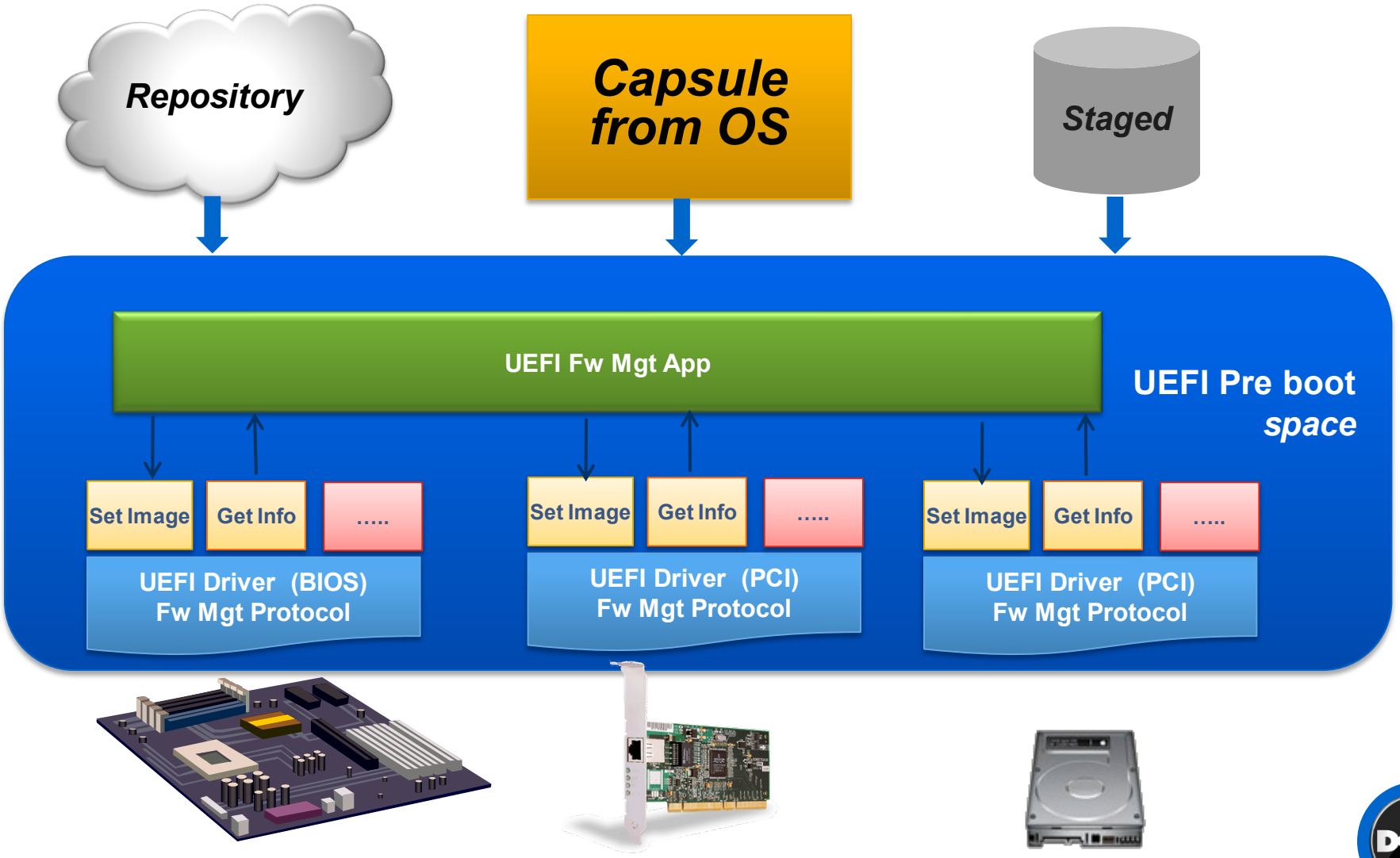
Firmware Management Protocol

- Industry standard interface
  - Defined in UEFI 2.3 Specification
- Abstracts device firmware management to common set of API
- Enables common management of different firmware using single interface / application

Firmware Management Protocol Overview

- Get information on firmware image(s)
- Check if firmware image is valid
- Program device with new firmware image
- Get a copy of firmware image
  - For management purposes
- Label all firmware images within a device

Possible Update Scenarios



AGENDA

- Why Firmware (FW) Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

FMP: Image Info/Image Descriptor

```
**********************************************************
// EFI_FIRMWARE_IMAGE_DESCRIPTOR
//
**********************************************************
typedef struct {
  UINT8                         ImageIndex;
  EFI_GUID                      ImageTypeId;
  UINT64                        ImageId;
  CHAR16                        *ImageIdName;
  UINT32                        Version;
  CHAR16                        *VersionName;
  UINTN                         Size;
  UINT64                        AttributesSupported;
  UINT64                        AttributesSetting;
  UINT64                        Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

Version: Numerical representation of versioning scheme

1.2 = 102

1.10 = 110

Newer version is always numerically greater than the older one.

FMP: Image Info/Image Descriptor

```
**********************************************************
// EFI_FIRMWARE_IMAGE_DESCRIPTOR
//
**********************************************************
typedef struct {
  UINT8                         ImageIndex;
  EFI_GUID                      ImageTypeId;
  UINT64                        ImageId;
  CHAR16                        *ImageIdName;
  UINT32                        Version;
  CHAR16                        *VersionName;
  UINTN                         Size;
  UINT64                        AttributesSupported;
  UINT64                        AttributesSetting;
  UINT64                        Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

VersionName: Text representation of versioning scheme

110 = L"1.1.0" or 110 = L"1.10"

102 = L"1.2" or 102 = L"1.0.2"

Used for display purpose

FMP: Image Info/Image Descriptor

```
  CHAR16                          *VersionName;
  UINTN                           Size;
  UINT64                          AttributesSupported;
  UINT64                          AttributesSetting;
  UINT64                          Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

- Value based on the current hardware support

FMP: Image Info/Image Descriptor

```
  CHAR16                              *VersionName;
  UINTN                               Size;
  UINT64                              AttributesSupported;
  UINT64                              AttributesSetting;
  UINT64                              Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

0x10001

0x20001

0x10001

0x20001

FMP: Image Info/Image Descriptor

```
  CHAR16                              *VersionName;
  UINTN                               Size;
  UINT64                              AttributesSupported;
  UINT64                              AttributesSetting;
  UINT64                              Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

- The typical usage of the compatibilities is for update app to make sure that the new image is compatible with the hardware.
- How the FW Mgt App will get the compatibility value for the image to be updated is out of UEFI spec leaving room for further innovation.☺
- FMP Check and Set routines should always do the internal compatibility check.

FMP: Image Info/Image Descriptor

```
  CHAR16                          *VersionName;
  UINTN                           Size;
  UINT64                          AttributesSupported;
  UINT64                          AttributesSetting;
  UINT64                          Compatibilities;
} EFI_FIRMWARE_IMAGE_DESCRIPTOR;
```

- Way to provide instruction to the update app like
  - IMAGE_ATTRIBUTE_RESET_REQUIRED – Reset the system after update. FMP does not reset the system on its own. Single reset after multiple updates
  - IMAGE_ATTRIBUTE_IN_USE – May be update app needs to stop the device driver before update
  - IMAGE_ATTRIBUTE_AUTHENTICATION_REQUIRED – We check ID!

AGENDA

- Why Firmware (FW) Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

Why Bother with Security?

- FW Management Protocol makes it easy
  - For trusted and untrusted users

"With great power, comes great responsibility"

Spiderman

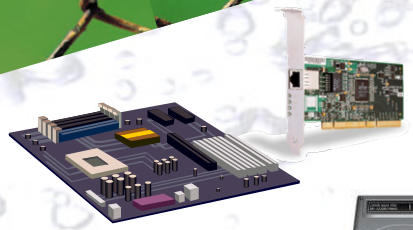
- One interface to affect many modules

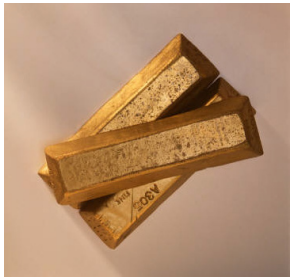
Potential Security Layers

FW Management Remote Service

FW Management Application

FW Management Protocol





Adding Security to FW Management

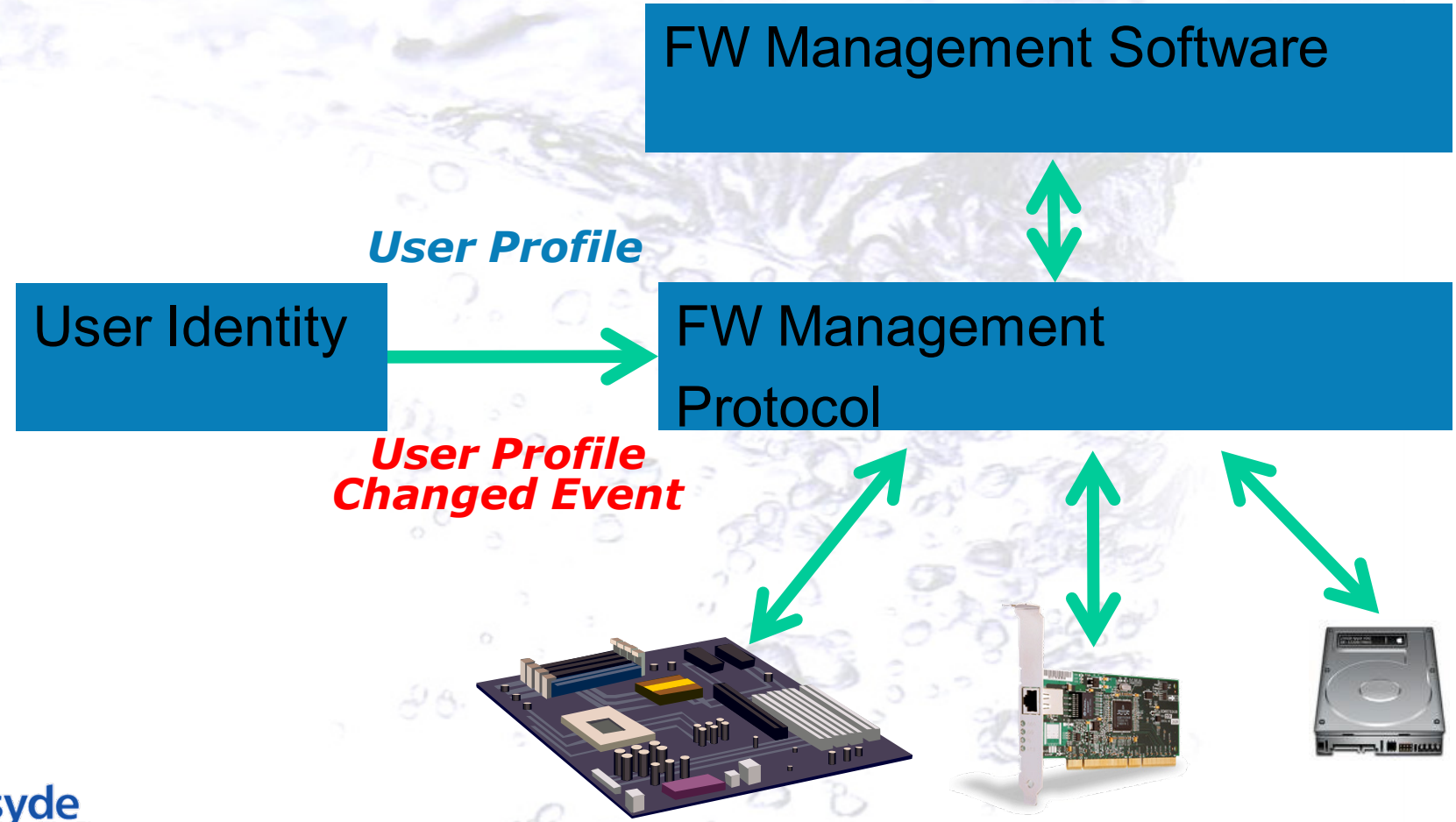
- Protect Access to Protocol
- Validate Image
- Authenticate Image

Protect Access to Protocol

- Require Credentials
  - User Identity Manager from UEFI
  - FW management protocol notified about user
- Conditional load of Protocol
  - LoadImage can defer image execution for security
    - User privileges not correct
    - EFI_DEFERRED_IMAGE_LOAD_PROTOCOL
- Physical access requirements
  - Verify user has physical access to platform

Know who is using the Firmware Management Protocol

Require Credentials



Validate Image

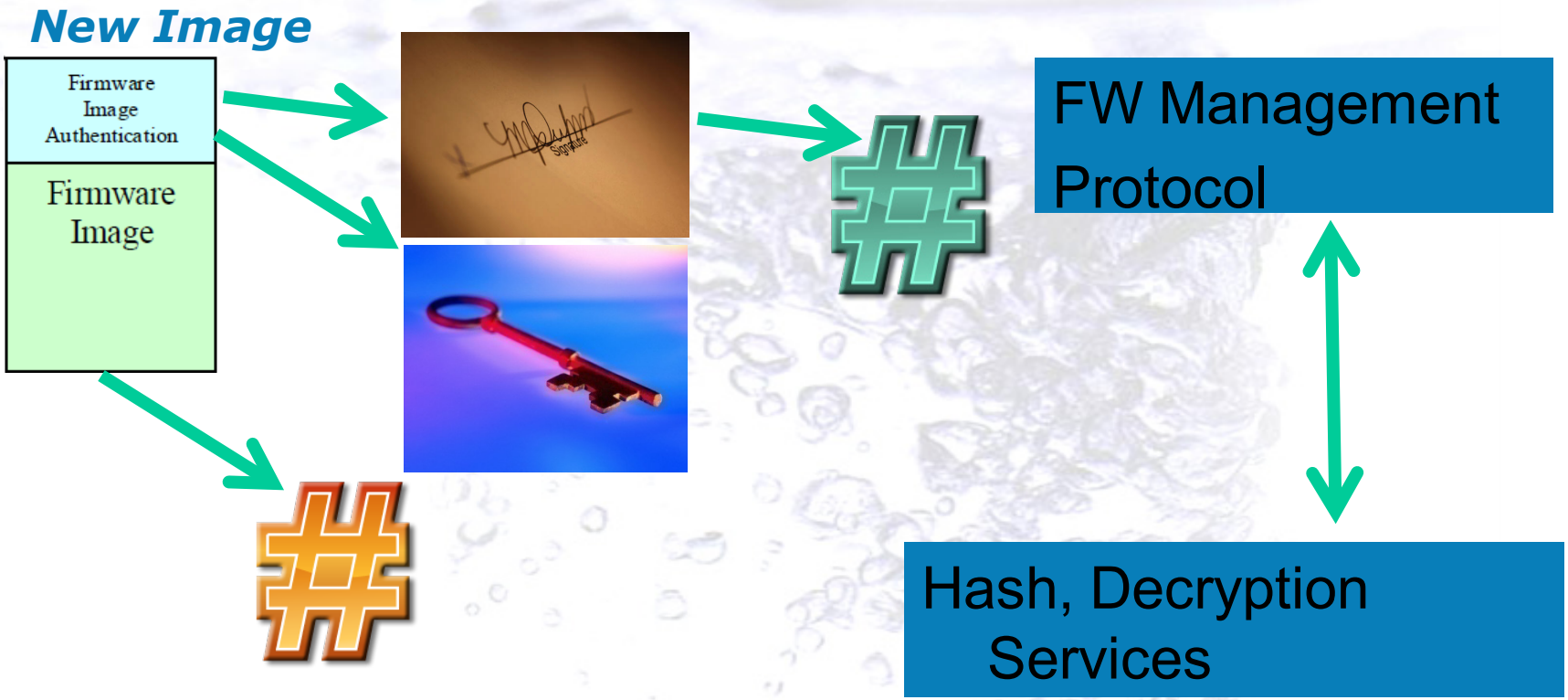
- Correct format for firmware image
  - Protection by obscurity – low security value
  - May prevent brick syndrome
  - Acceptable if device has internal security
    - Possible denial of service attack
- Use vendor specific policy
  - Can allow older firmware to be used

Authenticate Image

- Adds information to firmware image
  - Minimum information
    - Public Key
    - Signature
  - Can verify image source
  - Can verify image integrity
- Will require security support
  - UEFI Key Exchange, Hash & Decryption protocols
- Set image attribute
  - IMAGE_ATTRIBUTE_AUTHENTICATION_REQUIRED

Verify the image is good before commit!

Authenticate Image



Security Summary

- Protect the Firmware Management Protocol
- Validate or Authenticate the images

Secure the Firmware Management Protocol

AGENDA

- Why FW Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

Implementing FMP: UEFI Driver

- FMP implemented as a non-device driver
  - For BIOS, Management Firmware etc.
  - Installed with new handle
  - In this case management app strictly depends on information provided in image descriptor

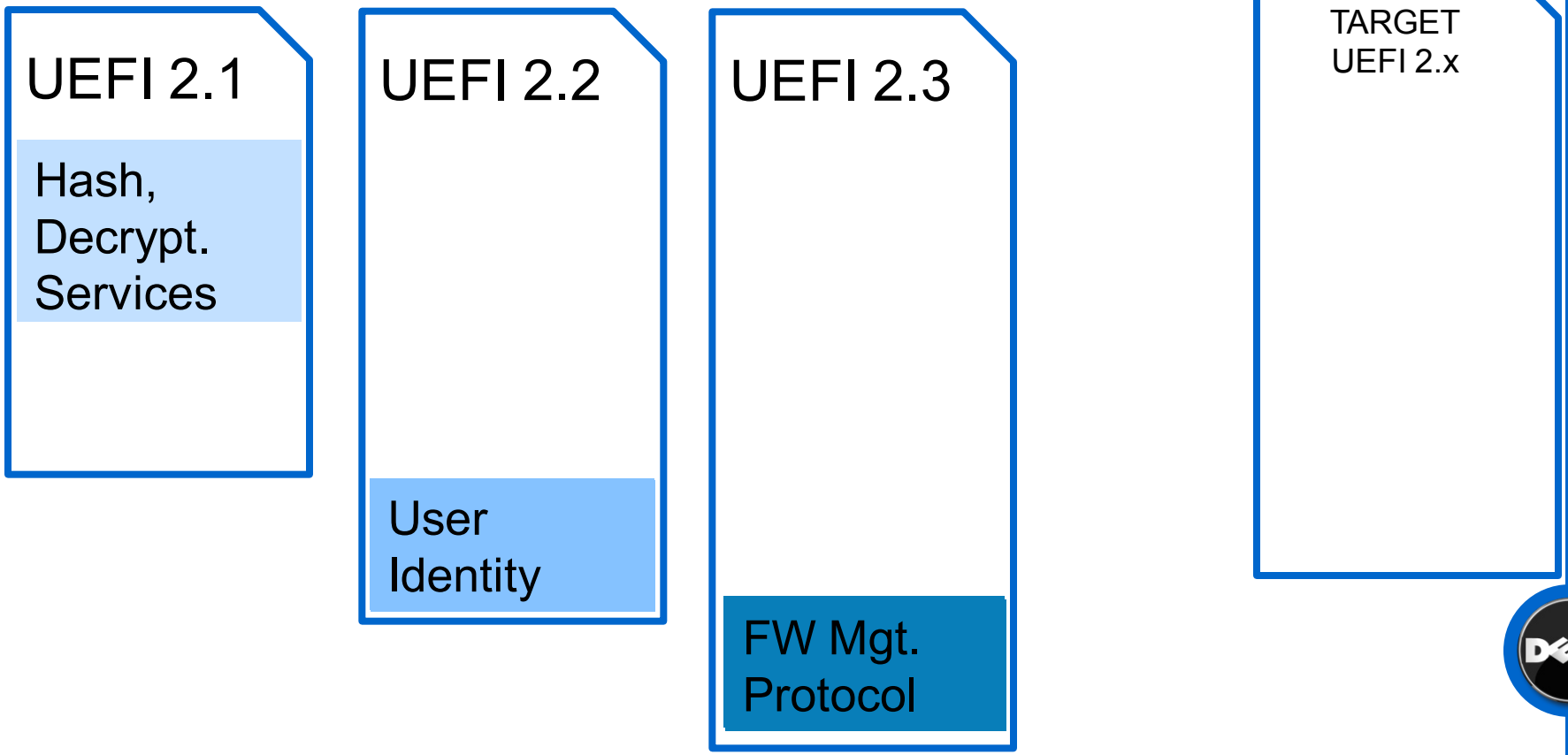
Implementing FMP: UEFI Device driver

- FMP implemented as a part of device driver
  - For PCI devices
    - Storage
    - network
    - Etc..
  - Installed on the same handle as the controller handle
  - Associating with the device allows management app to gather more relevant information like
    - Device ID, Vendor ID
    - Device Class
    - Component Name Too

Choose right implementation for added benefit

Implementation flexibility

- UEFI spec always builds on top of the previous one
- Choose your base support level
- FMP can be implemented independently
- Choose security measures as your base implementation

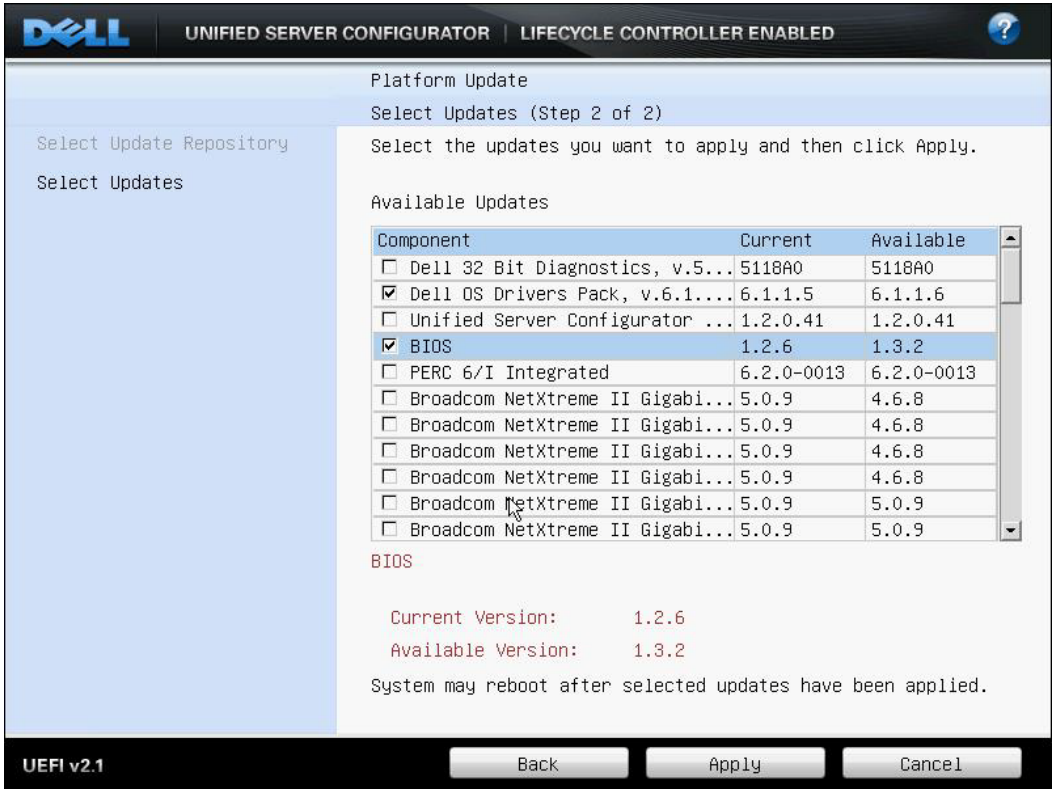


AGENDA

- Why FW Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Implementing FMP
- Demo

Demo

- Unified Server Configurator is Dell's embedded deployment infrastructure based on UEFI 2.1
- Dell's update manager that uses UEFI Firmware Management Protocol
  - Provides ability to upgrade or downgrade firmware image



AGENDA

- Why FW Management in UEFI
- FW Management Overview
- Some FW Management Subtleties
- Security and FW Management
- Demo
- Summary / Take aways

Summary/Take Aways

- Proprietary interface to common set of functions is not efficient
- Firmware management protocol makes managing firmware easy
- FMP abstracts only the external interface not the actual update logic allowing a common UI for all firmware updates
- FMP is part of UEFI 2.3 spec but can be implemented independently
- FMP is required for Dell enterprise servers
- Securing Firmware Management Protocol is essential

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- Visit UEFI Booth #136 & Insyde SW #312
- 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 Sessions

EFI#	Company	Description	Time	RM	D
P001 ✓	Dell, HP, IBM, Intel, Microsoft	Using UEFI as the Foundation for Innovation	10:15	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	UEFI Q & A session	15:40	2002	Th

✓ DONE

Session Presentation 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

Backup Slides

FMP: Get Image Info

- Retrieves Information about the firmware image(s) supported by the instance of FMP
  - BIOS
  - Option ROM1(Legacy), Option ROM2 (UEFI) …
  - Option Rom or Controller firmware