IDF2013
英特尔信息技术峰会

构建裸机安全
—增强并利用安全平台的实践

魏 东, 院士, 惠普
龙 勤, 软件架构师, 英特尔
沈 杰, 高级安全顾问, 迈克菲

PTAS002

英特尔®与你共创明天™ intel®

议程

- UEFI 及其安全处理概述
- 平台安全强化实践
- McAfee* Endpoint Encryption与安全启动

本课程演示文稿（PDF）发布在技术课程目录网站:
intel.com/go/idfsessionsBJ

该网址同时打印于会议指南中专题讲座日程页的上方

UEFI 及其安全处理概述

魏 东
院士，惠普
副总裁，UEFI 论坛

UEFI 论坛的最新进展

- Linux Foundation已签署协议，成为UEFI论坛贡献者
- UEFI 2.3.1d 勘误表即将面世
- UEFI 2.3.1c SCT 最终草案即将完成
- UEFI 2.4 内容确定
- PI 1.3 内容确定
- UEFI 未来将考虑增加系统配置与管理能力

现实世界!

Researchers find attack on Millions of printers

Can a hacker take control of you printer? Using it to sniff informat from the network, steal confident information, or even attack other machines. Researchers have foun attack impacting millions of printe around the world.

Is Mebroot the stealthiest Rootkit in the world?

Federal agents raided unnamed operators of the Rustock "botnet" vast network of computers aroun the globe infected with malicious software that allows distribution huge volumes of spam.

Link Discovered Between TDSS Rootkit and DNSchanger Trojan

TDSS rootkit, the sophisticated and difficult to remove malware behind many advanced attacks also appears to have helped spread the DNSchanger Trojan.

Researcher finds attack on Apple battery firmware. [Blackhat 2011]

The firmware used to control the charging of Apple's laptop batteries could be attacked by malware. Allowing the attacker to potentially override safety mechanism which could lead to an attack.

Advanced Persistent Attacks: BIOS Rootkit -"Mebromi"

Hamza Sirag, Nihant Bondugula, Rishabh Gupta
Graduate School of Computer Science, George Mason University, Fairfax, VA

1. Abstract

As cyberspace has evolved malware has also evolved. According to the United States Computer Emergency Readiness Team, malware is defined as malicious software that consists of programming (code, scripts, active content, and

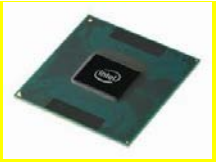
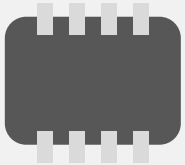
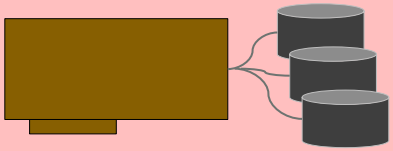
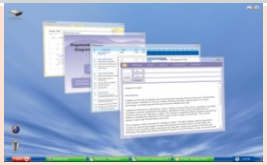
vulnerabilities associated with Mebromi, the tools that take advantage of those technological vulnerabilities, mitigation of the technological vulnerabilities, future of advanced persistent attacks, future of BIOS targeting, and provide a conclusion summarizing our research.

DE MYSTERIIS DOM JOBSIVS: EFI ROOTKITS

SNARE
@ SYSCAN SINGAPORE
APRIL 2012

assurance

资产与威胁

重启	资产	威胁
	**BIOS Flash** 硬件保护	ROM Swap Bit rot
	**System BIOS** - PEI 恢复 - SMM,UEFI Core - PK, KEK, CRTM	擦除flash 重写flash
	**Option ROMs** UEFI 驱动程序	擦除opROM 重写opROM
	**网络启动** 面向云计算的IPv6支持	网络攻击
	**预启动 UEFI 应用程序** OS 启动加载器	欺骗性UEFI应用

不同颜色代表不同供应商：

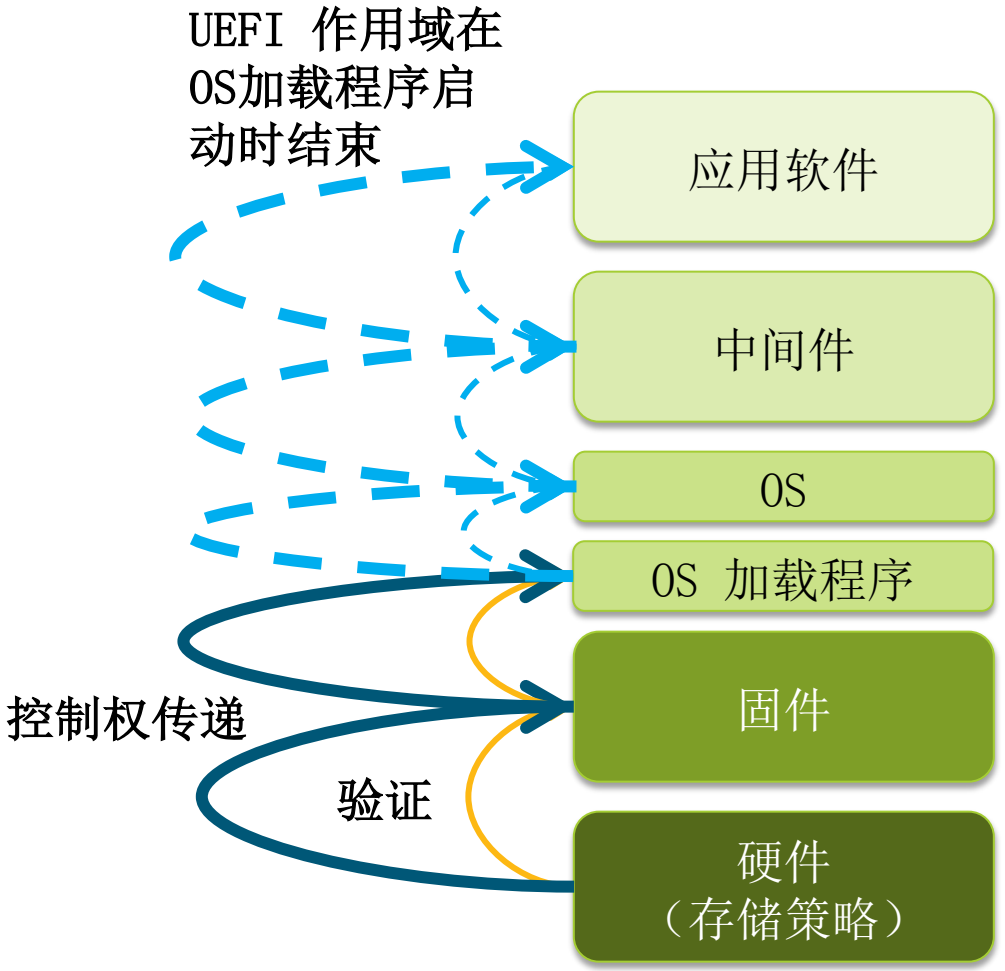
UEFI 安全 – 动机与历史

- 由于操作系统对攻击越来越具备抵抗能力，许多威胁开始瞄准启动链条中的最薄弱环节
- 历史
  - Phoenix* 发起安全启动需求的讨论
  - 针对这一方向，USST（UEFI 安全子组）成立
  - UEFI 2.3 规范定义了安全启动体系结构
  - UEFI 2.3.1 规范中，微软*为安全启动增加了一些额外的功能
    - 针对认证变量的Append支持
    - 基于时间戳的认证变量，防止rollback攻击
    - 授权 UEFI 使用Authenticode规范
    - Windows* 8 中对 UEFI 安全启动的支持

UEFI 安全支持是工业界共同努力的结果

UEFI 安全启动：强化启动策略

- UEFI 安全启动的概念是对引导链条中每一组件进行*验证*，并在其被允许执行前，根据给定的平台策略进行*授权*
- 可以利用数字签名，预先加载的哈希值等机制实现 UEFI 安全启动策略



从裸机开始保障安全

- UEFI 2.3.1 中的安全性增强功能专门解决“安全启动”问题
- 保障固件自身安全可进一步强化 UEFI 安全启动概念
  - *固件更新如何进行保护?*
  - *如何将固件置于“管理模式”?*
- NIST 制定了 BIOS 保护指南
  - 固件安全更新要求
  - 维护固件的核心信任根
- UEFI 2.3.1 包含用于开发安全固件更新的框架

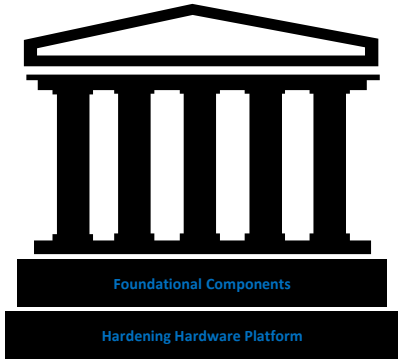
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

平台安全强化实践

龙 勤
软件架构师，英特尔

从一开始就关注安全性设计

- 实施纵深防御
  - 在设计与实现安全机制时，考虑使用多个保护层
- 安全性不依赖于“晦涩”的设计
- 智能、可靠、安全的故障恢复机制
  - 不要给黑客提供线索（例如，出错时暴露信息）
  - 记录错误与失败信息以方便审计
- 检查所有的返回值
- 保持安全关键代码的简短



开发实践 – 代码审查

- 避免不安全的函数调用（例如，类似gets()等函数）
- 使用 ASSERT 进行必要的错误检查
- 检查输入的有效性，拒绝其它一切无效输入
- 进行完整性检查和边界检查 – 类型、长度、范围、格式
- 当代码更改时，应尽可能广泛深入地进行验证，以防止意外的错误；并对编码的时间/性能进行均衡
- 注意边界情况（例如，off-by-one错误、数组下标）和附加条件（例如，反向逻辑）
- 不要实现自己构造的加密算法或协议

防御性编码 – 增加鲁棒性

- **在使用前对输入数据进行验证**
  - 网络数据包
  - 磁盘上的数据结构 / GPT表
  - UEFI变量
  - 设备路径
- **机密数据存储**
  - 尽可能避免
  - 使用完后清除缓冲区
- **密钥管理**
  - 对 PI 元素存储的访问控制. Intel® UDK2010 中基于 SMM 的认证变量驱动程序
- **模糊测试**
  - SCTs (Self-Certification Tests) – 正面测试，使用预期输入是否工作正常?
  - Fuzzing: 负面测试, 对非预期输入，会发生些什么？

不仅仅是功能校验

示例：可靠 vs 不可靠代码

示例：校验所有输入

```
PartEntry = AllocatePool (PrimaryHeader->NumberOfPartitionEntries
                          * sizeof (EFI_PARTITION_ENTRY));
Status = DiskIo->ReadDisk (
    DiskIo,
    MediaId,
    MultU64x32(PrimaryHeader->PartitionEntryLBA, BlockSize),
    PrimaryHeader->NumberOfPartitionEntries * (PrimaryHeader->SizeOfPartitionEntry),
    PartEntry
    );
```

A　B　C

存在的问题：

- 分配大小为 A 的内存
- 然而，ReadDisk中的块数据大小为 B
- 当代码读取GPT数据到 C 时，发生缓冲区溢出！

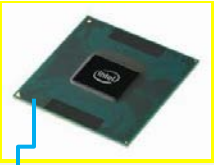
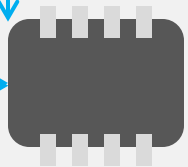
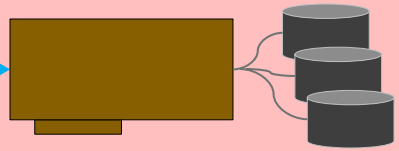
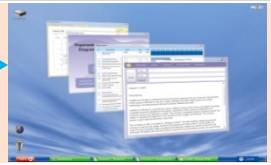
修复：

```
PartEntry = AllocatePool (PrimaryHeader->NumberOfPartitionEntries
                          * PrimaryHeader->SizeOfPartitionEntry);
```

输入检验的基本原理

UDK2010 代码示例：
http://edk2.svn.sourceforge.net/svnroot/edk2/trunk/edk2/MdeModulePkg/Universal/Disk/PartitionDxe/Gpt.c

技术 – 放在一起

重启	资产	威胁	
	**BIOS Flash** 硬件保护	ROM Swap Bit rot	Intel® 硬件
	**System BIOS** – PEI 恢复 – SMM, UEFI Core – PK, KEK, CRTM	擦除 Flash 重写 Flash	SP800 -147 Capsules
	**Option ROMs** UEFI 驱动程序	擦除 opROM 重写 opROM	UEFI 2.3.1c 规范
	**网络启动** 面向云计算的IPv6支持	网络攻击	
	**预启动UEFI 应用程序** OS启动加载器 *McAfee** *Endpoint Encryption*	欺骗性UEFI应用	

TCG Measurements into PCRs 0..7

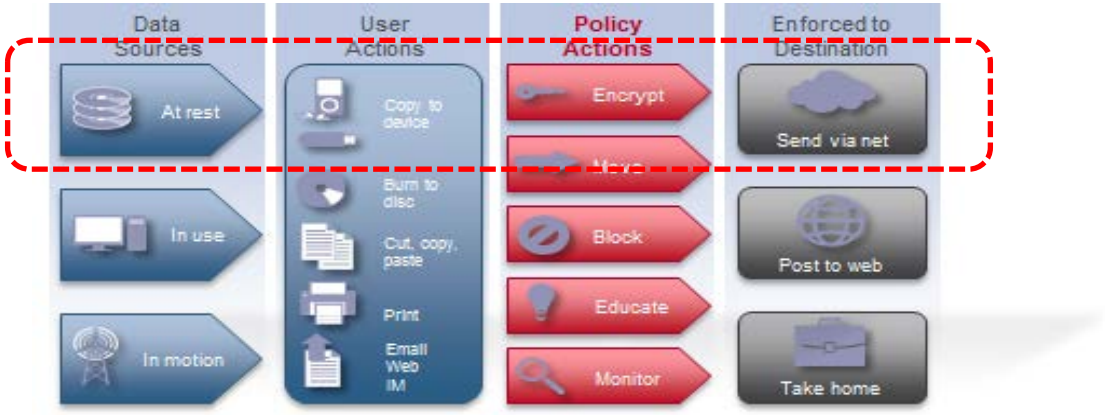
不同颜色代表不同供应商：

McAfee* Endpoint Encryption 与安全启动

沈 杰
高级安全顾问，迈克菲

产品概述

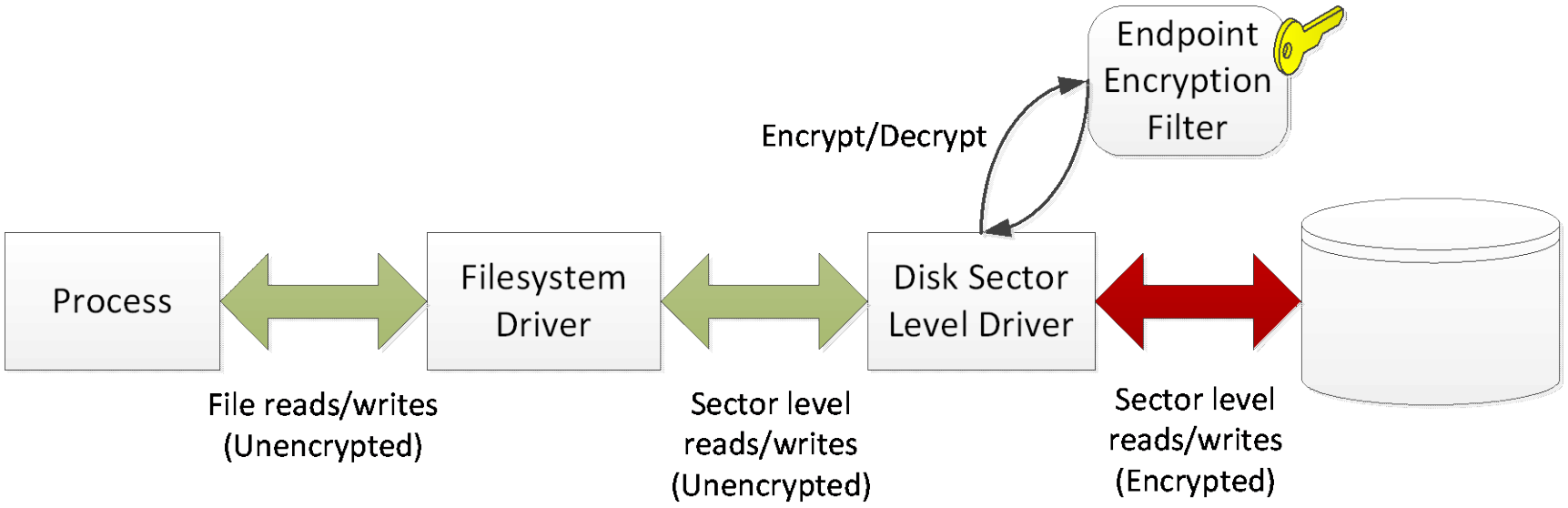
- McAfee* Endpoint Encryption是一个全磁盘加密产品
  - 提供 “静态数据” 保护



  - 操作系统数据和用户数据基于扇区级别进行加密
- 利用强加密算法保护数据
  - 多种数据加密方法可用
    - 基于软件的AES256 CBC (Cipher Block Chaining)实现
    - 利用AES-NI指令的硬件加速AES256 CBC实现
    - 自加密磁盘

什么是全磁盘加密?

- 以扇区级别加密数据
  - 产品没有目录或文件的信息
  - 加密对文件系统完全透明
  - 磁盘能够被部分加密，并仍可正常工作；这保证系统能够在使用过程中同时进行加密



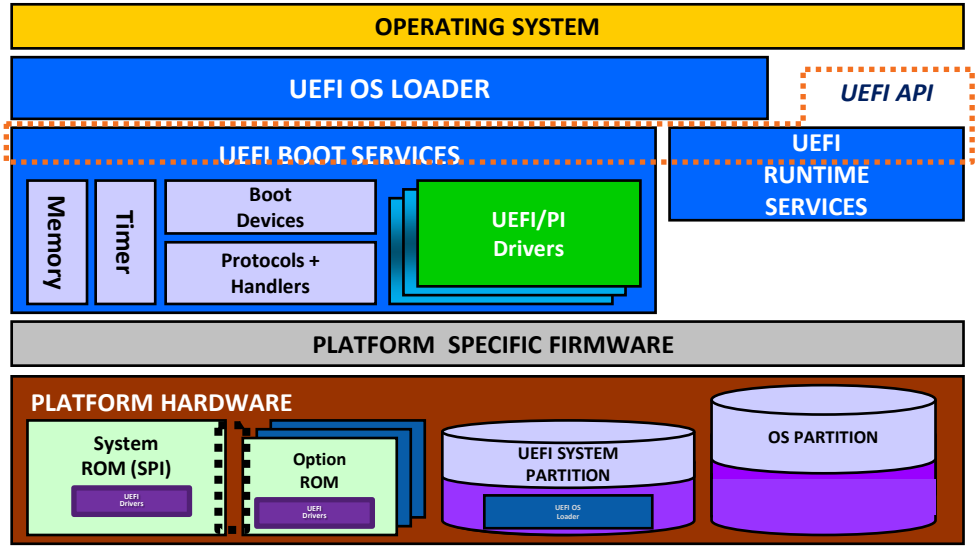
加密磁盘解锁

- 在用户完成身份认证，并获得加密密钥之前，加密磁盘上的数据无法访问
- 操作系统内核以及关键文件同样位于磁盘加密数据中
- 需要有一个“预启动应用程序”（PBA）进行身份验证和磁盘解锁

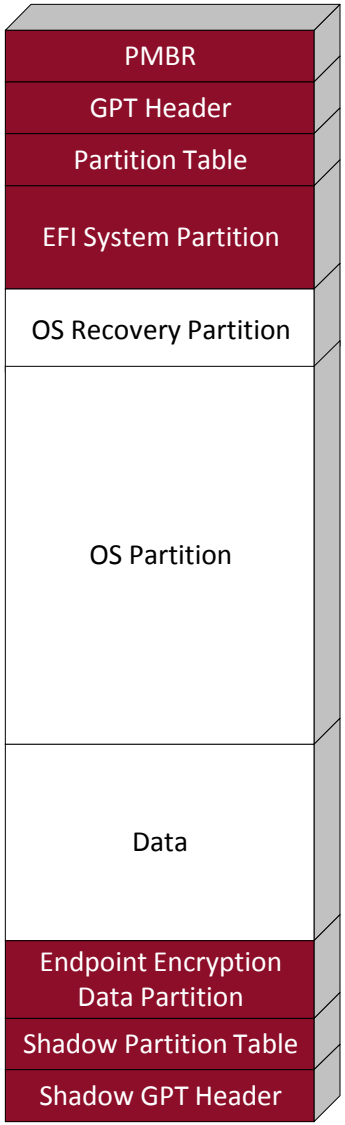
- 用户可以使用令牌、密码、智能卡、恢复进程等进行身份认证
- 一旦通过认证，令牌将释放磁盘加密密钥
- 磁盘加密密钥用于获取访问加密磁盘上的数据

McAfee* Endpoint Encryption PBA

- 一个 UEFI 应用程序
  - 在 Windows* bootloader启动前，由UEFI启动管理器进行加载
  - 使用标准的UEFI协议实现图形化（Graphics Output Protocol, Simple Pointer Protocol, 等.）
  - 使用标准USB协议支持USB智能卡读卡器和令牌

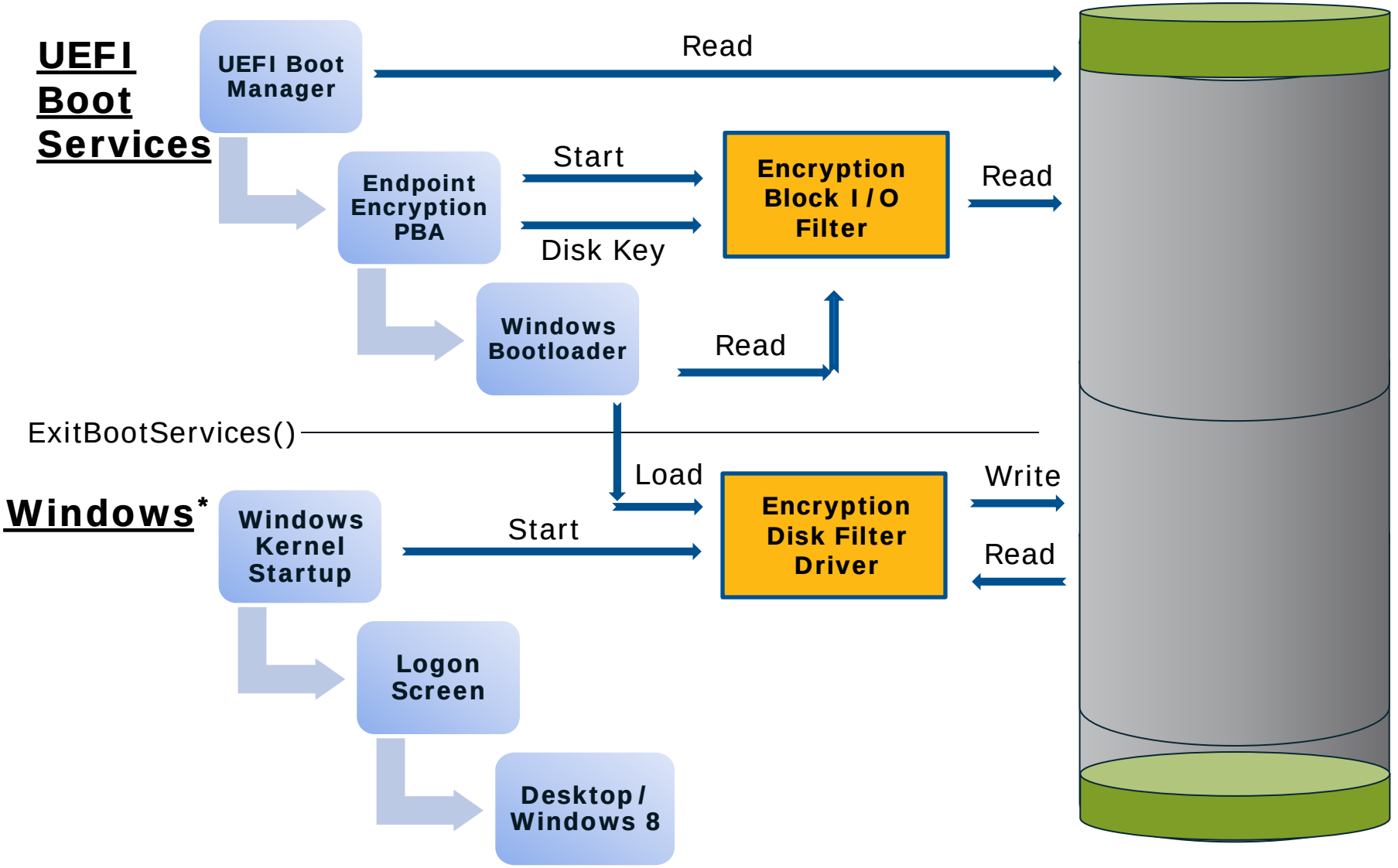


GPT磁盘：哪些被加密？



- PMBR, GPT 头和分区表 不能被加密
  - 磁盘解锁之前需要使用这些区域的数据
  - 磁盘无法被识别为有效的GPT磁盘，系统无法启动
- EFI系统分区 不能被加密
  - 包含可执行的 McAfee* Endpoint Encryption 预启动应用程序映像，将被UEFI启动管理器加载
  - 同时也包含 Block I/O 驱动程序，当用户认证完成，该驱动程序处理扇区级别的加密与解密
- Endpoint Encryption数据分区 不能被加密
  - 包含PBA使用的主题和本地化数据
  - 包含用户数据库和令牌数据
  - 在磁盘解锁前，PBA需要使用所有这些数据

启动过程



安全启动为Endpoint Encryption提供保障

- 没有安全启动，PBA很容易受到恶意软件的攻击，如键盘记录器、拒绝服务等
- 防篡改的PBA模块通过签名策略为平台提供配置文件的完整性检查

维护信任链！

恶意软件威胁：Keylogger

```
A BS->LocateHandleBuffer(ByProtocol, &simple_text_input_ex_protocol_guid, NULL, &num_handles,
                         &handles);
  for (i = 0; i < num_handles; ++i) {
B   BS->OpenProtocol(handles[i], &simple_text_input_ex_protocol_guid, &st, ImageHandle,
                     NULL, EFI_OPEN_PROTOCOL_GET_PROTOCOL);
C   hooked_protocols[i].st = st;
    hooked_protocols[i].orig_read_key_ex = st->ReadKeyStrokeEx;
    st->ReadKeyStrokeEx = keylogger_read_keystroke_ex;
  }
D   // Now chain load the original bootcode “EpeBoot.efi”
```

- 枚举所有支持EFI_SIMPLE_TEXT_INPUT_EX_PROTOCOL的设备，例如键盘和其它输入设备 – 代码 A
- 获取指向每个协议的指针 – 代码 B
- 将读取击键信息的函数指针替换为记录击键的恶意函数 C
- Keylogger 程序加载并执行原始的 UEFI 应用程序 – 代码 D

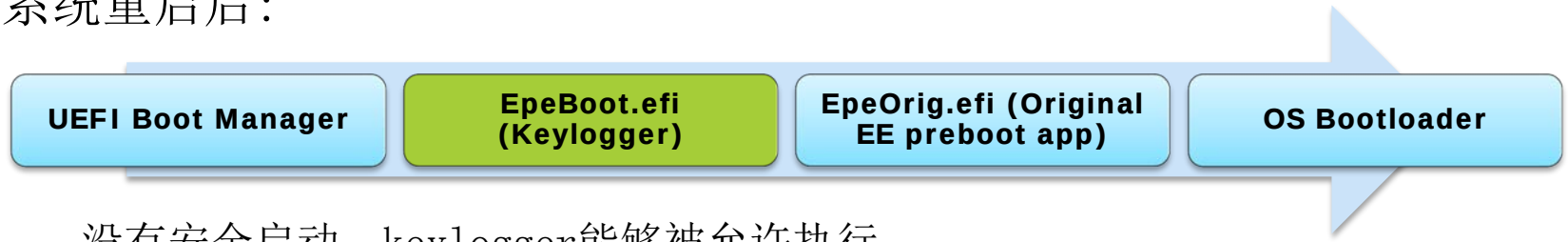
恶意软件威胁：Keylogger的安装

- 原始的，未破坏的启动过程：

- 没有安全启动，Keylogger的安装十分简单：

```
C:\> mountvol /s z:
C:\> copy z:\EFI\McAfee\EpeBoot.efi z:\EFI\McAfee\EpeOrig.efi
C:\> copy f:\keylogger.efi z:\EFI\McAfee\Epe\EpeBoot.efi
```

- 系统重启后：



  - 没有安全启动，keylogger能够被允许执行
  - Endpoint Encryption PBA 将执行，但所有的击键信息将被记录到磁盘上

恶意软件威胁：Keylogger的安装

- 原始的，未破坏的启动过程：

- 没有安全启动，Keylogger的安装十分简单：

```
C:\> mountvol /s z:
C:\> copy z:\EFI\McAfee\EpeBoot.efi z:\EFI\McAfee\EpeOrig.efi
C:\> copy f:\keylogger.efi z:\EFI\McAfee\Epe\EpeBoot.efi
```

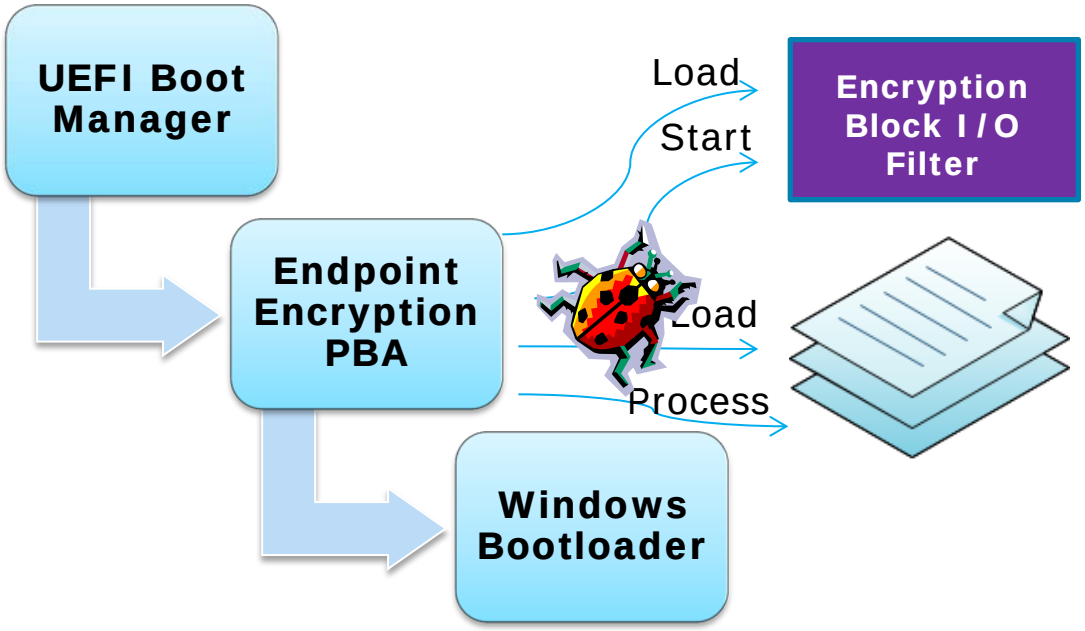
- 系统重启后：

  - 没有安全启动，keylogger能够被允许执行
  - Endpoint Encryption PBA 将执行，但所有的击键信息将被记录到磁盘上

安全启动能够阻止Keylogger的执行

还有什么可能出错？

- 即使有安全启动，但如果不小心，信任链仍有可能被破坏



- 安全启动确保 Endpoint Encryption PBA 和 Windows* Bootloader 是可靠的
- PBA 加载并执行Block I/O filter驱动程序
- PBA 加载和处理配置及数据文件
- 粗心的编码仍可能给恶意软件提供可利用的漏洞

信任链：可加载的模块

- Endpoint Encryption 的 UEFI 应用程序允许外插模块
  - 用于添加USB智能卡读卡器的支持
- **这造成对信任链的安全风险**
  - 此前，需要由 Endpoint Encryption UEFI 应用程序去担保不可信的代码不能被执行
- 现在，这一问题很容易解决：
  - 将可加载模块构建为 UEFI 驱动程序
  - 使用启动时服务，“LoadImage()”函数加载模块
  - 如果平台不信任该可加载模块，“LoadImage()”调用将返回 EFI_SECURITY_VIOLATION
  - **信任链从而被保持！**

信任链：数据文件

- 为什么数据文件对于信任链也是一种威胁?
  - McAfee* Endpoint Encryption PBA使用大量配置文件
  - 恶意软件可能恶意地修改配置文件，试图使PBA模块崩溃
  - 修改后的配置文件可以被构造来执行恶意代码
    - 常见的方式是能够利用栈缓冲区溢出，进而修改函数返回地址，从而跳转到未授权的代码中
    - *信任链被破坏!*
- 如何防止这类威胁?
  - *所有*来自磁盘的缓冲区数据需要被仔细检查，以防止缓冲区溢出
  - 数据文件签名可用于验证文件的真实性

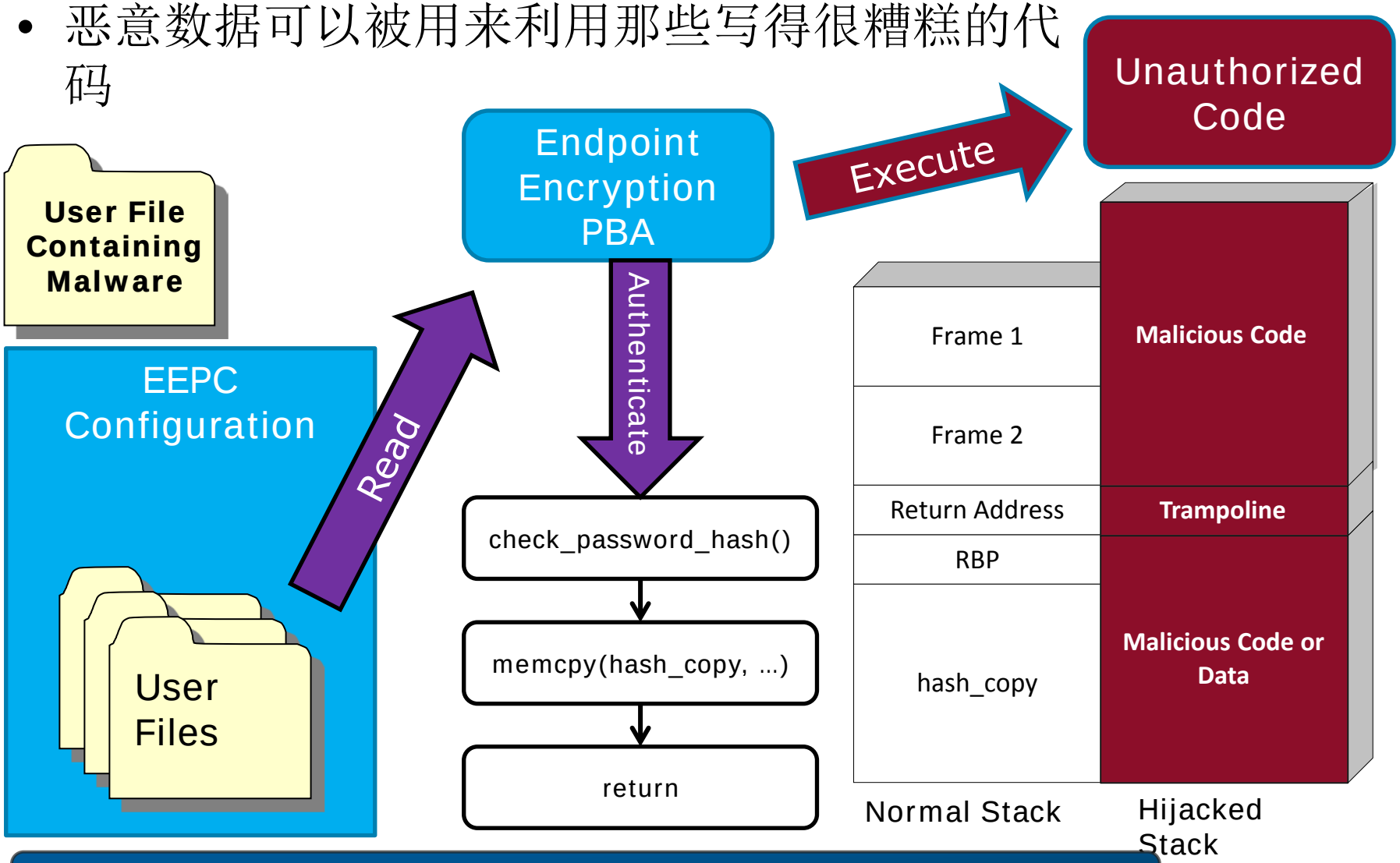
数据文件威胁

```
A struct USER_DATA {
    char    username[MAX_USERNAME_LENGTH + 1];
    long    hash_length;
    char    password_hash[MAX_PASSWORD_HASH_LENGTH];
  }
  int check_password_hash(USER_DATA* user_data, char* hash) {
B   char hash_copy[MAX_PASSWORD_HASH];
    // Take a copy of the hash so we can modify the buffer
    // !! No check to ensure the hash length is valid !!
C   memcpy(hash_copy, user_data->password_hash, user_data->hash_length);
    // Perform some calculation on the copied buffer
    ...
D   return success;
  }
```

- 模拟磁盘用户文件的数据结构定义于 A
- 在堆栈上分配定长缓冲区 B
- 未检验输入数据，直接进行磁盘缓冲区数据到堆栈的内存拷贝 C . 堆栈已被破坏.
- 函数返回地址 D 跳转到恶意代码

示例：恶意数据

- 恶意数据可以被用来利用那些写得很糟糕的代码



对所有配置信息和输入数据进行校验！

总结

- 由结合了众多技术和规范的软硬件组合对平台安全进行维护
- UEFI 安全启动是平台保护链条中至关重要的一环
- 信任链阻止了启动过程中恶意软件的渗透
- McAfee* Endpoint Encryption增加数据安全性，进一步强化了安全启动
- 谨慎编码以防止信任链被破坏

获取更多信息

- Intel UEFI 社区 - http://intel.com/udk
- UEFI 论坛学习中心
  - http://www.uefi.org/learning_center/
- 使用 TianoCore edk2-devel mailing list，寻求来自其他 UEFI 开发者的支持
- 从 tianocore.org 获取白皮书 “A Tour Beyond BIOS into UEFI Secure Boot”

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.

- A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
- Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
- The products described in this document 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.
- Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel representative to obtain Intel's current plan of record product roadmaps.
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number.
- Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
- Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm
- Intel, Sponsors of Tomorrow 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.
-

Legal Disclaimer

- Software Source Code Disclaimer: Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.
  Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. 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 company’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; supply constraints and other disruptions affecting customers; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Uncertainty in global economic and financial conditions poses a risk that consumers and businesses may defer purchases in response to negative financial events, which could negatively affect product demand and other related matters. 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. Revenue and the gross margin percentage are affected by the timing of 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 capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; segment product mix; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. Intel's results could be affected 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. 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. Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel’s current chief executive officer plans to retire in May 2013 and the Board of Directors is working to choose a successor. The succession and transition process may have a direct and/or indirect effect on the business and operations of the company. In connection with the appointment of the new CEO, the company will seek to retain our executive management team (some of whom are being considered for the CEO position), and keep employees focused on achieving the company’s strategic goals and objectives. 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, disclosure 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 Intel from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel’s results is included in Intel’s SEC filings, including the company’s most recent Form 10-Q, report on Form 10-K and earnings release.

Rev. 1/17/13