RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

预启动安全愿景

- 操作系统以外的威胁和防御

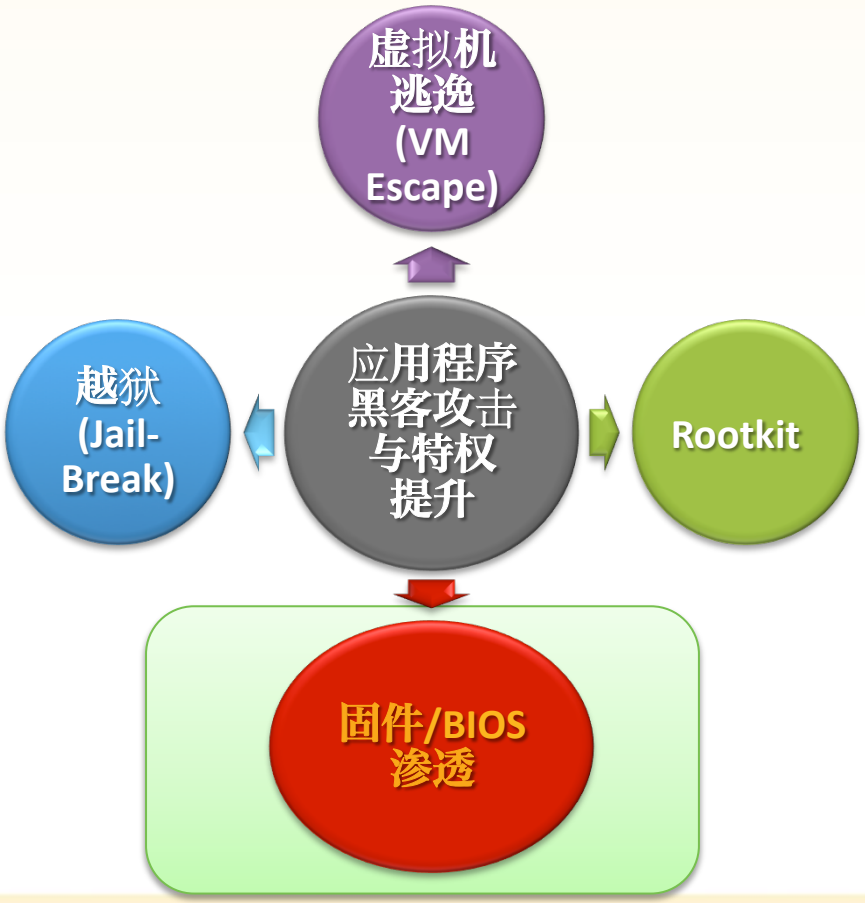
龙 勤， 软件架构师， Intel Corp.

高 瞻， 首席工程师， Byosoft Ltd.

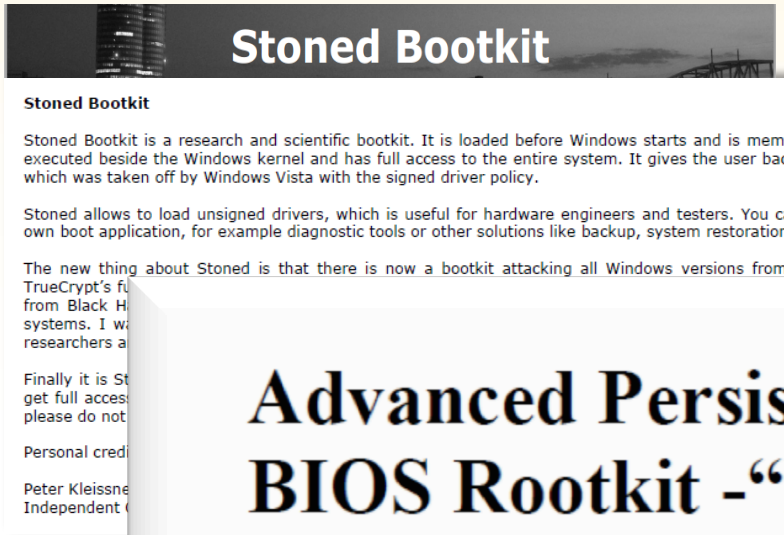
RSA CONFERENCE CHINA 2012

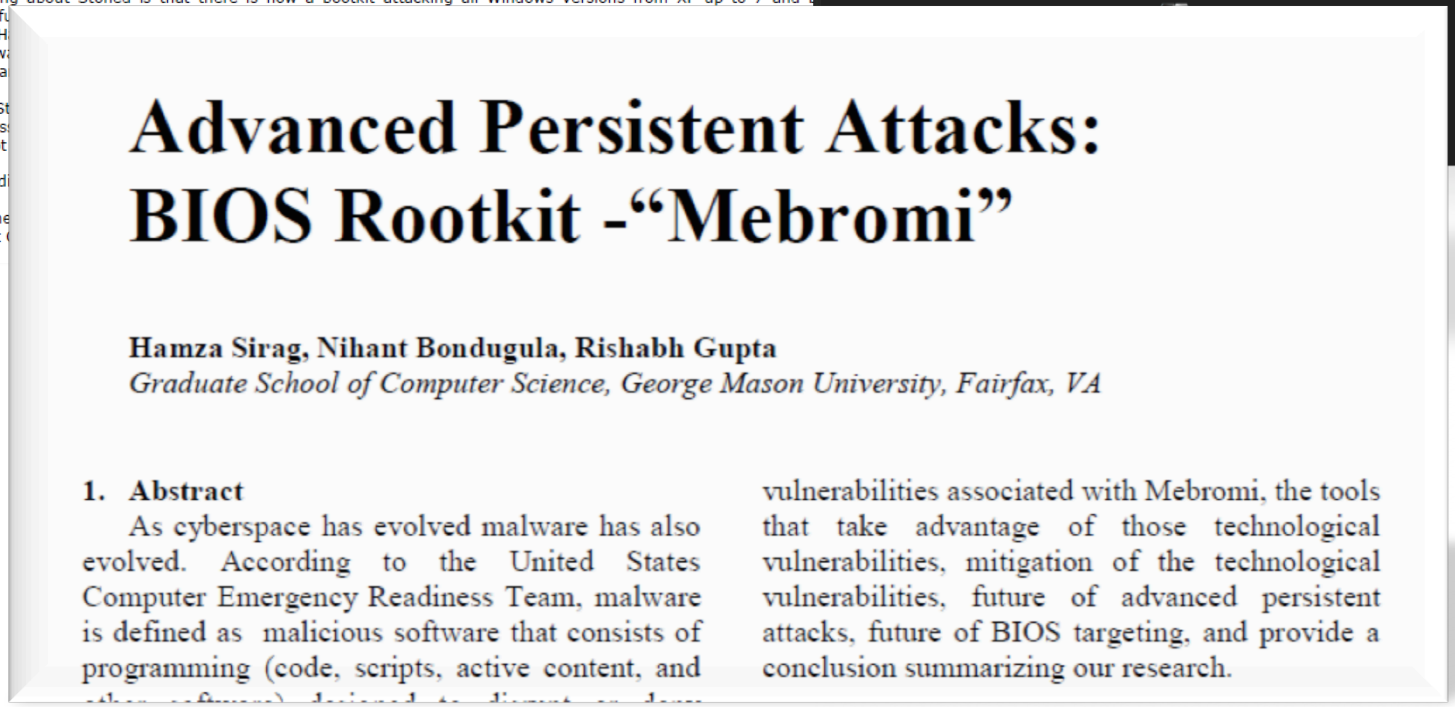
RSA信息安全大会2012

在您获得 root 或管理员访问权限之后.....
接下来该做什么？



Bootkit 和 APT





Advanced Persistent Attacks: BIOS Rootkit -"Mebromi"

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

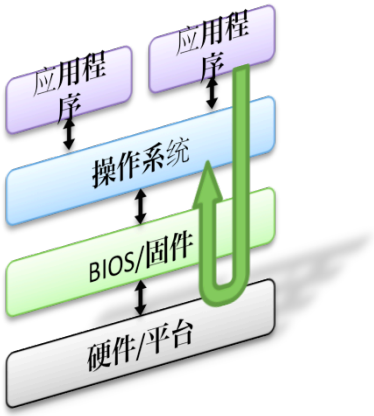
1. Abstract

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.

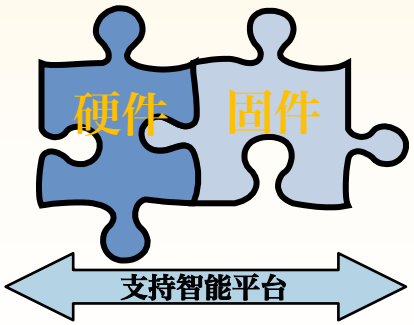
议程

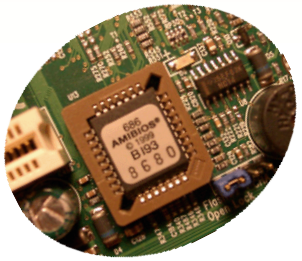
- 固件技术概述
- 问题陈述和动机
- 真实环境 – 预启动安全的攻击模式
  - 平台/固件漏洞的案例研究
- 平台安全防御和最佳做法
- 总结

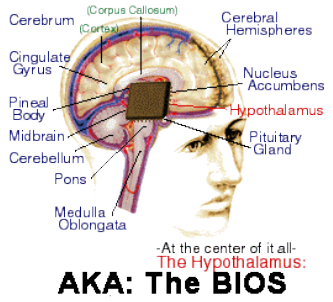


固件和 BIOS

- 固件 – 用于发挥芯片和平台功能的关键技术层
- 常见用法是驻留在 ROM 中的 BIOS
- BIOS – 基本输入/输出系统
  - 起源于 20 世纪 80 年代
  - 使计算机能够启动并存储有关计算机硬件的配置详细信息的程序
  - 处理 POST，并告知计算机中的操作系统如何启动，从何处加载、加载什么内容，存在的内存和 CPU 是什么，以及更多详细信息

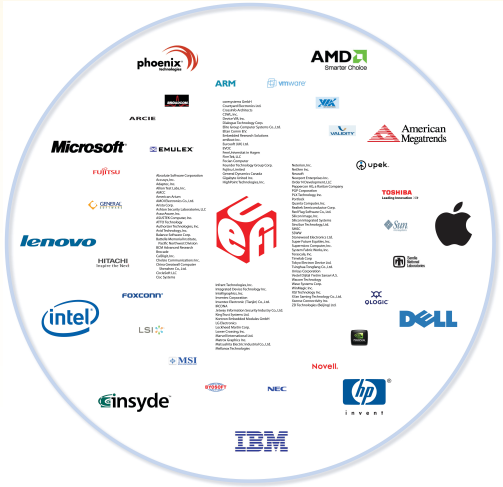


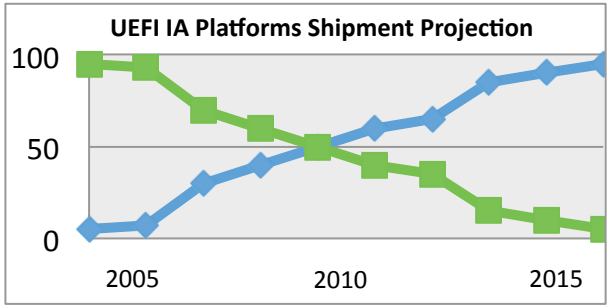




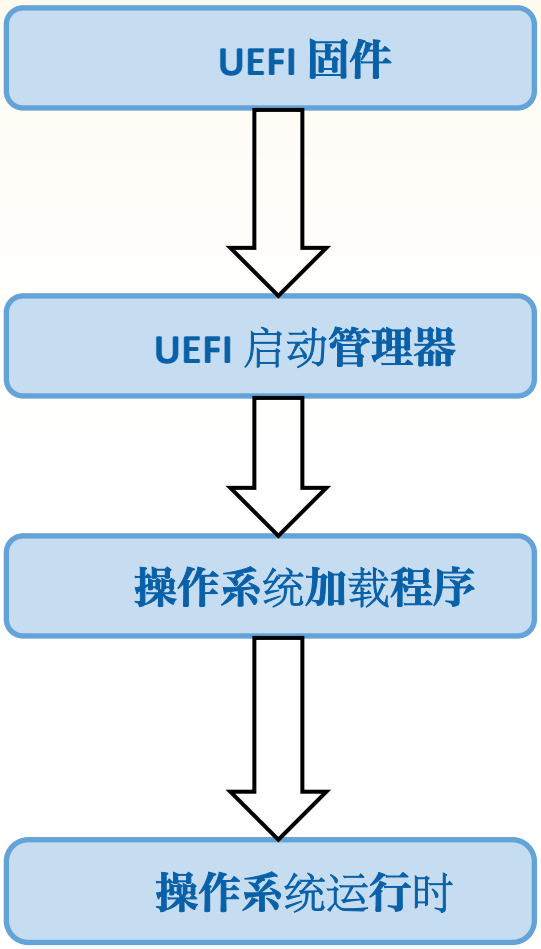
超越 BIOS – 从传统 BIOS 到 UEFI

- 传统 BIOS 的问题
- 超越 BIOS → UEFI（统一可扩展固件接口）
- 历史简介
  - 1981 – IBM 发布了“IBM PC”
  - 1982 – BIOS 产业创立
  - 1997 – 为 IPF 创建了 EFI（可扩展固件接口）
  - 1998 – Tiano 创建为“BIOS in C”
  - 2003 – Intel 推出了第一个基于 Tiano 的 EFI 平台
  - 2005 – UEFI 论坛建立（统一）
  - 2006 – UEFI EDK-II 发布（UEFI 2.0 规范级别）
  - 2006 - UEFI EDK 8.6.1 发布
  - 2010 – 针对最新 UEFI 2.3 规范的 UDK-2010 发布
  - ……





典型的 UEFI 操作系统启动流程



CPU/芯片组/平台初始化
准备 UEFI 系统表并分派 UEFI 驱动程序
枚举资源（PCI/ISA/USB/等）
生成 ACPI/SMBIOS 表
调用 UEFI 启动管理器

允许用户更改 UEFI 驱动程序选项以及选择 UEFI 启动选项
从启动选项的 UEFI 设备路径中调用操作系统加载程序

加载操作系统映像并调用 UEFI 启动服务 GetMemoryMap ()
设置操作系统运行上下文（例如页面表、GDT、X86 平台上的 IDT）
调用 UEFI ExitBootServices () 并将控制权交给操作系统

必要时调用 UEFI 运行时服务（变量、硬件错误记录）
调用/检索 ACPI/SMBIOS 表提供的服务/数据

问题陈述和动机

- 安全不仅是操作系统的事：黑白帽黑客与研究人员已开始关注操作系统之下的漏洞。
- 问题与挑战
  - 有吸引力的攻击目标：早期执行、特权、有价值的数据、SMM 等
  - 操作系统之下运行的恶意软件功能相当强大
    - 对系统资源的高特权访问
    - 很难检测；
    - 持久性 - 不会因操作系统重新启动或重新安装而消除；
    - 数据可能会丢失/被盗
    - 系统可能挂起/冻结
    - ……
- 现在应考虑有关平台和固件的更多安全事项！

为什么是固件/BIOS？

- 平台安全的主要基础
  - 受信任系统的基础
  - 几乎其他所有基础安全技术的基础：TXT、AT、AMT、IPT……
- 位于主板和附加卡上
- 计算机行业正在向基于 UEFI 的 BIOS 实现过渡
  - 已定义更多安全功能
  - 更大的攻击表面
  - 标准接口会使漏洞利用更易编写
  - 开源

现实世界！


DEFCON
CanSecWest
SyScan
InfoWorld
Researcher to demonstrate attack code for Intel chips
Kaspersky says CPU bugs are a growing threat, with malware being written that targets these vulnerabilities
PCWorld
Business Center
Researchers Detail Inte
Black Hat
Intel Releases Security BIOS Firmware Updates for Several Boards
The updates fix a bug in the Q35 chipset that can allow rootkits to run under SMM
DE MYSTERIIS DOM JOBSIVS:
MAC EFI ROOTKITS
IN CONCLUSION...
I HAD FUN.
ically we're all screwed
hat should you do?
Glue all your ports shut
Use an EFI password to prevent basic local attacks
Stop using computers, go back to the abacus
hat should Apple do?
mplement UEFI Secure Boot (actually use the TPM)
Use the write-enable pin on the firmware data flash properly
NB: They may do this on newer machines, just not my test one
Audit the damn EFI code (see Heasman/ITL)
Sacrifice more virgins
De Mysteriis Dom Jobsivs - SyScan
April, 2012
换硬盘也杀不掉的“BMW病毒”现身 危害远超CIH
BMW病毒
BIOS（主板芯片程序）
利用BIOS感染硬盘MBR
MBR（硬盘主引导区）
利用MBR感染Windows系统文件（32位）
Winlogon.exe(XP/2003)
Wininit.exe(Win7/Vista)
Windows系统文件
执行恶意代码，批量下载木马病毒
盗号/改主页/远程控制

“Bootkit（取代或绕过系统启动的恶意软件）也会威胁移动设备。 尽管获得用户自己的电话或电子书阅读器的根访问权限会使设备获取额外功能或取代操作系统，但它也可以允许攻击者加载他们自己的经过修改的操作系统。 移动 rootkit 只会修改现有操作系统以逃避检测， 而 bootkit 则可以为攻击者提供对设备的更多控制权。

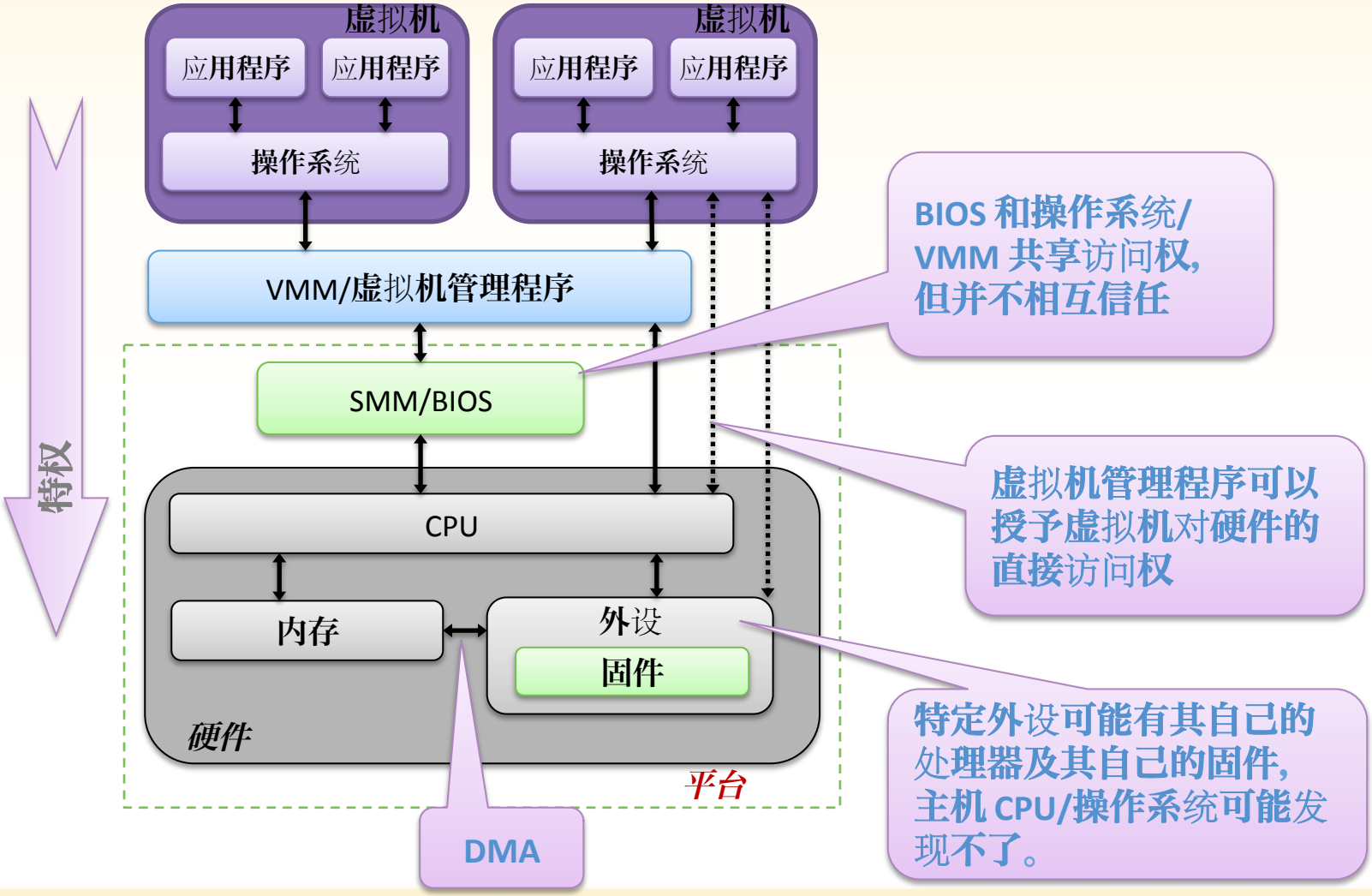
.....

攻击硬件和固件并不容易，但如果成功，将允许攻击者在网卡、硬盘驱动器甚至系统 BIOS 中创建永久的恶意软件“映像”。 我们预计整个 2012 年及以后，硬件和固件漏洞利用方面的投入将会增加，相关的实际攻击也会增多。

攻击层面 & 攻击模式

忘记历史就意味着背叛！

堆栈和攻击面


虚拟机
应用程序
应用程序
操作系统
虚拟机
应用程序
应用程序
操作系统
VMM/虚拟机管理程序
SMM/BIOS
CPU
内存
外设
固件
硬件
平台
特权
DMA
BIOS 和操作系统/VMM 共享访问权，但并不相互信任
虚拟机管理程序可以授予虚拟机对硬件的直接访问权
特定外设可能有其自己的处理器及其自己的固件，主机 CPU/操作系统可能发现不了。

威胁模型

- STRIPED
- S：假冒用户身份 – 例如，伪造密码以盗用信用卡信息
- T：篡改 – 修改数据或代码
- R：否认 – 声称未执行某项操作
- I：信息泄露 – 例如使信用卡数据处于未加密状态
- E：权限提升 – 例如可以在 0 环中运行或对 AV (SMM) 不可见

漏洞案例

- 未经授权的固件更新 – 未经检查或只经过简单的检查即更新固件（校验和 == 无）
- 未经授权的第三方代码 – 可能劫持系统 API 或提升特权
- 关键寄存器未加锁 – 如果未加锁，稍后可能被修改
- 缓冲区溢出 – 不仅是操作系统，也不仅是软件
- 使用密码后未清除 –恶意代码可能搜索内存中的密码
- 默认访问密码 – BORE 攻击（一旦攻破，将在所有位置运行）

BIOS 特定的：固件更新、关键寄存器。

漏洞与 威胁

漏洞案例：

- 未经授权的固件更新
- 未经授权的第 3 方代码
- 关键寄存器未加锁

威胁：

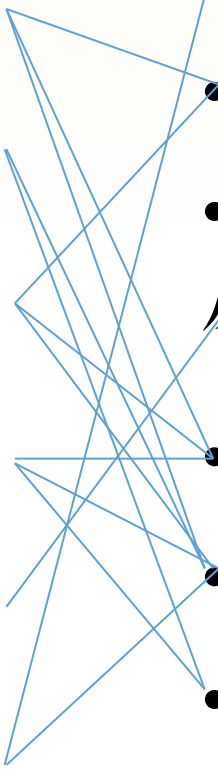
- S：假冒用户身份
- T：篡改
- R：否认

漏洞案例：

- 未经授权的固件更新
- 未经授权的第 3 方代码

威胁：

- S：假冒用户身份
- T：篡改
- R：否认

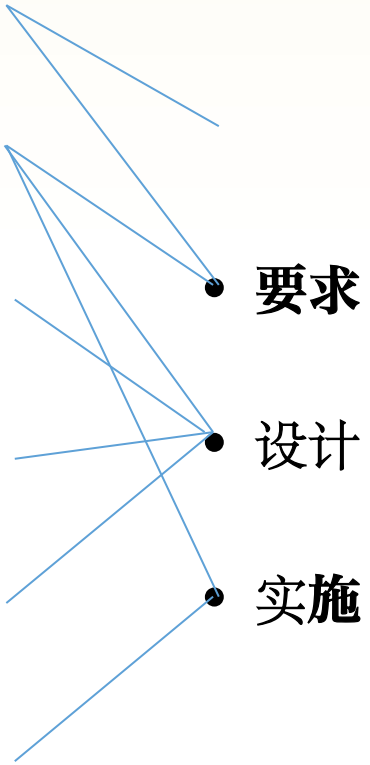


开发生命周期

漏洞案例：

- 未经授权的固件更新
- 未经授权的第 3 方代码

生命周期：
生命周期：



攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

使用密码后未清除

默认访问密码

CIH – 第一个攻击固件的病毒

- 在 1999 和 2000 年，Chernobyl 病毒（也称为 CIH）传播到了世界各地。（由台湾的 Chen Ing Hau (陳盈豪) 编写）
- Chernobyl 只发送几条命令，通知一种常见类型的闪存设备擦除存储所执行的第一条指令的数据块。
- 3 万 - 100 万个系统遭到破坏（PDoS – 永久拒绝服务），原因就是几十条指令。

未经授权的固件更新

Apple 键盘固件遭黑客攻击

- BlackHat 2009， K. Chen（乔治亚理工学院）演示了如何刷新 Apple 铝质键盘固件。
- 影响：
  - 一个按键记录器作为 rootkit 置入键盘固件中。
  - 击键记录器可以盗取密码，甚至可以发送命令以进行远程连接。

黑客破解苹果键盘固件 远程控制电脑

2009-08-03 CBSi中国·PChome.net 类型：转载 来源：驱动之家 责编：李昌

DELUX 多彩科技

如果你的电脑被黑了，就算完全格式化硬盘也无法逃脱黑客纠缠的时候，你是否想过有可能是键盘在作怪?日前在DEFCON 2009安全会议上，一位安全研究人员就展示了自己的最新成果：通过破解苹果键盘固件来攻克Mac系统.

这位名叫“K. Chen”（可能为华裔）的研究人员在会上展示了刷入破解固件的苹果铝制USB键盘，他通过破解苹果官方的键盘固件升级程序，将经过修改后 的固件刷入键盘. 这样，用户在键盘上输入的所有字符都会被键盘记录下来. 由于问题出现在键盘内部，即使在未进入系统比如输入BIOS密码时，它也同样能够 如实记录用户输入内容，这将让很多最严密的软件安全措施形同虚设.

更严重的是，一旦键盘固件被修改，黑客可以在其中预留代码，比如“等待用户无动作一小时后，自动输入命令与黑客电脑建立远程控制连接”. 这样一来，黑客即可轻松获得该机的全部控制权，而即使将硬盘全部格式化，只要继续使用该键盘，系统就还会被重新攻克.

未经授权的固件更新

如果你敢，就来打印吧（HP 打印机）

- 2011， Ang Cui（哥伦比亚大学）演示了如何远程更新 H
  - 打印机可以将打印的任何机密文档发送到任意位置。

数百万的

打印机

  - 自 1984 年以来已售出 1 亿台激光打印机，意味着数百万的打印机可能受到攻击。

此前MSNBC新闻网站引用哥伦比亚大学研究人员的话称，部分惠普激光打印机容易遭受攻击。黑客很可能会控制设备并使其着火或者利用漏洞渗透到其它安全网络中。

惠普今天在声明中表示，部分激光打印机存在“潜在安全隐患”，正在着手解决。惠普表示：“惠普正在进行固件升级来解决这一问题，并会提前和可能受此影响的用户、合作伙伴进行沟通。

未经授权的固件更新

终结 Cisco IOS rootkit

Groundworks rootkit topo' Muñiz（Groundworks Technologies 的共同创始人和安全研究员）演示了如何将 rootkit 放入 Cisco IOS 路由器中。

方法。

- 影响：
  - 劫持所有中断设备并截取/修改数据包。
  - 注意：在价格超过 1500 美元的路由器市场中，Cisco 占据 92% 的市场份额。并占据 71% 的企业交换机市场份额

Rootkit兵临城下 思科忙为路由器打补丁

2008-05-23 11:56 落英缤纷 译 51CTO.com 我要评论(0) 字号：T | T 收藏

思科系统公司在近日发布了三个安全补丁，用以修补可以导致其产品崩溃的三个缺陷。此间，该公司正收到SANS互联网风暴中心的安全警告，这些更新是于周三发布的，它修正了可用于维持思科路由器运行的IOS系统中的及思科服务控制引擎中SSH软件的拒绝服务漏洞。

AD：

【51CTO.com 独家翻译】据悉，思科说这些漏洞都是由其自己的研究人员发现的。

思科系统公司在近日发布了三个安全补丁，用以修补可以导致其产品崩溃的三个缺陷。此间，该公司正收到SANS互联网风暴中心的安全警告，这些更新是于周三发布的，它修正了可用于维持思科路由器运行的IOS系统中的及思科服务控制引擎中SSH软件的拒绝服务漏洞。

在其安全报告中，思科说所有的漏洞都是由其自己的研究人员发现的，但SANS警告说，研究人员有可能对这些补丁实施逆向工程，并可以公开地发布其漏洞利用代码。

这些特殊的更新正受到安全社团的额外关注，这种安全社团正紧锣密鼓地调查研究恶意软件在IOS上的运行机制。IOS是一个可以在很大程度上逃避严格监视的操作系统。在周四即昨天的时候，核心安全技术公司（Core Security Technologies）的分析师Sebastian Muniz在伦敦的EuSecWest应用安全大会上给出了一个广受关注的关于思科rootkit的展示，他称之为DIK（即da IOS rootkit）。

未经授权的固件更新

攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

使用密码后未清除

默认访问密码

Mebromi (BMW)

- 2007 年，中国黑客 Icelord 在 xfocus 中发布了文章。

BIOS Rootkit:Welcome home,my Lord!

创建时间: 2007-05-11
文章属性: 原创
文章提交: icelord (icelord_at_sohu.com)

[BIOS RootKit:Welcome Home,My Lord!...?]

[Author]: Icelord
[Contact]: icelord@sohu.com
[Data]: @2007/04/26->...

本文介绍一个简单BIOS rootkit的简单设计过程
意在抛砖引玉，期待高手们指点

其中涉及的几篇文字均可在blog.csdn.net/icelord上找到
http://blog.csdn.net/icelord/archive/2007/05.aspx

[申明]

未经授权的第 3 方代码

Mebromi (BMW)

- 到 2011 年，它确实发生了。（CIH 卷土重来）
- 影响：
  - 远程控制，盗取帐号，……
  - 超过 50,000 台计算机受到攻击。
  - 攻击 Award-BIOS。

换硬盘也杀不掉的“BMW病毒”现身 危害远超CIH

来源：360安全中心 发布日期：2011-09-01 已有779条评论 我要评论

北京时间9月1日，360安全中心发布2011年首个红色安全警报称，一种新型的BMW病毒正在大量发作，已攻击上万台电脑。据分析，该病毒能够感染电脑主板的BIOS芯片和硬盘MBR（主引导区），再控制Windows系统文件加载恶意代码，使受害用户无论重装系统、格式化硬盘，甚至换掉硬盘都无法彻底清除病毒。<<

最新消息：全球杀毒厂商围捕BMW电脑病毒

BMW病毒感染量突破5万 已遭全球杀毒厂商围捕

来源：中国新闻网 发布日期：2011-09-14 已有50条评论 我要评论

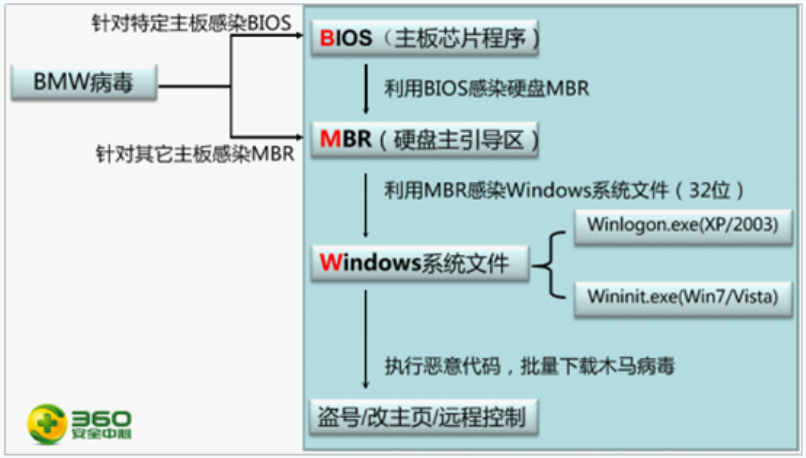
[中国新闻网消息]

中新网9月14日电 360安全中心发布最新统计数据称，新型BMW病毒 的感染量在过去半个月间增长了4倍，目前国内约有5万台电脑受到攻击，主要受害群体为关闭安全软件而使用外挂的游戏玩家。与此同时，BMW病毒受到了国际杀毒行业高度重视，赛门铁克、Norman等多家欧美厂商陆续发布分析报告，微软官方网站也通报了病毒疫情。

360安全中心发现，BMW病毒主要通过捆绑游戏外挂传播，欺骗用户关闭安全软件后再攻击电脑，感染特定型号的主板BIOS(AwardBIOS)；如果用户电脑主板BIOS并非AwardBIOS，病毒则会直接感染MBR，受害电脑同样难以清除。据统计，目前在5万余例受到BMW病毒攻击的电脑中，使用AwardBIOS并被病毒侵入主板的电脑比例接近10%。

BMW病毒被安全业界普遍视为“CIH噩梦重现”，后者被美国科技网站Techweb(www.techweb.com)评选为全球十大病毒之首，曾造成数千万美元的经济损失。赛门铁克分析报告使用“BIOS威胁又出现了”作为标题，其中这样描述：“我们很少遇到影响BIOS的恶意程序，1999年臭名昭著的CIH是其中一个。最近新的威胁又出现了，它能将恶意组件写入AwardBIOS，甚至比MBR更先控制系统。”

点击下载BMW病毒专杀工具 查看专杀使用说明 查看BMW病毒分析报告



未经授权的第 3 方代码

攻击 Intel 可信执行技术

攻击 Intel 可信执行技术

- 已修复（Joanna Rutkowska，在Invisible Things Lab）

找出了绕过 Intel 可信执行技术的方法，这是动态信任根的一种实现。

- 系统管理模式 (SMM) 中的这种实现缺陷可能调用 SMM 内存空间之外

- 影响：
  - 影响：

虚拟机服务器受Intel可信赖执行技术攻击

【TechTarget中国原创】可信赖执行技术（Trusted Execution Technology，TXT）攻击是很复杂的攻击方法，很难成功，但是安全研究人员Joanna Rutkowska和同事Rafal Wojtczuk利用这个安全bug，绕过Intel可信赖执行技术。这个应该引起安全专家的注意。特别是考虑使用TXT的可能应用Intel桌面、服务器和移动设备上执行虚拟化的安全专家。IT界还不需要紧张，因为还没有发现利用专家技术攻击的已知攻击和漏洞。

攻击值得关注是因为思杰和Vmware最近宣布使用Intel的vPro架构和TXT作为基础的主要合作关系。Intel正在研究漏洞，并保证TXT的安全性。

作为后台，Intel的vPro架构的构建可以提供操作系统和虚拟机执行的安全平台。主要的安全功能包括：虚拟机硬件的强制分离以分化攻击、可信平台模块（Trusted Platform Module，TPM）保护秘密存储以及TXT为受信机制上传系统软件，例如操作系统或者虚拟。TXT有一种潜力很大功能，它可以允许端点的离线和下班时间的配置管理，而在这些端点上TXT可以被用于更新电脑或者笔记本电脑以及在设备的不活跃的时候备份敏感数据。这就是漏洞的真正危机所在——破坏SMM的攻击可以强制TXT分配额已代码，绕过TXT完整性检查。

TXT漏洞的攻击相当困难，要求专家级的攻击。因此这种攻击才不能广泛传播。攻击明确的服务器要求有先进的攻击技术。主要的商业风险存在于分配服务器上，攻击者可以传递对服务器的访问，导致可以在分布到企业端点之间对系统软件的探查攻击。这种风险很低很低，但是如果发生，破坏性极强。

IT界应该确保软件和虚拟机分配服务器都在物理控制之下。主要的系统软件分配系统包括端点更新、补丁、虚拟机镜像，他们都需要网络中最受信任的服务。这些服务器属于数据中心，而在数据中心，物理和逻辑安全可以协同工作包括基础架构。

攻击者将会发现更多的漏洞，他们的攻击简单和获益要比TXT简单。这不是IT界主要的担心。但是，仍然建议确保关键系统软件和虚拟机服务器都被妥善地控制着，帮助防御在企业执行环境中的信任的流失。

未经授权的第 3 方代码

对 BIOS 防盗技术的攻击

BIOS 中存在一些设计漏洞，这将允许一种非常危险的 BIOS 回被盗的笔记本电脑。

- Computrace BIOS 中存在一些设计漏洞，这将允许一种非常危险的 BIOS 增强的 rootkit。
- 影响：
  - 反防盗。
  - 涉及所有 Computrace BIOS，如 Dell。

未经授权的第 3 方代码

攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

使用密码后未清除

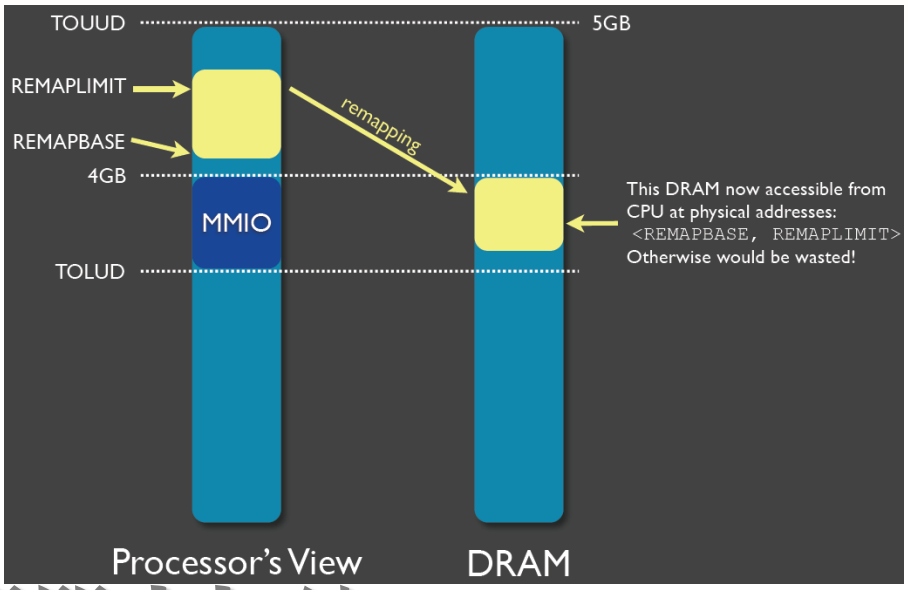
默认访问密码

芯片组重新映射

芯片组重新映射问题的 Intel 主板。

Rafal Wojtczuk

- 影响：
  - 在配置不当的系统中，将代码写入 SMRAM，并将代码注入 XEN 虚拟机管理程序。
  - 将特权从应用程序提升到虚拟机管理程序。
  - 影响 Intel 桌面 BIOS



关键寄存器器未加锁

攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

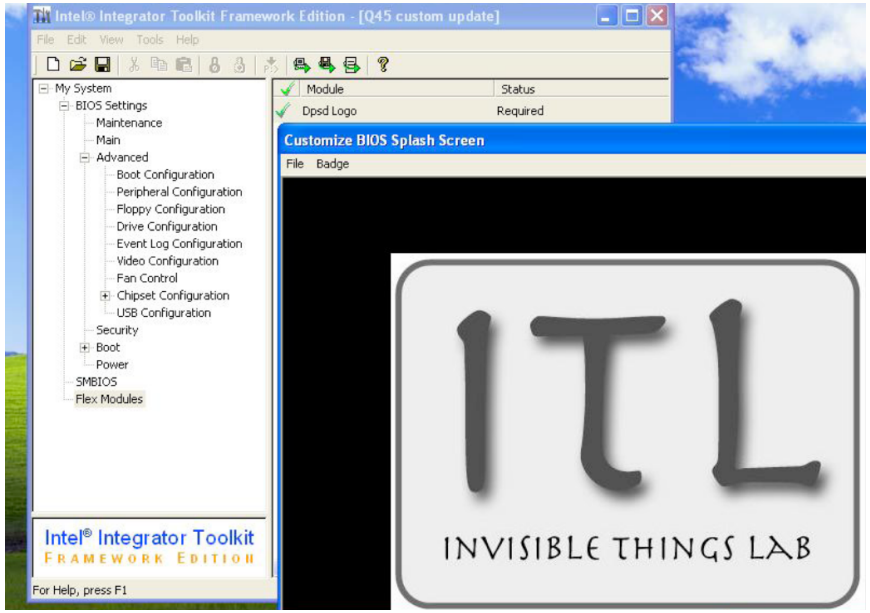
使用密码后未清除

默认访问密码

– 绕过 **BIOS 更新**检查。 Tereshkin (Invisible Things Lab)

利用 BIOS BMP 缓**冲区溢出漏洞**进**行** BIOS**更新**。

- **影响：**
  - 恶**意**软**件可以使用官方** BMP **徽**标**文件更新**应**用工具来更新** BIOS。
  - 绕过 **BIOS 更新**检查。
  - **影响** Intel **桌面** BIOS



缓冲区溢出

攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

使用密码后未清除

默认访问密码

预启动身份验证密码 - 绕过

预启动身份验证密码 - 绕过

- Defcon 2008，Jonathan Brossard (Toucan System) 发现在启动之前 PBA 中的 BIOS 键盘缓冲区未清除。
- 影响：
  - 绕过预启动身份验证
  - 绕过预启动身份验证泄露。

BIOS passwords :	Full disk encryption with pre-boot authentication capabilities :
Award BIOS Modular 4.50pg	Bitlocker with TPM chip under Microsoft Vista Ultimate Edition SP0.
Insyde BIOS V190	Truecrypt 5.0 for Windows (open source)
Intel Corp PE94510M.86A.0050.2007.0710.1559	DiskCryptor 0.2.6 for Windows (open source)
Hewlett-Packard 68DTT Ver. F.0D (11/22/2005)	Secu Star DriveCrypt Plus Pack v3.9
Lenovo 7CETB5WW v2.05 (10/13/2006)	

使用密码后未清除

攻击模式

未经授权的固件更新

未经授权的第 3 方代码

关键寄存器未加锁

缓冲区溢出

使用密码后未清除

默认访问密码

Apple 电池攻击

Apple 电池攻击

Charlie Miller (Accuvant Labs) 利用装配的电池中的漏洞

- 影响：
  - 用户可以更新智能电池固件。
  - 可能导致电池安全危险，例如过度充电、过热或者甚至会起火。

Apple Laptops Vulnerable To Hack That Kills Or Corrupts Batteries

Updated below to clarify Barnaby Jack's prior research.

A pile of dead Apple laptop batteries, victims of Charlie Miller's research.

Your laptop's battery is smarter than it looks. And if a hacker like security researcher Charlie Miller gets his digital hands on it, it could become more evil than it appears, too.

At the Black Hat security conference in August, Miller plans to expose and provide a fix for a new breed of attack on Apple laptops that takes advantage of a little-studied weak point in their security: the chips that control their batteries.

默认访问密码

预操作系统攻击摘要

- **受攻击功能：**还涉及安全功能
  - Apple、Cisco、Dell、HP、Intel、Lenovo、Siemens……
- **受攻击功能：**还涉及安全功能
  - **通常情况：永久拒绝服务**、RootKit。
  - **安全** BIOS **更新、防盗技术、可信执行技术**。

有志者事竟成！

摘要（续）

- **病毒数目：截止目前不太多**
  -
    病毒数目：截止目前不太多
  - **但是，的确存在真正的固件攻击实例。** （CIH、
    - ）

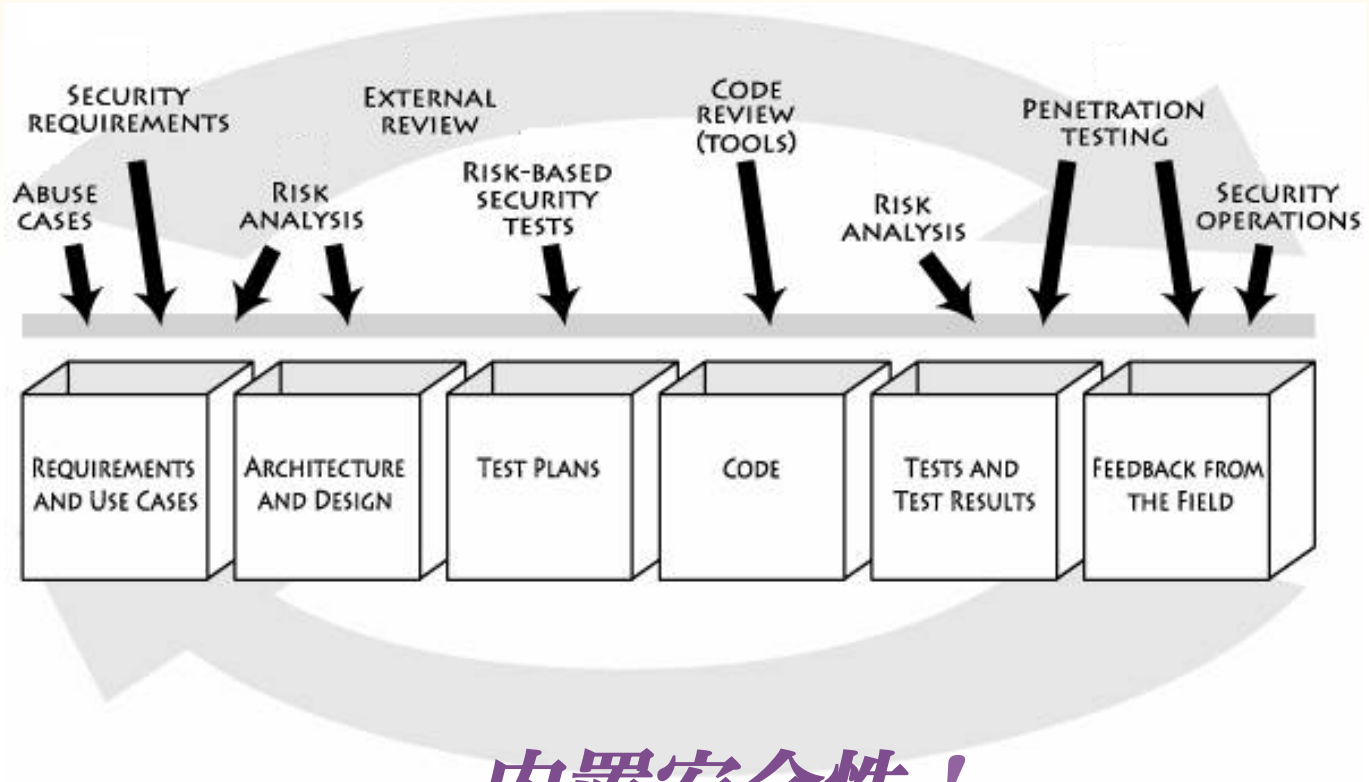
- **病毒影响：大**
  - CIH：3 万 - 100 万个系统遭到破坏。
  - 2fnxuef
  - Mebromi/BMW：50,000 多台计算机受到攻击
  - **核计划由于离心机损坏而推迟数月或数年**

我来了！我看见了！我征服了！

防御 & 行动呼吁

小洞不补，大洞叫苦！

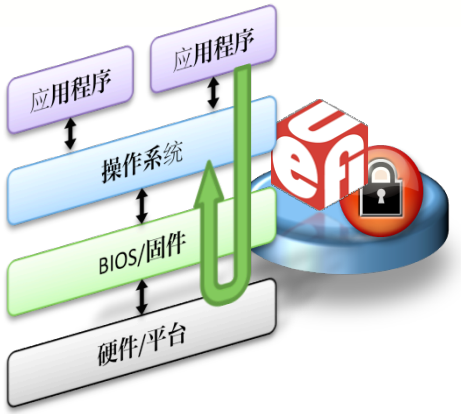
固件的安全开发生命周期



内置安全性！

应用 UEFI 安全

- .....
  - UEFI安全启动
  - 网络安全
- .....
- http://www.uefi.org
  http://tianocore.sourceforge.net



可信计算与度量启动

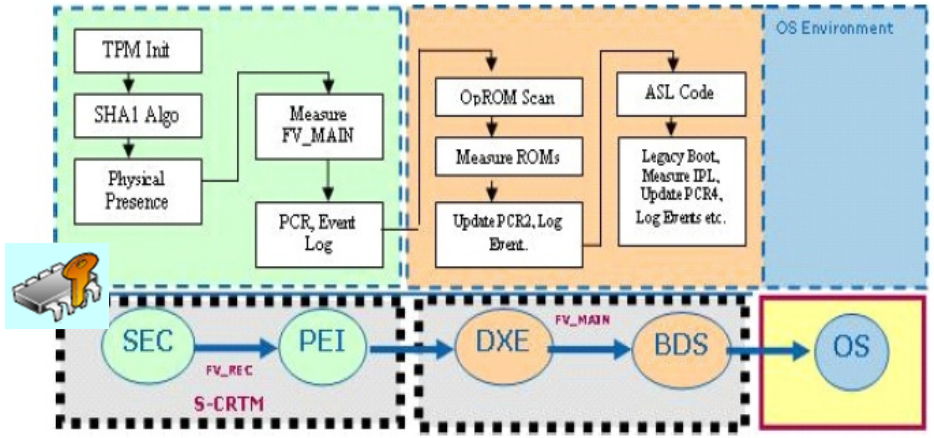
- 一个符合 TCG 标准的端到端解决方案

  旨在通过提供有关系统初始状态的可靠信息，证明哪些组件在控制权移交之前运行过。

- 度量值记录在 TPM 设备中

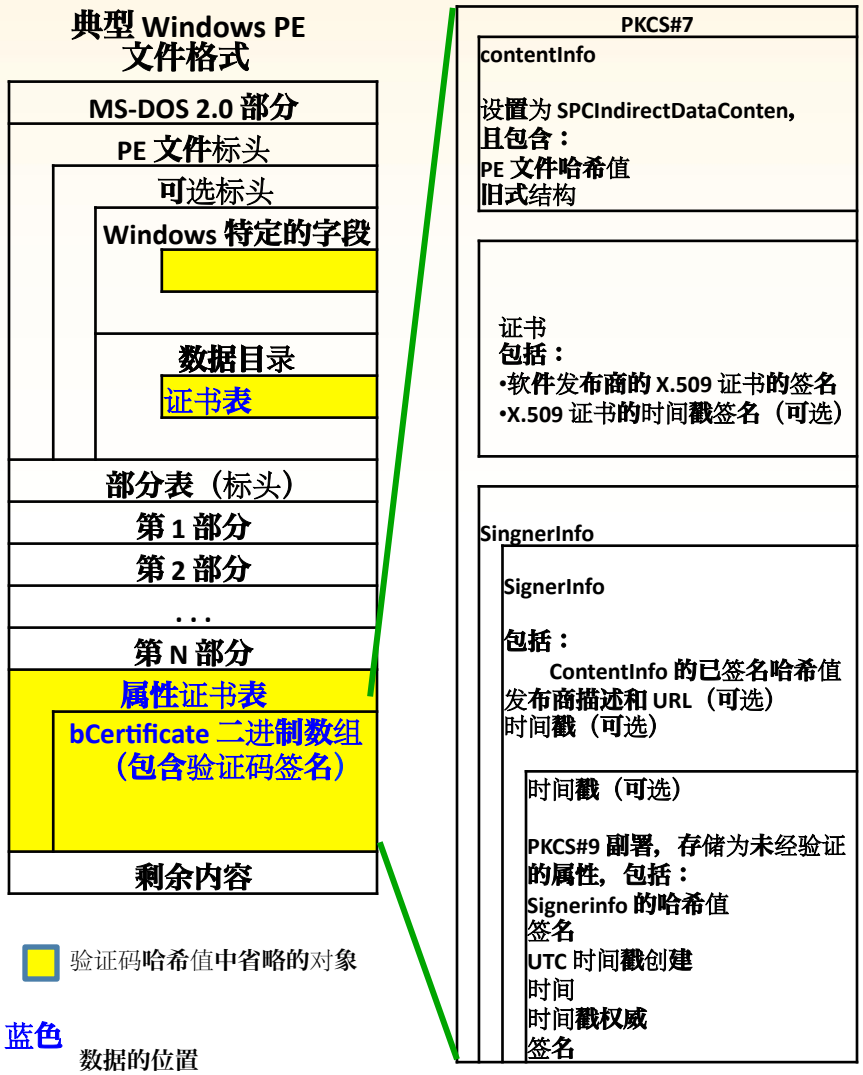
  在下次重置系统之前无法重置 – 防止恶意组件进行篡改

  - 连续启动平台会产生相同的测量值。

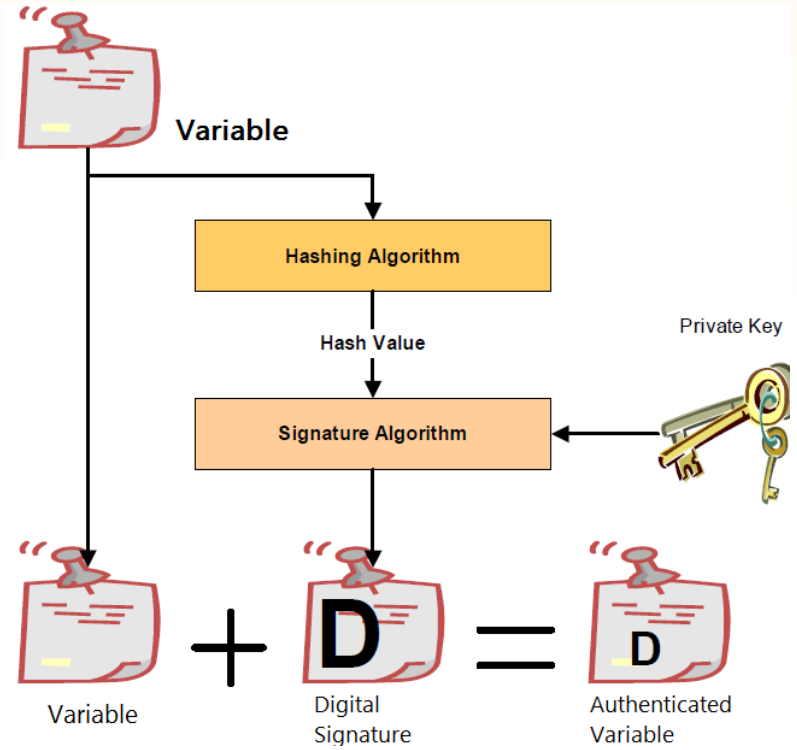


EFI 驱动签名

- 基于策略的UEFI 及第 3 方映像
  - 的可扩展性支持
  - 统中[illegible]的执行程序的控制
  - 检测/[illegible]的执行程序的控制权
  - 技术
  - 支持“已知良好”和“已知不良”的签名数据库
  - 基于策略更新列表类型（Windows Authenticode）



EFI 认证变量



- **基于计数器的**认证变量 (UEFI 2.3)
  - **使用**单调计**数以抵御可疑重放攻**击
  - **哈希算法** – SHA256
  - 签**名算法** – RSA-2048
- **基于时间戳的**认证变量 (UEFI 2.3.1)
  - **使用** EFI_TIME **作为回滚保护机制**
  - **哈希算法** – MD5/SHA1/SHA224/SHA256
  - 签**名算法** – X.509 证书链
    - **完整** X.509 证书链
    - **中**间证书**支持**（**非根**证书**作为受信任**证书）。

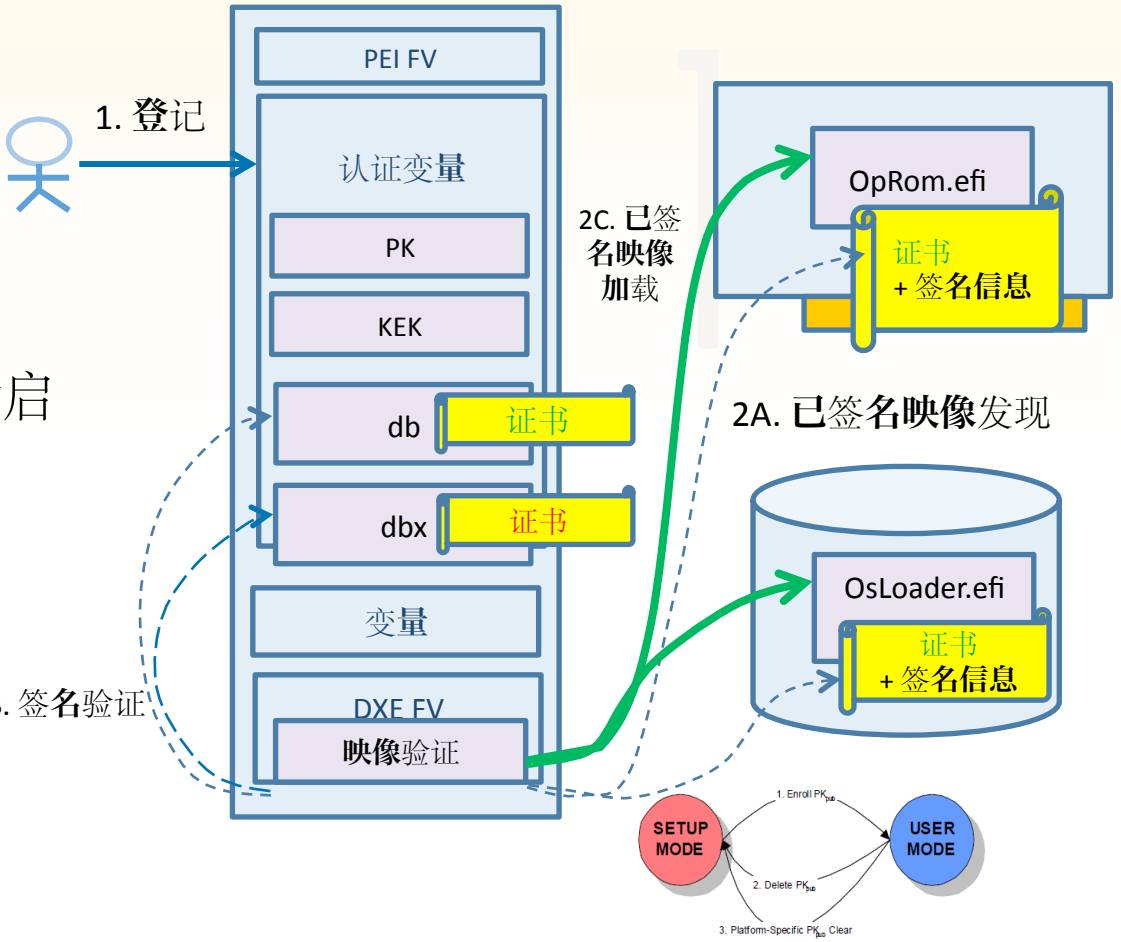
攻在一起 – UEFI 安全启动

- Microsoft Windows 8 认证
  -
- 要求Microsoft Windows 8 认证
  -
- 系统厂商加载程序和操作

消除传统威胁并在每个启动步骤中提供软件标识检

TianoCore

网站

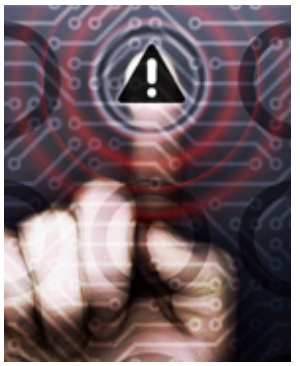


NIST 指南

- NIST 已创建 BIOS 保护指南
  - **SP800-147** - 安全闪存更新要求
  - **SP800-147B** – 针对服务器
  - **SP800-155** - 维护固件核心信任根
- 3 个基本要求
  - 固件/BIOS 必须受到保护
    BIOS 更新必须经过签署
  - BIOS 保护机制无法绕过

总结

- 平台安全开始于软件堆栈的最低级别 … 固件和操作系统加载程序
- 今天它已变为现实 – 操作系统以外的攻击和威胁！
- 管理固件的推荐做法，遵循 UEFI、NIST 规范
  - 经身份验证的固件更新
  - 完整性保护和经身份验证的启动
  - 不可绕过性



谢谢大家

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012