文章编号:1001 - 9081(2007)09 - 2174 - 03

基于 EFI 的信任链传递研究及实现

章 睿[1],刘吉强[1],彭双和[2]
(1. 北京交通大学 信息安全体系结构研究中心,北京 100044;
2. 北京信息科技大学 计算中心,北京 100085)
(05120475@ bjtu. edu. cn)

摘 要:为进一步提高 BIOS 的安全性,提出一种利用可信平台模块(TPM)在可扩展固件接口(EFI)中建立可信链的方案。该方案通过对 EFI 启动过程的分析,建立了一条从 EFI 的第一个阶段开始,一直到操作系统的可信链。从而较大地缩小了信任根的范围,使得 BIOS 的安全性得到很大程度的提高。随着 EFI 的普及,这将在实现安全计算机系统上具有较好的应用前景。

关键词:可扩展固件接口;可信链;哈希算法;可信平台模块;数字签名
中图分类号: TP309 **文献标志码**:A

Research and implementation of trust transition based on EFI

ZHANG Rui[1], LIU Ji-qiang[1], PENG Shuang-he[2]
(1. *Research Center of Information Security Architecture, Beijing Jiaotong University, Beijing* 100044, *China*;
2. *Computing Center, Beijing Information Science & Technology University, Beijing* 100085, *China*)

Abstract: To further enhance the safety of BIOS, this paper presented a new trust transition model with Trusted Platform Module (TPM) in Extensible Firmware Interface (EFI). This model established a trust chain from the first stage of EFI to the operating system by analyzing the process of EFI startup. Thus the model narrowed the scope of the root of trust and substantially improved the safety of the BIOS. With the popularity of EFI, this model has a good prospect in achieving security on computer system.

Key words: Extensible Firmware Interfaces (EFI); trust transition; Hashing algorithm; Trusted Platform Module (TPM); digital signature

0 引言

可扩展固件接口(EFI)是英特尔公司为其新一代 64 位处理器安腾(Itanium)架构的服务器设计的操作系统和平台固件之间的接口规范,同时也兼容英特尔 32 位平台。EFI 定义了许多重要的数据结构以及系统服务,实现了这些数据结构与系统服务,就相当于实现了一个真正的 BIOS 核心。

虽然 EFI 有传统 BIOS 无法比拟的优点,但是 EFI 并没有解决 BIOS 面临的安全威胁。而且 EFI 大部分程序是用 C 语言实现的,这就意味着很多人都可以很容易破译 EFI,这对 EFI 的安全性提出了更高的要求。怎样实现一个安全可信的 BIOS 成为目前对 EFI 研究的热点。

使平台可信的根基在于有可信赖的根,然后以某种技术使信任从根转移到平台上来,使平台可信。系统在程序代码运行控制转移过程中,对下一级可执行代码真实性和完整性加以验证,就可以通过可信链传递的模式建立安全可信的系

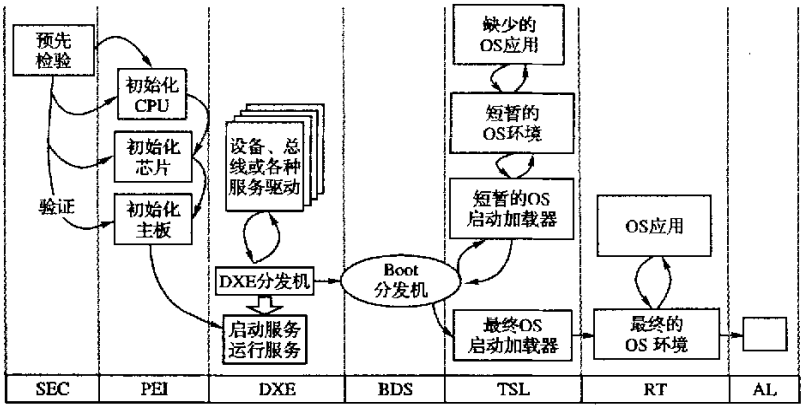

图 1 EFI 启动过程

收稿日期:2007 - 03 - 07;**修回日期**:2007 - 06 - 12。

作者简介:章睿(1981 -),女,浙江杭州人,博士研究生,主要研究方向:信息安全; 刘吉强(1973 -),男,山东海阳人,副教授,博士,主要研究方向:信息安全; 彭双和(1974 -),女,湖南衡阳人,讲师,博士,主要研究方向:信息与网络安全。

统运行环境。

可信计算组织(Trusted Computing Group, TCG)在 2006 年 9 月提出了基于 EFI 的 TCG 接口协议——EFI_TCG_PROTOCOL。[1,2]在 EFI 规范 2.0(Unified Extensible Firmware Interface Specification)中也提供了与安全相关的接口规范:安全启动(Secure Boot)、驱动签名(Driver Signing)和 HASH 算法(Hash)。[3]这为实现安全可信的 EFI 提供了统一的规范标准。

1　EFI 中可信链的构建

1.1　EFI 介绍

EFI 通过对特定平台的抽象,提出了一整套数据结构以及接口函数。整个 EFI 协议几乎是由许多不同的协议组组成。EFI 为驱动程序与应用程序的运行准备了一个完全模块化的运行环境,并且这些应用程序与驱动程序是用 C 语言开发的。开发者可以根据需要对 EFI 规范中某些相关协议组进行扩充(完成函数体的编写),实现需要的功能。[4]

EFI 开发软件包(EFI Develop Kit, EDK)是英特尔对于 EFI 规范的实现。EDK 以分阶段的方式初始化平台(如图 1 所示)。EDK 启动过程分为 4 个主要阶段:SEC(Security)阶段、PEI(PreEFI Initialization)阶段、DXE(Driver Execution Environment)阶段和 BDS(Boot Device Selection)阶段。SEC 阶段是电脑加电后的第一个阶段,主要负责验证平台硬件信息。PEI 阶段的目的只是为了找到并最少地初始化内存。DXE 阶段是大部分系统初始化的阶段,包括:DXE 核(DXE Core)、DXE 分发器(DXE Dispatcher)和一系列 DXE 驱动。DXE 核产生一系列的启动服务(Boot Services)、运行服务(Runtime Services)和 DXE 服务(DXE Services)。DXE 分发器负责发现和以正确的顺序执行 DXE 驱动。DXE 驱动则负责初始化处理器、芯片以及为系统服务、控制设备和启动设备提供软件提取的组件。BDS 阶段和驱动执行阶段一起建立控制台,并从启动设备中启动操作系统。EDK 启动完成后就进入 TSL(Transient System Load)和 RT(Run time)阶段。TSL 阶段是操作系统加载阶段。当操作系统加载完毕时,进入 RT 阶段。这时,从 DXE 阶段开始的大部分服务已终止,对处理器和平台资源的所有权从平台固件变为操作系统。AL(Afterlife)阶段是平台控制从操作系统返回到平台固件的阶段,是 RT 阶段的延长部分。AL 阶段以系统重启或以操作系统从睡眠状态醒来结束。

1.2　TCG 接口在 EFI 架构中的实现

可信计算的主要功能是由可信平台模块(Trusted Platform Module, TPM)完成的。TPM 也是建立可信链的主要部件。TPM 通过低脚位数(Low Pin Count, LPC)总线与 PC 芯片集结合在一起。它主要提供安全存储和平台完整性测量、存储和报告的功能。在建立可信链过程中,TPM 主要用来存储、管理密钥和对 EFI 各阶段进行完整性测量、存储。[5-7]

TCG 接口是作为 EFI 接口的一部分实现的,TPM 通过 TCG 接口来实现和平台的通信。在 EFI 中所有与 TPM 有关的活动是用 EFI_TCG 协议来描述的。EFI 中各种协议可以作为启动服务驱动(Boot Service Driver)来提供服务。同样,EFI_TCG 协议实例也可以作为一个启动服务驱动来提供有关 TPM 的启动服务。

1.3　可信链的构建

要实现可信的 EFI BIOS,关键就是要建立可信链。而要实现一个完整的信任链,必须满足两个条件:1)有一个可信的根,这个根是通过硬件封装和保护能力实现的;2)系统从可信根开始引导,每一级系统运行控制组件只有在确认其下一级系统运行控制组件是可信的时候,才将系统运行控制权转移给它。图 2 是在 EFI 架构中可信链传递的整个过程。

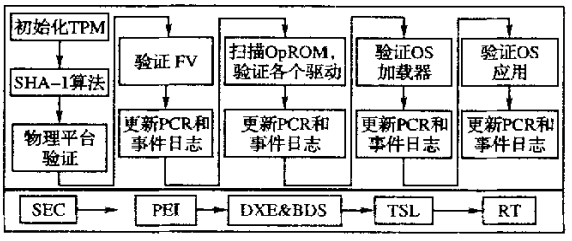

图 2　在 EFI 架构中可信链的传递

TPM 在 SEC 阶段进行初始化,并完成加电自检。由 SEC 代码得到系统硬件配置信息并对其真实性进行验证,其中包括 CPU、主板及 TPM 芯片。因此认为 SEC 阶段是可信的,并把它作为整个信任链的信任根。当 SEC 阶段执行完毕,调用 PEI 阶段代码时,需要对 PEI 的代码进行验证。由于 PEI 阶段的代码是放在一个固件卷(Firmware Volume, FV)中,并且代码量相对较少,因此只需对整个固件卷进行测量,然后用 EFI_TCG 协议中提供的函数对 TPM 相应 PCR 中的值和测量值进行 hash 运算,将哈希值保存到平台配置寄存器(Platform Configuration Register, PCR)中,更新事件日志(Event Log)。此时,信任就传递给了 PEI。进入 DXE 阶段后,需扫描 Option ROM,对将被加载的每一个驱动文件和设备文件进行完整性测量,更新 PCR 和事件日志。在 TSL 和 RT 阶段也做相似的操作,依次对操作系统加载器(OS Loader)、操作系统核心代码(OS kernel)和操作系统各种应用程序进行测量,然后更新 PCR 和事件日志。由此,信任依次传递,直到完成操作系统及其应用程序的加载,这样 EFI 中可信链的建立就完成了。

2　基于 EFI 的文件完整性验证

2.1　EFI Hash 协议在 32 位平台上的实现

哈希函数的目的就是要产生文件、消息或其他数据块的"指纹",即对任意大小的数据块进行"压缩"产生定长的输出。哈希函数又具有单向性和抗强、弱碰撞性,使它能够提供保密性、消息认证以及数字签名的功能。

在可信链的建立过程中,最关键的是对文件的完整性测量和验证。其中需要使用合适的哈希算法计算文件的哈希值,以此来保证文件的完整性。UEFI 规范 2.0 中提供了哈希服务接口协议,其中包括 EFI_HASH_SERVEICE_BINDING_PROTOCOL 和 EFI_HASH_PROTOCOL。

EFI_HASH_SERVEICE_BINDING_PROTOCOL 是哈希服务绑定协议,其作用是找到某一驱动支持的哈希服务,并且创建和撤销 EFI 哈希协议实例,这样使得多个驱动都能使用哈希服务。EFI_HASH_PROTOCOL 描述了几种重要的标准哈希函数,其中包括 MD5、SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512。

如图 3 所示,本文中实现的哈希算法是作为一个 DXE 驱动实现的。[8,9]

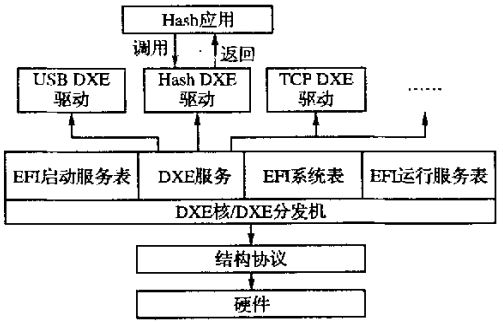

图 3 在 32 位平台的 EFI/EDK 上哈希算法的实现

当系统通过编译后会产生 Hash.efi 文件,这个文件就是 Hash DXE 驱动的可执行文件。这时,就可以调用 EFI_HASH_PROTOCOL 协议中的函数对文件进行完整性验证了。

2.2 文件完整性验证的实现

在可信链的建立过程中,为了保证文件的可信,可以根据策略对每一个被加载的文件进行数字签名,而在以后的每一次开机时系统会验证签名,这样就保证了每一个驱动文件的完整性。

当第一次初始化系统时根据策略选择某一哈希算法对每一个加载时需要验证的文件进行哈希运算,得到一个固定长度的哈希值,用签名算法的私钥对哈希值签名,把得到的签名值和公钥写入需要验证文件的文件头中,整个过程如图 4 所示。签名算法使用的私钥可以用 TPM 中的密钥树来管理。

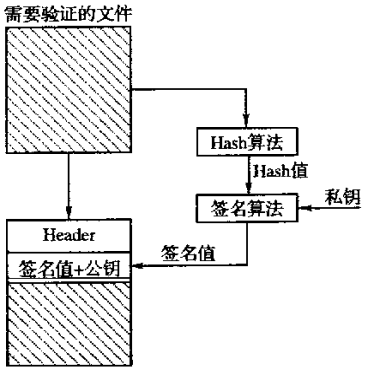

图 4 创建签名

以后的每次开机系统加载每个文件时会读取存放在文件头中的签名值和公钥,用签名算法的公钥对签名值解密,得到定长的哈希值。同时对文件的抽取出文件头以后的部分进行哈希运算也得到相同长度的哈希值。对这两个哈希值进行比较,如果一致,说明文件未被篡改或破坏;如果不同,说明文件已被破坏或篡改,系统会提示用户文件被破坏,并询问用户是否继续装载。如图 5 所示。

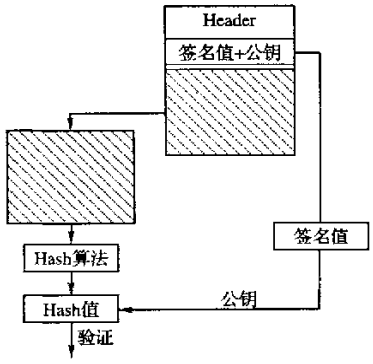

图 5 验证签名

需要加载的可执行文件通过验证后,才真正被加载,这样就保证了被加载文件的真实性与完整性。对文件完整性的验证是可信链传递过程中最重要的部分,只有通过验证,信任才能继续往下一级传递。

3 结语

基于可信根的信任链传递是实现可信平台的一个重要内容,是平台系统安全可信的根基。这方面的研究已有很多成果,但是大部分都是认为 BIOS 是可信的,把整个 BIOS 作为信任根,在此基础上建立信任链的研究。目前,对 BIOS 级可信链传递的研究还很少。

本文对 EFI BIOS 的可信链传递模型作了粗浅的研究,其中的许多技术还没有真正实现,如事件日志,密钥管理等,会在今后进行更深入地研究。

实现安全 EFI BIOS 仅仅依靠建立信任链是远远不够的,还需要实现很多安全技术,如 EFI BIOS 安全恢复和更新、关键数据区保护、用户管理等,对存在的安全漏洞和可能的攻击进行分析,不断完善 EFI,才能真正实现安全可信的 EFI BIOS。

参考文献:

[1] TCG. TCG EFI Protocol: Version 1.20 Final[S], 2006.

[2] TCG. TCG EFI Platform: Version 1.20 Final[S], 2006.

[3] Intel. Unified Extensible Firmware Interface Specification: Version 2.0[S], 2006: 1147 - 1165.

[4] 潘登, 刘光明. EFI 结构分析及 Driver 开发[J]. 计算机工程与科学, 2006, 28(2): 115 - 117.

[5] 秦中元, 胡爱群. 可信计算系统及其研究现状[J]. 计算机工程, 2006, 32(14): 111 - 113.

[6] 肖政, 韩英, 叶蓬, 等. 基于可信计算平台的体系结构研究与应用[J]. 计算机应用, 2006, 26(8): 1807 - 1809.

[7] TCG. TCG specification architecture overview specification revision 1.2[S], 2004.

[8] Intel. EFI driver library specification: Version 1.11[S], 2003.

[9] CHEN T Z, HE Z J. AES efficient implementation for extensible firmware interface[C]// Proceedings of the 17th IASTED International Conference. Montreal: [s.n.], 2006.

基于EFI的信任链传递研究及实现

作者： 章睿， 刘吉强， 彭双和， ZHANG Rui， LIU Ji-qiang， PENG Shuang-he
作者单位： 章睿,刘吉强,ZHANG Rui,LIU Ji-qiang(北京交通大学,信息安全体系结构研究中心,北京,100044)， 彭双和,PENG Shuang-he(北京信息科技大学,计算中心,北京,100085)
刊名： 计算机应用 ISTIC PKU
英文刊名： JOURNAL OF COMPUTER APPLICATIONS
年，卷(期)： 2007,27(9)
被引用次数： 7次

参考文献(9条)

1. TCG TCG EFI Protocol:Version 1.20 Final 2006

2. TCG TCG EFI Platform:Version 1.20 Final 2006

3. Intel Unified Extensible Firmware Interface Specification:Version 2.0 2006

4. 潘登;刘光明 EFI结构分析及Driver开发[期刊论文]-计算机工程与科学 2006(02)

5. 秦中元;胡爱群 可信计算系统及其研究现状[期刊论文]-计算机工程 2006(14)

6. 肖政;韩英;叶蓬 基于可信计算平台的体系结构研究与应用[期刊论文]-计算机应用 2006(08)

7. TCG TCG specification architecture overview specification revision 1.2 2004

8. Intel EFI driver library specification:Version 1.11 2003

9. CHEN T Z;HE Z J AES efficient implementation for extensible firmware interface[外文会议] 2006

本文读者也读过(10条)

1. 李晓勇.韩臻.沈昌祥.Li Xiaoyong.Han Zhen.Shen Changxiang Windows环境下信任链传递及其性能分析[期刊论文]-计算机研究与发展2007,44(11)

2. 刘皖.谭明.郑军.LIU Wan.TAN Ming.ZHENG Jun 基于平台可信链的可信边界扩展模型[期刊论文]-计算机工程2008,34(6)

3. 张海明 EFI下可信链建立关键技术研究与实现[学位论文]2008

4. 李莉.曾国荪.陈波.LI Li.ZENG Guo-Sun.CHEN Bo 基于时态逻辑的可信平台信任链建模[期刊论文]-计算机科学2008,35(4)

5. 邢彬 虚拟域可信链的设计与实现[学位论文]2009

6. 并行分类信任链传递模型[期刊论文]-计算机工程与应用2009,45(31)

7. 杨少谦 EFI BIOS安全增强方案设计与实现[学位论文]2009

8. 石文昌.单智勇.梁彬.梁朝晖.董铭.SHI Wen-chang.SHAN Zhi-yong.LIANG Bin.LIANG Zhao-hui.DONG Ming 细粒度信任链研究方法[期刊论文]-计算机科学2008,35(9)

9. 谭良.徐志伟.TAN Liang.XU Zhi-wei 基于可信计算平台的信任链传递研究进展[期刊论文]-计算机科学2008,35(10)

10. 徐锋.王远.张林.吕建.Xu Feng.Wang Yuan.Zhang Lin.Lü Jian 一个开放环境中信任链发现算法的设计与分析[期刊论文]-计算机研究与发展2006,43(z2)

引证文献(7条)

1. 陈峰 基于片上系统的EFI安全机制研究[期刊论文]-计算机应用 2009(z2)

2. 方炜炜.杨炳儒.周长胜.杨君 基于EFI的可信计算平台研究[期刊论文]-计算机应用研究 2009(8)

3. 邓子健.来学嘉.何大可 基于EFI和双核处理器的DRM agent[期刊论文]-计算机应用研究 2009(1)

4. 曾颖明.谢小权 基于UEFI的可信Tiano设计与研究[期刊论文]-计算机工程与设计 2009(11)

5.张颖.周长胜 EFI下基于便携式TPM的可信计算平台研究[期刊论文]-计算机技术与发展 2010(1)

6.张毅.梅挺 操作系统的可信平台安全性分析[期刊论文]-计算机工程与设计 2011(4)

7.Lei HAN.Jiqiang LIU.Zhen HAN.Xueye WEI Design and implementation of a portable TPM scheme for general-purpose trusted computing based on EFI[期刊论文]-中国计算机科学前沿 2011(2)

引用本文格式：章睿.刘吉强.彭双和.ZHANG Rui.LIU Ji-qiang.PENG Shuang-he 基于EFI的信任链传递研究及实现[期刊论文]-计算机应用 2007(9)