Computer Firmware Security Technology

计算机固件安全技术

周振柳 著

Zhou Zhenliu

清华大学出版社

计算机固件安全技术
Computer Firmware Security Technology

周振柳　著
Zhou Zhenliu

清华大学出版社
北京

内 容 简 介

本书内容涵盖作者在计算机固件安全领域多年的研究成果，是国内第一部公开出版的计算机固件安全领域的学术著作。

全书内容包括：计算机固件概念和功能、国内外固件产品和技术研究发展历程、固件开发基础技术与规范、固件安全研究历史与现状、传统固件 BIOS 安全技术研究开发实例、BIOS 安全漏洞及其威胁、BIOS 安全检测方法与实现、可信固件开发的安全策略和模型、可信固件中可信度量基础与方法、可信固件的开发实现。

本书可作为高等学校网络安全、信息安全专业教材，或相关专业人员的参考研究书籍。

图书在版编目（CIP）数据

计算机固件安全技术/周振柳著. --北京：清华大学出版社，2012.12
ISBN 978-7-302-30111-0

Ⅰ. ①计…　Ⅱ. ①周…　Ⅲ. ①固件－安全技术　Ⅳ. ①TP303

中国版本图书馆 CIP 数据核字（2012）第 217798 号

责任编辑：梁　颖
封面设计：
责任校对：李建庄
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张：**12.25　　**字　　数：**269 千字
版　　次：2012 年 12 月第 1 版　　**印　　次：**2012 年 12 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：049790-01

前　言

FOREWORD

计算机固件 BIOS 的发展历史并不长，它诞生于 1981 年出产的第一台个人计算机中。尽管固件 BIOS 产品一直是计算机中最底层、最核心的关键性部件之一，但却由于其位处后台，默默无闻，而少人关注。而在国内，BIOS 产品则成为我国计算机产业链中长期缺失的一环，只能依赖我国台湾地区和国外的产品。

1995 年初始，笔者有幸参与“FTPC-8086 柔性实验教学系统”的开发，负责下位机系统软件的编写工作，主要就是从开机上电的第一条指令开始编写，完成各硬件部件测试例程、单步中断（int 1）例程、断点中断（int 3）例程，以及其他常用的 BIOS 中断和 DOS 中断例程，并将例程执行结果通过串口通信返回给上位机上的集成调试运行环境，以使这些例程能被上位机运行的程序调用执行。其中下位机上从开机上电的第一条指令开始，每一个例程，都需要自己独立编写完成，工作的实质就是要写一个 Mini BIOS。因此不得不查阅学习了许多 BIOS 底层和 DOS 底层相关技术，并精熟了汇编语言程序设计。自此体会到底层固件开发的挑战和乐趣，也经常愿意在专业课教学中向学生炫耀这一段开发历程。这项工作，为笔者后来步入计算机固件安全研究领域奠定了技术基础。

大概在 2002 年 3 月的时候，刘军找到我，跟我讲了美国 BIOS 厂商 Phoenix 公司的 Phoenix. net 产品的事情，希望我能够对它研究一下。Phoenix. net 是 Phoenix 公司的一个 BIOS 产品项目，计划在计算机底层 BIOS 固件中嵌入一个“音序器”，指导并帮助计算机用户完成在操作系统安装后烦琐的应用软件下载和安装工作。笔者因此采用了逆向工程的方法，对 Phoenix. net 固件产品进行了研究剖析并提交了技术分析报告。这项工作，向笔者揭开了计算机固件层次安全的神秘面纱，自此发现计算机固件安全的别样洞天，成为笔者步入计算机固件安全研究领域的契机。后来一系列 BIOS 安全增强、BIOS 安全代理、BIOS 木马研究工作，都自此展开。非常怀念这一段美好神奇的研究开发之旅。

2005 年，笔者有幸拜入到我国著名网络安全专家许榕生先生门下，成为先生的博士学生。鉴于国内对计算机固件安全研究关注甚少，先生建议我对计算机固件安全开展系统性的研究工作。于是深入挖掘固件安全漏洞，研究其安全检测原理和方法。时值信息产业部（现工业与信息化部）在幕后者多年的努力推动下，终于启动并支持“新一代安全 BIOS 的研制和产业化”、“高安全与可管理 BIOS”等研究项目工作，笔者也参与其中，开展安全 BIOS 和可信固件的研究开发工作。

在以上历程中，每每感叹国内计算机固件 BIOS 领域资料的缺乏。时至今日，也只有台湾地区旗标出版社出版的陈文钦著《BIOS Inside BIOS 研发技术剖析》一书，可算国内唯一能找到的中文 BIOS 技术宝典，而涉及计算机固件安全的公开出版物，则尚未得见。有感如此，深感补此遗缺，乃我辈之责任。遂成书，以飨读者。

本书共 9 章，其内容可分为三部分。第一部分讲述计算机固件技术发展历程、安全研究现状、技术基础，包括第 1 章和第 2 章；第二部分阐述传统固件 BIOS 的安全技术、安全漏洞及其安全检测方法和系统，包括第 3 ~ 5 章；第三部分从可信理论出发，研究基于新一代 EFI 固

件的可信固件安全策略模型、可信度量基础和方法以及可信固件的开发实现，包括第 6 ~ 8 章；最后是对本书研究内容的总结和展望。

本书成书及出版，得到众多热心人的支持和帮助。在本书最后部分的致谢中，笔者要对他们致以衷心的感激之情。特别地要感谢清华出版社的编辑梁颖老师对本书出版的支持和跟踪追进。

周振柳

2012 年 7 月于沈阳

Computer Firmware Security Technology

第1章 引 言

计算机传统固件 BIOS 产品,由于其深处计算机运行后台,用户可见的运行周期少至只有几十秒,因此不为计算机用户所熟知。而传统固件 BIOS 技术,IBM 设计之初是开放的状态,但由于其底层地位和纽带作用,后来的发展陷入到封闭状态,只为少数几个厂商所掌握,外人知之甚少。基于这些原因,计算机固件安全这个领域,在国内很长一段时期内被忽视,无人瞩目。

本章介绍计算机固件产品的概念、功能和作用,简单叙述从传统 BIOS 到 EFI 固件的发展历程,从中引出固件 BIOS 安全研究的背景、历史与现状。以期引起对计算机固件安全研究的兴趣和重视。

1.1 固件在计算机中的地位和作用

计算机固件是计算机系统中不可缺少的底层基础系统。这些固件往往是以软件的形式固化存储在硬件芯片中。计算机主板上有最重要、最核心的计算机固件,通常称为 BIOS(Basic Input/Output System,基本输入输出系统),计算机加电时,中央处理

器(Central Processing Unit,CPU)取得并执行的第一条指令,就存储在 BIOS 固件中。因此,BIOS 固件首先取得计算机运行控制权,其后的硬件系统初始化和检测都由 BIOS 固件完成,最后才加载计算机操作系统,并把系统控制权移交给操作系统。但由于 BIOS 固件处在软件的最底层,很少直接同用户交互,因此往往被大多数人忽视。

1.1.1 固件和 BIOS 的概念

固件(Firmware)是一种底层软件或指令序列,早期常常存储于计算机或外部设备的可编程只读存储器(Programable Read-Only Memory,PROM)中。固件常用于对硬件设备进行配置,使得硬件设备能够完成指定的功能,或者为操作系统提供硬件操作接口。一些固件也可能成为操作系统内核的一部分,为操作系统的其他部分提供基本服务,并运行于特权模式下,这种情况多见于嵌入式系统和设备中。在计算机系统中,BIOS 就是一种核心固件。计算机系统中其他的一些外围设备(如显示卡、网卡等)上也存在着固件,用于初始化、驱动这些设备,为操作系统提供操作接口。

1981 年,IBM 在设计第一部个人计算机——IBM PC 时,工程师把一些开机时的硬件初始化/检测代码,从软盘或硬盘装载操作系统、完成开机程序的前导代码,以及一些最基本的外围设备处理的代码(如屏幕显示、磁盘驱动等),压缩存入一颗大约 32KB 大小的 PROM[1],这些代码组成了 BIOS。

当计算机开机的一瞬间,硬件特性就是设计成 CPU 从主板上 BIOS 芯片内取得指令码(对于 16 位计算机这个地址是 0FFFF0,对于 32 位计算机这个地址是 0FFFFFFF0),BIOS 内部的指令取得系统控制权,然后再跳转到 BIOS 固件其他位置的指令去执行。经过 CPU 的检测设定、配置内存、初始化南北桥芯片组,最后驱动磁盘把操作系统载入内存,将系统控制权转移给操作系统引导代码(OS Loader),BIOS 的开机引导工作就告一段落,改为从事幕后对操作系统的支持、协调工作,帮助操作系统或应用程序来处理外围设备的执行动作。

事实上除了主板上的 BIOS 外,另外如显卡、SCSI 卡、网卡、硬盘控制器等也都有各自的 BIOS 芯片。设计在主板上、负责整个主板运行的 BIOS,一般称为系统 BIOS

(System BIOS)或主板 BIOS(Mainboard BIOS),如果没有特别声明,BIOS 所指就是主板上的 BIOS;而显卡上的 BIOS 一般称为 Video BIOS,SCSI 控制卡上的 BIOS 则以 SCSI BIOS 称呼。这种扩展卡或控制器上的 BIOS 后来也统称为 OPROM(Option ROM)。

这种固件早期都存储在 PROM 芯片中,只能用特定的编程器对其进行读写操作,不能在主板等设备中直接对其进行读写操作;其容量也逐渐从 8KB、16KB、32KB、64KB 增加到 128KB、256KB 和 512KB 不等。从大约 1996 年以后,伴随 flash 芯片技术的发展,以及对 BIOS 固件在线更新的要求,以及计算机系统使用后期要求能够从 BIOS 固件更新 CPU 微代码(Micro Code),从而实现为 CPU 打补丁功能的出现,计算机系统中的固件存储逐渐从 ROM 芯片转换成 flash 芯片。其特征是:①芯片容量继续增大,以适应越来越多的应用加入到固件中的要求,②允许在操作系统运行过程中,通过指定技术直接对固件芯片中的内容进行更新写入。在为用户和系统维护带来更多的方便功能的同时,也就此引入了更多的安全风险。

1.1.2 固件功能及地位

计算机系统层次架构由硬件(Hardware)、固件(Firmware)、软件(Software)构成,传统上计算机固件的核心就是 BIOS,计算机软件的核心是操作系统,如图 1.1 所示。在这种层次架构中,BIOS 介于硬件和操作系统之间,为操作系统提供最直接、最底层的硬件控制,为操作系统的引导载入和正常运行提供良好支持。这种架构的好处之一,是 BIOS 能够为操作系统提供一定程度的硬件抽象层,使操作系统可以不涉及具

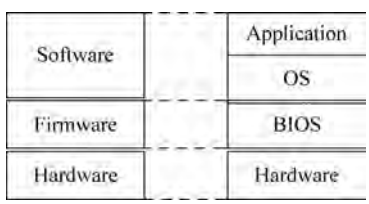

图 1.1 计算机系统层次架构

体的硬件操作,具有更好的平台无关性。

BIOS 是计算机的核心部件之一,计算机开机以后执行的第一条指令就由 BIOS 发出。BIOS 担负着系统最初的引导和启动任务,为操作系统对计算机系统硬件设备进行管理提供基础服务。没有 BIOS,计算机系统的所有硬件就无法工作。BIOS 的损坏直接导致计算机系统可用性遭到破坏,只能通过芯片级别的硬件维修才能够恢复。

BIOS 的主要功能可以概括为下面几点[1,2,3]:

(1) **开机自检(Power On Self Test,POST)** 计算机开机时系统将控制权交给 BIOS,BIOS 针对 CPU 各项寄存器、标志位等先检查 CPU 是否工作正常,接下来会检查 8254 定时器、8259A 可编程中断控制器、8237DMA 控制器等的状态,测试其是否工作正常。这些自检还包括 640KB 的基本内存、串并口、键盘、显卡等。一旦在自检过程中发现问题,BIOS 将给出提示信息或鸣笛警告。

(2) **系统初始化** 针对 CPU Cache、DRAM、南北桥芯片组、显卡、PCI 设备控制器、IDE 设备控制器、网卡等的寄存器作初始化操作,填充相应寄存器的值,设定成可支持的默认工作模式,并检测是否能够正常工作。查找并运行外围设备上存在的 Option ROM 使其对外围设备进行驱动。

(3) **提供常驻内存的运行时服务(Runtime Services)** 这些服务程序常驻在某一段系统内存中,操作系统和应用程序能够通过中断方式调用这些服务代码,典型的如 Int 10h、Int 13h、Int 15h 等。这些常驻内存的运行时服务使得系统控制权由 BIOS 转移给操作系统后,BIOS 代码仍然可以在适当的时机被执行。

(4) **系统设置** BIOS 提供文本或图形界面的设置程序(通常称为 BIOS Setup),供用户在进入操作系统前对系统的一些参数值进行设置,如 BIOS 密码、光盘/硬盘/软盘引导顺序、系统时间等。这些参数设置记载在非易失性存储体(Non-Volatile RAM)中,如 CMOS(Complementary Metal Oxide Semiconductor,互补金属氧化物半导体)芯片或 flash 芯片的扩展系统配置数据区(Extended System Configuration Data,ESCD)。

(5) **引导操作系统** BIOS 在执行的最后阶段,会按照设置中保存的启动顺序搜索软硬盘驱动器及 CD-ROM、网络服务器等,查找到有效的启动记录后,读入操作系

统引导代码,然后将系统控制权交给引导代码,并由引导代码来完成操作系统的装载启动。

1.2 相关领域国内外研究现状和趋势

在计算机系统中,固件处于一个很不显眼的位置,并且较少同用户直接交互。但固件却是计算机系统中不可或缺的底层软件系统,如果固件系统的安全得不到保障,则其上层操作系统的安全以及应用软件层的安全保障措施都可能失效。伴随固件和安全技术的发展,固件在信息安全中的重要性逐渐呈现出来[4]。

1.2.1 计算机固件产品研发现状和趋势

从1981年第一个BIOS产品出现以来,BIOS技术和产品的发展同IT行业其他领域发展相比较,呈现一个明显的滞后状态。在计算机中央处理器、外围部件和操作系统从8位到16位、32位、64位的快速发展过程中,BIOS技术则从最初的8位发展到16位后一直停滞不前。这里有两个重要的原因:一是BIOS技术处于底层,只需要完成对平台硬件初始化,引导操作系统即可,很少直接同用户交互,因此推动其发展的动力不足;二是BIOS技术和市场的垄断,使得BIOS厂商为保护自己的既得利益,不愿意去推动BIOS新技术和新产品的发展。

1998年,Intel公司开始封闭开发一种专用于其服务器的64位BIOS产品。2003年,Intel在将该新一代BIOS产品成功地应用于Intel 64位服务器的基础上,发布了32位和64位新一代BIOS产品的新规范——扩展固件接口(Extensible Firmware Interface,EFI)[5],并联合业界Microsoft、IBM、Hp、AMI、Dell、Phoenix、AMD等厂商推动该规范成为下一代BIOS的行业规范——Unified EFI(UEFI)[6,7]。通过随后几年的推动,目前UEFI已经成为新一代BIOS的行业标准,并且到2007年,Intel已经将其生产的所有主板、PC和服务器上的BIOS换成符合UEFI标准的新一代BIOS产品。BIOS

厂商 Insyde 和 AMI 也已经推出新的符合 UEFI 规范的 BIOS 产品。

从 BIOS 产品市场来看,公用 BIOS 产品一直由我国台湾地区和美国公司所垄断。1998 年之前,全球公用 BIOS 市场由美国 Phoenix、AMI 和我国台湾地区 Award 三家垄断,1998 年之后则是美国 Phoenix、AMI 和我国台湾地区 Insyde 三家垄断(Award 公司被 Phoenix 公司所收购,以弥补其在 PC 固件产品中市场占有不足的局面)。欧洲企业共同制定的 Open Firmware 规范由于缺乏 BIOS 厂商和芯片组厂商的技术支持,也只能在较小范围的专用服务器上形成可用产品。而一些开源 BIOS 项目如 LinuxBIOS[8,9]、TinyBIOS 也由于同样的原因只能用于少数定制的硬件平台和操作系统。由于牵扯到专利权与厂商之间的竞争因素,BIOS 产品的兼容性与合法性一直是试图进入这一领域的企业要面对的严肃问题。另外,芯片组技术和资料的垄断,也是形成 BIOS 技术和产品垄断的一个重要因素。

我国信息技术产业在 BIOS 领域长期以来处于空白局面,国内 PC 和服务器 BIOS 完全依赖上述三家 BIOS 厂商提供产品和服务。这不仅影响我国建立完整的信息产业链,对国家的信息安全来讲也是一个不可忽视的隐患。借助新一代 BIOS 发展的契机,2005 年我国信息产业部通过电子产业发展基金支持,启动“新一代安全 BIOS 的研制和产业化”、“高安全与可管理 BIOS”等项目,推动自主研发适合我国国情的 BIOS 产品的研究工作。其中获得 Intel 公司技术合作支持的包括中国电子科技集团信息化工程总体研究中心和南京百敖软件有限公司(BYOSOFT)。

1.2.2 BIOS 安全研究历史与现状

国内外对安全操作系统 30 多年的持续研究,在理论方法、技术和产品上都取得了丰富的成果[10,11,12,13,14,15,16],而对计算机 BIOS 系统的安全研究 20 多年来则几乎被忽略。William A. Arbaugh 等在 1997 年提出一种计算机安全引导架构 AEGIS[17]。AEGIS 基于 IBM PC 传统 BIOS,采用认证的方法保障 BIOS 固件代码的完整性,增强 BIOS 引导过程中 BIOS 代码的安全保护。但 AEGIS 缺乏硬件保护措施,也没有考虑

固件层对系统软件层的延伸保护。1998 年,Dexter Kozen 在基于语言安全研究[18,19,20,21,22]的基础上提出一种简化高效的语言证明方法 ECC[23],使用编译技术在代码执行前检查代码控制流、内存访问以及堆栈操作的安全逻辑,并针对 Open Firmware 语言和指令集进行了优化和实现。2002 年,Frank Adelstein、Matt Stillerman 和 Dexter Kozen 演示了在 Open Firmware 中如何利用 ECC 方法进行固件的恶意代码检测[24]。2003 年,Matt Stillerman 和 Dexter Kozen 开发了基于 ECC 的安全 Open Firmware 的原型系统[25],由于语言证明方法的复杂性,这种方法并不成熟,离实际应用尚有较大差距。

而从 1998 年开始,针对 BIOS 系统的公开性的安全事件和威胁时有发生。1998 年 7 月开始爆发的 CIH 病毒就实施了对计算机 BIOS 的攻击,造成全球大量 PC 不能使用。1999 年和 2000 年,美国 BIOS 厂商 Phoenix 公司的 PhoenixNet 产品在 BIOS 中嵌入的 ILS 模块具有远程安装、控制、回传、定位等功能,涉嫌控制用户计算机和暴露用户隐私,遭到广泛的抵制和批评[4]。2006 年全球 Black Hat 会议上,英国 Next-Generation 安全软件公司的首席安全顾问 John Heasman 阐述了一种新的 rootkit 技术[26],在计算机主板 BIOS 闪存中隐藏 rootkit 恶意代码并使之在操作系统运行过程中生效。2007 年的 Black Hat 会议上,John Heasman 继续其对固件 rootkit 技术的研究,这一次他将 rootkit 技术应用到了主板 PCI 板卡的 OPROM 闪存中[27]。

美国 2006 年的《计算机安全与信息保障研究与发展联邦计划》(Federal Plan for Cyber Security and Information Assurance Research and Development)[28]提出 12 项计算机安全和信息保障基础技术,其中“硬件和固件安全”名列首位。该文对硬件和固件安全重要性的描述如下(原文引用,第 69 页)[28]:

“Hardware or firmware attacks can undermine even the most sophisticated application-level controls or security mechanisms. Malicious firmware that has unrestricted access to system components (e.g., if it is part of the OS kernel) has considerable potential to cause harm, introduce backdoor access (an undocumented way of gaining access to a computer, program, or service), install new software, or modify existing software. If the underlying hardware and firmware cannot be trusted, then the OS and application security mechanisms