第33卷 第16期 计 算 机 工 程 2007年8月
Vol.33 No.16 Computer Engineering August 2007
·安全技术· 文章编号：1000—3428(2007)16—0114—03 文献标识码：A 中图分类号：TP309

计算机BIOS安全风险分析与检测系统研究

周振柳[1]，刘宝旭[1]，池亚平[2]，许榕生[1]
(1. 中国科学院高能物理所计算中心，北京 100049；2. 北京电子科技学院，北京 100070)

摘 要：介绍了计算机BIOS安全风险的形成及特点，总结了BIOS安全风险的分类，提出了BIOS安全威胁模型和基于BIOS安全隐患扫描和代码完整性度量的BIOS安全检测模型。实现了一个基于BIOS安全隐患库与BIOS标准代码样本库的BIOS安全检测系统。指出BIOS在信息安全基础解决方案中的进一步安全增强和安全扩展的研究方向。

关键词：BIOS；安全风险；安全隐患；安全检测

Research on Computer BIOS Security Risk Analysis and Detection System

ZHOU Zhen-liu[1], LIU Bao-xu[1], CHI Ya-ping[2], XU Rong-sheng[1]
(1. Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049;
2. Beijing Electronic Science and Technology Institute, Beijing 100070)

【Abstract】 This article introduces the progress and characteristics of BIOS security threat, summarizes the BIOS security risk classification, advances a model of BIOS security threat and a model of BIOS security detection which based on scanning of BIOS vulnerabilities and measuring of BIOS code integrity. A BIOS security detection system, based on the libraries of BIOS vulnerabilities and BIOS standard code samples, is implemented. Further study directions about enhancing and extending BIOS security role in information security fundamental solution are also presented.

【Key words】 BIOS; security risk; security vulnerability; security detection

1 概述

计算机BIOS(basic input/output system)是固化在计算机主板芯片里的软件系统，也称固件。计算机开机上电首先执行BIOS指令，完成基础硬件和外围设备的检测及初始化，装载为系统运行时提供的服务，最后引导操作系统[1]。

一般而言，传统信息安全威胁较多集中在软件系统上。而根据笔者多年的跟踪研究发现，固件BIOS的安全风险问题正日益突出。BIOS安全风险和威胁的出现是多种因素共同作用的结果。早期BIOS功能简单，其二进制代码体积小，烧录在32KB的PROM或EPROM芯片中。伴随BIOS功能扩展，容纳BIOS的芯片容量增加，逐渐扩大到512KB，甚至是1 024KB。

PNP, DMI, ESCD, SMBIOS等标准要求BIOS与操作系统交互[2]，主机板BIOS要能够记录外围设备变化情况和资源配置变动情况，并与操作系统交换数据，而在系统运行中对BIOS的更新需求也日益增多。为适应这些变化，主机板BIOS芯片逐步被可用软件改写更新的FLASH芯片取代。而显卡、网卡等OPROM也都改用FLASH芯片存储。主机板上设计有FLASH芯片读写硬件线路，使用软件方法，把FLASH芯片的写电压拉升到某种特定电压，或输入指定的擦除信号，就可以实现对FLASH整颗芯片的存储内容擦除改写，或擦除改写部分块(block)和分区(sector)。

这些新技术的发展使BIOS安全威胁逐步显示出来。BIOS安全风险来自2方面：(1)对BIOS芯片和存储内容的破坏，导致对计算机主机板硬件层和固件层攻击，CIH病毒是这种BIOS安全威胁的一个著名实例；(2)利用BIOS自身设计隐患，或利用BIOS芯片剩余空间嵌入非法程序，实现对计算机系统的远程控制，文献[3]对此有初步的描述。与传统的基于软件的信息安全风险相比较，BIOS安全风险存在于硬件芯片中，具有更隐蔽、不易检测、不易清除、不受操作系统和磁盘更新影响等特点。目前，国际国内信息安全领域对BIOS安全风险的研究几乎是空白。本文对这一新研究方向进行了初步的探讨研究。

2 BIOS安全威胁模型

BIOS安全风险分析，以BIOS安全威胁模型为基础。该模型描述和揭示BIOS安全威胁的来源、种类及危害，是BIOS安全风险分析和安全检测的理论基础。通过对BIOS安全问题的长期跟踪研究和分类归纳，本文建立了计算机BIOS安全威胁模型，如图1所示。

2.1 BIOS安全威胁来源

由图1可以看出，BIOS安全威胁来源主要有2种：(1)BIOS自身。由于BIOS自身扩充功能设计障碍可能导致本地计算机硬件、磁盘数据或系统软件造成损害，但不会被远程恶意者所利用，如图1中的①。(2)BIOS外部，外部恶意者

基金项目：国家自然科学基金资助项目(90412017)；北京电子科技学院科研基金资助项目

作者简介：周振柳(1971－)，男，博士研究生，主研方向：网络安全，可信计算；刘宝旭，副研究员；池亚平，副教授；许榕生，研究员、博士生导师

收稿日期：2006-08-29 **E-mail：**zhouzl@ihep.ac.cn

利用 BIOS 配置漏洞和设计缺陷，通过网络实施对本地计算机的侵入或破坏，如图 1 中的②，③，④。

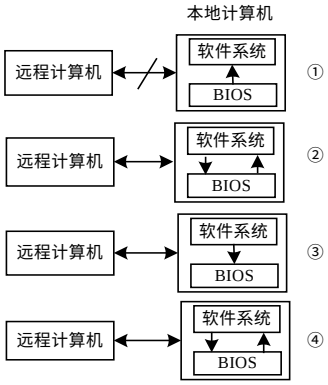

图 1　计算机 BIOS 安全威胁模型

2.2　BIOS 安全威胁种类及危害

BIOS 安全威胁模型，将 BIOS 安全威胁归纳为 4 种类型：

(1)BIOS 功能障碍。主板厂商从 BIOS 厂商处获取授权 BIOS 源代码后，会根据主板采用的芯片组情况，对 BIOS 源代码进行修改，定制满足自身主板要求的 BIOS。主板厂商为了增强自身主板的特点，也会在 BIOS 中集成一些自身开发或其他第三方开发的 BIOS 功能模块。这些功能模块不属于 BIOS 标准功能，在实际使用中由于硬件或软件兼容性问题，可能对计算机造成一定的功能障碍或一定程度的破坏。如集成在 BIOS 中的防引导扇区病毒模块会造成某些分区软件的失败，造成 Linux 操作系统装载软件失败；而集成的磁盘恢复精灵模块在某些情况下会造成硬盘恢复失败和数据丢失。这种类型的 BIOS 安全风险是由内及外的。该类威胁如图 1 中的①所示。

(2)BIOS 配置漏洞。利用本地计算机 BIOS 配置漏洞，远程计算机通过网络使用软件可以对本地计算机的某些 BIOS 选项设置，进而配合使用工具软件完成对本地计算机的远程存取和控制。由于 BIOS 的这些功能配置漏洞深入硬件底层，远程攻击者甚至可以在本地计算机关机的情况下，在特殊时段，通过工具软件开启本地计算机，不知不觉完成对本地计算机的存储访问。但这种威胁不会危及 BIOS 自身的芯片和代码安全。该类威胁如图 1 中的②所示。

(3)BIOS 物理攻击。不使用特殊烧录设备的情况下，使用软件手段提升主机板写入电压，可以对存储 BIOS 的 FLASH 芯片进行读写。远程计算机或网络向本地计算机植入病毒，利用 BIOS 的 FLASH 芯片这一特点，可以直接改写或擦除 FLASH 芯片存储的内容导致计算机不能正常启动，甚至造成主机板部分电路或芯片的物理损坏。CIH 病毒是这种物理攻击的典型案例。这种物理攻击的实现，在 Windows 系列操作系统下都可以通过采用设备驱动程序的编写方法，进入 RING0 级特权模式实施。这种安全威胁是由外及内的。该类威胁如图 1 中的③所示。

(4)BIOS 木马。BIOS 木马是指隐藏在 BIOS 芯片中的木马程序。主机板提供的 BIOS 芯片一般为 256KB, 512KB 或 1024KB，而 BIOS 二进制代码并没有完全占用这些空间。

据笔者的研究统计结果表明，BIOS 二进制代码一般只占用 FLASH 芯片 60%~70%的空间，往往 FLASH 芯片会剩余几十 KB 到几百 KB 的空间。恶意攻击者将木马包装成合法的 BIOS 功能模块，利用 Windows 或 Linux 下的 BIOS 读写工具软件，向 BIOS 芯片中植入木马。植入 BIOS 的木马能够反向释放到操作系统中运行。BIOS 木马能完成普通木马具备的所有功能，同时又具备普通木马所不能比拟的优势，如抗硬盘重分区、抗硬盘格式化、抗操作系统重装，甚至更换硬盘都不会对其产生影响。文献[3]对此有描述，而笔者在实验中也成功地实现了这一技术。该类威胁如图 1 中的④所示。

3　BIOS 安全隐患扫描

基于 BIOS 安全威胁模型，本文将 BIOS 安全隐患分为 2 大类：(1)BIOS 固有安全隐患。BIOS 开发标准要求 BIOS 软件提供 PNP、ACPI、远程管理设置、远程诊断调试等功能。这些功能的存在及 BIOS 选项配置的不合理导致 BIOS 存在安全隐患。这些都属于 BIOS 固有安全隐患。(2)BIOS 外来安全隐患。主板厂商及其他厂商、公司、单位、个人因某种需要而对 BIOS 功能进行扩展导致 BIOS 存在的安全隐患都属于这一类。

3.1　BIOS 安全隐患分析

采用安全隐患情景分析法[4]，发现并验证了BIOS中目前存在的 6 种已知安全隐患。对其他可能存在的BIOS安全隐患，暂时归为未知安全隐患。BIOS安全隐患如表 1 所示。

表 1　BIOS 安全隐患

隐患名称	隐患类型
远程开机隐患	固有安全隐患
定时开机隐患	固有安全隐患
ChipAwayVirus 隐患	外来安全隐患
磁盘恢复精灵隐患	外来安全隐患
Phoenix.Net 隐患	外来安全隐患
BIOS 木马隐患	外来安全隐患
其他未知隐患	固有/外来

BIOS 远程开机隐患允许在计算机关闭电源的情况下，使用特殊的工具软件，通过网卡或调制解调器，远程打开计算机电源。BIOS 定时开机隐患允许在计算机关闭电源的情况下，当 BIOS SETUP 中设定的日期时间到来时，BIOS 自动打开电源启动计算机，自动处理用户预先设定的任务。ChipAwayVirus 是主板厂商集成在 BIOS 中的反引导扇区病毒模块。某些情况下该模块会错误报警，阻止系统分区或引导。特别会引起 LILO 和 Linux 的引导及安装失败。集成在 BIOS 中的磁盘恢复精灵模块存在设计缺陷，工作不稳定，并且只支持微软的操作系统文件格式，不支持 Unix 和 Linux 的文件格式，某些情况下恢复操作可能导致用户磁盘数据被破坏。Phoenix.Net 模块由 BIOS 厂商 PHOENIX 集成在 BIOS 中。该模块具备在线网络验证、网络下载上传功能。有暴露网络计算机用户个人隐私、网络行为习惯的嫌疑。BIOS 木马是由恶意用户通过网络远程植入 BIOS 中的具有木马功能的模块。每次计算机系统启动后，植入的木马会自动从 BIOS 中释放到系统中运行。

收集不同的 BIOS 类型和样本，通过对 BIOS 二进制影像文件进行模块分解、解压缩，然后进行隐患特征分析、提取、验证，笔者获取了上述安全隐患的特征码。

3.2　BIOS 安全隐患库

通过对 BIOS 安全隐患分析，采用 6 元组描述已发现的 BIOS 安全隐患，本文建立了 BIOS 安全隐患库。BIOS 安全隐患的 6 元组描述表达为

$V=\{t, n, k, m, p, d\}$

其中，V 表示一种安全隐患；t 表示安全隐患类型；n 表示安全隐患名称；k 表示安全隐患的一组或多组特征码；m 表示

安全隐患涉及的一个或多个 BIOS 模块；*p* 表示对该安全隐患解决方案的建议；*d* 表示对该安全隐患的危害和利用情况描述。

利用建立的 BIOS 安全隐患库可以对 BIOS 实施隐患扫描。隐患库的数据规模则须随着 BIOS 安全研究的深入而进一步充实。

4 BIOS 代码完整性度量

在安全需求较高的计算或网络环境中，为保证 BIOS 的安全，需要进一步对 BIOS 模块代码进行完整性度量和报告。

BIOS 中模块可分为 3 类：(1)数据模块，存储 BIOS 字符数据、图形数据或资源配置信息，这类模块不包含可执行代码；(2)可直接在 ROM 中执行的模块；(3)需要装入到 SHADOW 或 RAM 中才可以执行的模块。后 2 种模块都包含可执行 BIOS 代码。

对包含可执行代码的模块，为防止代码被恶意修改，在高安全需求环境中，需要对代码模块进行完整性度量和报告。在实际研究中，通过建立 BIOS 标准代码样本库，并对各个标准代码样本模块生成 MD5 消息摘要，比较标准代码样本和被检测代码样本的 MD5 消息摘要，实现代码模块的完整性度量。

根据对 3 种主流 BIOS 厂商的 BIOS 产品的分解结果，归纳了 31 种常见的 BIOS 可执行代码模块标准类型。不同 BIOS 厂商 BIOS 产品和不同主板厂商的主板，这 31 种常见的可执行代码模块的代码可能存在差异。因此，BIOS 标准代码样本库中的代码模块要按照不同的计算机机型来建立。

5 BIOS 安全检测模型与技术实现

经过长期对 BIOS 安全的分析实践，本文建立了一个 BIOS 安全检测的自反馈闭路模型，该模型以 BIOS 安全隐患库和标准代码样本库为安全检测基础，如图 2 所示。

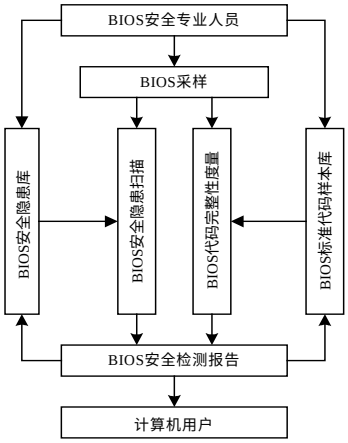

图 2 BIOS 安全检测模型

在该模型中，BIOS 安全专业人员根据研究分析结果预先建立 BIOS 安全隐患库和 BIOS 标准代码样本库。使用开发的专用 BIOS 安全检测系统对计算机 BIOS 进行安全检测。若检测结果发现未知的 BIOS 功能模块，安全分析人员进一步分析该模块的功能，并对模块提取特征代码。根据分析数据和结果，完善和充实 BIOS 安全隐患库或 BIOS 标准代码样本库。

BIOS 安全检测结果的反馈，补充和完善了 BIOS 安全隐患库和 BIOS 标准代码样本库；这 2 个库的补充和完善又进一步促进了 BIOS 安全检测结果的覆盖范围和准确性。

基于图 2 所示的模型，本文实现了一个 BIOS 安全检测系统。该系统由 4 部分组成：BIOS 采样工具软件，BIOS 样本存储服务器，BIOS 安全分析引擎，BIOS 安全检测用户界面程序。检测系统安全分析引擎由 BIOS 影像文件分解程序、BIOS 安全漏洞扫描程序、BIOS 安全隐患库和 BIOS 标准代码样本库构成。

系统提供 Windows 平台的专用工具软件对计算机 BIOS 进行采样，通过网络将 BIOS 样本和采样记录上传到 BIOS 安全检测专用存储服务器。安全检测用户界面程序和系统安全分析引擎安装在安全检测专用客户端计算机上。安全检测用户界面程序首先通过网络从专用服务器上取得将要检测的 BIOS 样本，然后调用安全分析引擎实施安全检测，最后根据安全分析引擎生成的结果，合成被检测计算机和本次安全检测操作的记录信息，生成并向用户提交 BIOS 安全检测报告。

安全检测报告度量被检测计算机存在的 BIOS 安全隐患、BIOS 代码完整状态，并提出针对该台计算机的 BIOS 安全修补建议措施。

6 小结

作为计算机系统的核心固件，BIOS 安全问题日益突出，而一直未引起信息安全界足够重视。由 Intel 首先提出的下一代 BIOS 的标准 EFI 和 UEFI 将进一步扩展和增强 BIOS 的功能，但有可能导致越来越多的 BIOS 安全隐患。

本文对BIOS安全问题进行了初步的探讨研究，提出了BIOS安全威胁模型和BIOS安全检测模型，建立了用于BIOS安全检测的BIOS安全隐患库和BIOS标准代码样本库。并将这些理论和方法用于BIOS安全风险分析和安全检测实践中，取得了很好的效果。笔者预测，BIOS安全问题将成为信息安全领域新的研究方向之一。TCG组织已经将安全度量的核心可信根(core root of trust for measurement, CRTM)与BIOS的启动区(BOOTBLOCK)捆绑在一起[5]，而下一代安全BIOS的研发也已经提上日程。

BIOS 安全问题研究，一方面促进 BIOS 安全检测技术发展，增强 BIOS 安全性能，防范由 BIOS 安全威胁所导致的软硬件系统及数据的损害和恶意攻击。另一方面，由于 BIOS 在计算机系统中的核心地位及 BIOS 所具有的软硬结合特性，增强和扩展 BIOS 的安全功能，发挥 BIOS 安全作用，为目前陷入困境中的基于软件的信息安全基础解决方案提供了新的思路。

参考文献

1 Compaq, Phoenix, Intel. BIOS Boot Specification v1.01[Z]. (1996-10). http://www.phoenix.com/NR/rdonlyres/56E38DE2-3E6F-4743-835F-B4A53726ABED/0/specsbbs101.pdf.

2 陈文钦. BIOS Inside-BIOS 研发技术剖析[M]. 中国台湾: 旗标出版股份有限公司, 2001.

3 杨 柳. 计算机安全：封堵 BIOS 漏洞[J]. 瞭望新闻周刊, 2004, (19): 52-53.

4 Einarsson S, Rausand M. An Approach to Vulnerability Analysis of Complex Industrial Systems[J]. Risk Analysis, 1998, 18(5): 535-546.

5 TCG. TCG Specification Architecture Overview v1.2[Z]. (2004-08). http://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf.