Computer Science and Application 计算机科学与应用, 2017, 7(4), 320-328
Published Online April 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.74039

Design and Implementation of Attack Detection System Based on UEFI Firmware

Yihua Zhou[1], Yang Liu[1,2], Guan Wang[1,2], Liang Sun[3]

[1]College of Computer Science, Beijing University of Technology, Beijing
[2]Key Laboratory of Trustworthy Computing in Beijing, Beijing
[3]ZD Technologies Ltd. (Beijing), Beijing
Email: zhouyh@bjut.edu.cn, 1005415619@qq.com

Received: Apr. 4th, 2017; accepted: Apr. 17th, 2017; published: Apr. 25th, 2017

Abstract

With the continuous development of network attack technology, attack against the firmware has emerged, causing a huge threat to the computer. This paper analyzes the function, characteristics and security threat of UEFI BIOS in detail, explaining the importance of firmware security. The malicious codes in the firmware are hard to be found and eliminated by the antivirus software. This paper has designed and implemented an attack detection system based on UEFI firmware by getting and analyzing the information about the firmware.

Keywords

UEFI, BIOS, Attack Detection

基于UEFI固件的攻击检测系统的设计与实现

周艺华[1]，刘　阳[1,2]，王　冠[1,2]，孙　亮[3]

[1]北京工业大学 计算机学院，北京
[2]可信计算北京市重点实验室，北京
[3]中电科技(北京)有限公司，北京
Email: zhouyh@bjut.edu.cn, 1005415619@qq.com

收稿日期：2017年4月4日；录用日期：2017年4月17日；发布日期：2017年4月25日

摘　要

随着网络攻击技术的不断发展，针对固件的攻击已经出现，对计算机造成了巨大的威胁。本文详细分析

文章引用: 周艺华, 刘阳, 王冠, 孙亮. 基于UEFI固件的攻击检测系统的设计与实现[J]. 计算机科学与应用, 2017, 7(4): 320-328. https://doi.org/10.12677/csa.2017.74039

了UEFI BIOS的功能、特点及安全威胁，诠释了固件安全的重要性。固件中的恶意代码难以被杀毒软件发现和消除。本文通过对固件层信息的获取和解析，设计与实现了一种基于UEFI固件的攻击检测系统。

关键词

UEFI，BIOS，攻击检测

Copyright © 2017 by authors and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

固件(Firmware)是计算机上电后首先执行的一组程序，运行在计算机底层，固化在 Flash 芯片中，常用于完成配置硬件设备，为操作系统提供硬件操作接口，引导操作系统的启动等功能，被业界称为是连接计算机基础硬件和系统软件的“桥梁”。UEFI (Unified Extensible Firmware Interface，统一可扩展固件接口)是新的固件标准，目前被业界广泛使用。UEFI 为固件和操作系统之间的接口制定了新的标准和规范，并为启动操作系统提供了所需的标准环境[1]。

BIOS (Basic Input/Output System)的主要功能[2]包括：1)开机自检，计算机启动时，BIOS 掌握着硬件设备的控制权，首先检查 CPU 是否工作正常，还包括定时器、可编程中断控制器、基本内存、显卡等的自检工作。2)系统初始化，初始化相应的硬件设备，并对外围设备进行驱动。3)BIOS 提供了系统设置功能，用户在进入操作系统之前可以进入 BIOS 设置界面，对系统的一些参数进行设置，如光盘/硬盘/USB 引导顺序、端口使能/禁用等。4)引导操作系统启动，BIOS 按照设置中保存的启动顺序读入操作系统引导代码，从而完成操作系统的加载启动。作为连接硬件和操作系统的枢纽，BIOS 的安全对计算机至关重要。Flash 芯片已经允许在操作系统运行过程中，通过特定的软件技术直接对 BIOS 中的内容进行刷新写入[3]，给用户和系统维护带来了便利，但与此同时也引入了很多的安全风险。

早期，众所周知的 CIH 病毒[4]就是直接向 BIOS 固件芯片和硬盘中写入乱码，篡改了 BIOS 中的正常代码，造成计算机无法启动，使用户数据严重破坏并无法还原。1999 年，Phoenix 公司提出并实现了通过在 BIOS 固件中嵌入一个代码模块 ILS [5] (Internet Launch System)，为用户自动连接网络，下载服务软件，启动 web 服务，后来此项目遭到了抵制，被终止。后来出现了 ACPI BIOS rootkit [6]和 PCI rootkit [7]，分别利用 ACPI 和 PCI 在固件中植入恶意代码。文献[8]根据 UEFI 自身和启动过程中存在的安全隐患，提出了基于 UEFI 存储攻击设备和劫持操作系统内核的两种攻击方式。BIOS 攻击的特点：不同于操作系统攻击和网络攻击，针对 BIOS 的攻击，在操作系统中是找不到的，在硬盘中也是看不到的，传统杀毒软件杀不掉，格式化硬盘或更换硬盘清不了，重装系统也无法去除。BIOS 恶意代码驻留在被攻击终端的计算机主板固件芯片中，难以检测和清除。随着信息技术的飞速发展，针对固件的攻击手段越来越多，计算机安全受到严重的威胁，BIOS 一旦被植入恶意代码，可能致使整个计算机瘫痪。因此，BIOS 攻击检测和防护成为当前亟待解决的问题。目前，对于 BIOS 攻击检测的研究和分析，国际国内的信息安全领域所做的相关工作还较少，固件安全领域的相关资料也较少，对开展固件攻击检测的研究和实现增加了一定的难度。

文献[9]提出了一种 BIOS 安全检测方法，即进行 BIOS 完整性度量。文献[10]提出对 BIOS 安全隐患

进行扫描，通过匹配安全隐患库特征码，判断 BIOS 是否存在隐患。本文研究 UEFI 固件技术并借鉴文献[9] [10]的检测方法，设计与实现了一个新的基于 UEFI 固件的攻击检测系统。本文针对 BIOS 镜像解析模块所采用的实现方式与以往不同。传统的 BIOS，对于不同的类型如 Award BIOS，AMI BIOS，Phoenix BIOS 等，各厂商的规范不尽相同，BIOS 镜像文件的格式处理和模块组成有很大差异，因此以往的 BIOS 安全检测系统通常是针对一种特定类型 BIOS 的研究与实现，有一定的局限性。目前，市面上新主板的 BIOS 普遍支持 UEFI 规范，不同的 BIOS 厂商都实现了 UEFI 规范所定义的接口。UEFI 规范定义了新的固件结构，BIOS 文件格式遵循 UEFI 组织发布的 PI 规范里定义的 Firmware Storage Specification。本文系统根据 UEFI 规范对 BIOS 镜像文件进行解析，设计与实现基于 UEFI 固件的攻击检测系统，增加了系统的通用性。而且，传统 BIOS 检测系统通常采用静态检测技术，本文系统客户端在 Windows 系统下开发，可以被广泛使用，不仅可以完成 BIOS 攻击检测工作，也可以使用户对 BIOS 有更深入的了解和认识。

2. 基于 UEFI 固件的攻击检测系统总体设计

本系统利用实验室已经实现的基于 UEFI 的固件木马攻击系统[11]来实施向 BIOS 中植入木马。固件攻击开发系统以原 X86 平台 BIOS 为基础，通过利用计算机 BIOS 中系统管理模式(SMM)的基本原理、接口设计以及 SMI 中断处理实现，可模拟对计算机固件的攻击。固件木马攻击系统网络拓扑图如图 1 所示。

固件木马攻击系统验证了木马能够被植入到 BIOS 中。基于固件木马攻击系统平台，本文所设计的系统主要通过获取 BIOS 镜像文件并对 BIOS 镜像进行解析，将 BIOS 采样和标准模块进行对比，对 BIOS 进行完整性度量，以此检测 BIOS 是否被篡改、是否受到木马攻击，并且检测出 BIOS 的哪一模块受到破坏。被篡改的模块可能隐藏着一定的安全漏洞，需要深入研究，提出防护措施。此外，本文系统利用 SMBIOS 实现了从固件层获取到计算机系统各组件的信息，包括 BIOS、主板、内存、CPU 及其他计算机设备的详细信息，对计算机硬件进行状态检测，便于用户监测系统状态，更好地进行攻击检测工作。整个固件攻击检测系统的总体架构如图 2 所示。

基于 UEFI 固件的攻击检测系统由客户端和服务器端组成，需要客户端和服务器端进行数据的通信。客户端按照功能划分总体上包含四个模块：BIOS 镜像解析模块，基准信息记录模块，计算机系统信息模块和检测分析模块。其中 BIOS 镜像解析模块是系统的核心模块和系统实现的关键环节，该模块包含的任务有：获取固件层 BIOS 镜像文件，对 BIOS 镜像进行模块分解和解压，并获取 BIOS 各个模块的 MD5

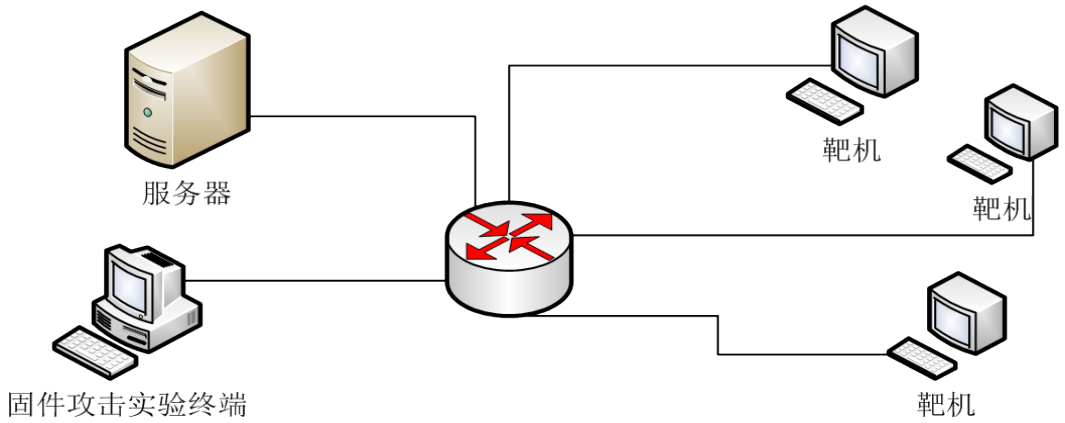

Figure 1. Firmware trojan attack system network topology
图 1. 固件木马攻击系统网络拓扑图

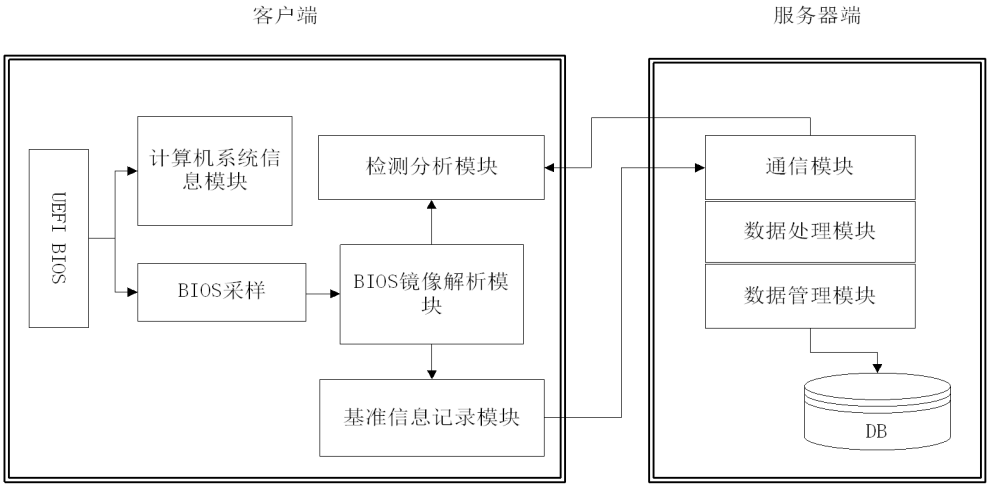

Figure 2. The overall framework of the firmware attack detection system
图 2. 固件攻击检测系统总体框架图

值。计算机系统信息模块显示了 BIOS、CPU、内存、缓存等计算机组件的详细信息。检测分析这一模块的功能是将解析后的被测 BIOS 文件与标准代码样本进行模块 MD5 值对比，检测 BIOS 是否被篡改，并具体显示出 BIOS 的哪一模块发生变化。服务器端利用通信模块与客户端进行通信，接收客户端发出的请求，并给出响应。数据处理模块是对客户端发出的请求进行处理，并对通信数据做加解密工作。木马攻击前的原 BIOS 叫做标准代码样本，当前不知道是否被攻击的 BIOS 是被测代码样本，被测代码与标准代码进行对比、检验，才能实现检测功能。因此，标准代码样本库需要安全地备份和存储，显然存储在本地并不安全，我们将 BIOS 标准代码远程存储在服务器上。服务器端通过数据管理模块对用户的 BIOS 标准样本和模块 MD5 进行统一的管理与存储。客户端记录基准信息时将标准 BIOS 文件和模块 MD5 值上传至服务器上。当系统调用检测分析模块时，服务器端会返回相应 BIOS 数据给客户端。

3. 基于 UEFI 固件的攻击检测系统流程设计

本系统的流程主要是获取到固件层 BIOS 镜像文件之后，将固件木马攻击之前的原 BIOS 镜像文件和当前被测 BIOS 镜像文件进行模块分解，由于 BIOS 实际是经过压缩、加密后存储在 Flash 芯片上的，所以需要对压缩存储的模块按照模块长度、压缩算法等进行解压缩，还原为最原始的 BIOS 二进制文件。对解析出的各个模块计算 MD5 消息摘要，将目标被测 BIOS 代码样本的各个模块分别与相对应的标准代码样本模块进行 MD5 值比较。如果全部一致，说明所有模块都没有变化，与原来代码一样，BIOS 并未受到攻击；如果有一个或多个模块对比不一致，说明 BIOS 受到攻击，MD5 消息摘要不一致的模块被破坏。固件攻击检测系统流程图如图 3 所示。

本系统实现的关键技术在于固件 BIOS 和操作系统之间的通信。UEFI BIOS 系统主要包括 8 个模块：UEFI BIOS 基础代码模块，硬件相关代码包括 CPU 代码、芯片组代码和设备代码，端口控制代码，兼容支持模块，UEFI OS 加载器，固件应用程序，文件系统驱动模块，SMI 中断处理模块。其中 SMI 中断处理模块以及文件系统驱动模块是 OS 和 BIOS 通信的桥梁，是本文系统实现的基础。

4. 基于 UEFI 固件的攻击检测系统的模块设计与实现

4.1. BIOS 镜像解析模块的设计与实现

BIOS 镜像解析模块需要完成的任务包括获取 BIOS 镜像文件，对 BIOS 进行模块分解，将压缩的部

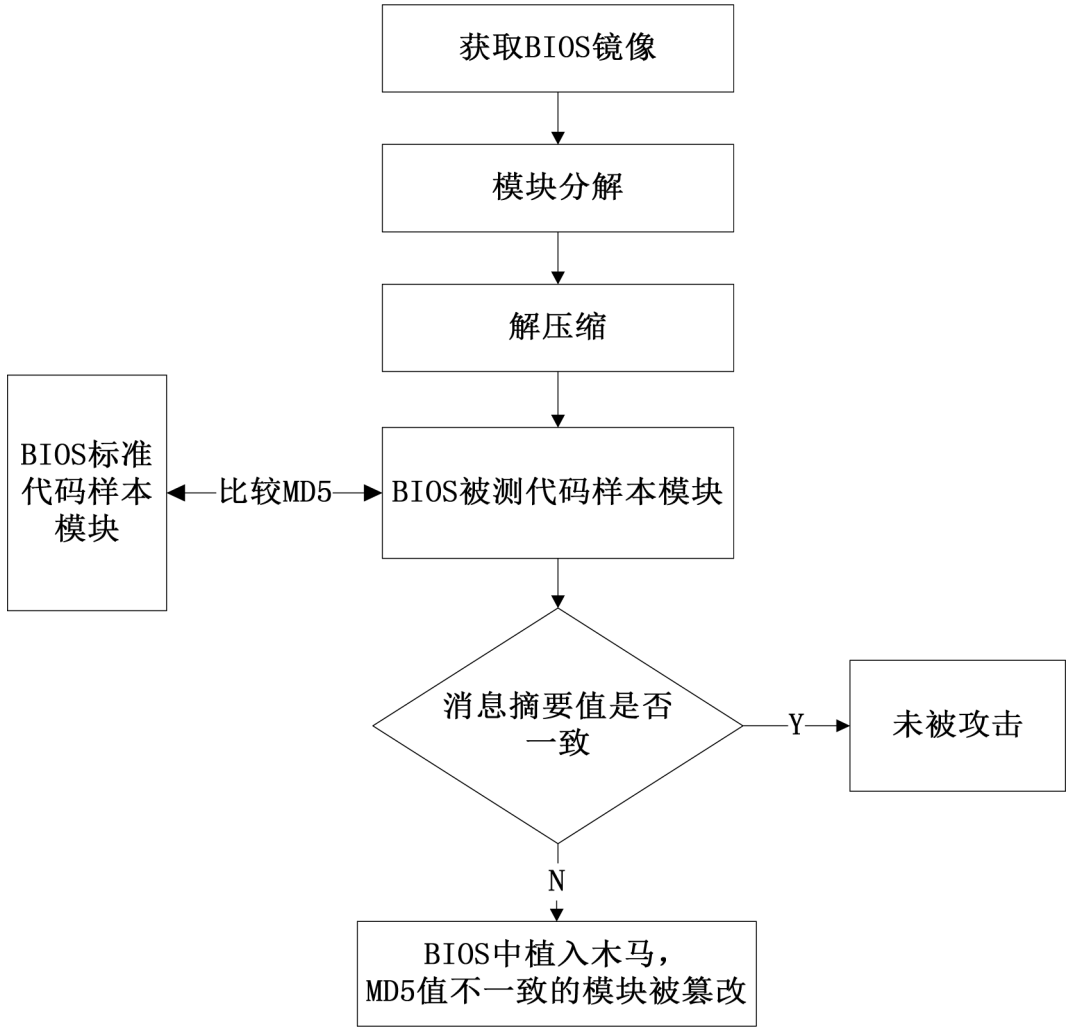

Figure 3. Firmware attack detection system flow chart
图 3. 固件攻击检测系统流程图

分进行解压缩得到最原始的 BIOS 二进制代码，并计算每个模块的 MD5 消息摘要。这一模块是整个 BIOS 攻击检测系统的最重要的部分，是实现检测、达到检测目标的基础。BIOS 在 Flash 芯片中是根据规范按照一定固件结构存储的，所有模块保存在固件结构单元中，此外，BIOS 厂商为了降低 BIOS 所需的存储空间，并增强代码的安全性，对 BIOS 的许多模块进行了压缩。因此，对 BIOS 模块进行攻击检测之前，首先需要将 BIOS 镜像文件分解，并对压缩的模块进行解压缩得到原始代码。

UEFI 作为广泛使用的新一代 BIOS 规范，为了方便 UEFI BIOS 的开发与扩展，为 Flash 芯片中 BIOS 镜像定义了新的存储结构。这种固件结构类似于一种文件系统，对固件设备文件的组织和存储进行了明确的规定，UEFI BIOS 的每个功能模块都存储在固件结构单元中。在这种规范中，整个 BIOS 被视为一个 FD (Firmware Device)，BIOS 镜像文件就是一个固件设备文件。FD (固件设备)是一片连续的存储区域，一个 FD 又分成多个逻辑区块，被称作固件卷。FV (Firmware Volume)是连续的格式化的存储空间，一个 FV 种又包含一个或多个 FF (Firmware File)，固件文件保存着 FV 中存储的数据和代码，是固件文件系统最重要的部分。而一个固件文件中又包含着固件文件段，Firmware File Sections 是不连续的段，是特定 File Type 里的独立部分。UEFI BIOS 镜像文件结构层次如图 4 所示。

固件文件系统(Firmware File System，FFS)描述了在固件卷FV上固件文件FF和空闲空间的组织关系，每个 Firmware Volume Image 包含 Header，FFS Image 和 Free Space，每个 FFS Image 包括 Header 和 File Sections。FFS 首部的格式如图 5 所示。其中 Type 字段描述了固件文件所属类型，固件文件类型有：PEI 核心固件文件、DXE 核心固件文件、UEFI 驱动文件等多种类型文件。

基于 UEFI 的固件攻击检测系统，通过读取 BIOS 所对应的内存地址获取 BIOS 镜像文件，得到 BIOS 镜像文件之后，利用 UEFI 固件文件规范对 BIOS 文件进行模块分解，对于压缩存储的 FV，根据固件文件段中描述的压缩方式，反向操作对其进行解压缩，便可得到 BIOS 二进制文件，完成 BIOS 镜像文件的解析。系统 BIOS 镜像解析效果如图 6 所示。

4.2. 计算机系统信息模块的设计与实现

计算机系统信息这一模块是对计算机中重要组件的详细信息进行展示，用来查看和检测硬件状态，便于用户监视系统状态。从此模块中可以获取到的信息有：BIOS 基本信息，系统信息，系统外围，处理器，缓存，端口连接器，系统插槽，物理存储阵列，内存阵列映射地址以及系统引导的详细信息。这些硬件信息是通过编程从 SMBIOS 中得到的，并以直观、易读的文本格式显示出来。SMBIOS (System

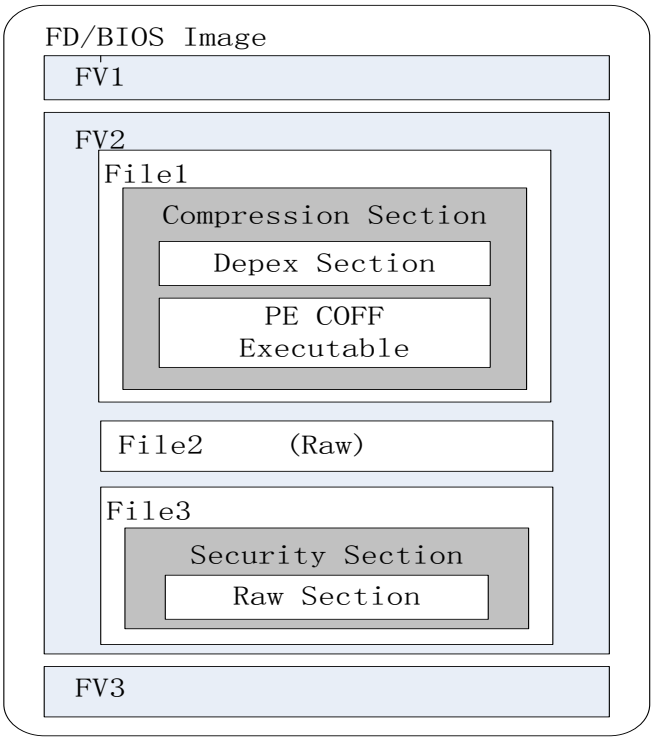

Figure 4. UEFI BIOS image file hierarchy diagram
图 4. UEFI BIOS 镜像文件结构层次图

Name		
IntergrityCheck	Type	Attributes
Size		State

Figure 5. FFS header format
图 5. FFS 首部格式

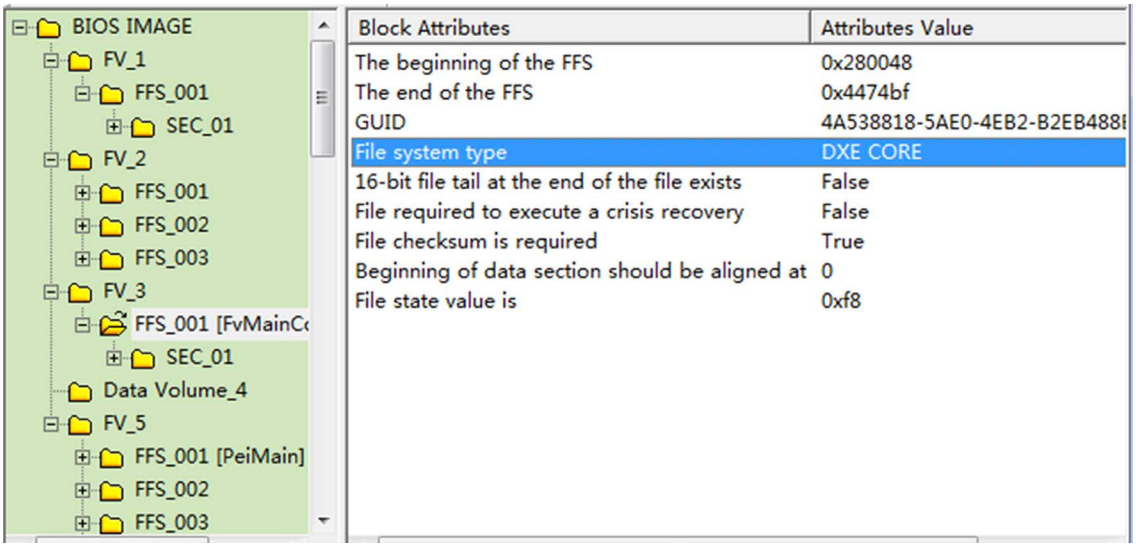

Figure 6. The BIOS image analytical results
图 6. BIOS 镜像解析效果

Management BIOS)参考规范描述了主板和系统供应商通过扩展英特尔架构系统上的 BIOS 接口如何将其产品的管理信息以标准格式呈现。DMI (Desktop Management Interface)是用来收集计算机系统自身以及其外围设备相关数据信息的管理系统，遵循 SMBIOS 规范，并将收集到的数据信息存在 BIOS 中。因此，我们可以从 SMBIOS 中获取到想要的计算机组件信息。在 SMBIOS 2.7 版本规范中为 SMBIOS 信息定义的唯一访问方法是基于表结构的方法。

编程实现从 SMBIOS 读取计算机系统信息的步骤：首先寻找 EPS 表，获取 SMBIOS 表的入口地址。SMBIOS 中数据的存储结构是由 EPS 表和 SMBIOS 表一起来描述的，EPS 表结构如表 1 所示。

在 EPS 表的 16H 处存储的是 SMBIOS 表的总长度，表的 18H 处存储了 SMBIOS 表的起始物理内存地址。根据 EPS 表结构，可以看出，找到“_SM_”并找到“_DMI_”，便找到了 EPS 表。而“_SM_”和“_DMI_”是用固定的 ASCII 码代表，很容易找到。找到 EPS 表后，根据表的 18H 处就可以得到 SMBIOS 的内存地址。SMBIOS 的首地址是 Type 0 的存储地址，Type 0 描述的是 BIOS 的基本信息。对 Type 0 表进行解析并以一定格式读出来，便获得了想要的 BIOS 信息。SMBIOS 表是由多个不同类型的表结构构成的，每一个表结构代表一种计算机组件的信息或者其他类型的系统信息。SMBIOS 2.7 版本描述了 Type 0 - 42，126 和 127 的表结构。本文所设计的系统只选取其中部分常见的计算机组件信息进行展示。Type 0 存储的是 BIOS 信息，Type 1 是系统信息，Type 3 是系统外围信息，Type 4 是处理器信息，Type 7 是缓存信息，Type 8 是端口连接器，Type 9 是系统插槽，Type 16 是物理内存阵列。Type 19 是内存阵列映射地址，Type 32 是系统引导信息。每个 SMBIOS 表都具有相同的头结构，每个表又划分为格式区域和字符串区域，字符串区域紧跟在格式区域之后。每个 Type 表的区域内容有所不同，部分 BIOS 表的格式区域见表 2 所示。

在 BIOS 表的 00H 处代表 Type 号，01H 中描述了其格式区域的长度，在格式区域之后是其字符串区域。根据表结构得知，字符串区域的第一个字符串描述的是 BIOS 厂商信息，第二个字符串代表的是 BIOS 版本，第三个字符串是 BIOS 发布日期。每一个字符串以 00H 结束，字符串区域以 0000H 结束。接着是 Type 1 的内容，获取其他 Type 信息的方法和 BIOS 信息类似，本文不再赘述。本文以一台实验机为例，直接获取到的 BIOS 信息的展示比较混乱，本文系统通过解析，将 BIOS 的基本信息以直观、易读的格式化文本形式显示出来，效果如图 7 所示。

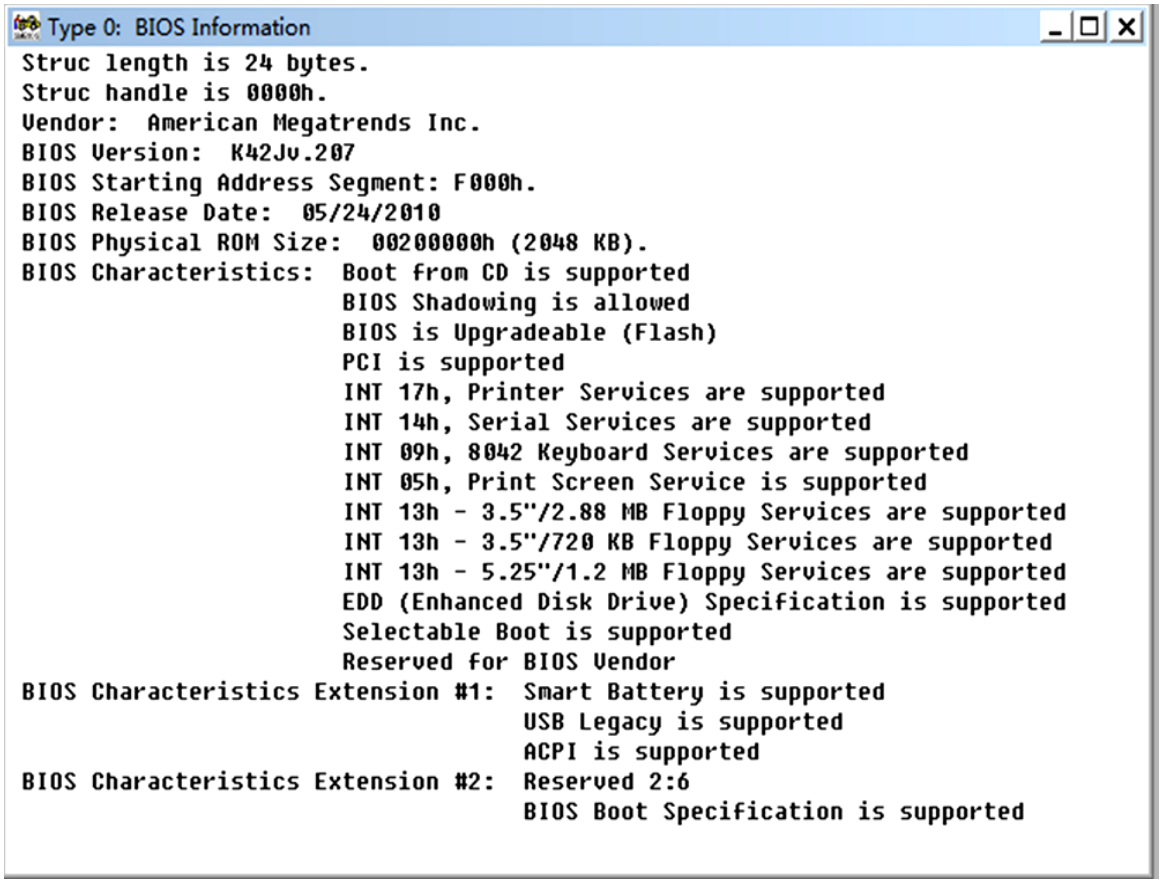

Figure 7. System BIOS information display effect
图 7. 系统 BIOS 信息显示效果

Table 1. EPS table structure
表 1. EPS 表结构

offset	name	length	description
00H	字串锚	4 BYTEs	“_SM_”,指定为四个 ACSSII 码(5F 53 4D 5F)
04H	EPS 校验和	BYTE	
05H	EPS 长度	BYTE	EPS 表的长度
06H	SMBIOS 主版本	BYTE	
07H	SMBIOS 次版本	BYTE	
08H	最大结构大小	WORD	最大的 SMBIOS 结构的大小
0AH	EPS 修正	BYTE	
0BH-0FH	格式化区域	5 BYTEs	
10H	中间锚串	5 BYTEs	“_DMI_”,指定为五个 ACSSII 码(5F 44 4D 49 5F)
15H	中间校验和	BYTE	
16H	结构表长度	WORD	SMBIOS 结构表的总长度
18H	结构表地址	DWORD	SMBIOS 表的起始物理地址
1CH	结构表数量	WORD	SMBIOS 结构表的总个数
1EH	SMBIOS BCD 修正	BYTE	

Table 2. Part of the BIOS table format area
表 2. 部分 BIOS 表格式区域

offset	name	length	value	description
00H	Type	BYTE	0	BIOS 信息指示
01H	长度	BYTE	Varies	Type0 格式区域的长度
02H	句柄	WORD	Varies	EPS 表的长度
04H	厂商	BYTE	01H	BIOS 供应商的信息， 一般为 01H 代表在字符串域中的第一个字符串
05H	版本	BYTE	02H	BIOS 的版本信息， 一般为 02H 代表在字符串域中的第一个字符串
06H	BIOS 起始地址段	WORD	Varies	
08H	BIOS 发布日期	BYTE	03H	一般为 03H，代表在字符串域中的第三个字符串
09H	BIOS ROM 大小	BYTE	Varies	

BIOS 镜像解析模块和计算机系统信息模块是系统通过固件层实现的主要模块，其他模块的实现相对简单，由于篇幅问题，在此暂时不作介绍。

5. 结束语

当今社会普遍将更多的关注点放在操作系统层的安全上，容易忽略计算机固件层的安全。而针对固件的攻击手段已经越来越多，BIOS 作为连接计算机硬件和操作系统的中间桥梁，在计算机中的地位极其重要，一旦受到攻击，将可能致使整个计算机瘫痪。固件攻击造成计算机安全面临严重的威胁，因此，BIOS 攻击检测和防护成为当前亟待解决的问题。针对传统 BIOS 安全检测系统的局限性，本文根据 UEFI 中固件存储结构规范设计和实现了一种基于 UEFI 固件的攻击检测系统，增强了系统的通用性。而且，传统 BIOS 检测系统通常采用静态检测技术，市面上还没有广泛投入使用的 BIOS 检测工具，本文系统客户端在 Windows 系统下开发，可以被广泛使用。系统根据 UEFI 固件文件系统实现了对 BIOS 镜像文件的解析，检测分析模块将被测 BIOS 的各个模块的 MD5 值与服务器中存储的标准 BIOS 的相应模块进行对比，可以检测出 BIOS 是否受到攻击，并显示出具体哪个模块受到攻击，定位攻击者的具体行为。此外，系统通过 SMBIOS 实现了对计算机硬件信息的获取和格式化展示，方便用户检测计算机硬件的状态。

参考文献 (References)

[1] 刘挺. UEFI BIOS 实现原理与结构分析[J]. 电子技术与软件工程, 2015(20): 171.

[2] 周振柳. 计算机固件安全技术[M]. 北京: 清华大学出版社, 2012: 13-14.

[3] 赵丽娜, 陈小春, 张超, 肖思莹. BIOS 安全更新及保护系统设计[J]. 微型机与应用, 2015(8): 2-4.

[4] 李越, 黄春雷. CIH 病毒的分析与清除[J]. 计算机科学, 2000(5): 104-105.

[5] Phoenix Technologies Ltd. (2000) Phoenix Net 1.4 PRD Revision 0.6.2000.6.

[6] Heasman, J. (2006) Implementing and Detecting an ACPI BIOS Rootkit. Next Generation Security Software Ltd., Manchester.

[7] Heasman, J. (2007) Implementing and Detecting a PCI Rootkit. Next Generation Security Software Ltd., Manchester.

[8] 何宛宛. 基于 UEFI BIOS 攻击方式的研究[D]: [硕士学位论文]. 北京: 北京工业大学, 2014.

[9] 王晓箴, 周振柳, 刘宝旭. BIOS 采样分析系统的设计与实现[J]. 计算机工程, 2011(11): 7-9.

[10] 张智, 袁庆霓. BIOS 安全检查系统设计与实现[J]. 计算机技术与发展,2012(2): 172-175 + 180.

[11] 孙亮, 陈小春, 王冠, 等. 基于 UEFI 固件的攻击验证技术研究[J]. 信息安全与通信保密, 2016(7): 89-93.

期刊投稿者将享受如下服务：

1. 投稿前咨询服务 (QQ、微信、邮箱皆可)
2. 为您匹配最合适的期刊
3. 24 小时以内解答您的所有疑问
4. 友好的在线投稿界面
5. 专业的同行评审
6. 知网检索
7. 全网络覆盖式推广您的研究

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org