Computer Science and Application 计算机科学与应用, 2016, 6(2), 72-76
Published Online February 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.62009

Hans汉斯

Design of Terminal Control Based on UEFI BIOS

Quanmin Wang[1], Xiaotong Zhao[1,2], Guan Wang[1,2], Liang Sun[3]

[1]College of Computer Science, Beijing University of Technology, Beijing
[2]Key Laboratory of Trusted Computing in Beijing, Beijing
[3]ZD Technologies (Beijing), Limited, Beijing
Email: bjgydxzxt@163.com

Received: Jan. 29th, 2016; accepted: Feb. 22nd, 2016; published: Feb. 25th, 2016

Abstract

At present, the phenomena such as illegal outreach, unauthorized access and illegal operation seriously threaten to the security of terminal system. Although there are a lot of terminal control systems, but they ignore the protection of control program. For these reasons, the design of terminal control based on UEFI BIOS will make control program run safely in UEFI. The control program is stored in the server. The client can connect to server through UEFI's network service. It authenticates identity, receives control program and accepts control from the program. This design protects control program and enhances the isolation of control program.

Keywords

Terminal Control, UEFI, Trusted Computing

基于固件的终端控制方法的设计

王全民[1]，赵小桐[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: bjgydxzxt@163.com

文章引用: 王全民, 赵小桐, 王冠, 孙亮. 基于固件的终端控制方法的设计[J]. 计算机科学与应用, 2016, 6(2): 72-76.
http://dx.doi.org/10.12677/csa.2016.62009

收稿日期：2016年1月29日；录用日期：2016年2月22日；发布日期：2016年2月25日

摘　要

目前，非法外联、非授权接入内网、用户非法操作等现象严重威胁着内网终端系统安全。虽然有大量厂商研发终端控制系统，但是在终端控制方面都存在重控制轻防护的现象。基于上述原因，基于固件的终端控制方法的设计，从固件层实现身份认证和授权开机，并使控制程序安全运行，将控制程序存放于服务器中，客户端可以在固件层通过网络连接远程服务器，进行身份验证并接收控制文件，接受控制文件对终端的控制，增强了控制代码的隔离性。

关键词

终端控制，UEFI，可信计算

1. 引言

当前网络技术飞速发展，内网已成为企业内部交流和传递信息的主要渠道。因此，内网的信息安全一直被人们所重视，对计算机终端进行管理控制，是保障企业信息安全的重要方面[1]。终端控制，就是在终端网络进行身份认证与查验，确保只有合法健康的终端才能够接入网络，并且完成对终端功能的控制，控制其访问域和终端的系统使用。在内网终端系统安全控制管理方面，已存在众多的解决方案，但传统的终端控制方案，大都采用的方法为在终端上的操作系统里植入程序，使程序在后台运行并与服务器进行通信，以达到控制目的。但这种方法非常容易被恶意的终端用户破坏篡改，达不到控制效果，且系统应用范围不广泛、安全性不高、易被破解，在不同环境下兼容性较差，移植性不高，对于终端资源和信息的掌控性不强，防范控制不足[2]。

传统的终端技术，基本都偏向于控制功能的开发，并且产品比较单一，单靠一种产品不能承担起对内网终端系统的全面控制；对终端上的控制代码没有进行有效的保护，以保证其安全性和生存性，一旦核心控制代码遭到人为破坏，控制功能就会失效，不能继续对终端进行控制和保护。

要克服传统终端控制解决方案的缺点，首先要保证控制代码的隔离性，从而对控制代码进行有效的防护，防止恶意的篡改和删除。其次要尽可能早地使终端被控制，从底层实现控制代码的安全性，加强控制能力，解决传统方案重功能轻防护的缺陷。参考以上思路，本设计在 UEFI 框架基础上，设计了一种基于固件层的远程终端控制系统，解决传统控制过程中的缺陷。

本文设计了一种 C/S 架构的基于固件的终端控制系统。首先，UEFI BIOS 可以从固件层实现控制程序的安全运行，使终端的操作系统在系统启动时就受到服务器端的控制。其次，服务器在终端每次加电启动时发送新的控制文件至终端的 UEFI BIOS，控制文件与用户之间具备很好的隔离性，每次开机后终端控制程序都必然存在，终端用户无法摆脱控制文件的控制，提高了系统的控制能力。

2. 基于固件的终端控制方法设计

2.1. 系统架构

UEFI BIOS 平台具备的模块化组件、可拓展的未来新平台新功能的等特性，使终端控制系统可以利用其建立更有效的控制机制，开发者可以在平台框架下开发新的功能，充分利用 CPU 和内存空间[3]。UEFI 支持多种网络协议，在系统启动阶段就可以进行网络通信、使用网络资源。网络协议栈被分为多个

模块，具有清晰的分层结构，可分为链路层、网络层、传输层和应用层。其中链路层协议有 ARP、MNP、SNP，以及网卡驱动；网络层协议为 IP 协议；传输层协议有 TCP、UDP；应用层有 TFTP 协议[4]。各层协议之间使用异步方式传递数据，通过事件机制和任务优先级机制保证事件的执行。

系统的工作过程为：客户端将本机信息发送至服务器，服务器通过身份验证后将控制文件发送至客户端，客户端在系统启动后受到控制程序的控制，完成终端的远程控制过程。系统由运行在 UEFI BIOS 平台的客户端和服务器端组成。系统大部分功能将在客户端实现，服务器端完成身份认证和发送文件的基本功能即可。客户端功能为发送主机信息与接收控制文件，执行终端控制。客户端系统主要功能在 UEFI BIOS 环境下完成，用户在操作系统环境下不能察觉控制程序的运行。服务器端主要由技术人员使用，根据管理策略发送与目标主机对应的控制文件。系统架构如图 1 所示。

2.2. 模块设计

2.2.1. 客户端模块设计

为增加系统的可拓展性和可维护性，结合 UEFI BIOS 的特性，客户端采用分层次分模块的方式设计。客户端功能分为 5 个模块：网络模块、文件接收模块、文件存储模块、文件保护模块、通信模块。

1) 网络模块功能为创建网络连接、解析服务器发送信息、调用其他模块完成功能。

2) 文件接收模块主要功能为接收服务器传送的控制文件。

3) 文件存储模块功能为控制文件的存储。

4) 文件保护模块功能为修改文件属性、对文件进行进程保护。

5) 通信模块功能为发送主机身份信息、客户端与服务器之间消息的传递。

2.2.2. 服务器端设计

系统服务器端运行在操作系统上，设计和实现较为简单，采用分模块方式设计。服务器端由 5 个模块和数据库组成：通信模块、认证模块、注册模块、密钥管理模块、策略管理模块。

1) 通信模块主要功能为与客户端之间传递消息。

2) 认证模块、注册模块功能都与身份认证服务有关：在首次注册阶段，客户端将 TCM 身份证书发送给服务器，服务器向客户端颁发密钥，并写入数据库；在之后每次的开机阶段，客户端使用密钥加密身份信息，发送给服务器，服务器通过认证模块调取数据库，完成认证[5]。

3) 密钥管理模块的功能为密钥的生成和存储颁发[6]。

4) 策略管理模块功能为控制策略、控制文件的编写和管理。

5) 数据库存储客户端身份信息和与之匹配的策略控制文件信息。

2.3. 流程设计

2.3.1. 客户端流程设计

1) 客户机加电后，进入 UEFI BIOS 平台，BIOS 读取本机硬件信息，将信息通过通信模块发送至服务器。

2) 服务器收到客户端发送的本机信息后，对客户进行身份验证，若通过身份验证，则根据数据库的策略列表项目，选择对应的控制文件，发送给客户端。文件接收模块识别从服务器传送的数据包是否为 TFTP 数据包，客户端读取数据包大小后，分配相应空间并接收数据包，判断数据包是否接收完成。

3) 在接收完成之后发送 ACK 信息，文件存储模块将控制文件存储，使用简单文件系统协议 EFI_SIMPLE_FLIE_PROTOCOL 与文件协议 EFI_FILE_PROTOCLE 等协议操作文件系统[7]。简单文件系统协议用于操作文件系统，文件协议用于操作文件接口。接收文件后，对硬盘进行写操作，将文件写入

硬盘的自启动区域。

4) 文件保护模块将修改文件属性与设置进程保护程序，保护程序文件的正常启动运行[8]。

5) 通过以上模块来将服务器发来的程序在 BIOS 阶段完成设置，从而保证了控制代码的隔离性，更早地使终端被控制。随后，客户端主机完成系统引导后，操作系统从 UEFI 接过控制权。终端控制文件运行于操作系统中，能够长期稳定地运行。控制文件将实现两方面的终端控制功能：系统配置的控制，如关机时间、阻止用户特定进程；外设的控制，如禁用摄像头、U 盘、网络等。根据客户端主机的不同身份和时间，发送至客户端的控制文件也将不同，充分实现多样化的终端控制技术。客户端运行流程如图 2 所示。

2.3.2. 服务器端流程设计

1) 通信模块接收客户端传输的 TCP 报文，其中包含了客户端经数字签名后的验证信息与验证请求。

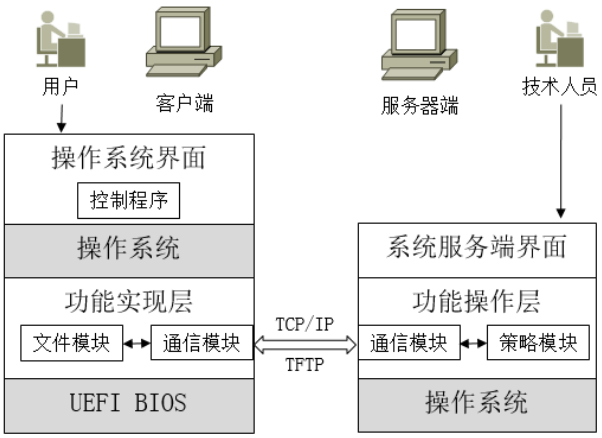

Figure 1. Architecture of system
图 1. 系统架构图

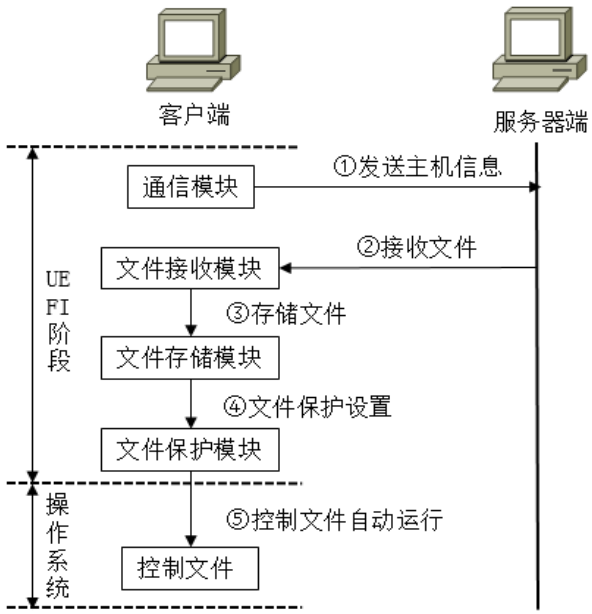

Figure 2. Process flow chart of client
图 2. 客户端运行流程图

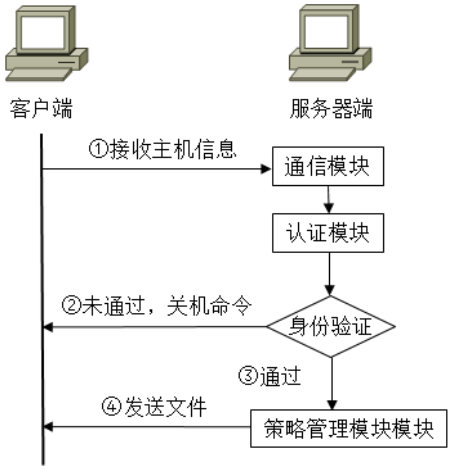

Figure 3. Process flow chart of server
图 3. 服务器端运行流程图

2) 通信模块将验证信息发送给认证模块，认证模块将客户端信息与服务器本地数据进行比对，如未通过验证，服务器端向客户端发送关机命令，使客户端直接关机，不允许其启动。

3) 如通过验证，策略管理模块将按照客户端的信息在数据库进行查询，确定客户端种类，按照既定管理策略与服务器时间，选择不同的控制程序，通过通信模块传输控制文件。系统管理员可以通过策略管理模块，增删客户端信息、修改控制策略，从而更加灵活控制终端的启动、关闭和其他终端功能。服务器端运行流程如图 3 所示。

3. 结束语

本文基于固件系统，通过研究 UEFI 的新特性，将控制程序与受控终端隔离开来，终端用户无法破坏篡改控制程序和阻止程序的运行，有效保护了控制代码的安全性。在服务器端可灵活更改控制策略，制定多样化的控制计划。并且使得计算机在不进入操作系统的情况下，接受服务器端的控制，整个系统灵活可变，可实现多层次、多角度的远程终端管理与控制。

基金项目

国家自然科学基金资助项目(61272500)。

参考文献 (References)

[1] 熊强, 肿伟俊, 李治文. 网络信息系统中信息安全防御资源分配策略分析——基于约束理论视角[J]. 运筹与管理, 2014(3): 163-169.

[2] 金波, 张兵, 王志海. 内网安全技术分析与标准探讨[J]. 信息安全与通信保密, 2007(7): 109-110.

[3] Trusted Computing Group (2011) Unified Extensible Firmware Interface Specification Version 2.3.1.

[4] 周伟东. 基于 EFI BIOS 的计算机网络接入认证系统的研究与实现[D]: [硕士学位论文]. 西安: 西安电子科技大学.

[5] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010(2): 139-166.

[6] 唐文彬, 祝跃飞, 陈嘉勇. 统一可扩展固件接口攻击方法研究[J]. 计算机工程安全技术, 2012, 38(13): 99-101.

[7] Intel Corporation (2008) Legacy BIOS and UEFI Boot Process. Intel Corporation SSG, Longmont.

[8] 蔺聪, 黑霞丽. 木马的植入与隐藏技术分析[J]. 信息安全与通信保密, 2008(7): 53-55.