

基于 TPCM 的服务器可信 PXE 启动方法

刘国杰^{1,2}, 张建标^{1,2}

(1. 北京工业大学信息学部, 北京 100124; 2. 可信计算北京市重点实验室, 北京 100124)

摘要: PXE 启动机制通过网络下载操作系统文件并启动操作系统, 广泛应用于服务器网络启动。通过可信计算技术保障 PXE 启动过程的安全可信, 防止 PXE 启动文件被恶意篡改, 确保服务器的安全可信运行。网络安全等级保护标准要求基于可信根对服务器设备的系统引导程序、系统程序等进行可信验证。根据等级保护标准要求, 提出一种基于 TPCM 的服务器可信 PXE 启动方法, 保障服务器的 BIOS 固件、PXE 启动文件、Linux 系统文件的安全可信。在服务器进行 PXE 启动时, 由 TPCM 度量 BIOS 固件, 由 BIOS 启动环境度量 PXE 启动文件, 由 PXE 启动环境度量 Linux 系统文件。以 TPCM 为信任根逐级度量、逐级信任, 建立信任链, 建立可信的服务器运行环境。所提方法在国产自主可控申威服务器上进行了实验, 实验结果表明所提方法是可行的。

关键词: 信息安全; 可信计算; 可信平台控制模块; 可信启动

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020079

TPCM-based trusted PXE boot method for servers

LIU Guojie^{1,2}, ZHANG Jianbiao^{1,2}

1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

Abstract: The PXE startup mechanism downloads operating system files through the network and starts the operating system, which is widely used in server network startup. It is widely used in server network startup. The PXE boot process is secured and trusted through trusted computing technology to prevent the PXE boot file from being tampered with maliciously, ensuring the safe and reliable operation of the server. The cyber security classified protection standard requires that the system boot program and system program of the server device be trusted and verified based on the trusted root. A TPCM-based server trusted PXE boot method based on the requirements of classified protection standard was proposed to ensure the security and trust of the server's BIOS firmware, PXE boot

收稿日期: 2020-08-26; 修回日期: 2020-10-24

通信作者: 张建标, zjb@bjut.edu.cn

基金项目: 国家自然科学基金(61971014); 国防科技实验信息安全实验室对外开放项目(2015XXAQ08)

Foundation Items: The National Natural Science Foundation of China(61971014), National Defense Science and Technology Laboratory of Information Security (2015XXAQ08)

论文引用格式: 刘国杰, 张建标. 基于 TPCM 的服务器可信 PXE 启动方法[J]. 网络与信息安全学报, 2020, 6(6): 105-111.
LIU G J, ZHANG J B. TPCM-Based trusted PXE boot method for servers[J]. Chinese Journal of Network and Information Security, 2020, 6(6): 105-111.

files, and Linux system files. When the server performs PXE boot, TPCM measured BIOS firmware, BIOS boot environment measured PXE boot files, and PXE boot environment measured Linux system files. Taking TPCM as the root of trust, one level of measurement, one level of trust, and a chain of trust were established to achieve a trusted server operating environment. The proposed method was tested on a domestically-controlled, self-controllable Shenwei server. The experimental results show that the proposed method is feasible.

Key words: information security, trusted computing, TPCM, trusted startup

1 引言

随着信息技术的发展,信息安全问题日益严峻^[1-3]。网络安全等级保护国家标准对我国信息安全工作非常重要,被应用于网络安全职能部门、网络安全管理部门以及等级测评机构的各项工作中,标准要求系统在启动时对信息设备的主板固件、引导程序、操作系统与关键应用程序进行可信验证,并在检测到被恶意篡改后发送报警信号^[4]。服务器作为云计算的关键基础设施,存在各种安全威胁。攻击者可以未经授权通过 PXE (PXE, preboot execution environment) 启动方式启动服务器,运行恶意程序,破坏或窃取重要数据,危害服务器的运行环境。必须从服务器的 PXE 启动开始,保障服务器整个 PXE 启动过程的安全可信,才能保障服务器运行环境与重要数据的安全可信^[5-7]。

国内外学者对服务器的可信启动进行了大量研究。文献[8]借助可信服务器实现终端可信启动,实现了基于第三方的在线可信度量^[9-10]。可信计算组织 (TCG, Trusted computing group) 提出了基于可信平台模块 (TPM, trusted platform module) ^[11] 的通过存储在 BIOS 固件的可信度量根核 (CRTM, core root of trusted for measurement) 作为可信根对 BIOS 的其余部分进行度量,然后由 BIOS 度量操作系统加载器 (BootLoader), 由 BootLoader 度量操作系统,形成一条信任链。TCG 提出的引导机制有 3 种硬件平台实现方案: ①将 TPM 芯片嵌入主板,需要对计算机硬件结构修改; ②通过外设部件互联标准 (PCI, peripheral component interconnect) 增加 TPM 芯片; ③通过 USB 接口增加 TPM 芯片,这种方式需要修改 BIOS 程序,可操作性差且工作量大^[12-15]。

TCG 提出的解决方案,以 TPM 为信任根作

为外挂部件被动调用,无法进行主动度量。我国学者提出了可信平台控制模块 (TPCM, trusted platform control module) ^[16-17], 作为可信计算平台的信任根,是可信计算的核心模块。TPCM 在其内部设有可信度量根。基于 TPCM 建立信任链,避免了 TCG 方案中的 UEFI 固件被篡改对信任根带来的安全威胁。本文提出了基于 TPCM 服务器的可信 PXE 启动方法。

2 相关工作

2.1 TPCM

TPCM 内部设有物理可信根,由可信度量根、可信存储根与可信报告根 3 个可信根组成,分别扩展实现可信度量、可信报告与可信存储功能。TPCM 采用基于多度量代理的信任链传递模型,对平台启动的不同阶段,定义基于不同策略的扩展度量代理模块 (EMM) ^[14]。从系统启动开始,TPCM 先于 CPU 启动,构建以 TPCM 为信任根的信任链,并利用度量代理节点 EMM,对主板、系统引导、系统内核和应用逐级进行可信度量,从而实现信任的传递与扩展^[18]。

2.2 PXE 启动工作流程

服务器的网络启动一般采用预启动执行环境。PXE 提供了一种使用网络接口 (network interface) 启动计算机的机制。这种启动机制可以让服务器在没有本地存储设备或操作系统情况下启动。这种网络启动服务器的方式需要搭建一台 PXE 服务端,提供 TFTP、FTP 与 HTTP 服务。首先启动网络的服务器作为客户端在 BIOS 启动阶段向 PXE 服务器请求 IP 地址并自动设定 IP 地址,然后通过 TFTP 下载启动文件到服务器内存并运行进入 PXE 环境,最后 PXE 通过 HTTP 下载操作系统文件并完成服务器操作系统的配置^[18]。PXE 的工作流程如图 1 所示。

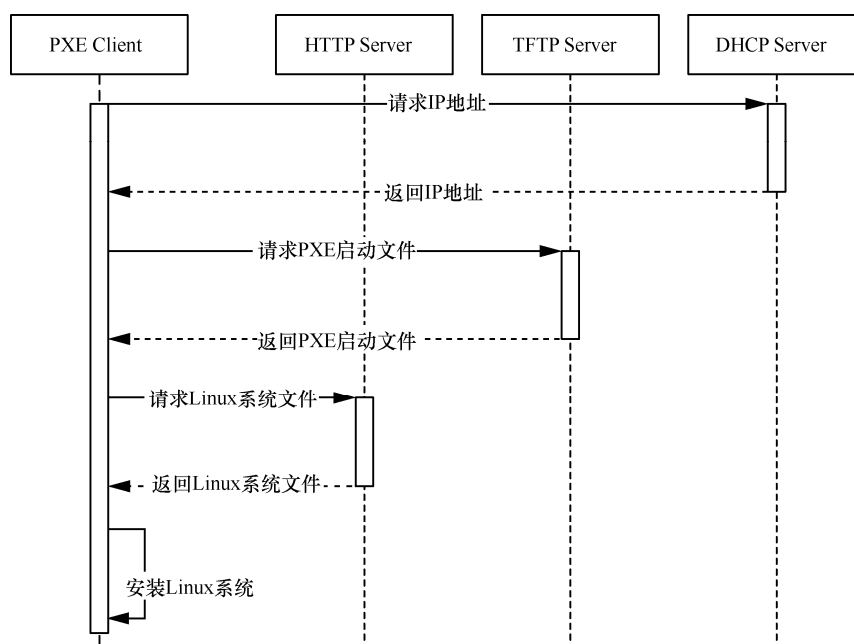


图1 PXE 启动工作流程
Figure 1 PXE boot workflow

3 可信启动模型

3.1 可信启动模型

在服务器系统中，启动过程可信是服务器可信运行的基础，对服务器启动过程进行安全防护具有重要研究意义。沈昌祥等^[14]提出了主动免疫可信计算，在进行运算的同时进行安全防护，运算过程可测可控，不被干扰，使运算结果总是与预期一样。本节基于主动免疫可信计算理论，并结合服务器的 PXE 启动特征提出了 PXE 可信启动模型。

定义 1 每个启动阶段的一个关键部件作为一个实体 E 。

定义 2 第一个启动阶段的关键部件作为实体 E_0 ，称为信任根。

定义 3 在启动过程中，上一个实体 E_{i-1} 启动当前实体 E_i ，其中 $1 \leq i \leq n$ 。如果每个启动阶段的每一个关键实体都验证为可信，则整个启动过程是可信的。为了确保当前实体 E_i 的可信性，必须首先信任上一个实体 E_{i-1} ，该信任模型为

$$E_{i-1} v_{i-1} E_i (1 \leq i \leq n) \quad (1)$$

其中， v_{i-1} 是上一个实体 E_{i-1} 的可信验证模块，用于对当前实体的可信性验证。

以信任根为起点，对实体进行逐级度量与验证，逐级信任，得到一个信任链。

$$E_0 \rightarrow E_1 \rightarrow E_2 \rightarrow \cdots \rightarrow E_n \quad (2)$$

本文提出的可信启动模型的实体为 TPCM、UEFI 固件、PXE 启动文件、Linux 系统文件，分别用实体 E_{TPCM} 、 E_{BIOS} 、 E_{PXE} 、 E_{Linux} 表示，以 E_{TPCM} 为信任根。在启动过程中由 TPCM 验证 UEFI 固件，UEFI 验证 PXE，PXE 验证 Linux 系统文件，得到可信启动的验证模型为

$$E_{\text{TPCM}} v_{\text{TPCM}} E_{\text{BIOS}} v_{\text{BIOS}} E_{\text{PXE}} v_{\text{PXE}} E_{\text{Linux}} \quad (3)$$

其中， v_{TPCM} 、 v_{BIOS} 、 v_{PXE} 为可信度量与验证模块，用于上一个实体对当前实体的可信度量与验证。

以 TPCM 作为起点，进行逐级度量与验证，最终得到一条信任链。

$$E_{\text{TPCM}} \rightarrow E_{\text{BIOS}} \rightarrow E_{\text{PXE}} \rightarrow E_{\text{Linux}} \quad (4)$$

3.2 可信 PXE 启动架构

PXE 服务端是一台通用的服务器，提供 DHCP 服务，响应 PXE 客户端的请求并为 PXE 客户端分配 IP 地址；提供 TFTP 服务，响应 PXE 客户端的请求，发送 PXE 启动文件的内容给 PXE 客户端；提供 HTTP 服务，响应 PXE 客户端请求，并发送 Linux 系统文件内容给 PXE 客户端。可信

PXE 启动架构如图 2 所示。

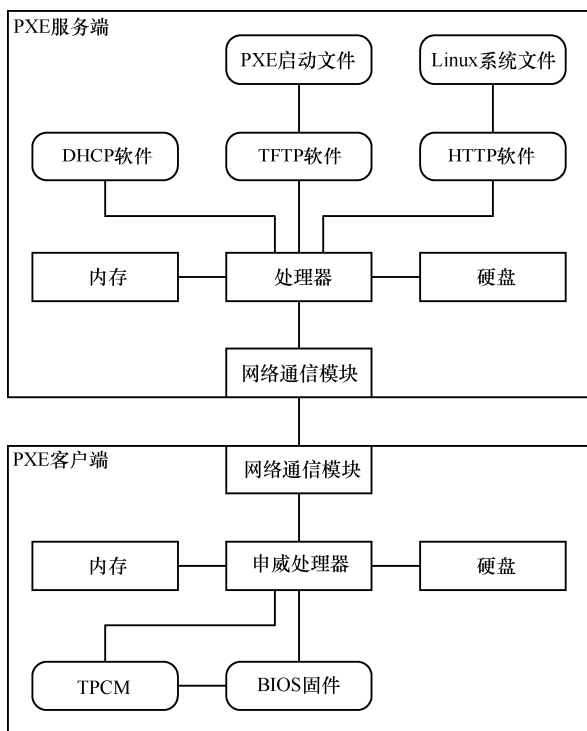


图 2 可信 PXE 启动架构
Figure 2 PXE trusted boot system structure

3.3 可信 PXE 启动过程

可信 PXE 启动过程比较复杂, 主要涉及 TPCM、BIOS 启动环境、PXE 启动环境 3 部分, 如图 3 所示。

(1) TPCM 先于 CPU 上电并启动, 由 TPCM 度量 BIOS 固件, 如果度量通过, 则启动 BIOS 进入 BIOS 启动环境; 如果度量不通过, 则发送报警信号。

(2) BIOS 启动环境选择 EFI Network 启动选项, 开始进行 PXE 启动。

(3) BIOS 启动环境向 PXE 服务端的 DHCP 服务发送获取 IP 请求, PXE 服务端响应请求, 分配 IP 地址给 PXE 客户端的 BIOS 启动环境, PXE 客户端设置自身 IP 地址。

(4) BIOS 启动环境向 PXE 服务端的 TFTP 服务发送获取 PXE 启动文件请求。

(5) PXE 服务端响应 PXE 客户端请求, 并发送 PXE 启动文件内容给 PXE 客户端。

(6) BIOS 启动环境通过可信平台模块度量 PXE 启动文件内容, 如果度量通过, 则启动 PXE

启动环境; 如果度量不通过, 则发送报警信号。

(7) PXE 启动环境向 PXE 服务端的 HTTP 服务发送获取 Linux 系统文件的请求。

(8) PXE 服务端响应 PXE 客户端请求, 并发送 Linux 系统文件内容给 PXE 客户端的 PXE 启动环境。PXE 启动环境通过 TPCM 度量 Linux 系统文件的内容, 如果度量通过, 进入下一步操作, 可信 PXE 启动完成; 如果度量不通过, 则发送报警信号。

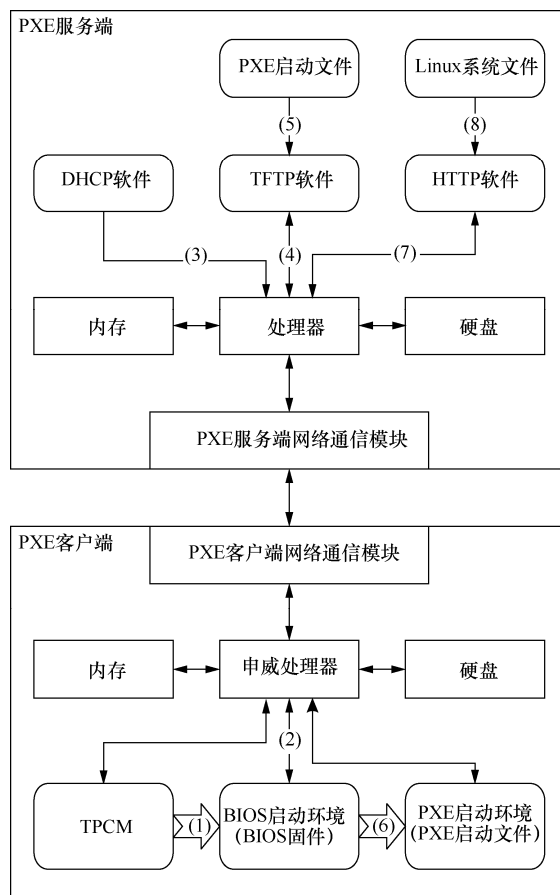


图 3 可信 PXE 启动过程
Figure 3 PXE trusted boot process

3.4 可信度量流程

TPCM 采用国密算法 SM2、SM3 与 SM4 作为密码算法。TPCM 的完整性度量摘要值计算函数为 SM3。根据 PXE 启动流程的 3 个阶段进行 3 次可信度量。基于 TPCM 的可信度量流程如图 4 所示。

(1) 由 TPCM 度量 BIOS 固件。在 BIOS 固件编译完成后, 通过国密算法 SM3 计算其摘要值作为基准值并存储到 TPCM 中。在 TPCM 启动后对 BIOS 固件进行可信度量, 生成度量值, 与基

准值进行比较,如果相等,则度量通过;如果不相等,则度量不通过。

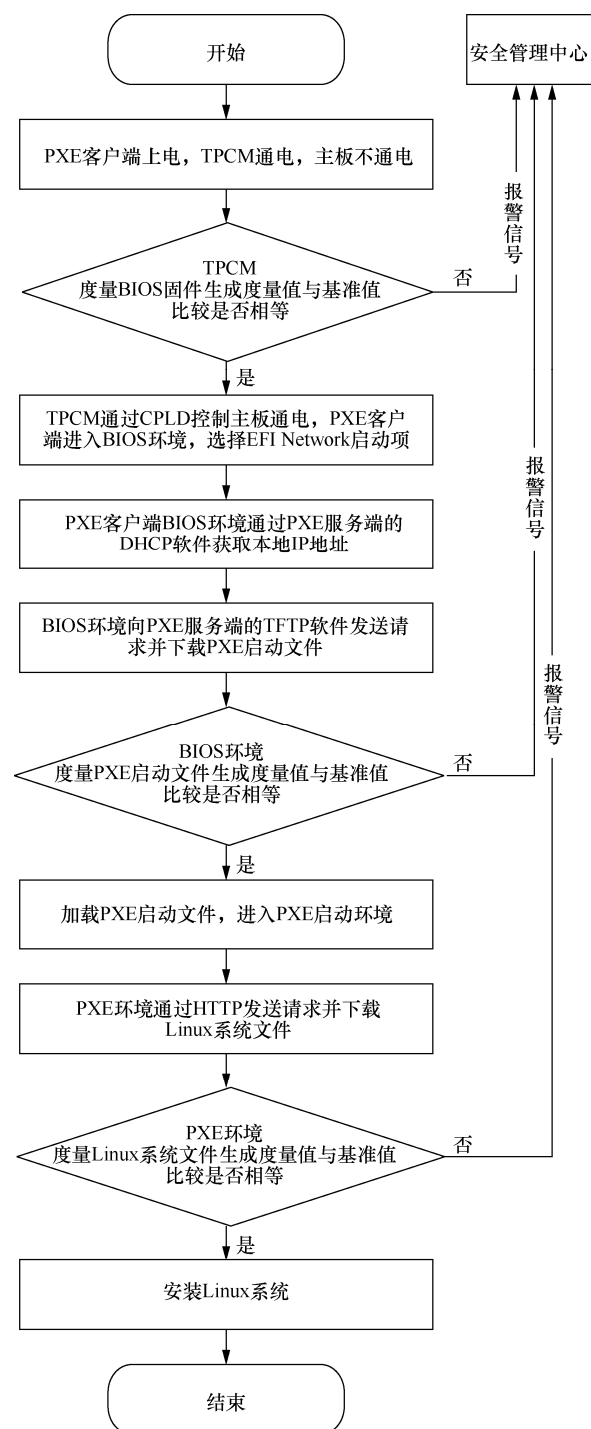


图4 基于 TPCM 的可信度量流程
Figure 4 Trusted measurement process based on TPCM

(2) 由 BIOS 启动环境度量 PXE 启动文件。在 PXE 启动文件编译完成后,通过国密算法 SM3

计算其摘要值作为基准值并存储到 BIOS 中。在 BIOS 启动环境从 PXE 服务端获取 PXE 启动文件后进行可信度量,生成度量值,与基准值进行比较,如果相等则度量通过,进入 PXE 启动环境;如果不相等,则度量不通过。

(3) 由 PXE 启动环境度量 Linux 系统文件。在 Linux 系统文件发布后,通过国密算法 SM3 计算其摘要值作为基准值并存储到 PXE 启动文件中。在 PXE 启动环境从 PXE 服务端获取 Linux 系统文件后进行可信度量,生成度量值,与基准值进行比较,如果相等,则度量通过,进入 Linux 系统;如果不相等,则度量不通过。

(4) 安全管理中心可以设定可信启动策略,并根据可信启动策略对报警信号进行处理。安全管理中心通过专用网络接口与 TPCM 进行通信。可信启动策略包括安全管理中心接收到报警处理信号时的处理方式,是继续启动使服务器进入不安全状态还是终止启动。例如,可信启动策略设定为 TPCM 对 BIOS 固件度量失败时,服务器终止启动,那么安全管理中心在收到 TPCM 对 BIOS 固件度量失败的报警信号后,对该信号存储备查,并发出终止服务器启动的控制指令。服务器收到安全管理中心的终止启动指令后,终止服务器启动。

4 实验分析

4.1 实验设置

本文所提方法的 PXE 客户端为申威 1621 服务器,处理器为申威 1621 处理器,内存 8 GB×4=32 GB,硬盘 1TB,网卡为 Inter 350 吉比特网卡。PXE 服务器端为通用服务器,在实验时用普通 PC 代替,CPU 为 i7-3920XM,内存 16 GB,硬盘 1 TB,网卡为 Intel 吉比特网卡。

对本文提出的方法进行实验,需要做以下开发工作。

(1) 编译申威 1621 服务器符合 UEFI 规范的 BIOS 固件,通过 SM3 算法计算其摘要值作为基准值,并存储到 TPCM 中。通过申威 1621 服务器的 BMC 烧录程序,将符合 UEFI 规范的 BIOS 固件烧录到申威 1621 服务的 BIOS 的 Flash 芯片中。

(2) 编译 PXE 启动文件,通过 SM3 算法计

算其摘要值作为基准值,并存储到申威 1621 服务器符合 UEFI 规范的 BIOS 固件中。

(3) 通过 SM3 算法计算 Linux 系统文件的摘要值作为基准值,并存储到 PXE 启动文件中。

(4) 搭建 PXE 服务端环境,安装 DHCP 服务器;安装 TFTP 服务,并将 PXE 启动文件放到 TFTP 服务的文件根目录;安装 HTTP 服务,并将 Linux 系统文件放到 HTTP 服务的文件根目录。

(5) 申威 1621 服务器安装并配置 TPCM 芯片。

4.2 实验结果

在 UEFI 固件中增加通过 TPCM 对 PXE 文件的可信度量模块,然后在服务端存放不同的 PXE 可信启动文件进行测试,结果表明,只有没有篡改的 PXE 启动文件被加载。可信启动实验结果如图 5 所示。TPCM 对 BIOS 固件的度量结果表明,只有 BIOS 固件的内容没有被篡改,才能够度量通过。PXE 启动环境对 Linux 系统文件的度量结果表明,只有 Linux 系统文件的内容没有被篡改,才能够度量通过。

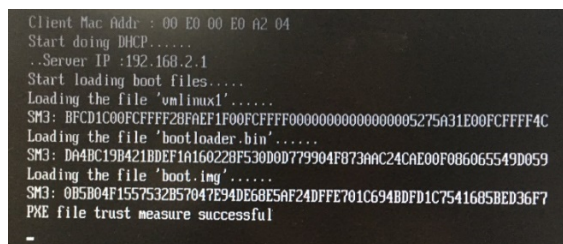


图 5 可信启动实验结果
Figure 5 Trusted boot experiment results

4.3 实验分析

4.3.1 安全性分析

本文提出的方法以 TPCM 为信任根,通用的可信计算节点具有很高的安全性。下面对可信 PXE 启动方法的安全性进行分析。

(1) 通过 TPCM 对申威 1621 服务器的 UEFI 规范的 BIOS 固件可信度量,有效防止了 BIOS 固件被篡改。

(2) 通过 BIOS 启动环境对 PXE 启动文件进行可信度量,有效防止了 PXE 启动文件被篡改。

(3) 通过 PXE 启动环境对 Linux 系统文件进行可信度量,有效防止了 Linux 系统文件被篡改。

以 TPCM 为信任根,一级度量一级,一级信任一级,形成一条完整的信任链,保障申威 1621

服务器运行在安全可信的环境中。

4.3.2 性能分析

基于深度操作系统通过 20 次实验,分别对 3 个不同可信度量阶段的度量过程进行计时发现,3 个不同阶段的可信度量时间之和小于 0.5 s,而整个 PXE 可信启动平均时间为 96 s,通过式(5)得出,可信度量时间比重为 $p_{\text{可信度量时间比重}} \approx 0.55\% < 1\%$,这对系统影响很小。通过实验得出操作系统文件越大,度量时间越长。由于麒麟操作系统镜像文件比深度操作系统文件大 2 倍多, PXE 可信启动时间与可信度量时间都会相应增加,但可信度量时间所占比重基本不变。

$$p_{\text{可信度量时间比重}} = \frac{v_{\text{可信度量时间}}}{t_{\text{PXE可信启动时间}}} \times 100\% \quad (5)$$

5 结束语

本文根据网络安全等级保护标准要求,基于可信计算理论提出了基于 TPCM 的网络可信启动方案,保障了服务器的 BIOS 固件、PXE 启动文件、Linux 系统文件的安全可信。以 TPCM 为信任根逐级度量,逐级信任,建立一条信任链与可信的服务器运行环境。本文提出的方法在申威服务器上进行了实验,实验结果表明了本文提出的方法能够及时发现被篡改的文件,并发出报警信号。只有没有被篡改的文件才能够度量通过,并能够及时发现被篡改的文件,发出报警信号,证明了本文提出方法能够保证服务器环境的安全可信运行。

本文提出的方法不包括服务器的操作系统实时运行时的应用程序的安全可信,以后的工作会对操作系统实时运行的应用程序进行动态可信度量,保障服务器环境运行过程的安全可信。

参考文献:

- [1] 冯登国,秦宇,汪丹,等.可信计算技术研究[J].计算机研究与发展,2011,48(8):1332-1349.
FENG D G, QIN Y, WANG D, et al. Research on trusted computing technology[J]. Journal of Computer Research & Development, 2011, 48(8): 1332-1349.
- [2] SHEN C X, ZHANG H G, WANG H M, et al. Research on trusted computing and its development[J]. Science in China Series F (Information Science), 2010, 53(3): 405-433.
- [3] ZHANG H G, LUO J G, JIN G, et al. Development of trusted com-

- puting research[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1407-1413.
- [4] 陈广勇, 祝国邦, 范春玲. 《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019) 标准解读[J]. 信息安全, 2019, 19(7): 1-7.
- CHEN G Y, ZHU G B, FAN C L. Information security technology—evaluation requirement for classified protection of cyber security(GB/T 28448-2019) standard interpretation[J]. Netinfo Security, 2019, 19(7): 1-8.
- [5] 何欣枫, 田俊峰, 刘凡鸣. 可信云平台技术综述[J]. 通信学报, 2019, 40(2): 158-167.
- HE X F, TIAN J F, LIU F M. Survey on trusted cloud platform technology[J]. Journal on Communications, 2019, 40(2): 158-167.
- [6] 刘川意, 王国峰, 林杰, 等. 可信的云计算运行环境构建和审计[J]. 计算机学报, 2016, 39(2): 339-350.
- LIU C Y, WANG G F, LIN J, et al. Practical construction and audit for trusted cloud execution environment[J]. Chinese Journal of Computers, 2016, 39(2): 339-350.
- [7] BAI G, HAO J, WU J, et al. TrustFound: towards a formal foundation for model checking trusted computing platforms[C]//International Symposium on Formal Methods. 2014.
- [8] VON BOMHARD N, AHLBORN B, MASON C, et al. The trusted server: a secure computational environment for privacy compliant evaluations on plain personal data[J]. Plos One, 2018, 13(9): 1-19.
- [9] 吴奇烜, 马建峰, 孙聪. 采用完整性威胁树的信息流完整性度量方法[J]. 网络与信息安全学报, 2019, 5(2): 50-57.
- WU Q X, MA J F, SUN C. Information flow integrity measurement method using integrity threat tree[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 50-57.
- [10] 胡浩, 刘玉岭, 张玉臣, 等. 基于攻击图的网络安全度量研究综述[J]. 网络与信息安全学报, 2018, 4(9): 1-16.
- HU H, LIU Y L, ZHANG Y C, et al. Survey of attack graph based network security metric[J]. Chinese Journal of Network and Information Security, 2018, 4(9): 1-16.
- [11] 田俊峰, 常方舒. 基于 TPM 联盟的可信云平台管理模型[J]. 通信学报, 2016, 37(2): 1-10.
- TIAN J F, CHANG F S. Trusted cloud platform management model based on TPM alliance[J]. Journal on Communications, 2016, 37(2): 1-10.
- [12] LI Y H, ZHANG Y D, LI P, et al. An efficient trusted chain model for real-time embedded systems[C]//International Conference on Computational Intelligence & Security. 2016.
- [13] CONG W N, CAO K. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(23): 1467-1479.
- [14] 沈昌祥, 张大伟, 刘吉强, 等. 可信 3.0 战略: 可信计算的革命性演变[J]. 中国工程科学, 2016, 18(6): 53-57.
- SHEN C X, ZHANG D Q W, LIU J G, et al. The strategy of TC 3.0: a revolutionary evolution in trusted computing[J]. Strategic Study of CAE, 2016, 18(6): 53-57.
- [15] 张兴, 黄强, 沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.
- ZHANG X, HUANG Q, SHEN C X, et al. A formal method based on noninterference for analyzing trust chain of trusted computing platform[J]. Chinese Journal of Computers, 2010, 33(1): 74-81.
- [16] 郭颖, 毛军捷, 张翀斌, 等. 基于可信平台控制模块的主动度量方法[J]. 清华大学学报(自然科学版), 2012, 52(10): 1465-1473.
- GUO Y, MAO J J, ZHANG C B, et al. Active measures based on a trusted platform control module[J]. Journal of Tsinghua University, 2012, 52(10): 1465-1473.
- [17] 王勇, 许荣强, 任兴田, 等. 可信计算中信任链建立的形式化验证[J]. 北京工业大学学报, 2016, 42(3): 387-392.
- WANG Y, XU R Q, REN X T, et al. Formal verification of establishment of chain of trust in trusted computing[J]. Journal of Beijing University of Technology, 2016, 42(3): 387-392.
- [18] HUANG G, YANG B. Research and improvement on PXE security of dynamic distributed network of non-fixed disk[J]. Journal of Computers, 2012, 7(7): 1681-1687.

[作者简介]



刘国杰(1982-), 男, 山东东营人, 北京工业大学博士生, 主要研究方向为网络与信息安全、可信计算。



张建标(1969-), 男, 江苏海门人, 博士, 北京工业大学教授、博士生导师, 主要研究方向为网络与信息安全、可信计算。