云环境下国产可信根 TCM 虚拟化方案研究*

赵 军[1],王 晓[2]

(1.张家口学院 数学与信息科学学院,河北 张家口 075000;2.天津财经大学 理工学院,天津 300222)

摘 要:将可信计算技术应用于云计算环境中是保证云安全的有效途径。针对国产可信计算的可信根可信密码模块(Trusted Cryptography Module,TCM)只适用于单机平台,无法为多虚拟机的云平台提供安全可信性保障的问题,对 TCM 的虚拟化方案进行研究,构建云可信根(Cloud TCM,C-TCM)架构。在 C-TCM 物理环境内部构造宿主可信根和虚拟可信根,分别为物理宿主机和虚拟机提供可信服务,同时在虚拟机监视器层部署虚拟可信根管理机制,实现虚拟可信根对 C-TCM 硬件资源的共享。该方案可有效保证云平台的安全可信性。

关键词:云安全;可信计算;可信密码模块 TCM 虚拟化;云可信根 C-TCM 架构

中图分类号:TP393 **文献标识码**:A **DOI**:10.19358/j.issn.2096-5133.2020.06.008

引用格式:赵军,王晓. 云环境下国产可信根 TCM 虚拟化方案研究[J].信息技术与网络安全,2020,39(6):44-48,67.

Research on virtualization scheme of domestic trusted root TCM in cloud environment

Zhao Jun[1], Wang Xiao[2]

(1.School of Mathematics Information Science, Zhangjiakou University, Zhangjiakou 075000, China;
2.Institute of Science and Technology, Tianjin University of Finance and Economics, Tianjin 300222, China)

Abstract: Applying trusted computing technology to cloud environment is an effective way to ensure cloud security. The trusted cryptography module(TCM) of domestic trusted computing is suitable for single platform, but can not provide security and credibility guarantee for cloud platform with multi virtual machines. Aiming at this problem, the virtualization scheme of TCM is studied, and the architecture of cloud TCM(C-TCM) is constructed. In the physical environment of C-TCM, host trusted root and virtual trusted root are constructed, which provide trusted services for physical host and virtual machine respectively. At the same time, virtual trusted root management mechanism is deployed in the virtual machine monitor layer to realize the resources sharing of C-TCM hardware. This scheme can effectively guarantee the security and credibility of the cloud platform.

Key words: cloud security; trusted computing; the virtualization of trusted cryptographic module TCM; the architecture of cloud trusted root C-TCM

0 引言

云计算环境中的信息安全问题是一个系统性的工程问题[1],以往的安全机制缺乏关联性,只是从某些方面去解决特定问题,不能构建整体性的解决方案[2]。可信计算技术作为信息安全的有力保障[3],基于可信根构建贯穿系统各个关键部分的信任链,从信任的角度入手整合系统中的各项安全机制,为系统提供整体性的安全支撑。将国产可信计算技术[4]应用于云计算环境中,构建国产可信的云安全基础设施环境,是解决我国云安全问题的有效途径。在最新颁布的《信息安全技术 网络安全等级保护基本要求》(等保 2.0)中[5-6],加入了基于国产可信计算技术的可信验证要求,因此基于国产可信计算构建安全可信的云计算环境具有重要现实意义。

可信根作为信任的源头是可信计算技术的核心组件。我国提出了自己的可信根可信密码模块(Trusted Cryptography Module,TCM)。传统的 TCM 适

* 基金项目:河北省教育厅科技项目(Z2017158)

用于单机平台，通过 TCM 可以保证单机计算系统的安全可信性，但是无法满足云计算环境中多虚拟机对可信根的使用需求。为了使 TCM 适用于云计算环境，本文提出一种 TCM 虚拟化方案，构建云可信根(Cloud TCM，C-TCM)架构，为云计算节点中物理宿主机及多虚拟机提供可信根服务，为构建安全可信的云计算环境提供有力支撑。

1 相关工作

目前针对可信根虚拟化主要有三种解决方案：基于软件的可信根虚拟化方案、基于硬件的可信根虚拟化方案和可信根半虚拟化方案。

基于软件的可信根虚拟化是指用软件模拟硬件芯片功能，虚拟可信根提供与物理可信根一致的访问接口，可实现可信根的大部分功能，只有少数对安全性要求较高的功能由物理可信根执行。最早提出基于软件的可信根虚拟化方案的是 IBM 的研究员 BERGER S[7]等人，他们基于 Xen 架构设计并实现了 TPM 的虚拟化架构。为了提高虚拟可信根的安全性，ANDERSON M J[8]等人和 MURRAY D G[9]等人对 BERGER S[7]等人的方案进行了改进，基于隔离增强安全性的思想，把 vTPM 实例运行在隔离域中。当前 Xen 架构采用 StubDom[10]机制，每个子域中运行一个 Mini-OS[11]。将虚拟根管理器和虚拟根实例分别放置在不同的子域中进行隔离，以增强安全性。HE R Y[12]等人提出了基于软件的虚拟可信根的 uTPM，HOSSEINZADEH S[13]等人提出了基于容器的可信根虚拟化方案。严飞[14]等人提出了一种基于 Intel 软件扩展保护(Software Guard Extension，SGX)技术的 vTPM 安全增强方案(vTPM Security Enhancement，vTSE)，为 vTPM 实例提供了有效的安全保障。在安全性方面，基于软件的虚拟化方案的隔离性较差，密码资源缺乏硬件保护；在效率方面，软算法与硬件相比性能不足，效率较低。

基于硬件的可信根虚拟化是指对物理可信根的设计实现进行改进，在可信根物理环境中同时运行多个虚拟根实例，实现虚拟根对硬件可信根资源的共享。刘明达[15]等人提出一种基于 SR-IOV 的 TCM 硬件虚拟化方案并构建了可信虚拟环境的信任链。张伶俐[16]等人基于嵌入式系统实现了虚拟 TCM 并构建了嵌入式系统中的信任链。王冠[17]等人对基于可信根服务器的虚拟 TCM 密钥管理功能进行了相关研究。段翼真[18]等人提出了一种支持多域访问的可信云终端设计，实现了 TCM 的虚拟化和信任链传递机制。与软件虚拟化方案相比该方案的安全性和执行效率更高。

可信根半虚拟化方案是指通过在虚拟机监视器层添加对底层物理可信根访问的调度机制，并对可信根内部资源进行虚拟化，实现虚拟机对物理可信根的共享。ENGLAND P[19]等人提出了 TPM 半虚化方案，通过在 Hypervisor 层添加软件组件，对物理根的使用进行调度协调，实现在多个虚拟机之间安全共享一个物理 TPM。YAP J Y[20]等人提出了基于 TPM2.0 规范的企业化 TPM 半虚拟化架构。该方案可为虚拟机提供物理可信根的功能，但有些功能接口会发生变化。

对各种可信根虚拟化方案的对比如表 1 所示。

表 1 可信根虚拟化方案对比

虚拟化方案	安全性	是否需要重新设计硬件芯片	是否需要改进 Hypervisor 层
软件虚拟化	低	不需要	需要
半虚拟化	高	不需要	需要
硬件虚拟化	高	需要	不需要

通过上述分析对比可知，每种虚拟化方案有各自的优势和缺点。本文结合硬件虚拟化和半虚拟化方案的特点，提出一种云可信根(Cloud TCM，C-TCM)设计方案，对 TCM 物理可信根进行扩展，并在虚拟机监视层添加管理机制，使资源有限的云可信根物理环境能同时支持多个虚拟可信根运行，在保障安全性同时，提高执行效率，从而满足云计算平台对可信根的使用需要。

2 云可信根 C-TCM 架构

针对物理 TCM 无法同时为云服务器的物理宿主机和虚拟机提供可信根服务的问题，提出一种适用于云计算环境的云可信根 C-TCM 架构。该方案结合了可信根硬件虚拟化方案和半虚拟化方案的特点，对 TCM 硬件芯片的设计实现进行改进扩展，并在虚拟机监视器层部署虚拟可信根管理机制，实现宿主机可信根和虚拟机可信根对 C-TCM 硬件资源的共享，同时满足物理宿主机及虚拟机对可信根的使用需求。云可信根 C-TCM 的总体架构如图 1 所示。

C-TCM 总体架构包括位于硬件层的 C-TCM 物理环境，位于宿主机操作系统层的 C-TCM 物理驱动和 vTCM 上下文安全存储机制，位于虚拟机监视器层的 vTCM 管理机制和 vTCM 后端驱动，以及位于虚

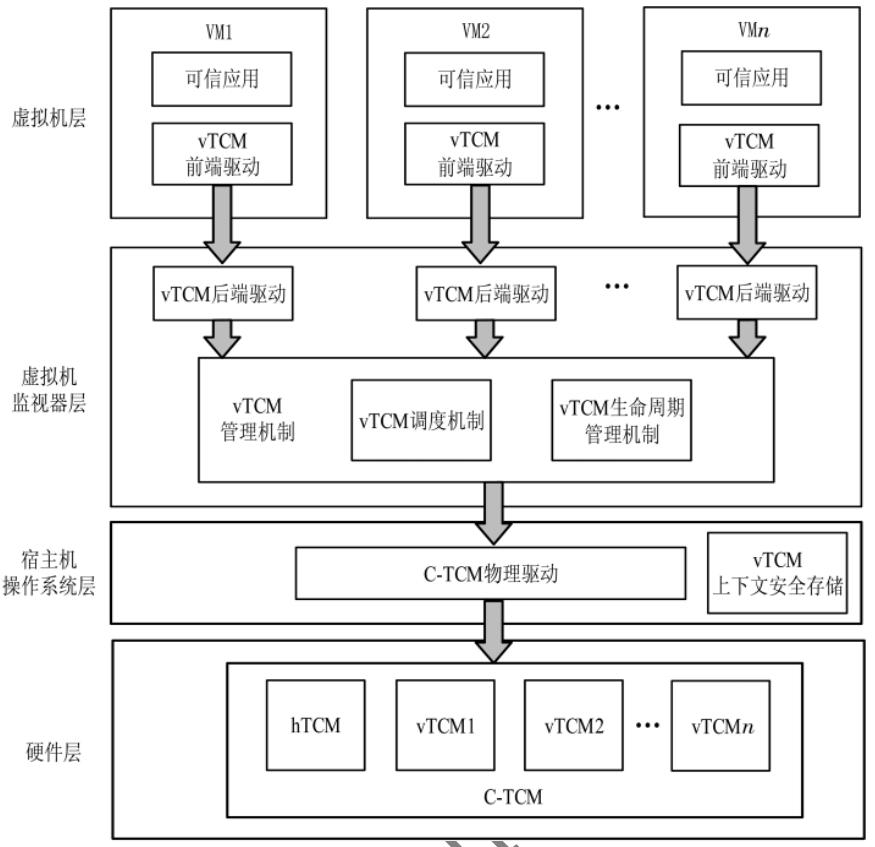

图 1 C-TCM 总体架构图

拟机层的 vTCM 前端驱动。

2.1 C-TCM 物理环境

在硬件层,对原有 TCM 硬件芯片的设计实现进行改进和扩展,构建 C-TCM 物理环境。为了同时满足物理宿主机和虚拟机的可信根使用需求,在C-TCM 物理环境中分别构建为物理宿主机提供可信功能的宿主机可信根(host TCM,hTCM),以及为虚拟机提供可信功能的虚拟可信根(virtual TCM,vTCM)。由于受资源限制,C-TCM 物理环境只能为有限个 vTCM 提供硬件资源支持。当虚拟机的数量多于 C-TCM 支持的 vTCM 数量时,通过 vTCM 调动机制对 vTCM 上下文进行调度,实现虚拟根对 vTCM 资源的共享,从而支持多个虚拟机的可信根使用请求。hTCM 始终位于 C-TCM 内部为物理宿主机提供可信支持,不参与调度。

2.2 C-TCM 物理驱动及 vTCM 上下文安全存储机制

C-TCM 物理驱动位于宿主机操作系统层,负责接收对 C-TCM 的使用及管理命令。C-TCM 物理驱动接收三种命令,分别为:物理宿主机对可信根 hTCM 的使用请求、虚拟机对可信根 vTCM 的使用请求以及 vTCM 管理机制对 C-TCM 的管理命令。为了区分 hTCM 命令及 vTCM 命令,在 vTCM 命令头添加 vTCM 标识及发出该命令的虚拟机编号。vTCM 调度机制根据虚拟机编号确定与其关联的虚拟可信根。

vTCM 上下文中存储了 vTCM 的关键信息,包括虚拟背书密钥(virtual Endorsement Key,vEK)、虚拟平台身份密钥(virtual Platform Identity Key,vPIK)、虚拟存储根密钥(virtual Storage Root Key,vSRK)、虚拟平台配置寄存器(virtual Platform Configuration Register,vPCR)值、非易失性寄存器值、各类证书以及与虚拟机保持绑定的关联信息等。当 vTCM 调度机制将 vTCM 上下文从 C-TCM 物理环境中调出时,通过 hTCM 将其加密存储到宿主机硬盘上。当需要重新调入到 C-TCM 物理环境中时,需 hTCM 对其进行解密后再调入。

2.3 vTCM 管理机制

受硬件资源限制,C-TCM 仅能支持数量有限的 vTCM。为了实现多虚拟机对 C-TCM 的共享,在虚拟机监视器层部署 vTCM 管理机制,包括 vTCM 调度机制和 vTCM 生命周期管理机制。

2.3.1 vTCM 调度机制

vTCM 调度机制负责接收从 vTCM 后端驱动传递过来的上层虚拟机的可信根使用请求，将其传递给相应的虚拟可信根。如果当前虚拟机对应的虚拟可信根在 C-TCM 物理环境中运行，则 vTCM 接收并执行请求命令，并将响应结果回传给虚拟机。如果虚拟可信根在 C-TCM 物理环境外部，则根据调度算法对安全存储在硬盘上的虚拟根上下文进行调度，将其从外存调入到 C-TCM 物理环境内部，再执行虚拟机的请求命令。在物理资源受限情况下，通过 vTCM 调度机制实现 vTCM 对 C-TCM 硬件资源的共享，支持了多虚拟机对可信根的使用请求。

为了减少 vTCM 上下文调度切换的次数，为每个 vTCM 创建一个命令缓存队列，如图 2 所示。将对 vTCM 的使用请求暂存在缓存队列当中，如对 vTCM1 的请求有 A_1、A_2、A_3。

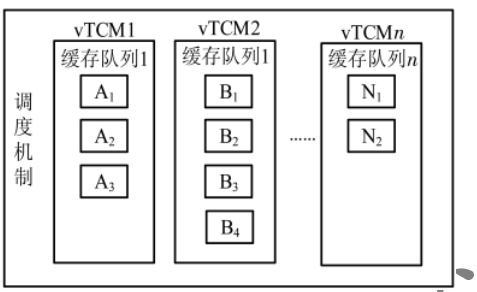

图 2 虚拟根命令缓存队列

为了提高调度效率，调度的优先级由虚拟机等待时间及缓存队列中的命令数共同决定。设定一个等待时间阈值为 ρ，当虚拟机的等待时间超过 ρ 时，优先对其 vTCM 上下文进行调度。当等待时间不超过 ρ 时，优先调度缓存命令数最多的 vTCM 上下文。设 vTCMn 缓存队列中的命令数为 ω_n，则所有等待调度的 vTCM 的命令数构成集合 W，$W=(\omega_1,\omega_2,\cdots,\omega_n)$。设 vTCMn 等待调度的时间为 τ_n，则所有 vTCM 等待调度的时间构成集合 T，$T=(\tau_1,\tau_2,\cdots,\tau_n)$。从集合 W 中选出缓存队列中最大值 $\omega_i=\mathrm{Max}(\omega_1,\omega_2,\cdots,\omega_n)$，$i\in 1,2,\cdots,n$。从集合 T 中选出等待时间最大值 $\varphi_j=\mathrm{Max}(\varphi_1,\varphi_2,\cdots,\varphi_n)$，$j\in 1,2,\cdots,n$。具体调度算法如下：

//当等待调度时间没有超过阈值 ρ 时

IF $(\tau_j<\rho)$

//则调度缓存队列中命令数最多的 vTCMi 上下文

dispatch vTCMi – context

ELSE

//否则，调度等待时间超出阈值 ρ 的 vTCMj 上下文

dispatch vTCMj – context

vTCM 上下文的调度优先级由等待时间和缓存命令数两个因素共同决定，既保证了虚拟机等待时间不会过长，也满足了对虚拟根使用较多的虚拟机的请求。

2.3.2 vTCM 生命周期管理机制

vTCM 生命周期管理机制负责对 vTCM 生命周期中的各个阶段进行管理，包括 vTCM 的创建、初始化、迁移、销毁等，从而实现 vTCM 与虚拟机的绑定及生命周期同步，保证虚拟机在整个生命周期中的安全可信性。

(1)虚拟可信根创建

云计算节点接收到控制节点发出的虚拟机创建指令后，由虚拟机监视器为虚拟机分配必要的资源，包括虚拟 CPU、虚拟内存、虚拟网络设备等。vTCM 生命周期管理机制在虚拟机创建之前为其创建一个空的 vTCM 上下文，并分配唯一的 ID 号、易失性存储空间、非易失性存储空间等资源。通过虚拟根 ID 及虚拟机 ID 实现 vTCM 与虚拟机的关联绑定。

(2)虚拟可信根初始化

在虚拟机启动之前，通过 vTCM 调度机制将 vTCM 上下文调入到 C-TCM 的物理环境中，对其进行初始化。由 hTCM 为 vTCM 生成各类关键密钥，包括 vEK、vPIK 及 vSRK，并为其颁发 vEK 证书。在虚拟机首次启动时，获取启动各阶段的度量值形成度量基准值，存储在 vTCM 的非易失寄存器中。

(3)虚拟可信根迁移

vTCM 生命周期管理机制截获到虚拟机迁移指令后，首先验证迁移源平台和目标平台的可信性，并建立迁移安全通道。通过安全通道将虚拟根数据迁移到目标平台，完成虚拟可信根的迁移。更新源平台及目标平台上的关联列表，保证虚拟可信根和虚拟机之间的绑定关系。

(4)虚拟可信根挂起

当 vTCM 生命周期管理机制拦截到虚拟机挂起指令时，需将其相应的虚拟根设置为挂起状态。通过 vTCM 调度机制将虚拟可信根上下文从 C-TCM 物理环境中调出，对其非易失性存储器中的虚拟根密钥信息、vPCR 值以及易失性存储器中的寄存器状态等信息进行安全存储，以备虚拟根恢复之用。

(5)虚拟可信根恢复

vTCM 生命周期管理机制拦截到虚拟机恢复运行指令时,首先恢复其虚拟根执行。将安全存储在物理磁盘上的 vTCM 上下文信息解密后调入 C-TCM 中,并根据挂起时保存的寄存器状态信息,恢复寄存器运行,准备为虚拟机提供安全服务。

(6)虚拟可信根销毁

vTCM 生命周期管理机制拦截到虚拟机销毁指令时,将与虚拟机绑定的虚拟根销毁。如果虚拟根上下文在 C-TCM 内部,则首先将其调出再进行销毁删除。如果虚拟根上下文在外部磁盘加密存储,则直接将其进行删除。

vTCM 生命周期管理机制解决了虚拟根生命周期管理问题,实现了虚拟根生命周期与虚拟机生命周期的一致性,保证了虚拟机全生命周期的安全可信性。

2.4 vTCM 前端驱动

在客户虚拟机上运行可信应用,vTCM 前端驱动负责接收虚拟机对可信根的使用请求,并传递到虚拟机监视器层的后端驱动,进一步通过 vTCM 管理机制、C-TCM 物理驱动将请求传递给虚拟可信根。当虚拟可信根完成请求时,将结果回传给虚拟机,完成对可信根的使用。

以上为 C-TCM 的总体架构,通过该架构实现 TCM 的虚拟化,同时为宿主机和各个虚拟机提供基于硬件可信根的保护,保证云服务器整体的安全可信性。

3 结论

本文提出一种国产可信根 TCM 的虚拟化架构,为云计算平台设计了云可信根 C-TCM,该方案解决了物理 TCM 无法应用于云计算环境为物理宿主机和虚拟机提供可信根功能的问题,通过 C-TCM 可保证物理宿主机和虚拟机启动和运行过程中的安全可信性。目前面临的主要问题是硬件虚拟化涉及对芯片的改进和扩展,实现难度较大。在下一步的研究中,将实现 C-TCM 芯片的原型系统,对其功能和性能进行相关验证。

参考文献

[1] 张玉清,王晓菲,刘雪峰,等.云计算环境安全综述[J].软件学报,2016,27(6):1328-1348.

[2] ALI M,KHAN S U,VASILAKOS A V.Security in cloud computing:opportunities and challenges[J].Information Sciences,2015,305:357-383.

[3] 田俊峰,杜瑞忠,蔡红云,等.可信计算与信任管理[M].北京:科学出版社,2014.

[4] 沈昌祥.用主动免疫可信计算 3.0 筑牢网络安全防线营造清朗的网络空间[J].信息安全研究,2018,4(4):282-302.

[5] 马力,祝国邦,陆磊.《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J].信息网络安全,2017(2):77-84.

[6] 陈卫平.可信计算 3.0 在等级保护 2.0 标准体系中的作用研究[J].信息安全研究,2018,4(7):633-638.

[7] BERGER S,GOLDMAN K A,PEREZ R,et al.vTPM:virtualizing the trusted platform module[C].Conference on Usenix Security Symposium,2006:305-320.

[8] ANDERSON M J,MOFFIE M,DALTON C I.Towards trustworthy virtualisation environments:Xen library OS security service infrastructure[J].HP Tech Reort,2007:88-111.

[9] MURRAY D G,MILOS G,HAND S.Improving Xen security through disaggregation[C].Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on virtual execution environments.New York:ACM,2008:151-160.

[10] Xen open source community.XenStubDom[EB/OL].(2012-12-11)[2020-03-10].http://wiki.xensource.com/wiki/StubDom.

[11] Xen open source community.Mini-OS[EB/OL].(2018-02-07)[2020-03-10].https://wiki.xen.org/wiki/Mini-OS.

[12] HE R Y,WANG S J,JIANG L.A user-specific trusted virtual environment for cloud computing[J].Information Technology Journal,2013,12(10):1905-1913.

[13] HOSSEINZADEH S,LAUREN S,LEPPANEN V.Security in container-based virtualization through vTPM[C].IEEE/ACM International Conference on Utility & Cloud Computing.IEEE,2017:214-219.

[14] 严飞,于钊,张立强,等.vTSE:一种基于 SGX 的 vTPM 安全增强方案[J].工程科学与技术,2017,49(2):133-139.

[15] 刘明达,曹慧渊,拾以娟,等.基于 SR-IOV 的TCM 硬件虚拟化构建可信虚拟环境[J].武汉大学学报(理学版),2017,63(2):117-124.

(下转第 67 页)

3 结论

本文设计了一款应用于卫星导航系统的多频圆极化天线。天线采用螺旋结构与微带结构相组合方式，实现北斗一代收发 L/S 频段、北斗二代 B1 频段和 GPS L1 频段的覆盖，天线具有良好的低仰角增益，通过螺旋结构可提高天线的低角搜星能力，同时具有更高的定位精度。仿真结果表明天线性能指标良好，满足卫星导航应用要求，具有很好的应用前景。

参考文献

[1] AGARWAL K, NASIMUDDIN, ALPHONES A. Triple-band compact circularly polarised stacked microstrip antenna over reactive impedance meta-surface for GPS applications [J]. IET Microwaves Antennas & Propagation, 2014, 8(13): 1057-1065.

[2] SO K K, WONG H, LUK K M, et al. Miniaturized circularly polarized patch antenna with low back radiation for GPS satellite communications[J]. IEEE Transactions on Antennas & Propagation, 2015, 63(12): 5934-5938.

[3] 吕凯波，陈乃阔，耿士华.一种提高北斗导航定位终端安全性能的设计[J].信息技术与信息化，2016(11)：42-43.

[4] 陈兆丰，潘锦.应用于北斗和 GPS 的双频小型圆极化微带天线[J].电子科技，2014，27(12)：116-119.

[5] 商锋，李文博，陈文学.一种适应于卫星定位的多频微带天线[J].西安邮电大学学报，2016，21(4)：67-71.

[6] 杨晓杰，袁家德.一种卫星导航终端多频圆极化微带天线的设计[J].微型机与应用，2016，35(4)：61-64.

[7] 王维.多频卫星导航天线设计与研究[D].昆明：昆明理工大学，2017.

[8] 宋跃，刘岚，韩国栋.北斗多模卫星导航天线设计[J].电子科技，2013，26(4)：137-139.

[9] YANG X J, YUAN J D. Dual-band and dual-circularly polarized microstrip antenna with low elevation gain improvement for CNSS applications[J]. Microwave & Optical Technology Letters, 2016, 58(5): 1016-1022.

[10] SU C W, HUANG S K, LEE C H. CP microstrip antenna with wide beamwidth for GPS band application[J]. Electronics Letters, 2007, 43(20): 1062-1063.

(收稿日期：2020-02-18)

作者简介：

臧志斌(1974-)，男，硕士，高级工程师，主要研究方向：电力芯片研发制造、电力行业信息化、电力工程设计。

傅宁(1981-)，男，硕士，高级工程师，主要研究方向：电力行业信息化、应急通信研究。

马军(1984-)，男，本科，工程师，主要研究方向：电力行业信息化、网络安全研究。

(上接第 48 页)

[16] 张伶俐，张功萱，王天舒，等.嵌入式系统可信虚拟化技术的研究与应用[J].计算机工程与科学，2016，38(8)：1654-1660.

[17] 王冠，袁华浩.基于可信根服务器的虚拟 TCM 密钥管理功能研究[J].信息网络安全，2016(4)：17-22.

[18] 段翼真，刘忠，施展.一种支持多域访问的可信云终端设计[J].华中科技大学学报(自然科学版)，2017，45(12)：32-38.

[19] ENGLAND P, LOSER J. Para-virtualized TPM sharing[C]. International Conference on Trusted Computing & Trust in Information Technologies: Trusted Computing-challenges & Applications, 2008.

[20] YAP J Y, TOMLINSON A. Para-virtualizing the trusted platform module: an enterprise framework based on version 2.0 specification[C]. International Conference on Trusted Systems. Springer, Cham, 2013: 1-16.

(收稿日期：2020-03-19)

作者简介：

赵军(1978-)，男，硕士，副教授，主要研究方向：网络空间安全、数据库技术。

王晓(1983-)，通信作者，女，博士，讲师，主要研究方向：信息安全、可信计算、云安全。E-mail：wangxiao8343@163.com。

版权声明