·CTCIS 2016 推荐论文· DOI:10.15961/j.jsuese.201601050

一种云计算适用的虚拟可信报告根构建机制

黄 强,孔志印,张德华,常 乐
(信息保障技术重点实验室,北京 100072)

摘 要:可信计算技术能够为云计算基础设施提供可信赖的状态及其验证手段,而可信报告这一可信平台基础功能在云环境的实现与普通主机有较大差异,如何构建虚拟可信报告根还没有通用和成熟的方案,将影响远程证明等可信技术在云环境的应用。为构建云计算适用的可信计算体系结构,解决为虚拟机提供唯一性身份标志和反映虚拟机与物理宿主机统一的完整性状态问题,明确了虚拟机应拥有各自独立的基于秘钥的身份标志以及虚拟机所属平台配置寄存器(PCR)类敏感信息必须是受保护的、可迁移的以适应虚拟机迁移需求。由进一步分析可知虚拟机完整性状态应包含以PCR值表示的虚拟机完整性状态和物理平台完整性状态。由此,在集中管理虚拟化/非虚拟化可信计算平台的模型预设条件下,基于国际可信计算组织(TCG)规范提出的身份证明秘钥(AIK)概念进行扩展,提出一种使用虚拟AIK作为虚拟机身份标志,并为每个虚拟机生成由其实际物理平台启动PCR值和虚拟机启动虚拟PCR值连接而成的PCR值的可信报告模型。设计了对应的虚拟PCR值复制机制、完整性报告机制、虚拟机敏感数据管理机制,并与TCG规范中方法进行了对比。该机制在兼容传统AIK验证机制的基础上,能够为每个虚拟机产生独立身份标识,向验证者证明自身完整性状态的同时简化了对虚拟机的验证流程。

关键词:可信计算;虚拟化;证书;远程证明
中图分类号:TP309 **文献标志码**:A **文章编号**:2096-3246(2017)02-0140-05

Construction Mechanism of Virtual Root of Trust for Report in Cloud

HUANG Qiang, KONG Zhiyin, ZHANG Dehua, CHANG Le
(Info. Assurance Technology Laboratory, Beijing 100072, China)

Abstract: Trusted computing technology can provide trustworthy state and corresponding verification method for cloud infrastructure. The first step of building trusted computing architecture is to build root of trust. The problem of building root of trust for report was not well solved in virtual trusted computing platform because of the differences between virtual machine and ordinary host. No universal and proven solution was developed, which affects the application of trusted computing technology, such as attestation in cloud environment. In this paper, by analyzing related works, it was concluded that the independent identity based on asymmetric key for each VM as well as protected and migratable storage of sensitive data such as platform configuration register (PCR) value and keys used in a VM were all required for constructing trusted computing architecture in cloud infrastructure. Furthermore, the integrity state of a VM reported with PCR should consist of both the physical PCR value emerged from physical booting procedure and virtual PCR value recording VM software boot procedure. With assumption of centralized and virtualization/non-virtualization unified trusted computing platform management, a model of building root of trust for report with virtual attestation identity key (AIK) as a virtual machine's identity was proposed. It can maintain a set of individual virtual and physical combined PCR values for each VM. Then the verification procedure of virtual trusted computing platform to identify itself with VAIK and report its unique integrity state with VPCR to verifiers including attestation challenger were proposed to support this model. At last, it was compared with TCG specification's method from several different management dimensions. Our model can build unambiguous identity for each VM. Meanwhile it can reduce complexity of verification procedure of VM and keep the compatibility of ordinary AIK verification mechanism.

Key words: trusted computing; virtualization; credential; attestation

收稿日期:2016-09-19
基金项目:国防重点预研项目资助(10502)
作者简介:黄 强(1977—),男,工程师,博士. 研究方向:可信计算与信息安全. E-mail:hqcc2007@163.com

可信计算技术近年来在国内外都获得了广泛的关注并取得了长足的进展。可信计算技术出发点是解决传统主机执行程序可被随意修改,系统完整性被破坏,从而导致恶意代码被植入和运行的问题。可信计算核心特征可以概括为:基于可信硬件设备构建的可信根,建立从底层软硬件到应用程序的信任链。

云计算在国内外发展迅速的同时,也越来越引发了人们对虚拟化桌面及服务器等虚拟化基础设施安全的关注,国际上工业界为主成立的 TCG 提出可信计算对云计算安全是天然适用的,可信计算技术提供了基于硬件的安全可信基。TCG 提出的可信虚拟化平台体系规范[1]主要集中在虚拟可信平台模块(VTPM)和深度远程证明(deep attestation),但由于其复杂性所限,该规范的实际应用尚未见报道。

TCG 规范从可信根核心功能出发,提出了可信度量根、可信存储根和可信报告根的概念[2],动态可信度量根与可信服务器虚拟环境验证关联较大,目的是实现在物理主机不重启情况下进入可信、可控的状态作为动态度量的起点,主要涉及体系结构和 CPU 相关的一些技术,如 Intel 的 TXT 技术和 AMD 的 SVM 技术;可信存储根也具有一些成熟方案,本文集中研究可信报告根。TCG 规范[3]提出,可信报告根在通用主机上是 TPM 硬件,由 TPM 内部可信的实施 PCR 扩展及签名操作。签名使用身份证明密钥 AIK(attestation identity key),AIK 由平台拥有者(具有实施 TPM 管理操作特权)产生,使用 AIK 而不使用绑定密钥 EK(endorsement key)这种与 TPM 绑定的密钥的目的是防止 TPM 身份被暴露。AIK 证书由可信第三方(如 TCG 规定的隐私性 CA,Privacy CA)在验证 TPM 的 EK 签名后颁发,在可信第三方配合下,通过使用 AIK 证书不暴露 EK 和 AIK 间的对应关系。

中国在可信计算领域发展上具有自己的特色,起步不晚,水平不低[4]。从一开始走的就是独立自主的道路,目前,已经形成以可信计算平台控制模块(TPCM)/可信密码模块(TCM)专用硬件设备(对应于 TCG 提出的 TPM 可信平台模块)为基础,以可信软件基(TSB)为核心,以可信应用系统为推动的可信计算体系,并已出台一系列相应标准规范[5]。

本文基于云计算环境提出一种扩展 AIK 用途用以动态标识虚拟机身份并向验证服务器报告虚拟机相关完整性状态的方法。

1　相关工作

TCG 的可信虚拟化平台体系规范[1]提出 AIK 证书包含一个可选的证书域 rtmType 用以标识可信平台是物理平台还是虚拟平台,远端的挑战者可以通过读取该数值确认该证书来自虚拟平台。文献[6]提出使用双 AIK 签名的方法:一个 AIK 代表物理 TPM,对前半部分代表物理平台可信状态的 PCR 值进行签名;一个代表虚拟 TPM,对后半部分代表虚拟机可信状态的 PCR 值进行签名。这种签名和报告方式导致虚拟平台与物理平台向远程认证服务器进行可信报告时其报告机制不统一,远程证明服务器必须事先知道报告者的类型,采取不同的验证流程才能分别进行验证。而且各虚拟机对应的 PCR 值只包含上半部分与软件相关的,不包含与硬件相关的 PCR 值,信息不完整。相关工作[7-9]指出与每个虚拟机对应的 PCR 值必须包含反映物理平台硬件相关信息的状态。文献[10]提出使用 VTPM 作为可信根保证虚拟机启动过程完整性,并使用可信审计技术对虚拟机运行态环境进行证据收集、证据审计,及时检测在实际使用中无法事先固定的用户运行环境的可信性。该方案未在虚拟化环境构建完整延伸到应用层的信任链,其原因是认为固化并事先验证所有用户安装的内核模块、应用程序在云环境不现实。本文认为在镜像文件及用户应用有限、可控的情况下,只要虚拟机初始状态是可信的,安装的软件来源可控可信,则信任链应延伸至虚拟机应用层,对用户应用实施可信验证和可信报告具有重要意义。换言之,只具备可信审计还不够,必须在可信报告值中包含虚拟机身份及应用层可信状态信息。

总结相关工作,AIK 在虚拟环境应用存在的问题是:普通物理主机上 TPM 外的实体无法读取 AIK 私钥或 PCR 值,只有授权用户能够产生 PCR 签名值用于向外部报告可信状态;虚拟机上由于 VTPM 运行于软件环境而不是硬件内部,攻击者可能在虚拟机(VM)层、虚拟机监控器(VMM)层获得 AIK 私钥从而伪造签名。因此云计算环境构建可信报告根机制的关键在于:

1)虚拟机生命周期中应拥有各自独立的密码身份标志;

2)虚拟机所属 PCR 类的敏感信息必须是受保护的、可迁移的,以适应虚拟机迁移需求。

2　基于 VAIK 的虚拟可信报告根构建机制

2.1　模型预设条件

在虚拟化体系结构下,可视为虚拟机监控器 VMM 直接操作和持有物理可信计算设备(如 TPM),

用户只能看到和使用提供给他们的虚拟机。因此，VMM 和物理 TPM 不需要直接向远程证明服务器报告其状态，需要报告状态的主体是虚拟机中的可信应用，也正是因为可信应用的存在和其安全需求，才需要部署 VTPM 这类软件机制将信任链延伸至虚拟机内部，可信应用应使用与其部署在物理主机一致的软件接口(TSS)和远程证明等协议接口进行可信操作。这是 VAIK 模型的一个预设条件。其他预设条件与对可信平台的管理机制有关，具体内容如下。

一是，满足集中的可信平台管理需求。云环境下，VTPM 的所有者是云使用方，配置 VTPM 的目的是满足高安全性、高可用性及可管理性需求，对比来说 TCG 规范的 TPM 所有者角色更倾向于是个人用户，适用于商用环境，更强调隐私性保护。因此，虚拟可信平台的管理更应该满足集中统一的要求，而不使用 TCG 规范提出的隐私性 CA 这类隐私性保护机制。

二是，满足虚拟化及非虚拟化可信平台统一管理需求。从管理角度，虚拟化和非虚拟化可信平台应具有一致的管理方式和管理界面，只有可信平台管理器能区分其差别。

2.2 VPCR 值复制机制

PCR 值动态代表了完整性状态，因此在可信报告机制中具有重要作用。文献[1]提出 VMM 启动后，平台 PCR 值必须包含代表 VMM 完整性状态值。虚拟机 PCR 值(简称 VPCR)应包含 VM 个体的完整性状态及物理平台统一的硬件和基础软件层(如 VMM)完整性状态，即记录物理平台启动状态和虚拟平台启动状态。因此需设计了 VPCR 值复制机制，用于复制物理平台启动后获得的 PCR 值到每个 VM 内对应前半部分 PCR 值位置。依据虚拟化平台体系结构的不同，该机制可以在 UEFI BIOS 或 VMM 层实现。

2.3 VAIK 概念及应用模型

基于 TCG 规范中 AIK 概念提出一类特殊的 AIK 称为 VAIK，为每个 VM 分配一个 VAIK，由 VAIK 代表 VM 身份，这与 TCG 规范中由 AIK 代表应用身份相类似。VAIK 应用模型由其功能和使用场景包括模型的预设条件决定。VAIK 应用模型如图 1 所示，VMM 生成虚拟机时产生对应的 VTPM、VAIK 和 VPCR 值并在 VM 生命周期中一直存续，VM 上的用户或应用也可以用通用方法申请其 AIK 使用，AIK 与 VAIK 的使用无冲突。

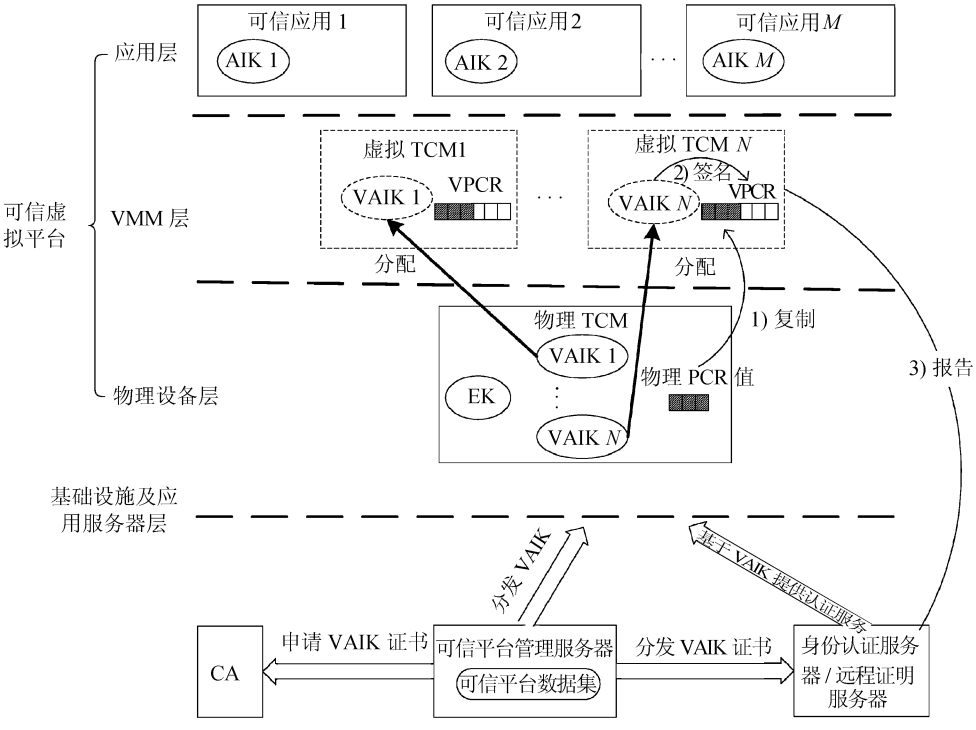

图 1 VAIK 应用模型

Fig. 1 Application model of VAIK

VPCR 的复制机制由图 1 中的 3 个步骤说明，物理可信设备记录物理平台可信状态，由 VMM 层复制物理平台可信状态到每个虚拟可信设备，当向远程证明服务器报告时，VM 对同时具有物理及 VM

软件层可信状态的 PCR 值使用 VAIK 进行签名后发送。

可信平台管理器维护所有可信平台的信息及秘钥等管理可信平台所需信息(图 1 中可信平台数据集),它通过在 VAIK 证书数据域中记录 TPM 标识的方法标记和维护物理平台及其所属虚拟机之间的关系。由可信平台管理器为物理和虚拟可信平台向 CA 申请证书,CA 只与可信平台管理器交互而不直接和可信平台交互,可信平台管理器向可信平台及验证服务器分发可信平台的 VAIK/AIK 等各类证书。

2.4　基于 VAIK 的报告方法

可信平台管理器可以根据每个物理平台需使用和管理的最大 VM 数量预先产生和置入对应数量的 VAIK 到物理可信密码设备中,所有 VAIK 私钥均存储于物理可信密码设备内部不可导出到外部。在每个虚拟机生成时 VMM 通过物理可信密码设备为其分配一个 VAIK,由该 VM 上层的可信应用使用该 VAIK,使用方式用于验证 VM 身份或对 VM 可信状态进行远程证明,使用 VAIK 进行签名的用法如式(1)所示,其中,{content}Sig(key)表示使用 key 对 content 进行签名,VM 向远程证明服务器报告公式(1)运算所得签名值。

$$\{PCR \parallel VPCR\}Sig(VAIK) \quad (1)$$

为便于比对,将文献[6]中使用的签名方法表示如式(2)所示。可见采用 VAIK 签名的方法生成结果更快更简易,签名端只需执行一次签名操作,远程证明服务器只需验证一个证书。

$$\{PCR\}Sig(AIK1) \parallel \{VPCR\}Sig(AIK2) \quad (2)$$

2.5　与 TCG 管理机制的比较

从密钥生命周期方面比较基于 VAIK 的管理方法和 TCG 规范中提出的管理方法。表 1 体现了 AIK/VAIK 在生命周期中各阶段管理实体、管理方式的差异,可见 VAIK 方法属于集中管理,更依赖于可信平台管理器,而 TCG 的方法更依赖于可信平台及 TPM 自身。

表 1　AIK/VAIK 生命周期各阶段管理实体及管理方式差异比较

Tab. 1　AIK/VAIK comparison of life-cycle management entities

	生成	生效	迁移	撤销
AIK	CA 和 TPM 配合生成	由应用请求	迁移控制器完成迁移	TPM 实现
VAIK	由 CA 和可信平台管理器配合生成	在虚拟机产生时生效	迁移控制器和可信平台管理器配合完成迁移	可信平台管理器实现

3　结　论

本文阐明了一种用于云计算环境中虚拟机标识自身身份并构建虚拟可信报告根的机制,其核心是 VAIK 的使用和 VPCR 值的构造。基于此,虚拟机可向外部提供验证自身身份和完整性状态的密码手段。该机制能够支持现有的物理可信密码设备及软硬件接口,并简化了验证流程。

下一步工作方向,需对 VAIK 应用模型进行进一步的安全性分析,并设计实现支持 VAIK 的可信平台管理器。

参考文献:

[1]Trusted Computing Group. Virtualized trusted platform architecture specification[R]. Portland Oregon: TCG Board, 2011.

[2]Trusted Computing Group. TCG specification architecture overview[EB/OL]. (2007 - 08 - 08)[2016 - 7 - 1]. https://www.trustedcomputinggroup.org/groups/TCG_1_2_Architecture_Overview.pdf.

[3]Trusted Computing Group. TPM main part 1: Design principles specification. version1.2[EB/OL]. (2006 - 11 - 04)[2016 - 07 - 01]. https://www.trustedcomputinggmup.org/home.

[4]Shen Changxiang, Zhang Huanguo, Wang Huaimin, et al. Research and development of trusted computing[J]. Science China Information Sciences, 2010, 40(2): 139 - 166. [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),2010,40(2):139 - 166.]

[5]Wang Guan. TPCM and trusted computing platform mainboard specification[J]. China Information Security, 2015(2): 66 - 68. [王冠. TPCM 及可信计算平台主板标准[J]. 中国信息安全,2015(2):66 - 68.]

[6]Sun Yuqiong, Song Cheng, Xin Yang, et al. Dual AIK sig-

ning mechanism on trusted virtualization platform[J]. Computer Engineering,2011,37(16):114-116.[孙宇琼,宋成,辛阳,等.可信虚拟平台中的双AIK签名机制[J].计算机工程,2011,37(16):114-116.]

[7] Cucurull J,Guasch Sandra. Virtual TPM for a secure cloud: Fallacy or reality? [C]//XIII Reunión Española sobre Criptologíay Seguridad de la Información(RECSI 2014). Alicante:Revistas Y Congresos,2014:197-202.

[8] Berger S,C′aceres R,Goldman K A,et al. vTPM:Virtualizing the trusted platform module[C]//Proceedings of the 15th Conference on USENIX Security Symposium. USA:USENIX Association,2006,15:305-320.

[9] Brohi S N,Bamiah M A,Brohi M N,et al. Identifying and analyzing security threats to virtualized cloud computing infrastructures[C]//2012 International Conference on Cloud Computing Technologies,Applications and Management. Piscataway:IEEE Press,2012:151-155.

[10] Liu Chuanyi,Wang Guofeng,Lin Jie,et al. Practical construction and audit for trusted cloud execution environment[J]. Chinese Journal of Computers,2016,39(2):339-350.[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.]

(编辑 张 琼)

引用格式:Huang Qiang,Kong Zhiyin,Zhang Dehua,et al. Construction mechanism of virtual root of trust for report in cloud[J]. Advanced Engineering Sciences,2017,49(2):140-144.[黄强,孔志印,张德华,等.一种云计算适用的虚拟可信报告根构建机制[J].工程科学与技术,2017,49(2):140-144.]

第十届中国传感器网络(物联网)学术会议暨2016年成都物联网高峰论坛在蓉成功举行

2016年10月29—30日,由中国计算机学会主办,中国计算机学会传感器网络专业委员会协办,四川大学、成都物联网产业发展联盟联合承办的"第十届中国传感器网络(物联网)学术会议暨2016年成都物联网高峰论坛"在四川成都举行。共有来自全国各地的三百余位专家学者参加了本次会议。

10月29日上午,四川大学晏世经副校长、中国计算机学会传感器网络专业委员会马华东副主任、四川省经济和信息化委员会张延川副主任、成都市经济和信息化委员会李长虹副主任先后为大会致辞。其后,举行了中国计算机学会传感器网络专委会成立十周年庆典。澳门大学副校长倪明选教授、清华大学刘云浩教授、海尔集团的首席技术官(副总裁)赵峰、四川长虹电器股份有限公司张锦星副总经理、香港理工大学曹建农主任以及密歇根州立大学的邢国良副教授,分别以"物联天下,传感先行:2007—2016""从互联网到新工业革命""U+:在物联和数据时代的智慧生活创新引领""工业4.0及长虹的思考""Distributed Coordination of Multi-Robots System""面向可持续发展的物联网:移动健康、绿色数据中心,及水资源监控系统"为主题做了大会特邀报告,分享了物联网研究领域前沿技术,探讨了产业发展的前景。

大会期间与会专家学者还对无线传感器网络相关理论与技术、物联网技术、移动感知相关理论与技术、海洋观测网络的理论与技术等问题进行了分场学术报告和研讨。本次大会旨在促进传感器网络、物联网领域的学术交流,促进展业发展,并为物联网产业政产学研用各单位提供学习交流合作洽谈的平台。

大会共收到231篇专题论文,经审稿后接收其中的117篇论文,并推荐到国内一流中英文学术期刊上发表。《工程科学与技术》共收到组委会推荐的专题论文7篇,经专家再次评审后录用其中的5篇,于2017年2期发表。