软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(10):2782−2796 [doi: 10.13328/j.cnki.jos.005174]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

虚拟可信平台模块动态信任扩展方法*

余发江[1,2], 陈 列[1], 张焕国[1,2]

[1](武汉大学 计算机学院,湖北 武汉 430072)

[2](软件工程国家重点实验室(武汉大学),湖北 武汉 430072)

通讯作者: 余发江, E-mail: fjyu@whu.edu.cn

摘 要: 将可信计算技术应用到虚拟计算系统中,可以在云计算、网络功能虚拟化(network function virtualization,简称NFV)等场景下,提供基于硬件的可信保护功能.软件实现的虚拟可信平台模块(virtual trused platform module,简称vTPM)基于一个物理TPM(physical TPM,简称pTPM),可让每个虚拟机拥有自己专属的TPM,但需要将对pTPM的信任扩展到vTPM上.现有方法主要采用证书链来进行扩展,但在虚拟机及其vTPM被迁移后,需要重新申请vTPM的身份密钥证书,可能会存在大量的短命证书,成本较高,且不能及时撤销旧pTPM对vTPM的信任扩展,也不能提供前向安全保证.提出了一种vTPM动态信任扩展(dynamic trust extension,简称DTE)方法,以满足虚拟机频繁迁移的需求.DTE将vTPM看作是pTPM的一个代理,vTPM每次进行远程证明时,需从一个认证服务器(authenticaiton server,简称AS)处获得一个有效的时间令牌.DTE在vTPM和pTPM之间建立了紧密的安全绑定关系,同时又能明显区分两种不同安全强度的TPM.在DTE里,vTPM被迁移后,无需重新获取身份秘钥证书,旧pTPM可及时撤销对vTPM的信任扩展,而且DTE可提供前向安全性.从原型系统及其性能测试与分析来看,DTE是可行的.

关键词: 可信计算;可信平台模块(TPM);虚拟可信平台模块(vTPM);信任扩展

中图法分类号: TP309

中文引用格式: 余发江,陈列,张焕国.虚拟可信平台模块动态信任扩展方法.软件学报,2017,28(10):2782−2796. http://www.jos.org.cn/1000-9825/5174.htm

英文引用格式: Yu FJ, Chen L, Zhang HG. Virtual trusted platform module dynamic trust extension. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2782−2796 (in Chinese). http://www.jos.org.cn/1000-9825/5174.htm

Virtual Trusted Platform Module Dynamic Trust Extension

YU Fa-Jiang[1,2], CHEN Lie[1], ZHANG Huan-Guo[1,2]

[1](School of Computer, Wuhan University, Wuhan 430072, China)

[2](State Key Laboratory of Software Engineering (Wuhan University), Wuhan 430072, China)

Abstract: The integration of trusted computing into virtual computing system can enable the hardware-based protection of trustworthiness in application areas such as cloud computing and network function virtualization (NFV). In a physical trusted platform module (pTPM) based virtual trusted platform module (vTPM), each virtual machine (VM) can be viewed as having its own private TPM. However, it is necessary to extend the trustworthiness of pTPM to vTPM so that a challenger can believe the vTPM is the root of trust of the VM. The existing techniques mainly use a certificate chain to build a trust link from pTPM to vTPM. But if these techniques were deployed in the scenario with frequent vTPM migrations, there would be very high cost of reacquiring new certificates for the migrated vTPM, moreover, pTPM couldn't revoke its trust extension in real time, and they couldn't provide forward security. This paper presents an approach of vTPM dynamic trust extension (DTE) to satisfy the requirements of frequent migrations. With DTE, vTPM is a delegation of the capability of signing attestation data from the underlying pTPM, with one valid time token issued by an authentication server (AS).

* 基金项目: 国家重点基础研究发展计划(973)(2014CB340600); 国家自然科学基金(61772384)

Foundation item: National Basic Research Program of China (973) (2014CB340600); National Natural Science Foundation of China (61772384)

收稿时间: 2016-07-25; 修改时间: 2016-09-29; 采用时间: 2016-10-27

DTE maintains a strong association between vTPM and its underlying pTPM, and has clear distinguishability between vTPM and pTPM because of the different security strength of the two types of TPM. In DTE, there is no need for vTPM to re-acquire identity key (IK) certificate(s) after migration, and pTPM can have a trust revocation in real time. Furthermore, DTE can provide forward security. Performance measurements and analysis of its prototype demonstrate that DTE is feasible.

Key words: trusted computing; trusted platform module (TPM); virtual trusted platform module (vTPM); trust extension

1 引 言

可信计算以一个硬件安全模块——可信平台模块(trusted platform module,简称 TPM)作为可信根,为宿主计算机提供平台身份认证、完整性保护和安全存储功能.除个人计算机外,TPM 被集成到服务器上,正变得越来越普遍,如 DELL PowerEdge R530 机架式服务器和 Cisco UCS B200 M4 刀片式服务器.将可信计算技术应用到基于服务器的虚拟计算系统中,可以在云计算、网络功能虚拟化(network function virtualization,简称 NFV)等场景下,提供基于硬件的可信保护功能.

在非虚拟化环境中,TPM 与宿主算机的比例是一比一[1].虚拟化技术允许多个虚拟计算机相互独立地运行在同一个物理平台上,由于资源有限,一个物理 TPM(physical TPM,简称 pTPM)不能同时供多个虚拟机使用.一种解决方案就是,为每个虚拟机提供一个软件实现的虚拟 TPM(virtual TPM,简称 vTPM)[2,3].对每个虚拟机而言,它们会觉得自己拥有一个专属的 TPM.pTPM 是整个平台的可信根,用户对 pTPM 的信任来源于对可信计算技术的认可,权威机构也对 pTPM 产品进行认证,确保其具体实现与技术规范相一致.软件实现的 vTPM 会被动态地创建和销毁,权威机构不可能对每个运行的 vTPM 实例进行一致性测评与认证,他们能做的只是对某个 vTPM 软件实现进行测评.对具体运行的 vTPM 实例的测评,可由配置有 pTPM 的宿主计算机来完成,一旦测评过,就需要将用户对 pTPM 的信任扩展到 vTPM 实例上,用户才会认可 vTPM 是虚拟机的可信根.

现有扩展方法主要是运用证书链来构建 pTPM 对 vTPM 的信任担保.如果将现有方法应用在 vTPM 频繁迁移的情景中,被迁移后的 vTPM 需重新获取证书,可能存在大量的短命证书,成本高昂.旧平台上的 pTPM 不能及时撤销它对 vTPM 的信任扩展,现有方法也不能提供前向安全保证.我们提出一种 vTPM 动态可信扩展(dynamic trust extension,简称 DTE)方法,以消除现有方法的弊端.

本文的主要贡献如下:

(1) 提出了一种适用于频繁迁移情况的 vTPM 动态可信拓展方法 DTE.DTE 在 vTPM 和 pTPM 之间建立了紧密的安全关联,DTE 将 vTPM 看作是 pTPM 进行虚拟机远程证明的代理,该代理权限的执行基于一个有效的时间令牌,令牌则需从一个认证服务器(authenticaiton server,简称 AS)处获取.DTE 能够明显地区分两种不同的 TPM,vTPM 和 pTPM 拥有不同的安全强度.当迁移发生时,旧 pTPM 可及时撤销对 vTPM 的信任授权,vTPM 无需重新获取身份秘钥(identity key,简称 IK)证书.同时,DTE 能够提供前向安全性.

(2) 基于 OpenStack 实现了针对 TPM 1.2 和 TPM 2.0 的 DTE 原型系统,从性能测试及分析结果来看,DTE 方法是可行的.

本文第 2 节介绍现有的 vTPM 信任扩展方法,分析其缺陷,提出 DTE 要达到的目标.第 3 节描述基于信任关系和可信测评的信任扩展模型.第 4 节描述 DTE 的详细过程和算法.第 5 节分析 DTE 的安全性.第 6 节介绍 DTE 原型系统的建立和性能测试与分析.第 7 节介绍相关工作.最后,第 8 节总结全文.

2 现有方法和 DTE 的目标

现有方法主要是运用证书链来对 vTPM 进行信任扩展.Berger 等人[2]用证书链将 vTPM 与 pTPM 相关联.他们提出的第 1 种机制,是在 vTPM 申请背书秘钥(endorsement key,简称 EK)证书时,用 pTPM 的身份秘钥 IK 证书进行担保.第 2 种机制,是使用 pTPM IK 证书担保 vTPM IK 证书.在一些场景里,为平衡计算资源,虚拟机可能会在不同的物理宿主机上进行迁移.当一个虚拟机被迁移到新的宿主机时,与之相关联的 vTPM 也被迁移.同时,也必须建立新 pTPM 到 vTPM 的信任扩展,而旧 pTPM 与 vTPM 之间的信任扩展需被撤销.若采用 Berger 等人

提出的第 1 种机制,迁移后的 vTPM 须基于新 pTPM 的 IK 证书重新申请 vTPM EK 证书,然后再申请 vTPM IK 证书.若使用第 2 种机制,迁移后的 vTPM 须基于新 pTPM 的 IK 证书,重新申请 vTPM IK 证书.目前还没有(certificate authority,简称 CA)专业提供平台 EK 和 IK 证书,我们假设平台证书的价格等同于(secure socket layer,简称 SSL)证书.在本文准备期间,我们查询了几个主要提供商的 SSL 证书价格,见表 1.若虚拟机频繁迁移,vTPM 也将频繁地获取 IK 证书,成本高昂.迁移之后,之前的证书将被遗弃,可能还远未到其过期时间,会有很多短命证书存在,是一种很大的浪费.另外,为了保护隐私,一个 vTPM 可能存在多个 IK 证书,这会带来更高的代价.

Table 1 The SSL certificate price comparison

表 1 SSL 证书价格对比

提供商及证书类型	1 年期价格	2 年期价格	3 年期价格
Rapid SSL 证书	$49 USD	$86 USD	$122 USD
Thawte SSL123 证书	$149 USD	$259 USD	$369 USD
DigiCert SSL Plus	$175 USD	$315 USD	$419 USD
GeoTrust True BusinessID	$199 USD	$348 USD	$498 USD
Symantec Secure Site	$399 USD	$695 USD	$995 USD

Danev 等人[4]提出了一种 vTPM 密钥层次结构,该结构有一个 pTPM 和 vTPM 之间的中间层,由一组 pTPM 的签名密钥(signing key,简称 SK)构成,用以连接 pTPM IK 和 vTPM IK.该方法也在 vTPM 和 pTPM 之间建立了绑定关系,但 pTPM SK 不能被迁移,故 vTPM 迁移之后,新的 pTPM 须重新生成 SK,vTPM 同样须重新获取 IK 证书.

在虚拟可信平台架构规范[3]中,可信计算组织(trusted computing group,简称 TCG)并没有明确定义如何创建 pTPM 和 vTPM 之间的连接关系,但 TCG 提出了一个“深度认证(deep attestation)”的概念.在远程实体完成对虚拟机的认证后,可能会继续认证其下层的虚拟机监控器(virtual machine monitor,简称 VMM)和虚拟机宿主平台,以确定它们是否足够可信,不会去破坏运行在其上的虚拟机.为了实现深度认证,远程实体需从 vTPM IK 证书扩展项中获取底层平台的信息,如 IP 地址或者统一资源标识符(uniform resource identifier,简称 URI).当虚拟机迁移发生时,vTPM 也需要获取新的 IK 证书,以包含新的宿主平台信息.

在前述的几种 vTPM 信任扩展方法中,vTPM 迁移后,它原来的 EK/IK 证书需被废除.废除证书最常用的方法就是证书撤销列表(certificate revocation list,简称 CRL).当 vTPM 被迁移时,与之关联的原 pTPM 便通知 CA,CA 将 vTPM 原有证书信息添加到 CRL 中,并对更新之后的 CRL 重新进行签名.在远程实体验证 vTPM 的远程证明报告时,先下载 CRL,检查 vTPM 当前使用的证书是否在 CRL 中.CRL 通常相当冗长,不会被频繁地下载.例如,1 周或者 1 个月被下载 1 次.因此,vTPM 的原有证书可能在迁移发生 1 个月之后才会被真正废除.在此期间,迁移后的 vTPM 仍然可以代表原 pTPM,生成虚拟机的证明报告,这是现有信任扩展方法的又一明显缺陷,pTPM 不能及时撤销它对 vTPM 的信任扩展.另外,一旦 vTPM 原有证书被加入到 CRL 中,即使在迁移之前由 vTPM 所生成的签名都将无效,故现有方法也不能提供前向安全性.

如果将现有扩展方法应用到虚拟机频繁迁移的场景中:(1) 将会造成大量的短命证书存在,成本高昂,浪费巨大;(2) pTPM 不能及时撤销它对 vTPM 的信任扩展;(3) 不能提供前向安全保证.我们提出的新方法——vTPM 动态信任扩展(DTE),应消除现有方法的这些弊端.DTE 的主要目标如下:(1) 在 vTPM 和 pTPM 之间建立紧密的安全关联;(2) 严格区分 vTPM 和 pTPM,这两种类型的 TPM 具有不同的安全强度;(3) 迁移后的 vTPM 无需重新获取 EK/IK 证书;(4) pTPM 可及时撤销对 vTPM 的信任扩展;(5) 提供前向安全性;(6) 是可行的.

3 基于可信测评的信任扩展模型

3.1 信任关系与可信测评

定义 1(信任关系). 实体 E1 信任 E2, 记作 E1 Tru E2. 信任关系具有如下性质.

(1) 自信任. E1 Tru E1.

(2) 传递性.若 E1 Tru E2, 且 E2 Tru E3, 则有 E1 Tru E3.