

云环境面向虚拟域的安全状态一致性保障机制研究

代炜琦, 邹德清, 金海, 夏妍

(华中科技大学计算机科学与技术学院, 湖北 武汉 430074)

摘要: 由于云环境虚拟化特性及高动态性(回滚、迁移等操作)给虚拟域带来了时间、空间状态不一致, 从而造成了严重的安全威胁。针对该问题, 提出了云环境虚拟域安全基础架构、时间安全状态一致性机制、空间安全状态一致性机制, 有效地保障了云虚拟域安全状态的一致性, 有助于提高公共服务效率和信息安全可控性。

关键词: 云计算; 可信计算; 虚拟域; 虚拟机回滚; 状态一致性

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00103

Research on consistency protection mechanism for secure states of virtual domain in cloud environment

DAI Wei-qi, ZOU De-qing, JIN Hai, XIA Yan

(School of Computer Science Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: The traditional trusted computing architecture was suffering from the cloud uncertainty and dynamics caused by VM rollback or migration, which was a fatal threat to the cloud security. following investigations were conducted. Secure cloud virtual domain basic architecture; Time state consistence and collection mechanism. Cyber state consistence and collection mechanism. This study guaranteed security state consistence of virtual domain and improved the security and efficiency of the online service platform for both government institutions and companies.

Key words: cloud computing, trusted computing, virtual domain, virtual machine rollback, state consistency

1 引言

云计算在给人们带来巨大便利的同时也产生了不可忽视的安全问题。自2013年“棱镜”事件被曝光之后, 世界各国纷纷开始关注信息安全, 云安全是其中必不可少的一部分。近年来, 云安全事件频出: 2014年8月, 苹果 iCloud 服务遭遇攻击, 致使租户隐私数据泄露以及服务中断等后果; 2015年6月, 美国联邦人事管理局发生泄密

事件, 这起事件影响到2 210万人。云安全问题使许多企业和机构对云计算望而却步。

目前, 我国许多关键应用领域, 如航空、航天、金融、证券、交通、医疗、电子政务等都开始与云计算进行融合。2014年10月, 北京市海淀区政府借助阿里云计算建成中国首个统一的综合性政务云平台^[1]。通过云计算构建智慧城市的模式并不是单例, 2015年5月上海市政府也与阿里巴巴集团签署了智慧城市相关战略合作协议。

收稿日期: 2016-08-25; 修回日期: 2016-09-05。通信作者: 代炜琦, wqdai@hust.edu.cn

基金项目: 国家自然科学基金资助项目(No.61602200); 中央高校基本科研业务基金资助项目(No.HUST2016YXMS087)

Foundation Items: The National Natural Science Foundation of China (No.61602200), The Fundamental Research Funds for the Central Universities (No.HUST2016YXMS087)

云计算以其低廉的使用成本和高性价比，在推动数字化政、企平台的建设中起到了不可或缺的作用。如图 1 所示，在云环境中，不同企业或政府机构的云服务都是以云虚拟域的形式存在。云虚拟域是云提供商分配给某个企业或机构用以完成特定服务的一组跨物理节点的虚拟机。这种以虚拟域为单位的服务模式越来越多地被各类企业与公共服务机构所采用，然而云环境中虚拟机回滚、迁移特性给虚拟域在时间和空间上增加了不确定性与动态性，使现有的方法很难对云虚拟域的计算资源和服务进行有效的监控，同时云虚拟域时空状态变化也给多虚拟机关联服务的共享数据带来安全隐患，使云服务的安全性得不到保障。因此，基于虚拟域的划分模式以及安全监控模式提出云虚拟域安全构建机制会大大有利于云环境的安全构建，保证云虚拟域的安全可信。

云虚拟域安全构建体现在 3 个重要方面。1) 云环境虚拟域安全基础架构，恶意攻击者利用操作系统漏洞破坏云租户应用程序的执行，给构建安全可信的云环境虚拟域带来了巨大的挑战。2) 时间安全状态一致性，云环境虚拟域的状态回滚增加了时间状态的动态性，给保障虚拟域时间安全状态一致性带来了巨大的挑战。3) 空间安全状态一致性，跨节点多虚拟机加入或退出虚拟域以及虚拟机迁移增加了空间状态的动态性，给保障

虚拟域空间安全状态一致性带来了巨大的挑战。

2 研究现状

下面将从云环境虚拟域安全基础架构、云环境虚拟域安全回滚机制以及云环境虚拟域安全管理机制研究 3 个方面介绍国内外现状。

1) 云环境虚拟域安全基础架构研究

硬件可信平台模块 (TPM, trusted platform module)^[2]提供了平台状态寄存器 (PCR, platform configuration register)、信任链、密钥管理、远程证明等安全手段。但是由于 TPM 的设计并未考虑到云环境的迁移特性，在云环境中使用物理 TPM 并不适合，已经有研究说明了这一问题。例如 Flicker^[3,4]利用动态可信度量根构建安全执行环境来保护应用程序代码片段，但由于 TPM 的限制，Flicker 创建安全执行环境时，需要暂停整个物理硬件的工作，这并不适合多租户并行的云环境。针对虚拟化环境中单一 TPM 无法满足所有的虚拟机安全需求的问题，提出了虚拟化的可信平台模块 (vTPM)^[5]，它保留了传统 TPM 的安全特性。但仍然不适用于云环境，只是简单地将传统架构进行虚拟化，依然存在许多安全漏洞和威胁。

在可信计算的其他应用方面，CloudVisor^[6]利用嵌套式虚拟机化技术和权限分离的思想来对

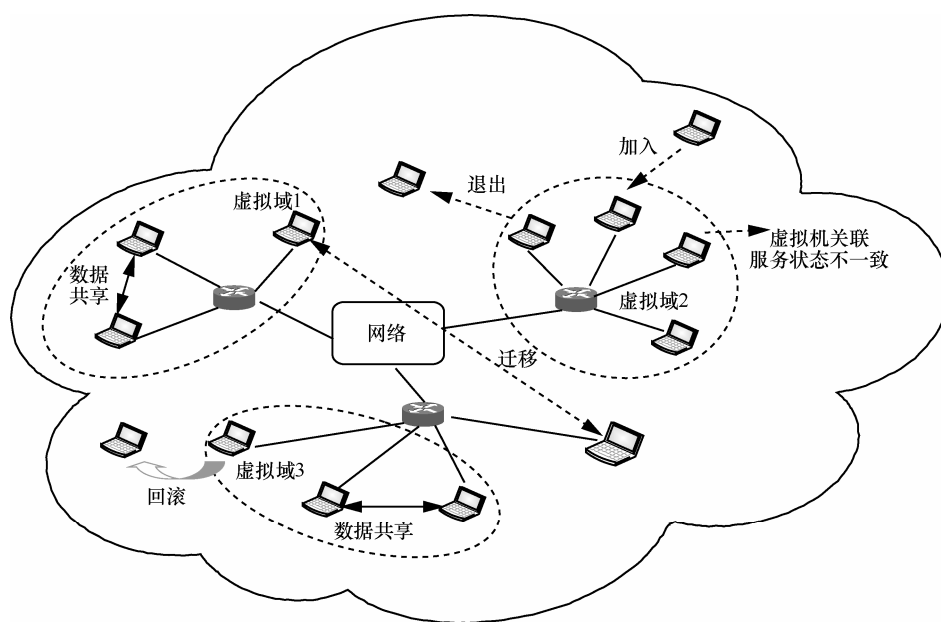


图 1 云虚拟域场景描述

云租户执行环境进行保护,使其安全性不受管理域的影响。项国富^[7]等提出一种虚拟机化的监控框架,用于监控虚拟机的安全行为。在可信云服务方面,CRISWELL等^[8]提出基于编译器插装和传统的SVM(secure virtual machine)技术,构建可信硬件层,实现对应用程序的全面保护。MiniBox^[9]系统结合了TrustVisor^[10]的内存隔离机制和Native Client^[11]的沙盒检测,为应用和操作系统提供双向保护。通过将应用程序的系统调用接口分为敏感调用和不敏感调用,在安全隔离的环境下处理安全敏感调用,有效防御了Iago攻击。

目前,针对云环境虚拟域基础架构的安全措施主要是基于传统安全手段,云环境虚拟机的迁移、回滚以及虚拟机加入、退出都使云环境虚拟域具有极高动态性和不确定性,现有的解决方案无法解决云环境虚拟机动态性带来的安全威胁。需要针对虚拟域动态性导致的安全状态不一致问题提出云环境虚拟域安全基础架构。

2) 云环境虚拟域安全回滚机制研究

Fu等^[12]的研究发现回滚操作已经成为云环境中错误恢复的核心操作。而回滚操作给云环境的可靠性保障与错误恢复带来巨大便利的同时也带来了严重的安全威胁。Garfinkel等^[13]最早发现虚拟机的回滚机制可能导致严重的安全问题,云环境的动态性将回滚产生的安全威胁进一步放大。Goldman等^[14]研究发现,可信平台芯片每次进行操作后计数器都会增加,这一发现可以用来防御重放攻击。然而这也意味着一旦虚拟机被回滚,计数器的单调性无法保持,可信平台芯片的信任链也被破坏。针对这一问题,England等^[15]提出把可信平台芯片移到hypervisor层来避免计数器随着虚拟机回滚。Xia等^[16]真正地对虚拟机回滚机制本身存在的安全问题进行深入分析探讨。Parno等^[17]实现了健壮的程序状态回滚机制,该机制确保了回滚不会使操作系统崩溃。

云环境中的虚拟机回滚操作无论是对于虚拟机内部还是外部都是难以感知的,或者说回滚对于它们是透明的。云环境特有的虚拟机外部的安全监控模式Hookscout在虚拟机运行的过程中每15 s进行一个快照操作^[18],之后根据快照内容对虚拟机运行过程中的恶意行为进行分析。恶意的

回滚会将Hookscout工具记录的连续运行快照碎片化,使其变得不具备安全分析的条件,类似的工具无法感知虚拟机的回滚操作。Chow等^[19]针对目前运行日志记录过于臃肿的问题提出了基于时间以及基于抽象层次的2种日志分割策略。允许虚拟机或者进程在回滚后根据特定的需求恢复某时间段内某一抽象层次的操作。Chow等的日志分割对安全敏感信息进行剔除处理,这样做虽然减轻了敏感信息泄露的危险,但是限制了回滚的灵活性(回滚后的虚拟机无法和其他虚拟机进行安全状态同步,或者同步到不安全的状态)。这些研究成果都是针对单一虚拟机或者单一服务的状态进行保护的解决方案,并没有提出统一的回滚安全框架。

目前的研究都只是应用层面或者单一虚拟机层面,并不能解决云环境虚拟域多个服务关联的虚拟机回滚导致的安全状态不一致问题。当虚拟域的多个关联虚拟机之间发生回滚时导致交互状态丢失,将会引发整个虚拟域的安全状态不一致。需要在基于虚拟域的服务模型下,结合云的动态性以及不确定性研究云平台安全回滚机制。

3) 云环境虚拟域安全管理机制研究

文献[20,21]提出了一个管理大规模云的云管理框架SnowFlock,基于该框架通过快速克隆虚拟机的方式可以很快搭建一个并行计算环境。但以这种方式部署的虚拟域由于缺乏可信身份,明显存在安全性薄弱的问题。

Cabuk S等^[22,23]针对虚拟数据中心提出了一个安全架构,该架构有效结合了虚拟化技术和可信计算,实现了自动实例化虚拟基础实施与自动部署安全机制,通过保证不同客户资源的相互隔离,达到了虚拟域中租户安全访问共享资源的目标。SCHAEFER M和CALERU J M At等^[24,25]针对云计算提出了集中授权管理模型和授权系统架构,以联合路径为基础,对不同等级的身份进行访问控制。

可信虚拟域(TVD, trusted virtual domain)^[26,27]广泛应用于数据中心等场景中,后来又经过扩展,添加了安全访问控制策略、完整性检测和隔离机制。此外还通过基于信任的虚拟域分层管理模型来扩展TVDC的管理模式^[28]。Davi等^[29]实现了移

动终端上部署 TVD 安全架构。

目前的研究都只针对单机的安全问题进行研究，而虚拟域中各虚拟机之间的信任关系是孤立的，并不足以支持云中以虚拟域为单位的架构，即使是关于 TVD 方面的研究也没有考虑虚拟域的整体安全状态，缺乏以虚拟域为单位的安全状态视图，无法高效地监控虚拟域安全状态，同时也无法实时记录跨节点多机关联云服务的状态变化。云环境下虚拟机的加入、退出和迁移行为会导致虚拟域空间状态的变化，因此需要为保证虚拟域空间状态一致性提供一个安全可信的支撑系统。

3 云环境虚拟域安全基础架构

云环境虚拟域安全基础架构首先要保证虚拟域中每个虚拟机的安全可信，然而通用操作系统过于庞大、结构复杂，存在着大量漏洞。因此，需要为虚拟域中的每个虚拟机构建可信执行环境。传统的静态可信度量技术只能保证系统启动时刻的可信，无法保证系统运行时的可信，而如前文所述，基于动态可信度量技术的 Flicker^[3,4]系统也无法适用于云虚拟域。因此，需要结合云环境下动态构建可信执行环境机制实现虚拟机的安全，确保为云租户提供安全可靠的云服务，这是构建安全虚拟域的基础。

Dai 等^[30,31]提出了结合虚拟化技术与可信计

算在云环境下动态构建可信执行环境（TEE，trusted execution environment）的思路。图 2 是 TEE 的系统架构。首先，与 Flicker 系统不同的是，TEE 并不直接使用动态可信度量根（DRTM, dynamic root of trust for measurement），而是应用虚拟化的动态可信度量根（vDRTM, virtual dynamic root of trust for measurement）。其次，在动态构建可信执行环境时，不能仅基于虚拟化的可信平台模块，因为 vTPM 是基于静态可信度量根的，只能在虚拟机启动时提供安全的系统环境，更重要的是，vTPM 不能分辨指令来源，不能辨别指令是来自不可信的用户操作系统还是可信的执行环境。因此，TEE 系统应用 DRTM 来帮助 vTPM 对指令来源是否可信进行验证。最后，TEE 可以在租户需要的时候启动，为云平台上多个用户虚拟机动态创建可信执行环境，并提供细粒度的保护和证明措施。

TEE 系统的关键技术如下。1) 在云环境下为多租户多虚拟机提供了类似于 DRTM 的可信执行环境。2) 提出 LPC（low pin count）通道，让每个 vTPM 都可以精确判断命令来源于可信执行环境还是不可信的用户操作系统，确保不可信的操作系统无法通过欺骗 vTPM 来获取租户的敏感数据。3) 提出云可信执行环境的安全分级技术，隔离可信执行环境和不可信执行环境的 vTPM 数

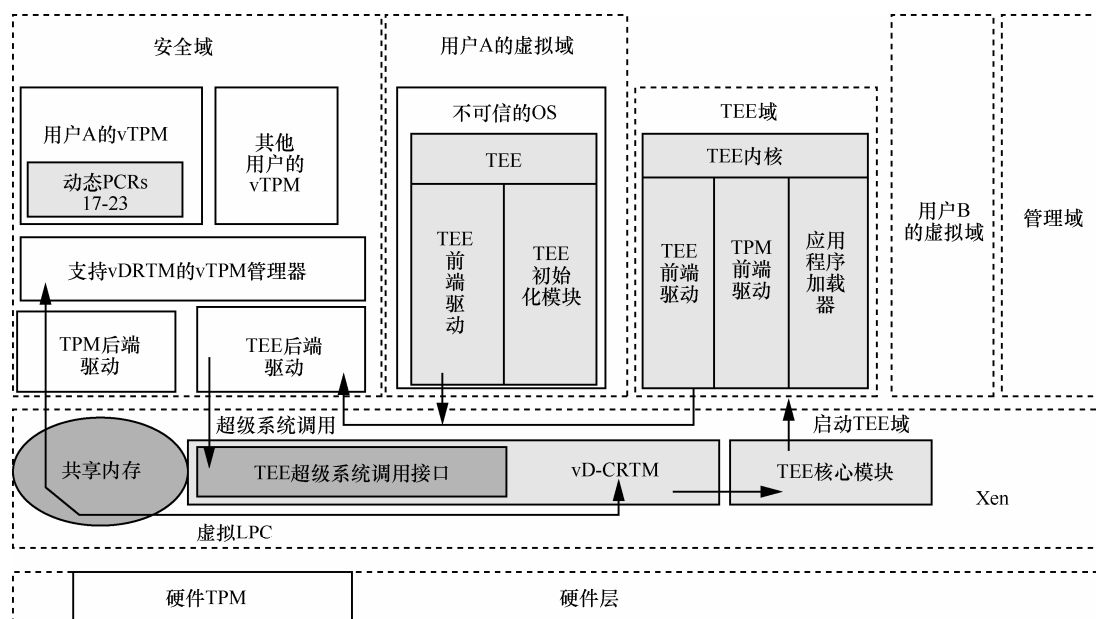


图 2 TEE 架构

据空间, 保证数据安全。4) TEE 可以根据租户需要在任意时刻启动运行安全敏感应用而无需重新启动虚拟机, 并且能向第三方提供可信证明。

动态可信执行环境具有强大的隔离性, 但如果多个租户都在运行相同的服务或者密码库, 此时动态构建可信执行环境则会导致资源利用率不高。因此, 需要一个可以为云平台上所有租户提供安全云服务的可信云服务构建机制。

为了解决上述问题, Dai 等^[32]提出了 ADS (assured digital signing) 系统, 主要针对数字签名这一基础服务来设计应用场景, 展示如何为云租户提供可信的云服务。该系统能在请求签名应用本身是恶意软件或者客户操作系统是恶意操作系统的情况下保证数字签名的可信性。ADS 系统采用虚拟化技术和可信计算相结合的思想, 将安全敏感的签名密钥和签名服务隔离, 放入可信的虚拟机中执行, 在用户虚拟机中仅执行对安全不敏感的部分, 利用共享内存和内存保护机制对通信通道、应用程序以及输入输出进行了安全保护, 为租户程序提供安全可信的数字签名服务, 并且不需要修改应用程序的代码。

如图 3 所示, ADS 系统主要由用户虚拟机、Xen 虚拟机管理器和可信虚拟机组成。

1) 用户虚拟机中主要包含 Stub 模块、安全监控器 (security monitor) 和内核模块这 3 个部分。Stub 模块对用户虚拟机密码库的签名函数进

行修改, 使应用程序在不需要修改代码的情况下, 以链接一个普通的密码库的方式去链接 ADS 密码库, 获得安全的数字签名服务。安全监控器是用户域中唯一需要保证安全可信的组件。所在内存由可信域分配, 用户域的内核无法映射读写篡改, 负责使用超级系统调用与可信域的签名服务通信。内核模块仅仅负责初始化这类与安全无关的操作, 因此不需要保证可信。

2) Xen 虚拟机管理器中包含调用门、新增的超级系统调用和内存保护这 3 个部分。调用门的作用包括: 用 Xen 去保证 GDT 表的安全, 让 Stub 模块直接使用 GDT 中新增的调用门项, 从而绕过用户域中不可信的内核直接跳转到安全监控器的代码。新增的超级系统调用用于可信的虚拟域中后端监控器 (backend monitor)、用户域的安全监控器以及 Xen 之间的安全通信, 具体包含设置共享内存信息、映射内存页、设置 GDT 表调用门项、发送虚拟中断以及内存保护功能。内存保护机制保护应用程序、安全监控器以及被签名信息和签名所在内存的安全, 主要通过读写权限以及页表保护实现。

可信虚拟域中主要包含密码服务、带策略引擎的后端监控器以及远程证明服务这 3 个部分。密码服务为租户应用程序提供签名服务。带策略引擎的后端监控器负责分配内存、安装安全监控器, 验证请求签名应用程序的有效性。远程证明服务用于挑

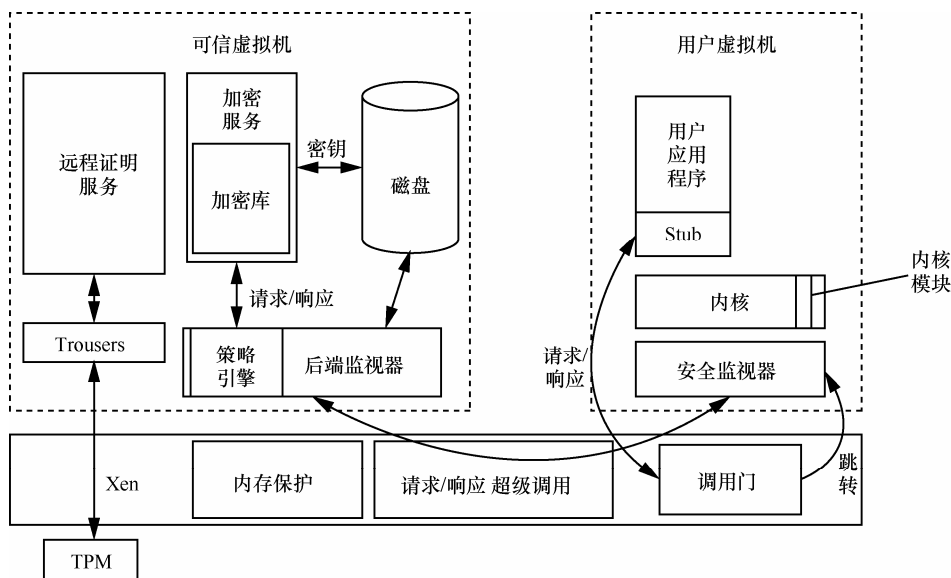


图 3 ADS 系统结构

战者验证签名程序，输入、输出是否被篡改。

结合 TEE 动态构建可信执行环境机制和 ADS 可信云服务构建机制，可以保障云环境虚拟域中虚拟机个体的安全可信，为保障虚拟域时空安全状态一致提供了安全基础。

4 云环境虚拟域时间安全状态一致性保障机制

传统的可信架构并不能适用于基于虚拟化的云环境，云的高动态性（虚拟机回滚）导致云虚拟域时间安全状态不一致，给虚拟域的安全可信带来了极大的挑战。为解决该问题，需要保障单机时间安全状态一致和多机时间安全状态一致。单机时间安全状态一致首先保证了虚拟域中每个虚拟机的回滚安全，包括 vTPM-VM 状态一致性保障和回滚感知无状态恢复机制，为多机时间安全状态一致性保障机制的实现提供了基础。多机时间安全状态一致对虚拟域多服务的交互安全状态一致性提供了保护，实现了云环境虚拟域时间安全状态的一致。

如图 4 所示，单机时间安全状态一致性保障主要包括以下 2 个方面。1) 基于 vTPM-VM 架构的状态同步机制。简单地回滚 vTPM 将破坏 vTPM 自身的单调性，导致 vTPM 受到回滚重放攻击。因此，本文设计了基于 vTPM 的细粒度安全回滚策略，对安全相关的数据进行细粒度划分，针对不同的 vTPM 数据采取不同的状态信息同步策略，保障 vTPM-VM 的安全状态一致，从而抵御回滚攻击。2) 基于 vTPM 的服务状态验证接口。首先对原有可信平台芯片进行功能扩展，增加额外的平台状态寄存器记录虚拟机快照、回滚事件信息，完成虚拟机的安全状态记录，为多机时空状态收集提供基础。然后为云应用提供抵御回滚的平台寄存器接

口，帮助服务对自身状态与虚拟机状态进行感知与验证。云应用将自身的状态度量值扩展到额外的状态寄存器形成状态度量链，在回滚发生时，云应用通过特定的策略对度量链进行验证，找到自身丢失的状态，从而恢复由回滚造成的状态丢失。

针对虚拟域多虚拟机之间时间安全状态变化的度量问题，在云虚拟域单机时间安全状态一致的基础上，提出了多机时间安全状态一致性保障机制。具体实现主要包括以下 2 个方面。

1) 回滚安全监控机制

外部监控虚拟机无法感知监控目标虚拟机上因回滚而产生的 vTPM-VM 安全状态不一致，监控程序的结果可能因此碎片化、无效化，所以提出回滚安全监控机制来解决这一问题。如图 5 所示，通过在虚拟机监控器上构建轻量级的可信监控域，提供监控域抗回滚接口，对外部虚拟机的回滚信息以及状态周期进行度量值验证。设计并实现抵御回滚监控域管理模块，该模块利用多虚拟机状态监控机制，在回滚发生时，将可信监控域中的监控软件状态进行切换，协助监控虚拟机进行全虚拟机生命周期的安全监控，保障监控到的状态与虚拟机的时间安全状态一致。

2) 交互状态恢复机制

针对云环境中由回滚导致的多虚拟机交互状态丢失问题，提出云服务的交互状态恢复机制。如图 5 所示，首先，构建针对云应用的状态恢复与验证接口，交互虚拟机利用该接口将跨节点多虚拟机的回滚信息以及安全状态信息扩展到相关的平台状态寄存器。利用平台状态寄存器保存的多机状态度量链进行验证能够帮助交互云服务确定自身与交互方的运行周期，从而对丢失状态进行验证与恢复。其次，通过交互事件记录与外部重放恢复云服务丢失的交互状态，保障多虚拟机

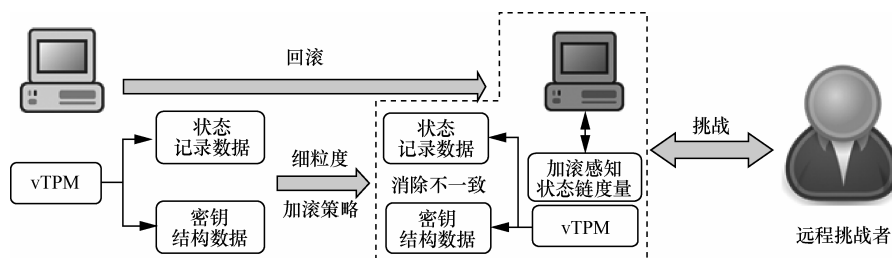


图 4 单机时间安全状态一致架构

服务的状态一致性。针对日志记录中敏感信息与操作存在的信息泄露问题,利用可信平台寄存器将敏感事件密封在当前的安全状态下。在对敏感行为进行恢复的过程中,通过使用额外的可信平台寄存器对回滚后的状态进行恢复校验,当状态恢复不正确时,先前的密封事件以及数据将无法解封,保护敏感信息不被泄露。

5 云环境虚拟域空间安全状态一致性保障机制

传统的可信架构并不能适用于基于虚拟化的云环境,云的高动态性(虚拟机迁移)导致云虚

拟域的空间安全状态与度量状态不一致,给虚拟域的安全可信带来了极大的挑战。为解决该问题,提出跨节点虚拟域空间状态收集机制和多服务状态变化度量机制,收集和记录跨节点多虚拟机的空间动态变化行为,度量多个服务状态变化的有序性,监控整个域的安全状态。

1) 跨节点虚拟域状态收集机制

针对云环境下虚拟机加入、退出虚拟域以及迁移等动态特点,在单机节点状态收集的基础上提出跨节点的多虚拟机安全状态收集机制。图6是一个公共的安全监测设备,该安全设备可随时获取组内各个虚拟机节点的安全状态,构建虚拟域所有节点

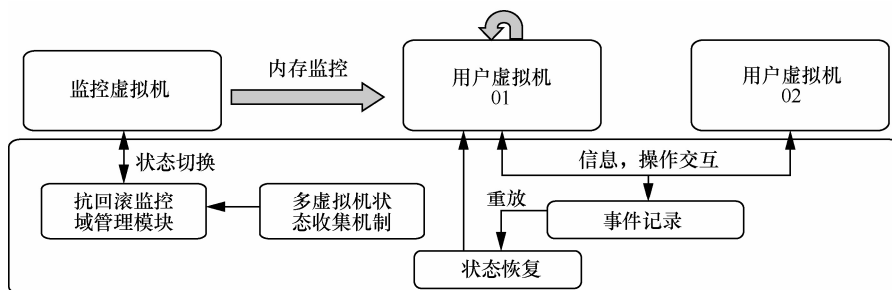


图5 多机时间安全状态一致架构

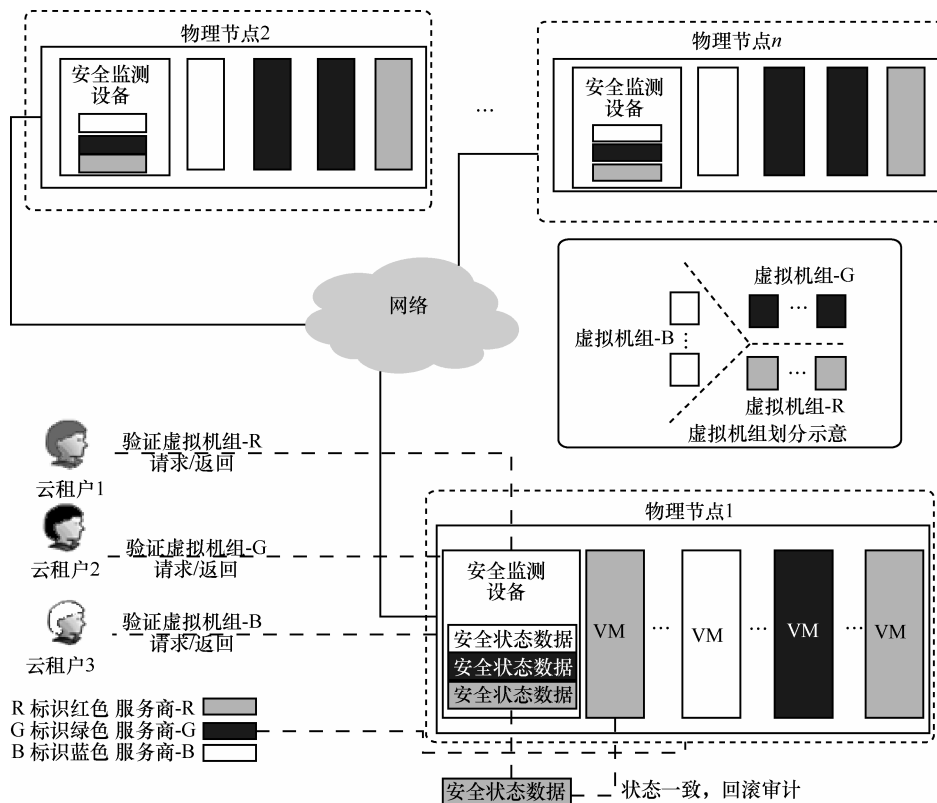


图6 跨节点虚拟域状态收集架构

的全局安全状态视图，用以监控虚拟域安全状态。同时，针对云虚拟域中的成员加入、退出以及迁移等空间上的动态变化，该安全设备都可将其行为记录下来，保证虚拟域在空间状态上的一致性，为虚拟域时间安全状态一致性提供基础。

2) 跨节点多虚拟机关联服务状态变化的可信度量机制

如图 7 所示，具体包含以下 2 个方面：1) 服务状态信息收集机制，在虚拟域增加额外的公共平台状态寄存器，用以记录虚拟域中各个服务的状态信息。2) 信任链建立机制，以时间为序收集跨节点多服务的状态变化信息，当多个服务按序启动时，规定每个服务完全启动后，就将关键的应用程序和配置文件等信息扩展到新增的平台状态寄存器中，依次建立信任链。在一个服务启动前，先度量上一个服务的完整性，若上一个服务的完整性遭到破坏，信任链断裂，服务将无法继续启动。通过这一机制保证多个服务状态变化的有序性，防止多个服务状态无序变化导致的系统脆弱性，从而能避免由于系统脆弱性而带来的各种攻击。

由此，设计并实现了安全高效数据共享机制与细粒度数据共享机制，提高了跨节点多服务交互过程中数据共享的安全性和高效性，并为多

个服务的安全交互提供更细粒度的共享。

1) 安全高效数据共享机制

针对基于传统可信平台模块的多机数据共享方式存在密钥不安全（选择密文攻击）和复杂的密钥协商导致的效率低两方面问题，提出密钥集中管理机制，将密钥的生成和管理全部交由一个安全设备集中负责，避免多机在数据共享过程中频繁地协商密钥，降低通信和计算开销，从而达到提高数据共享效率的目的。同时密钥集中管理机制使密钥在其整个生命周期都处于安全设备中，提高了密钥的安全性。

2) 细粒度数据共享机制

针对服务交互过程中对数据共享安全级别的需求不同，提出一种细粒度的数据共享机制，使共享数据可绑定到多机的时空状态。针对安全敏感数据，该机制将安全敏感数据绑定到整个虚拟域的安全状态，一旦某个虚拟机加入、退出、迁移以及回滚导致虚拟域的时空状态不一致，所有虚拟机都无法解密数据；针对一般交互数据，该机制让某个服务将数据绑定到多个指定虚拟机的安全状态，若某个虚拟机加入、退出、迁移以及回滚改变其自身的时空状态，则该虚拟机无法解密数据，但其他未改变状态的指定虚拟机仍可解密数据。

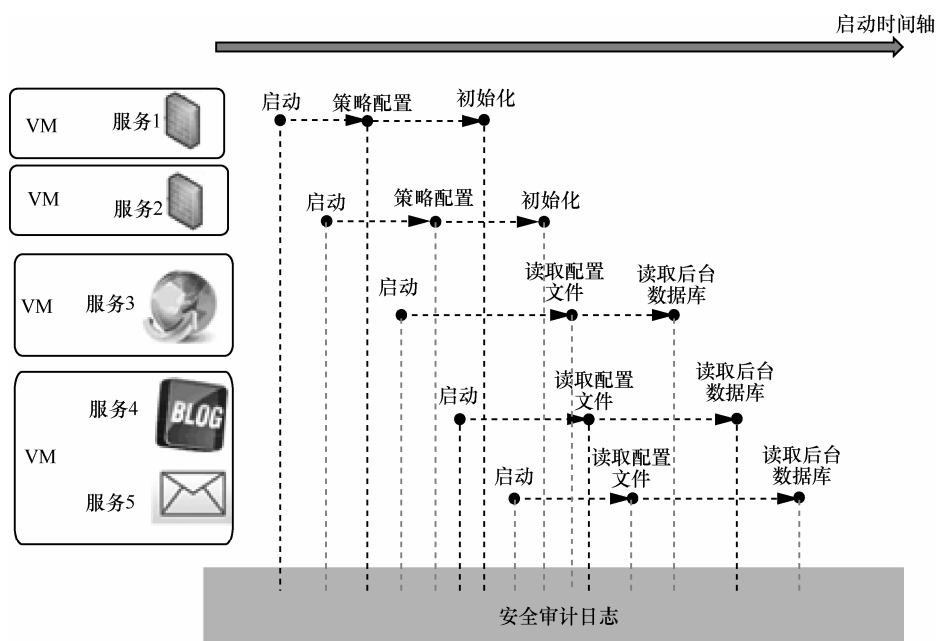


图 7 多个服务的状态变化度量过程

6 结束语

在云环境中,虚拟机的加入、退出、回滚、迁移等动态操作都会给虚拟域在时间和空间上增加不确定性与动态性,而现有的云环境安全保障机制缺乏对这种不确定性和动态性的应对方案,对云环境造成严重的安全威胁。本文提出云环境虚拟域安全基础架构,提出动态可信执行环境构建机制和可信云服务构建机制,解决操作系统漏洞被攻击造成服务不可信的问题;提出云环境虚拟域时间安全状态一致性机制,解决单机服务状态丢失以及由回滚产生的多虚拟机交互状态丢失的问题;提出云环境虚拟域空间安全状态一致性机制,解决跨节点多虚拟机由加入、退出和迁移等动态行为造成虚拟域空间安全状态难以监控的问题;本文的研究将有利于解决云环境虚拟域由于时空状态不一致所产生的安全问题。

参考文献:

- [1] [EB/OL]. <http://news.163.com/14/1111/06/AOGEHRH00014AEE.html>. 2016.
- [2] SAILER R, ZHANG X, JAEGER T, et al. Design and implementation of a TCG-based integrity measurement architecture[C]// Proceedings of USENIX Security Symposium. 2004: 223-238.
- [3] MCCUNE J, PARNO B, PERRIG A, et al. Flicker: an execution infrastructure for TCB minimization[C]//ACM Eurosys'08. 2008: 315-328.
- [4] MCCUNE J, PARNO B, PERRIG A, et al. Minimal TCB code execution[C]//IEEE Symposium on Security and Privacy (SP'07). 2007: 267-272.
- [5] PEREZ R, SAILER R, DOORN L V. vTPM: virtualizing the trusted platform module[C]//The 15th Conference on USENIX Security Symposium. 2006:305-320.
- [6] ZHANG F, CHEN J, CHEN H, et al. Cloudvisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization[C]//ACM SOSP. 2011: 203-216.
- [7] 项国富, 金海, 邹德清, 等. 基于虚拟化的安全监控[J]. 软件学报, 2012, 23(8): 2173-2187.
XIANG G F, JIN H, ZOU D Q, et al. Virtualization-based security monitoring[J]. Journal of Software, 2012, 23(8): 2173-2187.
- [8] CRISWELL J, DAUTENHAHN N, ADVE V. Virtual ghost: protecting applications from hostile operating systems[C]//The 19th International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS'14. 2014: 81-96.
- [9] LI Y, MCCUNE J M, NEWSOME J, et al. MiniBox: a two-way sandbox for x86 native code[C]//2014 USENIX Annual Technical Conference. 2014.
- [10] MCCUNE J M, LI Y, QU N, et al. TrustVisor: efficient TCB reduction and attestation[C]//IEEE Symposium on Security and Privacy. 2010: 143-158.
- [11] YEE B, SEHR D, DARDYK G, et al. Native client: a sandbox for portable, untrusted x86 native code[C]//IEEE Symposium on Security and Privacy. 2009.
- [12] FU M, BASS L, LIU A. Towards a taxonomy of cloud recovery strategies[C]//Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on IEEE. 2014: 696-701.
- [13] GARFINKEL T, ROSENBLUM M. When virtual is harder than real: Security challenges in virtual machine based computing environments[C]//Proceedings of HotOS. 2005: 20.
- [14] GOLDMAN K, BERGER S. TPM Main part 3 – IBM commands[EB/OL].<http://domino.research.ibm.com/>.
- [15] ENGLAND P, LOSER J. Para-virtualized TPM sharing[C]//The 1st International Conference on Trusted Computing and Trust in Information Technologies: Trusted Computing Challenges and Applications. 2008: 119-132.
- [16] XIA Y, LIU Y, CHEN H, et al. Defending against vm rollback attack[C]//The 2012 IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W). 2012: 1-5.
- [17] PARNO B, LORCH J R, DOUCEUR J R, et al. Memoir: practical state continuity for protected modules[C]//The 2011 IEEE Symposium on Security and Privacy. 2011: 379-394.
- [18] YIN H, POOSANKAM P, HANNA S, et al. Hookscout: proactive binary-centric hook detection, detection of intrusions and malware, and vulnerability assessment[M]. Berlin Heidelberg: Springer, 2010: 1-20.
- [19] CHOW J, LUCCHETTI D, GARFINKEL T, et al. Multi-stage replay with crosscut[J]. ACM Sigplan Notices, 2010, 45(7): 13-24.
- [20] LAGAR-CAVILLA H A, WHITNEY J, SCANNELL A, et al. Snowflock: rapid virtual machine cloning for cloud computing[C]//The 4th ACM European conference on Computer systems (EuroSys'09). 2009: 1-2.
- [21] PATCHIN P, LAGAR-CAVILLA H A, LARA E D, et al. Adding the easy button to the cloud with snowflock and MPI[C]//The 3rd ACM Workshop on System-level Virtualization for High Performance Computing. ACM, 2009:1-8.
- [22] CABUK S, DALTON C, RAMASAMY H, et al. Towards Automated provisioning of secure virtualized networks[C]//The 14th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, 2007. 235-245.
- [23] CABUK S, DALTON C I, ERIKSSON K, et al. Towards automated security policy enforcement in multi-tenant virtual data centers[J]. Journal of Computer Security, 2010, 18(1):89-121.
- [24] SCHAEFER M. If A1 is the answer, what was the question? an edgy naïf's retrospective on promulgating the trusted computer systems evaluation criteria[C]//The 20th Annual Computer Security Applications Conference (CSAC 2004). 2004: 204-228.
- [25] CALERO J M A, EDWARDS N, KIRSCHNICK J, et al. Toward a multitenancy authorization system for cloud services[J]. IEEE Security & Privacy, 2010, 8(6): 48-55.
- [26] BERGER S, CACERES R, PENDARAKIS D, et al. TVDc: Managing security in the trusted virtual datacenter[J]. ACM SIGOPS Operating Systems Review, 2008, 42(1): 40-47.
- [27] GRIFFIN J L, JAEGER T, PEREZ R, et al. Trusted virtual domains: toward secure distributed services[C]//The 1st IEEE Workshop on Hot Topics in System Dependability. 2005.
- [28] BERGER S, CACERES R, GOLDMAN K, et al. Security for the

- cloud infrastructure: Trusted virtual data center implementation[J]. IBM Journal of Research and Development, 2009, 53(4): 560-571.
- [29] DAVI L, DMITRIENKO A, KOWALSKI C, et al. Trusted virtual domains on OKL4: secure information sharing on smart phones[C]// The Sixth ACM Workshop on Scalable Trusted Computing. ACM, 2011: 49-58.
- [30] DAI W Q, JIN H, ZOU D Q, et al. TEE: a virtual DRTM based execution environment for secure cloud-end computing[J]. Future Generation Computer System (FGCS), 2015, 49: 47-57.
- [31] DAI W Q, JIN H, ZOU D Q, et al. TEE: a virtual DRTM based execution environment for secure cloud-end computing[C]//The 17th ACM Conference on Computer and Communications Security (CCS Poster), Hyatt Regency Chicago, IL, USA, 2010: 663-665.
- [32] DAI W Q, PARKER T P, JIN H, et al. Enhancing data trustworthiness via assured digital signing[J]. IEEE Transactions on Dependable and Secure Computing (TDSC), 2012, 9(6): 838-851.



邹德清（1975-），男，湖南长沙人，博士，华中科技大学计算机学院副院长、教授、博士生导师，主要研究方向为虚拟化安全与云安全、网络攻防与漏洞检测、大数据安全、容错计算。



金海（1966-），男，上海人，博士，华中科技大学教授，主要研究方向为高性能计算、分布式计算、云计算、大数据、云安全。

作者简介：



代炜琦（1984-），男，湖北武汉人，博士，华中科技大学讲师、硕士生导师，主要研究方向为云计算安全、可信计算、虚拟化安全、SDN 安全等。



夏妍（1993-），女，辽宁朝阳人，华中科技大学硕士生，主要研究方向为云计算安全、虚拟化安全。