基于 Xen 的虚拟化访问控制研究综述

柯文浚 董碧丹 高 洋
(中国航天系统科学与工程研究院 北京 100048)

摘 要 虚拟化作为云计算的核心技术,在广泛应用与迅速发展的同时,其安全威胁也日益凸显,严重阻碍了虚拟化的发展,是亟待解决的重要问题。学术界提出各种解决方案,其中访问控制技术作为虚拟化安全的重要屏障,获得广泛关注和研究。首先回顾了访问控制技术的发展及其对比,其次分析了 Xen 虚拟化环境中的安全问题以及所采用的访问控制技术,最后对目前国内外虚拟化安全访问控制的研究进行了总结。

关键词 虚拟化,云计算,虚拟化安全,访问控制,Xen 虚拟化
中图法分类号 TP393 **文献标识码** A

Survey of Virtualization Access Control Research Based on Xen

KE Wen-jun DONG Bi-dan GAO Yang
(China Academy of Aerospace Systems Science and Engineering, Beijing 100048, China)

Abstract Virtualization is the core technology of cloud computing, with its wide application and rapid development, the security threat has become increasingly prominent, seriously hindering the development of virtualization, which is an important issue to be resolved at the same time. Academic circles put forward various solutions, including access control technology, it's viewed as an important barrier to virtualization security, attaining a wide range of attention and research. This paper started with a review of access control technology development and contrast, followed by analysis of the Xen virtualization environment security issues, as well as access to the control techniques. Finally, researches on the current domestic and foreign virtualization security access control were summarized.

Keywords Virtualization, Cloud computing, Virtualization security, Access control, Xen virtualization

虚拟化技术[1]起源于 20 世纪 60 年代,虚拟化环境下硬件资源能够得到高效利用,一台服务器能够支撑具有各自系统的若干台虚拟机,可处理不同的业务,虚拟机在共享底层硬件和资源的情况下可以为用户提供高可靠的计算环境。随着云计算的发展,虚拟化技术作为云计算的核心技术也日渐成熟,使得企业和用户受益的同时,也不断产生了诸多安全威胁。虚拟化安全[2]问题日益严重,已经成为遏制虚拟化发展的重要因素。因此,学术界致力研究适合虚拟化环境的高可行的安全策略。

本文从访问控制入手,阐述了为适应虚拟化环境,国内外研究人员从访问控制技术入手对虚拟化的安全问题进行研究。随着虚拟化技术的快速发展,信息处理模式和用户策略都发生变化,传统的访问控制技术由于其局限性难以适用于不断发展的虚拟化环境。学术界和产业界针对此问题进行了大量研究,主要包括虚拟化环境下的访问控制[3]和加密机制的访问控制[4],其中虚拟化环境下的访问控制领域中的虚拟机访问控制[5]尤其受到关注。目前各种虚拟机系统包括 Xen[6],VMware,KVM 等,通过对比显示,Xen 因其开源性以及性能上的优越被本文作为重点研究对象。

1 虚拟化访问控制技术的发展

访问控制技术起源于 20 世纪 70 年代,主要是为了满足主机系统中授权访问所带来的资源数据共享需求。访问控制实质上是使得系统的主要资源得到有条件的访问,只有合法用户才能访问被授予权限的系统资源。管理人员在访问控制的基础上制定相应的安全策略,结合用户认证,禁止或允许用户对数据进行访问以及控制访问范围,从而实现对关键数据资源的保护,避免非法用户使用数据以及系统用户的不正确操作而对系统产生不可恢复性的损坏。

B. W. Lampson 于 20 世纪 60 年代末利用矩阵思想提出访问控制矩阵的概念,这是一种较早的访问控制方式。随着计算机以及网络的发展逐步产生了自主访问控制、强制访问控制、基于角色的访问控制、基于任务的访问控制、UCON 控制模型等。

如今访问控制技术作为实现安全虚拟化的重要手段,是保证虚拟化环境中信息机密性与完整性的关键技术,由表 1 可知,各种访问控制模型在不同安全解决方案的应用过程中也凸显出其特有的优势和不足。

本文受中国航天系统科学与工程研究院智慧城市项目"智慧宁东"关于云计算虚拟化技术研究(2015X03XC03-01),中国工程物理研究院网络与信息安全重点实验室开放基金(J-2014-KF-01)资助。
柯文浚(1988—),男,硕士生,主要研究方向为信息安全,E-mail:kwj1124@qq.com;董碧丹(1957—),女,研究员,硕士生导师,主要研究方向为智能信息处理、信息安全;高 洋(1984—),男,工程师,主要研究方向为系统集成、信息安全。

表 1　虚拟化访问控制技术对比

访问控制名称	典型控制模型	优点	缺点	虚拟化访问控制模型性能对比			
				安全性	细粒度控制	授权灵活性	动态变化
自主访问控制	HRU 模型	可自主将权限授予其他客体，拥有一定的授权灵活性	系统中权限泛滥，管理员失去对权限的控制			√	
强制访问控制	BLP 模型	分等级的权限机制，大大提高了系统的安全性	缺乏灵活性，使用领域相对狭窄	√	√		
基于角色的访问控制	RBAC96 模型	权限、用户、角色 3 个元素关联，具有一定的灵活性，也保证了系统的安全性	应用环境范围小，仍在不断研究改进	√		√	
基于任务的访问控制	TBAC 模型	实现动态授权	任务往往较多，造成较多的冗余、系统负荷较大				√
使用控制模型	UCON 模型	适用于动态多变的分布式环境	目前仅在理论研究阶段，难以实际运用		√	√	√

2　Xen 环境下安全问题分析及访问控制技术

2.1　Xen 虚拟化安全问题分析

虚拟化系统的架构体系，虚拟机、虚拟机监视器、底层物理硬件均需通过相应的访问控制技术来保护信息资源，访问控制技术为虚拟化体系结构提供重要的安全保障。虚拟机系统中面临的安全威胁包括虚拟机的提权[7]、虚拟机之间的非法共享[8]、隐蔽信道[9]、无法抵御非控制数据攻击[10]等，这些安全威胁为访问控制技术的深入研究提出了更高的要求。目前，国内外各大虚拟化服务商（亚马逊、谷歌、微软、华为等）均采取了不同的访问控制机制来为各种虚拟化平台提供安全支持，学术界主要从保障资源共享和数据安全的层面对虚拟化访问控制问题进行研究，但是仍然存在许多问题。

（1）访问控制模型方面。随着虚拟化技术的发展，传统的访问控制模型已经不能满足虚拟化安全需求，以传统的基于角色的访问控制模型 RBAC96 为例，虚拟化环境中主体和客体的定义发生了变化，虚拟化主要是以用户为核心，以数据资源共享为基础的服务模式，因此为了使传统访问控制模型适用于虚拟化环境，需要在对其重新设计和完善的同时，主体、客体角色的适用范围也需要重新界定。

（2）安全构建方面。对于虚拟机系统的安全构建问题，传统的访问控制技术在模型以及规则方面不能很好地满足虚拟化平台安全架构的要求。虚拟机系统安全的要求包括：1）确保组成部件（bootloader，VMM，OS 等）映像未被篡改；2）基于 TPM 构建虚拟机系统信任链。基于以上两点安全要求，虚拟化平台对访问控制策略提出了更高的挑战。

（3）体系机制方面。1）虚拟化环境下，除实现按比例分配硬件资源之外，对其上的虚拟机使用 CPU、内存和 IO 无其他限定，需要采用访问控制实现准物理的安全隔离机制，以便有效解决底层隐蔽通道问题；2）虚拟机系统中各类应用处于不同的安全级别，在虚拟化平台下，当用户需要跨密级或跨域访问资源时，需要统一考虑应用策略、用户授权、资源共享等问题；3）虚拟化环境中虚拟机之间的相互信任问题也直接关系到访问控制。

虚拟化作为云计算的核心技术，其中虚拟机 Xen 相比传统操作系统有较为显著的优势：VMs 间的隔离可以通过 CPU 环保护机制实现，并且 VMs 间的内存可通过 IOMMU 实现隔离，在一定程度上其稳定性和可靠性要优于传统操作系统。但是，Xen 虚拟化技术[11]在某种程度上保障了系统安全，同时也产生了新的安全问题。如图 1 所示，目前虚拟机、虚拟机监视器、底层硬件等产生的安全问题体现在以下几个层面。

（1）虚拟机层。1）在同一台服务器的虚拟机，存在 DomU 和 Dom0，DomU 利用某些攻击手段绕过 Hypervisor 直接访问 Dom0，获取 Dom0 特权从而可以控制其他 DomU，利用 Dom0 从事一些破坏活动和攻击活动；2）虚拟机之间经常共享 CPU、I/O、内存，这些共同访问的资源产生恶意攻击；3）虚拟机和物理机一样都存在被病毒木马等恶意攻击。

（2）虚拟机监视器层。虚拟机监视器在 Xen 虚拟化环境中对于虚拟机和硬件层之间，虚拟机对于硬件的访问具有一定的访问和控制的功能，处于核心地位。因此 Hypervisor 经常成为被攻击的对象，例如：攻击者将程序代码写入内存，Hypervisor 运行后如果运行代码，虚拟机系统将在恶意攻击者的范围内，典型攻击为 Blue 形式的 VMBR 攻击。

（3）底层硬件层。传统环境，可利用防火墙、IDS、IPS 对不同的物理机之间进行访问控制。在虚拟化环境下，同一台物理服务器中，这些传统防护不适用于虚拟机池。例如其中一台客户虚拟机受到外来攻击，这台虚拟机就会被作为跳板，绕过一些虚拟机内部的安全保护机制，对别的客户机造成破坏威胁。

除了上诉安全威胁之外，还存在一些常见的安全问题，比如 VM 的 Rootkit[12]攻击，快照、数据备份与恢复的安全隐患，DMA 攻击等。

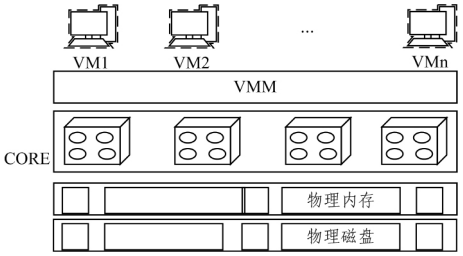

图 1　虚拟化平台架构图

2.2　Xen 环境下的访问控制技术

国内外的虚拟化技术中，虚拟化 Xen 平台因其开源性和高效的优势得到业界一致好评，国内外学者在 Xen 访问控制安全方面做了大量研究，主要从以下 3 个方面分类。

（1）虚拟机间的访问控制研究，通过访问控制模型制定控制策略，处理 VM 间的安全隔离和 VM 间的安全共享。

（2）Hypervisor 的安全研究，在防护 Hypervisor 层的同时，保护虚拟机间各种不同资源的隔离、数据的安全以及虚拟机间相互通信的安全等。

（3）对底层硬件的安全隔离，防止同一个主体为有利益冲

突的两个客体服务，进而损害客体的利益。采取特定的访问控制机制，提供更好的隔离机制同时进一步提高硬件资源的利用效率。

2.2.1 虚拟机间的访问控制研究

虚拟化环境下，虚拟机需采取和实体机一样的安全策略，同时须考虑在虚拟化环境下虚拟机的一些特有的安全威胁。目前虚拟化环境下 Xen 的安全策略相对比较原始，体现在以下 3 点：1）基于中等 ELA4 标准的安全、有利益冲突的虚拟机不能共存；2）极大地影响系统效率；3）可共享数据的虚拟机间无安全共享机制，影响系统安全。因此，通过虚拟机间的访问控制，制定合适的控制策略及访问控制模型来保证虚拟机资源高效安全共享。如图 2 所示，通过重新设计和修改 BLP 强制访问控制策略，采用钩子（hook）函数，保证主体和客体虚拟机的多级安全防护。

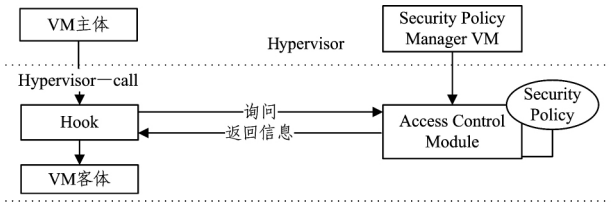

图 2 虚拟机访问控制图

2.2.2 Hypervisor 层的研究

Hypervisor 是虚拟化环境中处于虚拟机和底层硬件的中间层，对于虚拟化的安全性研究，也是以 Hypervisor 层安全为重点。目前国内外对 Xen 的 Hypervisor 访问控制主要包括 XSM（Xen Security Module），Xenon，Virt-BLP 等。

（1）XSM[13]：Xen 平台的一种安全架构，为 Xen 提供安全接口，在 Xen 源码中通过编译直接安装，实现对 VMM 资源和 VM 的强制访问控制。XSM 安全策略有 3 个模块：系统默认的 Dummy 安全策略、IBM 公司开发研究的 ACM 安全机制、NAS 开发的 Flask 安全机制。

1）Dummy：Xen 系统默认安装 Dummy，DomU 之间不存在信息流，即 DomU 之间相互隔离，实现纯隔离的安全策略。

2）ACM：是 IBM 在虚拟机监视器层面上研发的一种安全 Hypervisor，即 sHyper，它主要对虚拟机系统实现强制访问控制技术，可以实现 VMs 间的安全通信。主要设计目标为：①管理同一个物理硬件上多个 VM 之间的通信；②管理 VM 对硬件资源的访问；③控制有资源冲突的虚拟机不能在同一个服务器平台上同时运行。如今在 sHyper 中有中国墙（Chinese Wall）和简单 TE 两种安全策略。Huang 等人在 sHyper 基础上对访问控制框架进行扩展，基于理论实现单向可控的信息流。

3）Flask/NAS：美国国家安全局开发的 Flask 安全机制可提供细粒度的访问控制，实现虚拟机监视器资源的安全。与 ACM 相比可更细粒度地实现对虚拟机监视器资源的访问控制，通过相应的安全模型，结合安全机制，如 BLP、RBAC 等，可以更细粒度地提供访问控制机制和更安全的保护虚拟化环境。

（2）Xenon：美国海军实验室对 Xen 的二次开发，构建一个有较高安全级的虚拟机系统。Xenon 具有以下几个优点：1）简洁化，主要致力于 Xen 中的代码优化，使其高效简单；2）模块化，采取技术对虚拟化系统进行模块细化；3）分层结构，对安全信息进行等级分层，易于管理与实现单向信息流。Xenon 对 Xen 目前的代码有较多改变，且该技术仍在研究中。

（3）Virt-BLP：上海交通大学“虚拟计算系统安全可信机制研究”[14]基于 Xen 提出一种结合可信计算与访问控制机制的安全可信机制。设计一种对系统资源和数据进行等级分层的模型，主要是在强制访问控制经典模型 BLP 基础上的改进，对模型中的定理、元素、变化规则进行改进和完善，实现虚拟机系统间通信的分等级的保护。并且结合可信计算和密码学技术实现虚拟机之间的可信机制和安全协议，有效建立虚拟机环境中各虚拟机之间的相互信任关系和安全通信方式。

2.2.3 底层硬件的安全隔离

在虚拟化环境中通过不同的分区实现虚拟机在物理上的隔离，主要是不同虚拟机运行在不同服务器中，这种物理隔离可以实现高安全性，但是设备利用率极低。然而，在 Xen 虚拟化环境下，Xen 对底层硬件并无访问控制，除实现按比例分配硬件资源之外，对其上的虚拟机使用 CPU、内存和 IO 无其他限定，这种方式对硬件具有高利用率，但是存在安全威胁。因此，在 Xen 环境下可以通过制定访问控制策略，实现底层硬件层面的隔离，可以有效解决安全问题。李明禄等人[15]采用中国墙策略实现虚拟化系统底层的安全隔离，使有安全冲突的 VM 可以设定运行在不同的 CPU 和内存集合上，实现准物理的安全隔离机制，这种访问控制隔离机制可以有效防止底层的隐蔽通道。

3 虚拟化安全访问控制的研究

通过对 Xen 虚拟化环境的认识，其他平台如 VMware，KVM，hyper-v 等均面临以上安全问题。目前学术界主要通过以下几种方式对虚拟化中的访问控制策略进行研究：虚拟化访问控制模型、基于加密机制的虚拟化访问控制、虚拟机系统访问控制研究。

3.1 虚拟化访问控制模型

虚拟化中的访问控制模型大都以传统的访问控制模型为基础进行重新设计和完善，并将其运用于虚拟化环境。诸多访问控制模型侧重的内容和方式不尽相同，所具备的功能也有所差异。针对虚拟化环境的特殊性，目前研究主要围绕基于 BLP 的访问控制模型、基于角色的访问控制模型、基于属性的访问控制模型等[16]。

刘苏娜等人[17]使用网络中的基本元素和遵循的通信协议对 BLP 模型进行延伸，设计实现一种可以细粒度控制虚拟机系统通信的机制，称为 NBLP 控制模型。NBLP 模型可以细粒度控制网络连接和数据传输，使得不同安全密级的信息实现安全传输。这种访问控制方式为政府、银行、军队等对数据安全需求较高的机构提供了严格的访问控制策略，保障了系统数据的机密性和完整性。对于 VM 之间的访问控制策略，刘谦等人[18]研究虚拟机系统在运行期间的安全，提出确保虚拟系统内部安全隔离、确保有效防止外界非法入侵、确保虚拟机间的安全共享。

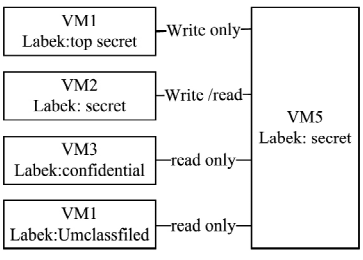

图 3 基于密级的虚拟机安全图

如图 3 所示，在虚拟机层次上，各虚拟机间的访问控制建立多级安全级别，保证有冲突的虚拟机相互隔离并且无法知晓相互的存在，协同的虚拟机间提供安全共享机制，这种控制策略模型可以为 VM 之间提供多级安全，对虚拟机间实现细粒度的访问控制，同时兼顾安全与效率。

文献[19]提出 T-RBAC 模型，将 RBAC 中一些公理和任务模式相结合，将虚拟机系统间的访问流程划分为相互联系的任务，继而通过角色来实现各个任务点。文献[20]在可延伸的虚拟化工作任务中提供 RBAC 模型策略，在保证工作任务可延伸的情况下，该策略模型可以高效处理工作任务中虚拟机系统中的用户的权限分配，提供可靠安全机制。李春燕等人[21]对基于角色的访问控制模型进行改进，结合 3 种权限分开的思路和运用秘钥技术实现对系统用户的不同权限的控制，主要首先通过对用户身份进行认证，然后通过系统访问控制机制验证所具有的权限，最后对通信资源进行验证并且使用加密技术对其加密，在 VM 系统中具有一定的安全性与灵活性。

张永胜等人[22]基于传统属性访问控制原型，针对其中加密效率过低、缺乏连续性、策略检索效率低等问题，对传统基于属性的访问控制进行改进。通过增加秘钥属性、私钥生成点模块及数据加解密点模块实现两种属性库的共享，实现对用户数据的同步加解密；引进 UCON 模型中的义务概念，增加状态机制，实现决策连续性及状态相关性，使其具有动态多次授权的特点；引入链表与平衡二叉树的概念，提出基于冲突检测链表和冲突检测树的两种静态冲突检测方法。ABAC 模型具有高度的灵活机制、支持后续扩展、访问控制粒度高等优点[23]。然而，在虚拟化环境下进行进一步研究具有重要意义，包括如何令 ABAC 数据加密机制既高效又安全，如何保证策略冲突被正确检测，如何确保授权操作不会出现权限冗余，同时也要考虑如何令 ABAC 属性分配机制在虚拟环境下的处理更加高效，提高系统效率。

3.2　基于加密机制的虚拟化访问控制

加密机制访问控制技术的设计，确保了在一些非可信虚拟化环境中的数据的机密性和可靠性，主要是在数据存储之前对数据进行加密，控制特定用户对秘钥的获取来实现访问控制，使得只有具备相应秘钥的用户才能解密。

ABE[24]是一种常见的密码机制，Sahai 等人在 ABE 基础上分别提出 KP-ABE 和 CP-ABE。其中，KP-ABE 中解密秘钥主要通过策略树来获得，而且主动加密者对数据不存在控制权，适用于较大型网络拓扑环境下的秘钥控制管理；CP-ABE 中，通过访问控制策略树与密文相互关联，解密秘钥用一系列属性进行描述。朱等人将 ABE 密码体制与 RBAC 控制模型结合，系统用户利用 RBAC 策略同时访问数据和加密，通过对算法进行改善来将二者结合起来，达到控制数据泄露的效果。刘斐等人[25]通过 Hypervisor 利用数据加密技术和哈希校验方法对虚拟机中的磁盘数据进行安全防护，能够确保磁盘数据在被虚拟机访问过程中的隐秘性和完整性，保障 VM 磁盘数据的安全。武越等人[26]针对涉密环境提出虚拟化多层次分级的安全模型，满足一些对系统安全性要求较高的涉密环境，实现对于虚拟化的安全分等级防护需求，结合数据加密解密的访问控制，对所存的文件信息进行安全处理，并且将对称和非对称秘钥系统进行有效结合，在保护数据机密性的前提下，降低秘钥的监管难度；通过修改文件秘钥树的方式实现对虚拟磁盘的访问权限变更，使得授权方式更加灵活。

3.3　虚拟机系统访问控制研究

邹德清等人[27]以虚拟域内访问控制机制的原型系统为基础，修改 Xen 平台下 VM 的管理程序，利用 VM 管理程序的间隔性与其特有权限，提出一种防护系统内核完整性和虚拟域内访问控制的安全策略模型，在功能性方面能够有效抵御 Rootkit 攻击。

王静等人[28]利用无干扰安全策略模型，并且结合最小特权的原则，提出 LPNIM 安全策略模型实现虚拟化平台中数据的机密性和完整性。该模型强调机密性无干扰约束条件、完整性无干扰约束条件、静态完整性无干扰约束条件，当且仅当系统满足这 3 个条件时，系统是安全的。王静结合 LPNIM 模型，构建一个高安全强度的虚拟化 Xen 系统平台，达到的目标主要有：1）明确制定策略规定系统中 DomU 在没有授权的情况下，不存在信息流的交互；实现 DomU 之间的隔离策略，有效避免 VM 之间的攻击；同时，DomU 之间有时可能需要共享一些信息，基于 LPNIM 策略，实现 Xen 虚拟机支持一种单向的、满足最小特权的两级安全策略，即满足虚拟机监视器和管理虚拟机的两级控制，实现虚拟机之间共享更细粒度的访问控制。2）将 Dom0 的特权最小化，保留一些 Dom0 与 DomU 之间的必要操作，如创建、启动和删除等，把对硬件的接口操作特权从 Dom0 中转移到其中一个特殊的 DomU 中，这样可以有效减少 VM 对 Dom0 攻击后所产生的严重后果。

2015 年的云计算报告大会提出了一项名为 CloudPolice：Taking access control out of the virtual machine 的专题，提出实现多用户间安全的结构，主要在 Hypervisor 上实现一种访问控制。主要根据主体和客体之间的情况来动态地调整虚拟化环境的访问控制策略，主要包括对主体和客体间通信实施隔离，在安全前提下允许他们之间的通信，允许利用授权表实现主体和客体之间的共享资源等。通过这种方式，可以在实现灵活地对资源进行有效安全的利用的同时，保障虚拟机之间通信的安全。

综上所述，虚拟化的安全与合适的访问控制模型与其制定的策略紧密相关。需要考虑众多因素：虚拟化平台的控制策略，虚拟化平台内部数据和资源对用户需求的访问控制，访问控制的控制粒度，新的访问控制必须对虚拟化环境灵活支持、可伸缩和网络独立等。需要对虚拟化技术中的 CPU 虚拟化、内存虚拟化、I/O 虚拟化有全面深入的了解，进而在这基础上延伸，提出高效、安全的访问控制策略。

结束语　随着虚拟化技术在云计算方面的发展日趋成熟，其凸显出来的一系列安全问题也逐渐受到学者们的关注。随着研究的深入，虚拟化暴露出来的安全隐患越来越多，使得这一领域在寻求发展的同时无疑面临巨大的挑战。虚拟化访问控制是解决安全威胁行之有效的手段，也是现今安全领域研究的重要课题之一。本文重点分析了国内外学者当前在虚拟化访问控制方面的各种研究成果，分析了其实现要点和得到的效果，对遗留的问题（存在的不足）和后续的研究方向以及技术措施进行了综合性论述。在对前人的研究成果进行归纳总结的基础上，需要在后续的研究中考虑各种安全模型和安全措施的不足，对其进行改进，进而设计出更加合理高效的访问控制模型。

参 考 文 献

[1] 李树波,罗林,杨艳. 云计算与虚拟化技术研究[J]. 软件导刊,2013,12(1):141-143.

[2] 冯国登,张敏,张妍. 云计算安全研究[J]. 软件学报,2011,22(1):22-28.

[3] 房晶,吴昊,白松林. 云计算的虚拟化安全问题[J]. 电信科学,2012,12(4):135-140.

[4] 张兴杰,马文平. 基于加密的访问控制在云计算中的应用研究[D]. 西安:西安电子科技大学,2014.

[5] 秦中元,沈日胜,张群芳,等. 虚拟机系统安全综述[J]. 计算机应用研究,2012,29(5):1618-1623.

[6] 石磊,邹德清,金海. Xen 虚拟化技术[M]. 武汉:华中科技大学出版社,2009.

[7] 丁滁,王怀民. 可信云服务[J]. 计算机学报,2015,38(1):133-149.

[8] WU J Z,DING L P. Identification and evaluation of sharing memory covert timing channel in Xen Virtual Machines[C]// Washington DC:IEEE Computer Society. 2011:283-291.

[9] 王永吉,吴敬征,曾海涛. 隐蔽信道研究[J]. 软件学报,2010,21(9):2265-2283.

[10] DING B,HE Y,WU Y,et al. HyperVerify:a vmm-assinted architecture for monitoring hypervisor non-control data[C]// Proceeding for the IEEE 7th International Conference on software Security and Reliability Companion. Gaitheraburg, MD, USA, 2013:26-34.

[11] 孟江涛,卢显良. Xen 虚拟机研究[D]. 成都:电子科技大学,2003.

[12] RILE Y R,JIANG X,DONG Y. Guest-transparent prevention of kernel Rootkits with VMM-based memory shadwing[C]// Proc of the 11th International Symposium on Recent Advances in Intrusion Detection. Berlin:Springer,2008:1-20.

[13] 石磊,邹德清,金海. Xen 虚拟化技术[M]. 武汉:华中科技大学出版社,2009.

[14] 马喆,禹熹,袁傲,等. Xen 安全机制探析[J]. 理论研究,2011,9(11):31-36.

[15] 刘谦,李明禄. 面向云计算的虚拟机系统安全研究[D]. 上海:上海交通大学,2012.

[16] 李凤华,苏芒,史国振. 访问控制模型研究进展及发张趋势[J]. 电子学报,2012,40(4):805-813.

[17] 刘苏娜,潘理. 虚拟化平台下基于 BLP 的网络访问控制机制研究与实现[D]. 上海:上海交通大学,2011.

[18] 刘谦,李明禄. 面向云计算的虚拟机系统安全研究[D]. 上海:上海交通大学,2012:1-122.

[19] WANG X W,ZHAO Y M. A task-role-based access control model for cloud computing[J]. Computer Engineering,2012,38(24):9-13.

[20] 赵明斌,姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用,2012,32(S2):267-270.

[21] 李春燕,张亚平. 云计算环境下基于角色的访问控制模型研究[D]. 天津:天津大学,2012.

[22] 邹佳顺,张永胜. 云环境下基于属性的访问控制模型及应用研究[D]. 济南:山东师范大学,2015.

[23] WANG X M,FU H,ZHANG L C. Research progress on attribute-based access control[J]. Chinese Journal of Electronics,2010,38(7):1660-1667.

[24] VIPUL G,AMIT S,OMKANT P,et al. Attribute-Based encryption for fine-grained access control of encrypted data[J]. Proc. of the ACM conf on Computer and Communications Security,2006,14(3):89-98.

[25] 刘斐,任兰芳,柏洪涛. 客户虚拟机磁盘数据安全性的保护方法[J]. 计算机应用与软件,2015,32(2):71-76.

[26] 武越,刘向东. 涉密环境桌面虚拟化多级安全系统设计与实现[J]. 计算机工程与设计,2014,9(1):101-104.

[27] 邹德清,杨凯,张晓旭. 虚拟域内访问控制系统的保护机制研究[J]. 山东大学学报,2014,49(9):135-142.

[28] 王静,徐开勇. Xen 无干扰安全策略模型及安全机制研究[D]. 郑州:解放军信息工程大学,2012.

(上接第 18 页)

[37] 杨萍,侯宏旭,蒋玉鹏,等. 基于双语对齐的汉语-新蒙古文命名实体翻译[J]. 北京大学学报(自然科学版),2016,52(1):148-154.

[38] LAM W,HUANG R,CHEUNG P S. Learning phonetic similarity for matching named entity translations and mining new translations[C]// Proceedings of the 27th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM,2004:289-296.

[39] HUANG F,VOGEL S,WAIBEL A. Improving Named Entity Translation Combining Phonetic and Semantic Similarities[C]// HLT-NAACL. 2004:281-288.

[40] HUANG F,ZHANG Y,VOGEL S. Mining key phrase translations from web corpora[C]// Proceedings of the Conference on Human Language Technology and Empirical Methods in Natural Language Processing. Association for Computational Linguistics,2005:483-490.

[41] ZHANG Y,VINES P. Using the web for automated translation extraction in cross-language information retrieval[C]// Proceedings of the 27th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM,2004:162-169.

[42] CHENG P J,TENG J W,CHEN R C,et al. Translating unknown queries with web corpora for cross-language information retrieval[C]// Proceedings of the 27th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM,2004:146-153.

[43] ZHANG Y,VOGEL S,WAIBEL A. Interpreting BLEU/NIST scores:How much improvement do we need to have a better system[C]// Proceedings of Language Resources and Evaluation. 2004:2051-2054.

[44] KIM S,TOUTANOVA K,YU H. Multilingual named entity recognition using parallel data and metadata from Wikipedia [C]// Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics:Long Papers-Volume 1. Association for Computational Linguistics,2012:694-702.

[45] NOTHMAN J,RINGLAND N,RADFORD W,et al. Learning multilingual named entity recognition from Wikipedia [J]. Artificial Intelligence,2013,194:151-175.