云平台特权行为管控与审计系统

杨春鹏[1]，刘川意[2]

（1. 北京邮电大学计算机学院，北京 100876；
2. 哈尔滨工业大学（深圳）计算机科学与技术学院，广东深圳 518055）

摘要：云管理员客观上具备滥用特权以控制与窃取云中用户数据的技术手段与金钱动机，如何细粒度划分云平台特权、实时管控与事后审计云管理员操作，成为极具挑战的问题。研究实现了云平台攻击实例，验证恶意云管理员可利用特权窃取用户数据。之后梳理相关研究工作中的主要技术路线：云平台管理权限划分与云平台运行时特权验证。最后，设计并实现了云平台特权行为管控与审计系统，提高了云平台管理权限划分与云平台运行时特权验证的适用性。

关键词：数据安全与计算机安全；云计算；权限划分；特权管控；日志审计
中图分类号：TP309.2 **文献标识码：**A **文章编号：**1674-2850(2017)04-0356-09

Cloud platform privileges control and audit system

YANG Chunpeng[1], LIU Chuanyi[2]

(1. *School of Computer Science*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*;
2. *School of Computer Science and Technology*, *Harbin Institute of Technology* (*Shenzhen*), *Shenzhen*, *Guangdong* 518055, *China*)

Abstract: Objectively, cloud administrators have both technical means and monetary motivation to misuse privileges to control and steal users' data in the cloud platform. It is challenging to divide the least privileges, real-time control and post-audit cloud administrators' operations. This paper firstly performs several attacks on the cloud platform to demonstrate that malicious cloud administrators can take advantage of privileges to steal users' data. Secondly, this paper summaries the main technical approaches of recent researches: cloud administrators' privileges division and run-time permissions control. Finally, this paper designs and implements a cloud platform privileges control and audit system to improve the applicability of cloud platform management privilege division and cloud platform runtime privilege verification.

Key words: data security and computer security; cloud computing; permissions division; privileges control; log audit

0 引言

内部威胁是云计算安全面临的最严重挑战之一[1]。2016 年 2 月，云安全联盟（Cloud Security Alliance，CSA）在报告中列举了云计算模式下的十二大风险，其中恶意内部人员（malicious insiders）威胁赫然在列[2]。在内部威胁的诸多类别中，公司员工、外包商或合作伙伴的恶意特权行为，即故意滥用或误用自己对网络、系统或数据的访问权限以损害公司信息或信息系统的保密性、完整性、可用性，危害甚广[3~5]。2016 年埃森哲（Accenture）咨询公司与 HfS 研究公司联合发布的报告显示，69%的企业安全管理人员曾

基金项目：国家高技术研究发展计划（863 计划）（2015AA016001）；广东省产学研合作项目（2016B090921001）；山东省自主创新及成果转化专项（2014ZZCX03411）
作者简介：杨春鹏（1991—），男，硕士研究生，主要研究方向：云计算与云安全
通信联系人：刘川意，副教授，主要研究方向：云计算与云安全、数据安全与数据保护. E-mail: cy-liu04@mails.tsinghua.edu.cn

经发现来自特权人员的数据非法访问和盗窃企图[6]。

云计算模式的本质是数据所有权与管理权的分离[7]。云租户将自己的数据和业务系统迁移到云提供商的云平台上，失去了对原有数据和业务系统的直接控制能力。而云提供商随即获得云租户数据和业务系统的直接控制能力，并能获知和监控用户的操作行为数据。这就给云管理员，如服务器管理员、云平台管理员、虚拟机镜像管理员、虚拟机系统管理员、应用程序管理员，窃取用户隐私数据的特权，在客观上拥有技术手段和金钱动机滥用特权。

因此，云平台特权行为的管控与审计是一个极为重要且亟待解决的问题。针对上述问题和挑战，本文设计并实现云平台特权行为管控与审计系统。基于对云平台管理权限的细粒度划分，系统无缝对接OpenStack[8]、VMware vSphere[9]云平台，实现对管理员特权行为的动态管控与审计。

1 云平台特权行为攻击实例

为揭示云计算模式下管理权限划分模糊、特权行为滥用误用问题，通过对当前主流云平台（如OpenStack、VMware vSphere、QEMU+KVM[10~11]、XEN[12]）的体系结构、权限划分、日志审计等方面进行梳理与分析，本文真实实现了恶意云管理员窃取用户数据的攻击实例。

1.1 恶意云管理员制作并上传带病毒或木马的虚拟机镜像

一个云平台动辄需要上百上千个虚拟机进行数据分析，虚拟机操作系统中运行的中间件和应用软件一定不可能是将虚拟机一个一个地安装部署，而是通过镜像方式批量生成大规模虚拟机环境。若虚拟机镜像文件由恶意云管理员制作，该恶意云管理员可在镜像中轻松植入木马或后门程序，并上传到镜像库中。如图1所示，只要是该镜像启动的所有虚拟机，其中的用户数据均可通过木马或后门程序发送给恶意云管理员。

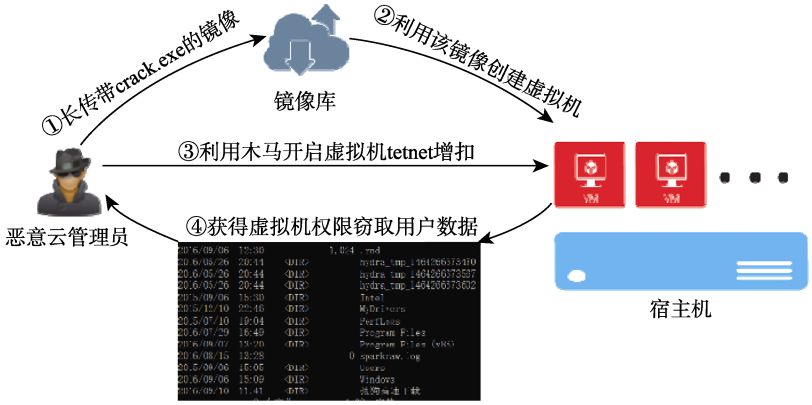


图1 恶意云管理员制作、上传带病毒或木马的虚拟机镜像

Fig. 1 Malicious cloud administrators make and upload a virtual machine image with virus or Trojan horse

1.2 恶意云管理员篡改 Windows 虚拟机密码

虚拟机租户唯一掌管着运行于云平台上的 Windows 虚拟机的用户名及密码，但恶意云管理员可通过挂载 Windows ISO 镜像文件，启动 Windows 操作系统的修复模式，替换应用程序，使其能够在 Windows 登录界面启动管理员命令行程序，修改用户名及密码，登录到虚拟机窃取用户数据。具体操作如图2所示。

1.3 恶意云管理员删除 Linux 虚拟机密码

虚拟机租户唯一掌管着运行于云平台上的 Linux 虚拟机的用户名及密码。但恶意云管理员可借助对云管理平台的访问权限，查找出虚拟机磁盘文件具体路径并修改磁盘文件，删除用户密码，登录 Linux 虚拟机。具体步骤如图3所示。

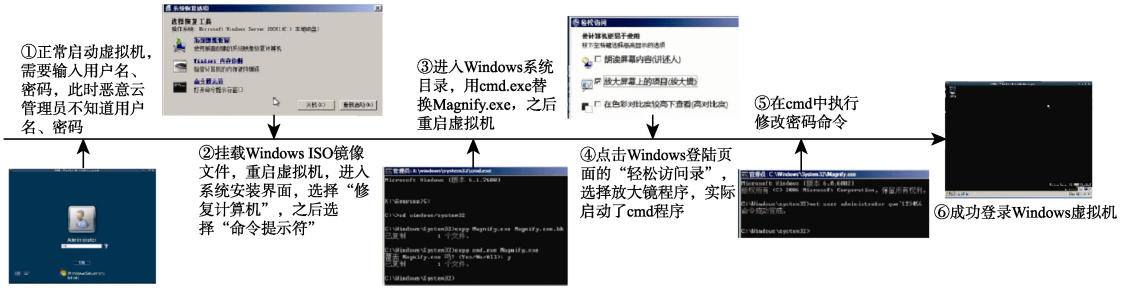


图 2 恶意云管理员篡改 Windows 虚拟机密码

Fig. 2 Malicious cloud administrators tamper Windows virtual machines' passwords



图 3 恶意云管理员删除 Linux 虚拟机密码

Fig. 3 Malicious cloud administrators remove the Linux virtual machines' passwords

1.4 恶意云管理员进行虚拟机带外内存分析

如图 4 所示，云租户使用虚拟机时输入某网站用户名与密码。恶意云管理员可使用虚拟机自省（virtual machine introspection，VMI）[13]工具，转储正在运行的虚拟机内存，并使用内存取证工具，如 Volatility[14]，分析虚拟机内存具体语义，得到云租户访问网站的用户名与密码[13]。

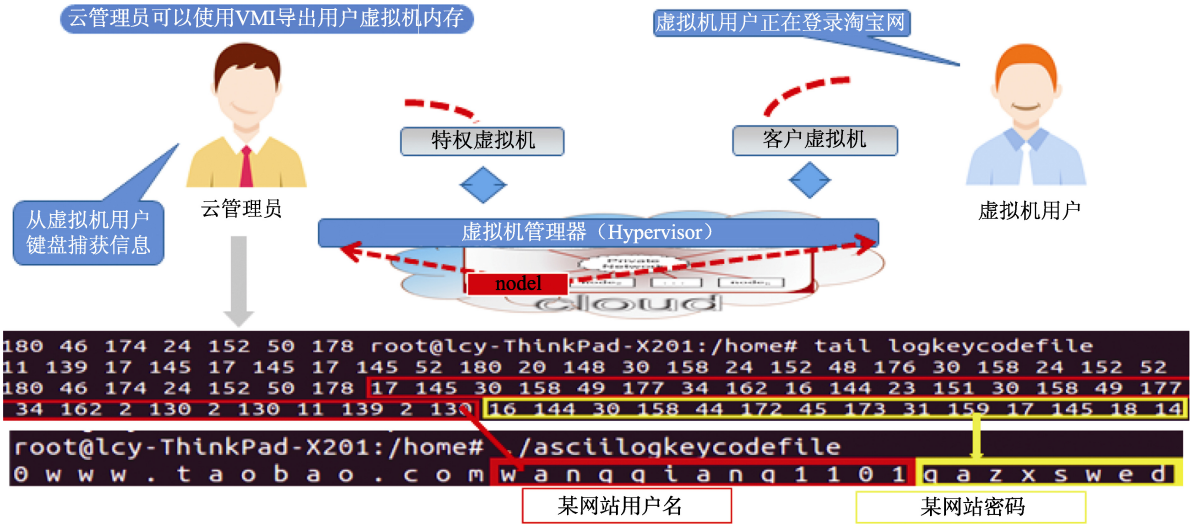


图 4 恶意云管理员导出虚拟机内存并分析

Fig. 4 Malicious cloud administrators export and analyze the memory of virtual machines

2 相关工作

云平台特权管控与审计现有工作分为两大类：云平台管理权限划分与云平台运行时验证。云平台管理权限划分主要是对云平台中的操作、资源、数据制定细粒度权限划分规则；云平台运行时验证主要是在虚拟机管理器层制定执行验证策略，使特权管理员经过验证后才能执行操作。

2.1 云平台管理权限划分

在 Xen 虚拟化环境中，包含 2 个组成部分。一个是虚拟机监视器（virtual machine monitor，VMM），VMM 层在硬件与虚拟机之间，直接控制物理硬件；另一部分是管理域（domain0），拥有启动/关闭虚拟机、修改虚拟机配置、监控物理资源利用率等较高特权。在整个虚拟机生命周期中，云管理员使用配置程序直接控制 domain0.

自服务云（self-service cloud）[15]提出一种新的权限模型以分割 domain0 的特权。如图 5 所示，自服务云权限模型将原来 domain0 的特权分割为系统管理域（Sdom0）和用户元域（Client's Meta-Domain）。其中，用户元域权限又细分为用户管理域（Udom0）、用户域（User Domain）、服务域（service domains，SD）和互信服务域（mutually-trusted service domains，MTSD）。在用户元域中，每个虚拟机为一个用户域，具体用户域用 UdomU 表示。每一个虚拟机用户可管理自己的虚拟机，对虚拟机进行特权操作；在系统管理域中，云管理员没有权限查看虚拟机内用户的代码、数据。自服务云使用独立的域构建器（domain builder，domB），负责创建虚拟机的任务，使该特权不再驻留系统管理域。MTSD 允许在云服务提供商与云租户之间构建相互可信的服务，以满足监管合规性（Regulatory Compliance），同时 SD 提供给云租户构建其他安全服务（Security Service）的权限以保护自身的敏感数据与应用。

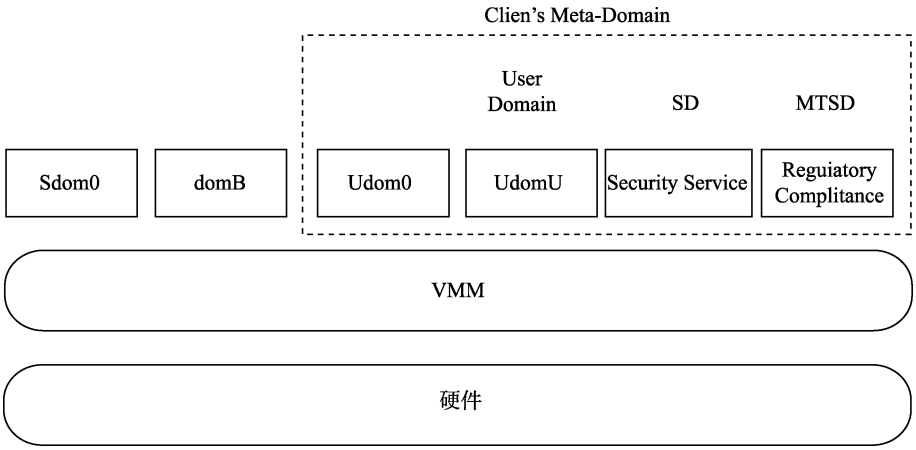


图 5 自服务云系统架构

Fig. 5 System architecture of self-service cloud system

自服务云将 VMM 中的特权操作分为 6 组：

1）虚拟机控制（VM control）操作，如暂停/取消暂停、调度、销毁虚拟机。

2）隐私敏感（privacy-sensitive）操作，如对虚拟机内存、vCPU 的操作。

3）只读（read-only）操作，如虚拟机 vCPU、内存分配数等在宿主机上的物理参数。

4）建设（build-only）操作，包括虚拟机创建期间的特权操作。

5）虚拟 I/O（virtual I/O）操作，如宿主机与虚拟机间隧道、共享内存、共享目录等 I/O 操作。

6）云平台配置（platform config）操作，如终端控制器、时钟源配置。

其中，Sdom0 为分割特权后的系统管理域，由云管理员直接控制。Sdom0 保留了部分虚拟机控制操作、只读操作、虚拟 I/O 操作和云平台配置操作的特权，但禁止其访问用户元域的状态及数据，确保虚拟机内的安全性和保密性。domB 负责建设操作，执行初始虚拟机流程。Udom0 为面向用户的管理域，拥有部分虚拟机控制权限，并可执行虚拟机内部隐私敏感操作、只读操作和虚拟 I/O 操作。SD 为虚拟机用户提供可自定义的服务域，如用户定制服务检测虚拟机是否存在带外内存自省行为、验证虚拟机完整性、虚拟机流量加密等。MTSD 是云提供商与虚拟机用户共同协商执行安全防护的域。如表 1 所示，不同域对应不同特权操作。这种权限模型的不足是云平台需要配合安装安全芯片，同时需要定制化 VMM，实施困难。

表 1　不同域对应不同的特权操作

Tab. 1　Different domains correspond to different privileged operations

操作	Sdom0	domB	Udom0	SD/MTSD
虚拟机控制	√		√	√
隐私敏感			√	√
只读	√		√	√
建设		√		
虚拟 I/O	√		√	√
云平台配置	√			

2.2　云平台运行时验证

云平台运行时，在 VMM 和虚拟机之间插入安全管理层，截获并验证特权操作和内核行为，以保护用户数据。CloudVisor[16]利用嵌套虚拟化技术实现在 VMM 层之下插入安全管理层 CloudVisor，仲裁 VMM 与虚拟机之间的特权行为。CloudVisor 是在最高特权层级上运行的轻量级安全检测器，VMM 和虚拟机处于相对特权较少的层级。CloudVisor 强制隔离和保护每一个虚拟机使用的资源，解耦虚拟机管理与虚拟机安全。传统的虚拟化功能，如资源管理、虚拟机创建与销毁，虚拟机调度等操作仍由 VMM 控制，但 VMM 不能读取虚拟机 CPU、内存、磁盘数据。

如图 6a 所示，在传统虚拟化（traditional virtualization）中，VMM 运行在最高级特权层，处于主机模式（host mode），虚拟机运行于客户模式（guest mode）。CPU 硬件辅助虚拟技术包括两类转换，即 VM 进入（VM_ENTRY）与 VM 退出（VM_EXIT），VM_ENTRY 即 VMM 切换到虚拟机的转换过程，VM_EXIT 即从虚拟机返回 VMM. 当虚拟机用户层（user）需要系统调用时，虚拟机内核层（kernel）调用 VM_EXIT，切换到 VMM，处理之后调用 VM_ENTRY，返回虚拟机。而如图 6b 所示，CloudVisor 嵌套虚拟化（nested virtualization with CloudVisor）运行在最高级特权层，VMM 和虚拟机被放置在用户层。特权操作执行流程如下：

1）当虚拟机执行特权事件时，CloudVisor 截获每一个 VM_EXIT 事件，进行验证；

2）CloudVisor 保存 CPU 上下文，分析 I/O 指令，将 VM_EXIT 转发给 VMM；

3）CloudVisor 从 VMM 拦截 VM_ENTRY，进行验证；

4）恢复 CPU 上下文，恢复相应虚拟机的执行。

CloudVisor 通过干预 VMM 与虚拟机之间的所有控制转移事件，实现嵌套虚拟化透明介入；干预从虚拟机内存物理地址到主机内存物理地址的地址转换，实现基于虚拟机的内存所有权追踪；VM 在使用磁盘 I/O 时透明地加密解密数据，实现 I/O 保护。但 CloudVisor 需要依赖安全硬件保证其安全，并且需

要修改 VMM，故存在兼容性问题。

overshaw[17]和 inktag[18]在虚拟机操作系统被恶意利用的情况下，在虚拟机底层引入更高权限的 VMM，截获并验证虚拟机对底层硬件操作和系统调用，保护虚拟机内敏感应用程序的安全执行。但在有特权层频繁切换的情况下，如虚拟机内进行频繁的 I/O 操作，此类方式会造成较大的性能损耗。

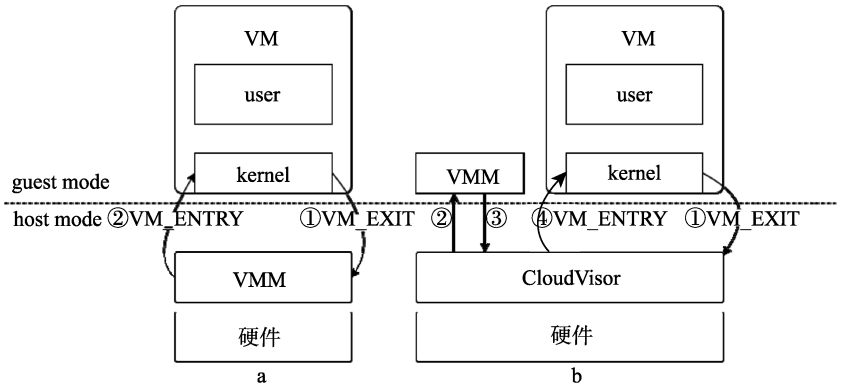


图 6 传统虚拟化（a）与 CloudVisor 嵌套虚拟化（b）

Fig. 6 Traditional virtualization (a) and nested virtualization with CloudVisor (b)

3 系统设计与实现

基于对 OpenStack、VMware vSphere 的特权行为统计与分析，设计并实现了云平台特权行为管控与审计系统。系统的设计目标是基于对云平台的管理权限细粒度划分，无缝对接 OpenStack、VMware vSphere 等当前主流云平台，实现管理员特权行为的动态管控与审计。

1）云平台管理权限细粒度划分

根据云管理员不同职责，如服务器管理员、云平台管理员、虚拟机镜像管理员、项目管理员、虚拟机用户，使用基于角色的访问控制（role-based access control，RBAC）[19]的方式，预先给不同角色划分不同权限。

2）无缝对接云平台

对于当前已部署使用的云平台，无须修改 VMM 和管理工具，无须云平台配合，实现与现有云平台的快速集成与部署，不改变管理员与用户的使用习惯。

3）特权行为动态管控与审计

实现云平台运行时云管理员执行危险操作的截获、动态授权、执行的工作流程，并提供云管理员全部操作的审计日志。

云平台特权行为管控与审计系统架构如图 7 所示。云管理员操作云平台，发送操作请求。系统截获该云管理员操作，并解析该请求协议中的 URL/API，之后添加云管理员操作记录，包括操作者、操作时间、操作对象、具体操作，形成完整的云操作记录。验证特权模块收到解析出的 URL/API，查询权限数据库。权限数据库返回该用户的权限划分策略。验证特权模块根据返回结果验证该用户操作类别（正常操作、拦截操作、动态复核操作），并将验证结果记录日志。根据验证结果不同，数据转发模块转发正常操作请求给云平台，拦截危险操作请求，转发动态复核操作请求给上级管理员审批。上级管理员根据具体情况同意或拒绝该操作。若同意，操作请求发送给云平台。数据转发模块接收云平台操作回执，数据转发模块将操作回执转发给云管理员。

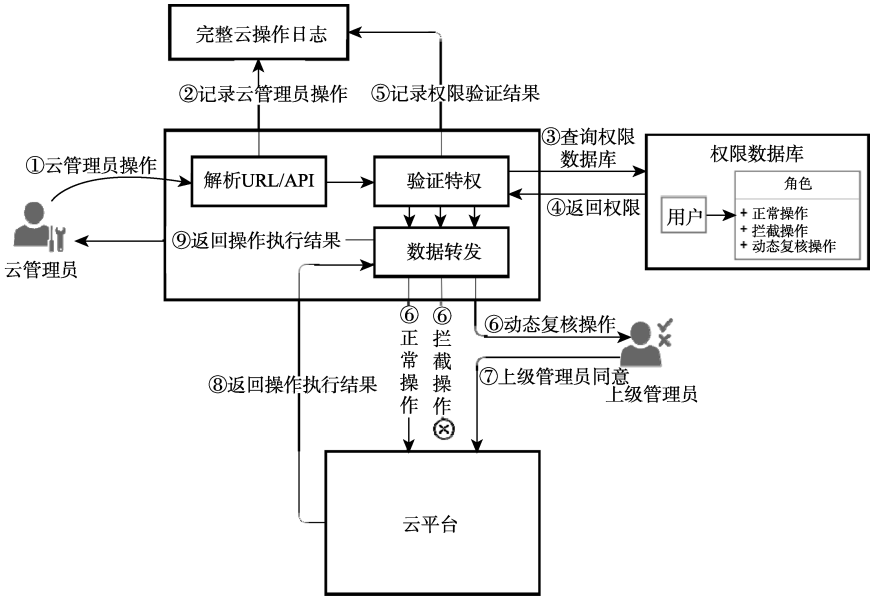


图 7 云平台特权行为管控与审计系统架构

Fig. 7 Architecture of cloud platform privileges control and audit system

4 实验

对云平台特权行为管控与审计系统进行功能评估与性能评估。功能评估主要测试系统适配的 OpenStack、VMware vSphere 两类云平台的功能实现；性能评估主要测试系统对响应用户操作的性能损耗。系统部署硬件环境配置英特尔至强 E3-1220 3.0 GHz CPU 8 核，8 G 内存，1 TB 磁盘，带宽 5 Mbit/s. 实验采取对照的方法，实验组将云平台与系统集成部署，对照组无系统集成。

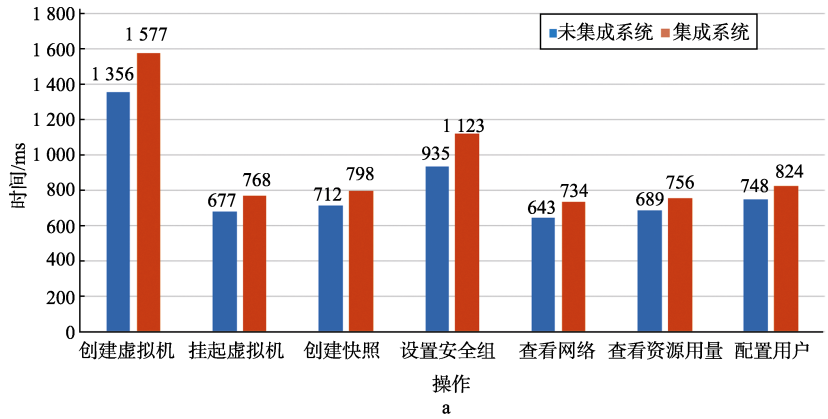
如表 2 所示，针对 OpenStack、VMware vSphere 云平台，系统实现两类云平台细粒度权限划分、无缝适配、特权管控与日志审计功能。

表 2 功能测试结果

Tab. 2 Results of the functional test

云平台	细粒度权限划分	无缝适配	特权管控	日志审计
OpenStack	√	√	√	√
VMware vSphere	√	√	√	√

性能评估测试管理员正常操作的响应时间损耗。不考虑拦截操作、动态授权操作，这两类操作因控制逻辑导致不再连贯，数据不能体现性能影响。实验挑选 OpenStack、VMware vSphere 典型操作，结果如图 8 所示，引入系统仅引起正常操作响应时间 15%～20%的损失。这种性能损失保持在毫秒级，对用户操作的流畅性影响较小。



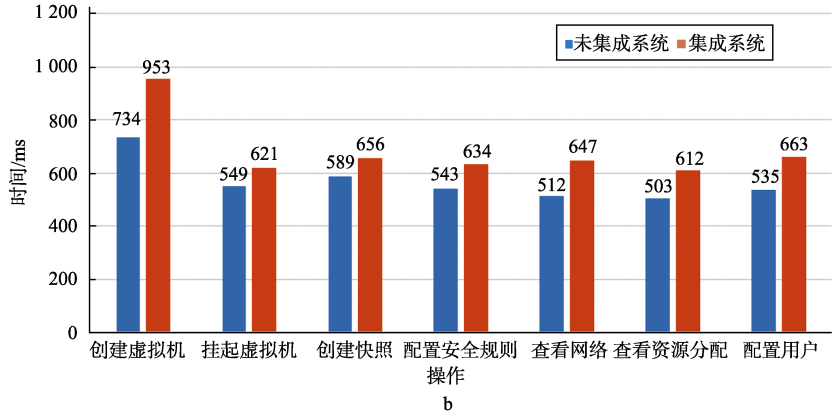


图 8 OpenStack（a）、VMware vSphere（b）云平台性能测试结果

Fig. 8 Results of performance tests on OpenStack (a) and VMware vSphere (b) cloud platforms

5 结论

本文通过对云平台的攻击实例证实并分析了云平台特权威胁。梳理了国内外相关研究文献，总结出云平台管理权限划分和云平台运行时验证两类主要技术路线。为提高以上两类技术路线的可操作性和适用性，本文研究并实现了可无缝适配云平台的云平台特权行为管控与审计系统，可与现有云平台快速集成，实施特权管控与日志审计。但由于要管控审计不同云平台，需深入分析云平台特权行为，并与云平台编程接口对接，存在较多的适配工作量。

[参考文献] (References)

[1] CLAYCOMB W R, NICOLL A. Insider threats to cloud computing: directions for new research challenges[C]//Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual. Izmir: IEEE, 2012: 387-394.

[2] ALLIANCE C S. The treacherous twelve' cloud computing top threats in 2016[R/OL]. Cloud Security Alliance, 2016[2016-02-29]. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

[3] CAPPELLI D M, MOORE A P, TRZECIAK R F. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes[M]. New Jersey: Addison-Wesley Professional, 2012.

[4] CAPPELLI D M, MOORE A P, TRZECIAK R F, et al. Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1[R]. Pennsylvania: Carnegie Mellon University, 2009.

[5] SILOWASH G, CAPPELLI D, MOORE A, et al. Common sense guide to mitigating insider threats[R]. Pennsylvania: Carnegie Mellon University, 2012.

[6] MCCLIMANS F, FERSHT P, SNOWDON J, et al. The state of cybersecurity and digital trust 2016[R/OL]. Accenture and HfS Research Ltd., 2016[2016-07-04]. https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf.

[7] 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.
LIU C Y, WANG G F, LIN J, et al. Practical construction and audit for trusted cloud execution environment[J]. Chinese Journal of Computers, 2016, 39(2): 339-350. (in Chinese)

[8] JACKSON K, BUNCH C, SIGLER E. OpenStack cloud computing cookbook[M]. Southport: Packt Publishing, 2015.

[9] LOWE S. Mastering vmware vsphere 5[M]. Alameda: SYBEX Inc., 2011.

[10] BARTHOLOMEW D. Qemu: a multihost multitarget emulator[J]. Linux Journal, 2006, 2006(145): 68-71.

[11] KIVITY A, KAMAY Y, LAOR D, et al. kvm: the Linux virtual machine monitor[J]. Proceedings of the Linux Symposium,

2007, 1: 225-230.

[12] BARHAM P, DRAGOVIC B, FRASER K, et al. Xen and the art of virtualization[J]. ACM SIGOPS Operating Systems Review, 2003, 37(5): 164-177.

[13] GARFINKEL T, ROSENBLUM M. A virtual machine introspection based architecture for intrusion detection[J]. Proceedings of the Network & Distributed Systems Security Symposium, 2003, 3: 191-206.

[14] GRAZIANO M, LANZI A, BALZAROTTI D. Hypervisor memory forensics[C]//16th International Workshop on Recent Advances in Intrusion Detection. Heidelberg: Springer Berlin Heidelberg, 2013: 21-40.

[15] BUTT S, LAGAR-CAVILLA H A, SRIVASTAVA A, et al. Self-service cloud computing[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security. Alexandria: ACM, 2012: 253-264.

[16] ZHANG F, CHEN J, CHEN H, et al. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization[C]//Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. Cascais: ACM, 2011: 203-216.

[17] CHEN X, GARFINKEL T, LEWIS E C, et al. Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems[J]. ACM Sigarch Computer Architecture News, 2008, 36(1): 2-13.

[18] HOFMANN O S, KIM S, DUNN A M, et al. Inktag: secure applications on an untrusted operating system[C]//Asplos International Conference on Architectural Support for Programming Languages & Operating Systems. Houston: ASPLOS Proc., 2013: 253-264.

[19] FERRAIOLO D, CUGINI J, KUHN D R. Role-based access control (RBAC): features and motivations[C]//Proceedings of 11th Annual Computer Security Application Conference. Michigan: IEEE Computer Society Press, 1995: 241-248.