专题:信息安全

云计算虚拟化安全技术研究

王笑帝[1],张云勇[1],刘　镝[1],张　尼[1],于一鸣[2]
(1.中国联合网络通信有限公司研究院　北京 100032;
2. 北京邮电大学　北京　100876)

摘　要:近年来,伴随云计算服务的发展和普及,其安全问题也逐渐凸显。而其中的虚拟化安全则是云服务商和安全厂商关注的重点。梳理了云计算虚拟化环境中主要面临的安全威胁,提出了云计算虚拟化安全技术架构,包含基于 KVM 的虚拟化安全技术框架和虚拟化集中管控平台两个部分,并依照技术架构开发了"沃云"安全管理平台原型系统,对云计算虚拟化安全技术架构进行了理论验证。

关键词:云计算;虚拟化安全;KVM
doi: 10.11959/j.issn.1000-0801.2015154

Research on Security of Virtualization on Cloud Computing

Wang Xiaodi[1], Zhang Yunyong[1], Liu Di[1], Zhang Ni[1], Yu Yiming[2]
(1. Research Institute of China United Network Communications Group Co., Ltd., Beijing 100032, China;
2. Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In recent years, followed by developing and popularizing of cloud computing service, the security problems appear. One of the problems, virtualization security, draws most attention of cloud services providers and security manufacturers. The main security threats of cloud computing virtualization environment were combed and cloud computing virtualization security technology architecture which contains virtualization security technology framework based on KVM and virtualization centralized management and control platform was proposed. Also Wo-Cloud security management platform prototype system was developed according to technical architecture, and theoretical verification for cloud computing virtualization security technology architecture was carried out.

Key words: cloud computing, virtualization security, kernel-based virtual machine

1　引言

云计算对于如今的生活具有重要意义。它不仅有效提升了数据中心基础资源的使用率，还为传统 IDC(internet data center)的商业模式带来了巨大的改变。云计算已经成为信息通信技术行业中最热的话题之一,所有人都期待看到这个新市场的发展潜力。但是随着全球云计算规模的扩大、用户数的增加,云中信息的价值也越来越受到黑客的"关注",仅在 2014 年内就有大量云安全事件发生,给 CSP(云服务提供商)和用户带来了极大的损失。

2014 年 1 月,由于操作系统更新时升级脚本中的一个小错误,导致云存储公司 Dropbox 核心服务宕机近 48 h。

收稿日期:2015-01-28;**修回日期**:2015-06-13

论文引用格式:王笑帝,张云勇,刘镝等. 云计算虚拟化安全技术研究. 电信科学,2015154
Wang X D, Zhang Y Y, Liu D, *et al*. Research on security of virtualization on cloud computing. Telecommunications Science, 2015154

2月,提供防御分布式拒绝服务(DDoS)攻击服务的云计算公司 Cloudflare 遭遇了史上攻击流量最大的 DDoS 攻击,峰值流量超过 400 Gbit/s。6 月,提供代码托管服务的 Code Spaces 被黑客窃取了其亚马逊云计算服务控制面板的权限并被随机删除其中的大量文件,从而直接导致了公司的倒闭。9 月,iCloud 因其漏洞遭到“针对用户名、密码和安全问题的定向攻击”,导致好莱坞百名女星存放在云中的私密照片被泄露,引发了人们对于 iCloud 在隐私方面的担忧。11 月,Xen 开源管理程序中的一个安全漏洞导致包括 AWS(Amazon Web Services)、Rackspace 和 SoftLayer 等多个公有云服务商被迫紧急重启,中断了很多客户的业务运营。

在“云计算”快速推进、广泛普及的同时,有必要对云安全技术进行研究,在云中引入更强大的安全措施,否则,云中的特性以及云提供的服务不仅无法控制,还将对国家、企业、用户带来严重的安全威胁。

2 云计算虚拟化安全威胁

虚拟化是云计算的核心技术,也是区别于传统计算模式的重要特征。通过对物理资源的虚拟化,不但利用率得到提升,还使资源具有动态性,可以根据用户需求分配,为用户提供弹性的计算资源。但是,虚拟化带来众多性能优势的同时也产生了更多的安全问题,传统的安全防护手段已经不能满足云计算的需求,云计算虚拟化安全已经成为 CSP 和安全厂商关注的焦点。

虚拟化环境中面临的主要安全威胁如下。

(1)虚拟机之间流量不可视

在虚拟化环境中,每台物理机上都承载着多台虚拟机,虚拟机之间通过虚拟化平台提供的虚拟交换机(vSwitch)通信,例如 OpenStack 提供的 Open vSwitch。同一个 vSwitch 上的虚拟机可以相互通信,如果这些虚拟机不属于同一用户,则可能会造成数据泄露或相互攻击。并且传统的防护手段位于物理主机的边缘,如果一台物理机中的多台虚拟机发生通信,这部分流量将无法被外部安全设备监控和保护。

(2)虚拟机之间共享资源竞争与冲突

在虚拟化环境中,由于多台虚拟机共享同一物理机资源,所以会造成资源竞争。如果不能通过正确配置限制单一虚拟机的可用资源,则可能造成个别虚拟机的恶意资源占用,从而导致其他虚拟机拒绝服务。另一方面,如果同一物理机上的虚拟机同时进行病毒扫描等大量占用物理资源的动作,当物理机资源耗尽时就会造成宕机,致使虚拟机业务中断。

(3)云平台对虚拟机的控制

由于虚拟机完全受到云平台的控制,况且通常同一个云平台中管理着单个节点中的所有虚拟机,所以云平台自身的安全就显得尤为重要。如果云平台组件遭到篡改或者病毒感染,轻则云服务的运营受到影响,重则导致用户数据泄露,虚拟机资源被非法用户控制。

(4)云数据安全存在风险

首先,大量用户数据集中存储,容易吸引黑客大规模攻击;其次,多租户共享存储资源,且用户数据和系统数据共存,无法对重要数据进行特殊处理,如果对不同用户的存储数据隔离不当,则会存在数据泄露风险;最后,虚拟机数据大多以明文存储,如果一旦遭到入侵,由于虚拟机间部分流量不可视且缺乏流量行为审计,黑客可以轻易将数据转到其他虚拟机或外部服务器,用户很难发现数据被盗。

(5)云计算管理权限问题

由于在传统的 IDC 机房中,用户直接租用服务器或机柜,服务器权限大多由用户自己管理,而管理员大多只负责机房网络环境、物理机状态维护等。在云计算环境中,用户失去了对物理机的控制,而管理员则拥有更高权限,极有可能因为管理员故意或无意的操作导致用户服务的终止,甚至数据丢失。

3 云计算虚拟化安全技术架构

随着云计算的发展,虚拟化作为云计算的典型特征也同样发展迅速。Red Hat、Cisco、VMware、Microsoft 等诸多厂商都已涉足虚拟化领域并开发其自主的虚拟化产品——KVM(kernel-based virtual machine,基于内核的虚拟机)、XEN、VMware 和 Hyper-V。在开源阵营中,KVM 由于其性能、可扩展性上的优势更受到 CSP 的欢迎,并且已作为组成部分集成至 RHEL(Red Hat enterprise Linux)、CentOS、Fedora、Ubuntu 等主流 Linux 发行版,使得 KVM 能够更加充分地利用 Linux 底层资源,从而更好地完成云中的虚拟化工作。但作为开源产品的 KVM 在安全性方面必然没有 VMware 等商业化产品考虑得周全,所以当 CSP 使用 KVM 作为其虚拟化技术时,也会带来更多的安全风险,包括漏洞和安全威胁。在虚拟化层面,KVM 缺乏完整的安全机制,较弱的漏洞扫描机制,需要手动升级补丁,Linux 操作系统中 QEMU(QEMU 是一款通用的开源虚拟模拟器,与

KVM 模块配合共同实现虚拟化功能)及 KVM 之间没有安全通信通道,这些弱点都将影响 KVM 的虚拟化安全。在虚拟机层面,没有防病毒方案,较弱的防 DDoS 机制以及欠佳的审计同时也会影响 KVM 虚拟化安全。此外,如何处理虚拟机内的数据丢失及如何合理地监控和管理云中的多个虚拟化环境也是亟待解决的问题。

3.1 基于 KVM 的虚拟化安全技术框架

为了解决 KVM 虚拟化安全问题,其虚拟化层和虚拟机的安全问题是需要首先讨论的。当前 KVM 已经被 RHEL、CentOS 等作为内核集成至 Linux 操作系统中。KVM 的虚拟化功能是由 Linux 中的 QEMU 和 KVM 模块共同实现的。KVM 模块负责调用宿主机硬件资源,包括 CPU、内存、存储和网络等,为虚拟机提供资源分配。基于 KVM 的虚拟化安全技术框架如图 1 所示。

(1)QEMU 与 Libvirt 间的通信安全

尽管 Libvirt 是 Linux 操作系统中管理 Hyper-V 层的重要 API,但若操作系统中存在漏洞,则可能导致 KVM(QEMU)与 Libvirt 间的通信被窃听甚至被拦截。及时更新操作系统补丁或者在 Linux 操作系统内部信道部署加密算法,这样就可以保证 KVM 与 Libvirt 间的通信安全。

(2)QEMU 模块安全

QEMU 作为重要的虚拟化模块,如果存在漏洞被黑客利用,很可能直接导致所有虚拟机实例被控制,不但用户数据会被泄露,这些虚拟机还可能被黑客利用作为攻击工具,届时将对 CSP 造成极大的影响。所以 QEMU 模块的安全补丁应当定期及时更新。

(3)QEMU 与 KVM 模块间的通信安全

位于用户空间内的 QEMU 模块与位于内核空间内的 KVM 模块共同协作完成所有的虚拟化操作。黑客可能通过内部信道的漏洞干扰 KVM 模块的正常运行。所以,增加两模块间的安全通道或安全机制是非常有必要的。

(4)KVM 模块安全

若 KVM 模块出现漏洞,黑客就能够直接调用 CPU、内存或网络等主机上的物理资源,这将会影响整个云服务的正常运行。所以应该考虑为 KVM 模块增加安全机制。

(5)虚拟机完整性检查

如果虚拟机操作系统文件被篡改,不但无法保证虚拟机内的数据安全,还可能被黑客获取操作系统权限沦为“肉机”,攻击其他虚拟机或外部服务器,对 CSP 造成极大影响。所以有必要通过定期检查系统文件散列值等方式保证虚拟机系统文件的完整性。

(6)虚拟机数据保护

如何保护虚拟机内的数据安全是业界的重点研究问题之一。可以考虑利用 Linux 自有安全机制 SELinux(security-enhanced Linux)中的虚拟化实例 sVirt,其为虚拟机提供的沙箱机制可以隔离不同的应用,防止各种应用间相互访问导致的数据泄露情况出现,也可以考虑增加应用间访问控制机制,或者对虚拟机数据进行全部或选择性加密。

(7)虚拟机网络安全

为了保护虚拟机不被外部服务器、其他虚拟机攻击或者病毒入侵,需要在服务器内部部署或将单独虚拟机作为可动态分配资源的虚拟化防火墙,通过流量重定向或流量复制等手段将发送到目标虚拟机的流量转发或复制到所属虚拟化防火墙进行流量分析,从而保证进入虚拟机流量的安全性。

3.2 虚拟化集中管控平台

当然,仅仅以虚拟机个体角度来考虑云计算虚拟化安

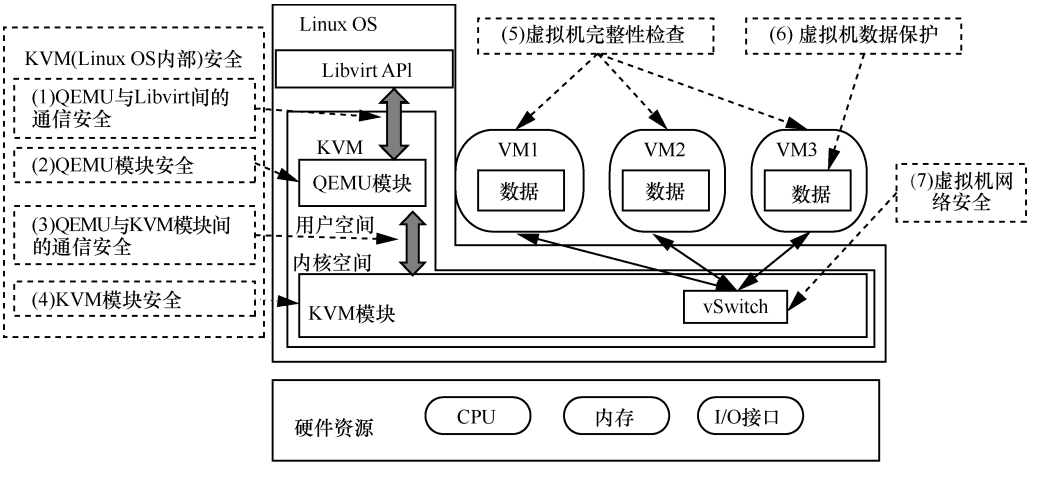


图 1 基于 KVM 的虚拟化安全技术框架

全是远远不够的，如果云平台的安全出现问题，则会导致大范围虚拟机故障，直接影响云的运营。同时，由于每台虚拟机或者云服务器都需要部署相应的安全组件，如果都依赖于运维人员手动配置，不但无法保证安全措施部署和更新的及时性，也大大增加了 CSP 的运维成本。所以 CSP 需要虚拟化集中管控平台来统一管理所有的虚拟机和安全组件，应当包括的功能如图 2 所示。

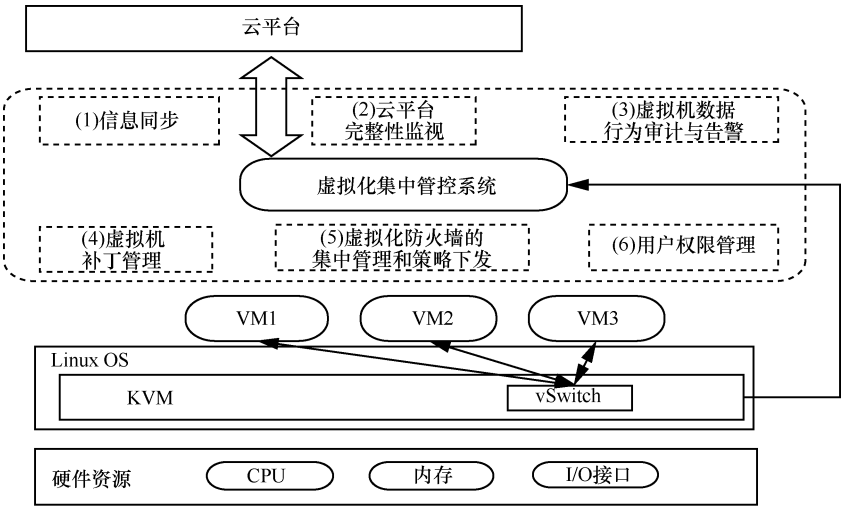


图 2　虚拟化集中管控平台框架

(1)信息同步功能

虚拟化集中管控平台应该定时或按需自动同步虚拟化防火墙和云平台信息，为其他组件提供云平台、虚拟机的信息及状态变化，及时了解云平台健康状况和虚拟化防火墙的状态。

(2)云平台完整性监视

如果云平台组件被他人恶意篡改，则有可能造成云平台的不稳定甚至数据泄露，所以保障云平台的完整性对于 CSP 来说至关重要。可以通过云平台信息及状态对其完整性进行监控，及时发现系统平台、组件的变化并通知管理员，从而保证云平台的正常运行。

(3)虚拟机数据行为审计与告警

虚拟化防火墙可以保证单台虚拟机流量的安全性，但虚拟机的数据异常行为则无法判断，这时就需要虚拟化集中管控平台通过对虚拟化防火墙上传的流量日志进行审计，发现其中的流量异常，并向运维人员进行告警，保证用户信息不被其他未授权虚拟机或外部服务器窃取。

(4)虚拟机补丁管理

为了修补虚拟机操作系统的漏洞，虚拟化集中管控平台应当包含补丁管理功能，将运维人员测试过的系统补丁根据预先设置的策略在适当时间下发，在尽量不影响业务运营的同时完成补丁更新，降低系统漏洞所带来的安全风险。

(5)虚拟化防火墙的集中管理和策略下发

随着云规模的增大，如何对云平台中的虚拟化防火墙进行管理就成了 CSP 必须要解决的问题。虚拟化集中管控平台可以通过信息同步数据获取云平台中所有虚拟化防火墙信息，使运维人员能够通过 Web 界面对其状态进行监控，及时发现虚拟化防火墙的状态异常，并且能够支持策略配置及策略的集中下发，同时对迁移的虚拟机进行虚拟化防火墙迁移或安全策略迁移，从而降低 CSP 的运维成本。

(6)用户权限管理

由于云计算的多租户特性，为了避免用户间越权访问，需要对用户的权限进行管理。应该将用户划分为多种身份并为其分配权限，保证用户只能访问其所属的虚拟机，并根据用户需求对其子用户权限进行配置，而管理员虽然可以管理、监控所有虚拟机，但是没有权限访问用户的虚拟机。同时通过云平台同步信息对用户访问行为进行审计并对越权行为进行告警，保证用户虚拟机不被他人控制。

4　“沃云”虚拟化安全技术验证

根据第 3 节提出的云计算虚拟化安全技术架构，对该架构进行了技术验证，并开发了“沃云”安全管理平台原型系统。“沃云”安全管理平台可以全面监控虚拟化网络通信，包括虚拟化平台内外通信以及虚拟机间通信、集中监控虚拟化环境的威胁，实现统一配置，集中管控。

“沃云”安全管理平台原型系统由“沃云”安全管理平台、安全代理、虚拟化安全网关、虚拟化平台接入引擎模块共同组成，如图 3 所示，各模块具体介绍如下。

- “沃云”安全管理平台。集中管理虚拟机的安全策略，并实现安全策略的迁移功能。依靠在客户系统内安装的安全代理，收集客户系统的日志信息，进行脆弱性检查、权限控制等。

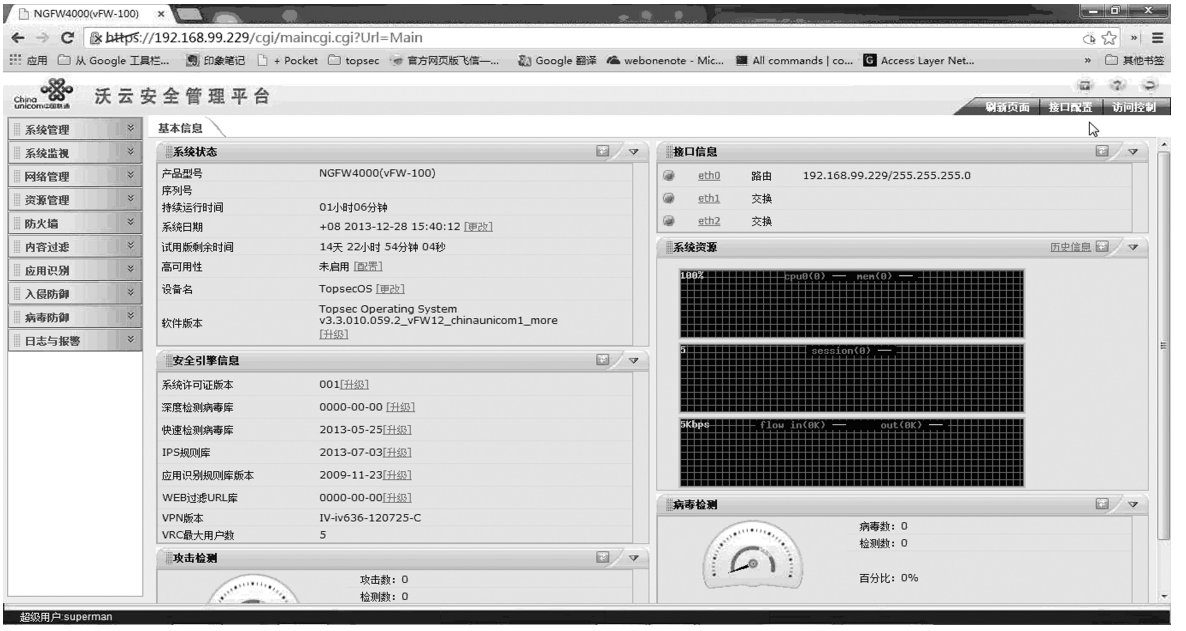


图 3 “沃云”安全管理平台原型系统

- 安全代理。安装在客户操作系统,负责收集客户系统的日志信息,对脆弱性进行检查,同时实现对外设的权限控制等功能。
- 虚拟化安全网关。以虚拟机形式部署在虚拟化平台上,实现虚拟机防护的所有安全功能,同时通过虚拟化平台接入引擎获得虚拟化平台的网络通信数据,保障所有虚拟机之间以及虚拟化平台本身的网络通信安全。
- 虚拟化平台接入引擎。将网络数据重定向至虚拟化安全网关进行安全监测，并对虚拟化平台自身系统进行安全加固以及基于 Hyper-V 层的权限控制,例如虚拟机外设控制、虚拟机操作权限控制等。

5 结束语

本文分析了云计算虚拟化环境中面临的安全威胁,包括虚拟机之间流量不可视、虚拟机之间共享资源竞争与冲突、云平台对虚拟机的控制、云数据安全存在风险、云计算管理权限问题。为解决以上安全问题,提出了云计算虚拟化安全技术架构,其中包含两个组成部分:基于 KVM 的虚拟化安全技术框架负责保护 KVM 虚拟机内部和对外的通信安全、虚拟机各模块及整体安全、虚拟机数据安全;虚拟化集中管控平台负责对云平台及所有虚拟机的安全进行统一管理，同时负责管理虚拟化防火墙和用户权限。同时,根据以上技术架构开发了沃云安全管理平台原型系统,对云计算虚拟化安全技术架构进行了理论验证。

参考文献

1 张尼,刘镝,张云勇等. 云计算安全技术与应用. 北京:人民邮电出版,2014
Zhang N, Liu D, Zhang Y Y, *et al*. Cloud Computing Security Technology and Practice. Beijing: Posts & Telecom Press, 2014

2 刘鹏. 云计算(第 2 版). 北京:电子工业出版社,2011
Liu P. Cloud Computing (Second Edition). Beijing: Publishing House of Electronics Industry, 2011

3 中国电信网络安全实验室. 云计算安全：技术与应用. 北京:电子工业出版社,2012
China Telecom Network Security Laboratory. Cloud Computing Security: Technology and Practice. Beijing: Publishing House of Electronics Industry, 2012

4 汪来富，沈军，金华敏. 云计算应用安全研究. 电信科学,2010,26(6): 67~70
Wang L F, Shen J, Jin H M. Research on cloud computing security. Telecommunications Science, 2010,26(6): 67~70

5 李玮. 云计算安全问题研究与探讨. 电信工程技术与标准化,2012(4): 44~49
Li W. Study and exploration on cloud computing security. Telecom Engineering Technics and Standardization, 2012(4): 44~49

6 房晶，吴昊，白松林. 云计算的虚拟化安全问题. 电信科学,2012, 28(4):135~140

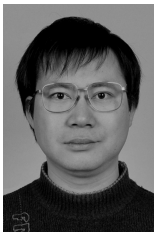
(2015154-6 接排在 2015157-6 后)

2 Global Platform. Global platform card secure element configuration V1.0. http://www.globalplatform.org/specificationscard.asp, 2015
3 Global Platform. Global platform device technology secure element access control V1.0. http://www.globalplatform.org/specificationdownload.asp?id=7768, 2013
4 刘知贵. 基于 PKI 技术的数字签名身份认证系统. 计算机应用研究, 2004(9)
Liu Z G. The system of digital signature authentication based on PKI. Application Research of Computers, 2004(9)
5 开放移动接口 V2.0. http://simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI3_1_.pdf/,2015
Open mobile API specification V2.0. http://simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI3_1_.pdf/, 2015

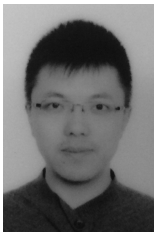
[作者简介]

胡博，男，中国联合网络通信有限公司研究院终端与测试实验室工程师，主要研究方向为智能卡、智能终端、移动互联网应用等。

严斌峰，男，博士，中国联合网络通信有限公司研究院终端与测试实验室主任，主要研究方向为移动终端、智能卡、终端数据等。



仇剑书，男，中国联合网络通信有限公司研究院终端与测试实验室高级工程师，主要研究方向为智能卡、移动互联网应用、移动终端等。



董双赫，男，中国联合网络通信有限公司研究院终端与测试实验室工程师，主要研究方向为智能卡、智能终端、移动互联网应用等。

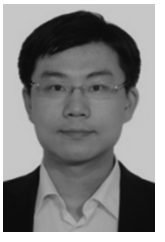
(上接 2015154-5)

Fang J, Wu H, Bai S L. Virtualization security issues in cloud computing. Telecommunications Science, 2012,28(4):135~140
7 沈余锋, 余小军. 云计算环境下虚拟化安全探讨. 电力信息与通信技术, 2013(11): 6~11
Shen Y F, Yu X J. Study of virtualization security in cloud computing. Electric Power Information and Communication Technology, 2013(11): 6~11
8 余秦勇, 童斌, 陈林. 虚拟化安全综述. 信息安全与通信保密, 2012(11):41~46
Yu Q Y, Tong B, Chen L. Overeview virtualized security. Information Security and Communications Privacy, 2012 (11): 41~46

[作者简介]

王笑帝，男，中国联合网络通信有限公司研究院云计算实验室工程师，主要研究方向为信息安全、云计算安全等。

张云勇，男，博士后，中国联合网络通信有限公司研究院副院长，中国通信学会、电子学会、计算机学会高级会员，主要研究方向为下一代开放网络、移动互联网及业务、云计算、智能终端等。



刘镝，男，博士后，中国联合网络通信有限公司研究院云计算实验室工程师，主要研究方向为认证安全、云计算、终端安全等。

张尼，男，博士后，中国联合网络通信有限公司研究院云计算实验室高级工程师，主要从事移动互联网安全、云计算安全、信息安全等领域研发工作。

于一鸣，男，北京邮电大学在读。