虚拟机系统安全综述*

秦中元[1,2]，沈日胜[1]，张群芳[3a]，狄予兴[3b]
(1. 东南大学 信息科学与工程学院，南京 210096；2. 信息网络安全公安部重点实验室，上海 201204；3. 南京炮兵学院 a. 计算机教研室；b. 通信教研室，南京 211132)

摘　要： 随着云计算的广泛应用，虚拟机技术得到了复苏和长足的发展，但同时也带来了新的安全威胁，因此对于虚拟机的安全威胁和防御的研究成为目前计算机安全界的研究热点。以目前广泛应用的虚拟机 Xen 为例，针对虚拟机的技术特征分析了所存在的漏洞和威胁，并从计算机安全学的角度提出了相应的防御和保护方法。较为全面地总结了目前国内外针对虚拟机安全各方面相关的研究成果，通过系统的比较分析，指出了目前存在的问题，探讨了下一步的研究方向。

关键词： 虚拟机；Xen；安全；防御
中图分类号： TP309　　**文献标志码：** A　　**文章编号：** 1001-3695(2012)05-1618-05
doi:10.3969/j.issn.1001-3695.2012.05.004

Survey on virtual machine system security

QIN Zhong-yuan[1,2], SHEN Ri-sheng[1], ZHANG Qun-fang[3a], DI Yu-xing[3b]
(1. *School of Information Science & Engineering*, *Southeast University*, *Nanjing* 210096, *China*; 2. *Key Laboratory of Information Network Security for Ministry of Public Security*, *Shanghai* 201204, *China*; 3. *a. Computer Department*, *b. Communication Department*, *Nanjing Institute of Artillery Corps*, *Nanjing* 211132, *China*)

Abstract: With the widely spread of cloud computing, virtual machine technology revives and gets rapid development, meanwhile, new threats are also introduced. Researches on the threats and defenses of virtual machines have become a hot topic. This paper firstly analyzed the vulnerabilities and threats of virtual machines, taking Xen as an example. Secondly, it introduced the defense and protect methods which put forward to improve the security. Furthermore, it reviewed the state-of-the-art methods on the virtual machine security. Finally the paper discussed the existed problems and presented future directions.
Key words: virtual machine; Xen; security; defense

虚拟化技术最早起源于 20 世纪 60 年代，是计算领域的一项传统技术，虚拟化技术支持在一个单一的服务器之上运行多个操作系统的服务器。虚拟机技术是虚拟化技术在计算机上的一种体现，通过内存、CPU、网络等虚拟化技术实现资源的隔离和可靠利用。目前有很多流行的虚拟机，如 VMware、KVM、Xen[1,2]，通过研究分析对比，开源的 Xen 虚拟机在性能上十分优越，被认为是未来最有前途的虚拟化解决方案之一[3]。

虚拟化技术作为云计算的关键核心技术，使得云计算成为能够提供动态资源池、虚拟化和高可用性的下一代计算平台[4]，给企业和用户带来了很多的益处；硬件和资源的共享既节约了开销，也为管理带来了方便，同时也革新了许多传统 IT 技术。然而从安全角度来分析，却又带来了很多威胁，除传统的攻击威胁之外，如隐蔽通道[5]、基于 VM 的 Rootkit 攻击(VMBR)[6]以及新的恶意软件等也随之而来。虚拟化技术作为云计算的核心技术，必须向其用户提供安全性和隔离保证[7]。2009 年，在 IDC 以虚拟化技术为基础的云计算的用户调查中就显示，安全是用户最关心的关键点[8]。

本文从虚拟机系统的原理、架构入手，从虚拟机系统的关键技术如资源隔离、共享等方面研究系统可能存在的安全威胁，然后，根据安全隐患提出理论上的保护方法。在总结前人研究成果的基础上，较为全面地总结了目前国内外针对虚拟机安全各方面相关的研究成果，指出了目前存在的问题，探讨了下一步的研究方向。

1　虚拟机技术

虚拟机技术最早由 IBM 于 20 世纪 60 年代提出，被定义为硬件设备的软件模拟实现，通常的使用模式是分时共享昂贵的大型机。目前，虚拟机中用到的虚拟化技术主要有网络、内存、CPU、硬盘虚拟化技术。在虚拟机环境中，硬件层与虚拟机系统之间存在一层虚拟机监视器(virtual machine monitor, VMM)，是虚拟机的核心层，负责上层虚拟机系统的资源分配和底层交接。

1.1　虚拟机架构

本文将以虚拟机 Xen 为例，介绍虚拟机架构和原理。Xen 是由英国剑桥大学计算机实验室开发的一个开源项目[9]。Xen 主要由两个组成部分，一个是虚拟机监控器 VMM，也叫 Hypervisor。Hypervisor 层在硬件与虚拟机之间，是最先载入到硬件的第一层。在 Xen 中，虚拟机称为 Domain，其中 Domain 0

收稿日期： 2011-09-30；**修回日期：** 2011-11-12　**基金项目：** 信息网络安全公安部重点实验室开放课题(C11605)；江苏省网络与信息安全重点实验室开放课题基金资助项目(BM2003201)

作者简介： 秦中元(1974-)，男，河南安阳人，副教授，博士，主要研究方向为云计算安全(zyqin@seu.edu.cn)；沈日胜(1986-)，男，硕士研究生，主要研究方向为虚拟机安全；张群芳(1981-)，女，助教，硕士，主要研究方向为网络安全；狄予兴(1973-)，男，讲师，硕士，主要研究方向为通信网安全.

扮演着很重要的角色,负责其他虚拟机的控制管理和硬件驱动等,同时 Domain 0 还负责其他 Domain 的数据传递。Xen 的架构如图 1 所示。

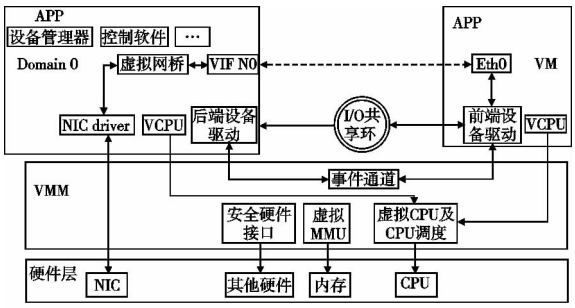


图1　Xen虚拟机架构

在 Xen 虚拟机系统中,在安全级别上分为四个等级(0 ~ 3-ring),VMM 运行在特权模式(0-ring),负责控制资源的隔离、共享、数据处理等,为每个虚拟机虚拟一套独立于实际硬件的虚拟硬件环境(包括处理器、内存、I/O 设备等),并仲裁虚拟机 OS 对底层硬件的访问。

1.2　虚拟机安全特征

将虚拟机架构抽象化,那么虚拟机主要由硬件、VMM、VMs 及 Domain 0 四部分组成。下面将列出这四部分的一些关键特征,以及在安全角度上分析其可能带来的安全影响。

1.2.1　硬件

随着虚拟机技术的广泛应用,目前,很多硬件针对虚拟化技术进行了拓展,如 AMD 和 Intel 相继针对全虚拟化拓展了 AMD-V 和 Intel VT[10] 技术,通过多余的指令集来控制虚拟过程。除此之外,虚拟机技术的硬件特征体现在陷进执行[11] 和可信模块上[12]。

a)陷进。在所有 x86 的硬件平台下,陷进执行是支持虚拟化的重要特征,虚拟域本身并不能直接访问本虚拟域以外的物理资源,但是虚拟域可以通过超级调用(hypercall)向 Hypervisor 申请各种服务,如 MMU 更新、I/O 处理、对虚拟域的管理等。

b)可信模块。它是可选硬件特征,目前可信计算已成为了安全工具的一部分,而通过可信计算来确保 VMM 代码上的完整性也是保护虚拟机系统的重要方法之一。

1.2.2　虚拟机管理器

在虚拟机环境中,VMM 是核心。VMM 可以完成如下一些功能:a)网络管理,配置网络及网络数据包的转发,而 VMM 的这一特征也可以用于数据包过滤,如为上层的安全服务提供入侵检测[13];b)安全日志管理,通过监测,VMMs 能对 VM 的事件行为进行记录,并保存在 VM 的空间外,可以利用这些日志信息对 VM 进行入侵分析[13];c)认证,当 VM 运行时,对 VM 的关键数据和进程进行 hash 存储,当 VM 系统发生数据改变或者进程调用时,可以用于认证依据。这个功能在 VM 完整性保护和可信模块上可以得到很好的利用[14]。

1.2.3　Domain 0

Domain 0 是 VM 的控制域,相当于所有 VMs 中拥有 root 权限的管理员,其他 VM 的创建、启动、挂起等操作都由 Domain 0 控制。除此之外,Domain 0 还具有直接访问硬件的权利,在 Domain 0 中安装了硬件的原始驱动,担任着为 Domain U 提供硬件服务的角色,如网络数据通信(DMA 传输除外)。Domain 0 在接收数据包后,通过虚拟网桥技术,根据虚拟网卡地址将数据包转发到目标虚拟机系统中,因此,拥有 Domian 0 的控制权限就控制了上层所有虚拟机系统,这也致使 Domain 0 成为了攻击者的又一个主要目标。

1.2.4　VM

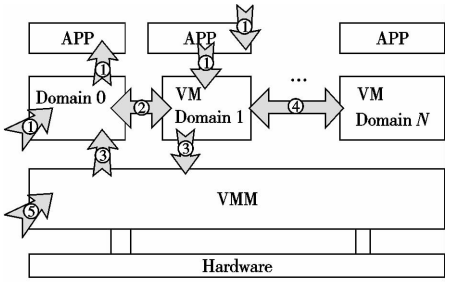
VM 的 OS 运行与传统意义上的操作系统并无两样,但是因为 VMM 的存在,VMM 可以将 VM 当做软件一样进行镜像存储和系统快照,以用于复制、备份、状态保留等。

2　虚拟机安全分析

在前面的章节中系统地介绍了虚拟机的一些关键特征,并且从安全角度进行了分析。本章中将从整个虚拟机的架构上对虚拟机存在的安全威胁进行分析。

2.1　攻击威胁

虚拟机系统比起传统的计算机系统存在更多的攻击点及安全隐患。通过分析,得到虚拟机的攻击模型如图 2 所示,图中箭头表明所受攻击威胁来源。本文只考虑虚拟机系统中存在的安全分析,针对 VM 的传统攻击,诸如病毒攻击和网络攻击等将不再细述。



说明:①—传统攻击 ②—guest到host攻击
③—VM到VMM攻击 ④—VM到VM攻击
⑤—VMM的外部攻击

图2　虚拟机威胁分析

2.1.1　VMM 的外部攻击

目前针对 VMM 的外部攻击主要有两种,一种是基于 VM 的 Rootkit 攻击,另一种是恶意代码攻击。

a)VMBR[15, 16]。攻击者利用 Rootkit 隐藏自己的踪迹,通过保留 root 访问权限,留下后门的程序集。VMBR 的攻击会在 VMM 的启动之前将程序代码写入内存并运行,一旦攻击者得逞,那么所有虚拟机系统都将在攻击者的控制范围之内。目前比较出名的 VMBR 攻击有 Blue pill 等。检测及防御 VMBR 攻击的方法分析如下:(a)通过计时的方法,有一些指令的执行是通过虚拟出来的,所占用的 CPU 周期会比真实的时间长,可以通过这种方法来进行检测;(b)通过可信模块 TPM 来进行 VMM 的保护[17],通过启动过程的完整监测,可以防止 Rootkit 的隐蔽插入,TPM 的设计不但可以抵御 VMBR 的攻击,同时也可以防御其他破坏 VMM 完整性的攻击。

b)恶意代码。攻击者可以利用远程攻击方法,虚拟机系统的远程管理技术大多是用 HTTP/HTTPs 来连接控制的,因此,VMM 必须运行服务器来接受 HTTP 连接。那么攻击者就可以利用 HTTP 的漏洞来进行恶意代码的攻击,如 Xen 的 Xen API HTTP 接口就存在 XSS(cross-sit scripting)漏洞,攻击者可以通过浏览器执行恶意代码脚本。

2.1.2　VM 对 Domain 0 的攻击

Domain 0 具有管理其他 VM 的特权,VM 到 Domain 0 的攻击体现在 guest-to-host 的攻击来获取 host 的特权,而 VM escape[18] 就是这种模式的攻击。VM 通过应用程序,绕过 VMM 的监控而直接访问 Domain 0,从而获取 Domain 0 的特权,而一旦获取到了 Domain 0 的控制权后,就可以控制所有 VM。这些

攻击是利用所发现的 bug 来实施的,如 VMware Workstation 6 CVE-2007-4496[19],通过用户授权,进行内存访问和运行恶意代码。另外,VM 还可以利用共享内存通信方式对 VMM 进行病毒分析。

2.1.3 VM 之间的攻击

VMs 之间的攻击体现在通过共同访问的资源来进行恶意攻击。其中隐蔽通道是一个难以解决的问题,攻击者通过进程、内存共享或内存错误,甚至其他错误信息来进行代码的植入和攻击[15],目前也尚未得到很好的解决。

2.2 其他安全隐患

a)备份、快照及还原漏洞。在虚拟机中,VMM 提供了备份、快照和还原的功能,一旦系统崩溃了,可以通过快照进行还原,这为系统的维护带来了方便且具有实效性。然而这也导致了新的问题发生:(a)这种机制使得 VMs 容易受到新的攻击,因为许多安全攻击是依赖于线性时间的,重新访问以前的系统状态会违反这些协议;(b)还原后,系统以前存在的漏洞会全部出现,可能没有安全补丁,或旧的安全机制(防火墙规则、反病毒签名等),重新激活先前那些封锁的账号和密码,这都带来了很多的安全隐患。

b)DMA 攻击。在虚拟中有一种数据传输不受 VMM 控制,这就是 DMA 传输。VM 通过 Domain 0 与硬件建立 DMA 连接,而后将数据控制权交由 VM 进行数据传输,在数据传输的过程中,数据将直接从网卡传输到目的 VM 中,在大数据量的传输效率上有很大的提高。然而,这也为攻击者提供了方便,攻击者将轻而易举地利用 DMA 方式将恶意代码或者病毒文件等传入没有安全防范的目标机中,从而达到攻击的目的。

3 虚拟机系统研究现状

目前针对虚拟安全的研究可以分为如下几类,如图 3 所示。

a)安全 Hypervisor。在保护 Hypervisor 的同时,保护 VMs 资源隔离性、数据安全性、通信安全性以及代码完整性等。

b)针对专门攻击的防御研究。针对特定攻击,如 VMBR[16]攻击、网络攻击、通信数据保护等。

c)可信计算。以 TPM 为硬件基础,建立可信 Hypervisor、可信安全域或通过可信链确保上层安全。

d)安全应用。如通过入侵检测和蜜罐等技术来进行系统保护。

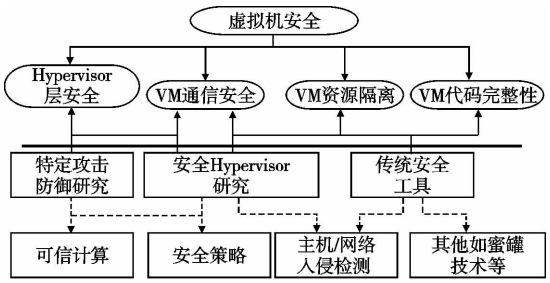


图3 虚拟机安全研究分类

3.1 安全 Hypervisor 研究

Hypervisor 是虚拟机的核心层,而虚拟机的安全研究也是以 Hypervisor 为核心。很多研究人员提出了安全 Hypervisor 的概念,目前针对安全 Hypervisor 的研究较多。

IBM 研究人员 Sailer 等人[20]提出了一种安全的 Hypervisor 架构 sHype,利用安全模型,通过访问控制模块(access control module,ACM)来控制系统进程、内存的访问,实现内部资源安全隔离。sHype 可以实行多种安全模型,但只是针对明确数据流进行限制,而并未过多顾虑隐蔽通道[5]威胁。Sailer 等人[21]在虚拟机 Xen 上进行了 sHype 架构的实现。目前在 Xen 虚拟机上,已经可以配置 ACM 安全模块。

Garfinkel 等人[14]提出了基于虚拟机的可信架构 Terra,利用 TPM 来保护 Hypervisor 的启动,然后通过可信虚拟机监视器对 VM 进行硬件资源隔离。这种设计保证了 Hypervisor 启动的安全,同时可信链的存在可以对系统事件进行认证。但 Terra 的提出只是在理论上进行了研究分析,在实际中还未完成真正的实现,这也是 Terra 架构的一大主要问题。

Wang 等人[18]提出了 HyperSafe 架构,针对代码和控制数据的完整性保护提出了相关的模型研究。文中提到了两种技术:a)Non-bypassable memory lockdown,是一种内存保护技术,通过特殊位 WP 来控制是否能写,除了安全更新之外,其他时间都处于保护状态,保证了执行期间的数据和代码完整性;b)Restricted pointer indexing,通过将控制数据指针限制到一个自己建立的表中进行监控。HyperSafe 能灵活地控制数据流的完整性。

一些研究人员针对当前虚拟机中安全机制的一些漏洞进行了分析和改进,Jansen 等人[22]提出一种 PEV(protection、enforcement、verification)架构,通过加密解封的协议、安全策略等技术进行数据检测和保护,并使用 TPM 建立可信区域来保护关键数据;但是其关键数据是通过数据类型日志形式来保存的,对数据日志项的加/解密势必影响整个虚拟机系统的性能。针对 DMA 攻击, Shinagawa 等人[23]通过先开辟内存缓冲区进行数据检测,然后从缓冲区将安全数据拷贝到目标系统的物理内存区。他们提出了一个 parapass-through architecture 的架构,将很多设备的驱动直接交由客户系统本身,而自身只配置了一个 parapass-through drivers 驱动集,通过在 Hypervisor 中对指令和数据的截取来进行安全监控,从而提高了整个系统的可靠性。

Azab 等人[24]提出了 HyperSentry。当完整性检测模块在激活时,如果 VMM 已经被攻击,那么在激活过程中会擦除以往的攻击痕迹,因此文章提出了一种隐蔽的激活方法,通过外部的 out-of-band 信道 IPMI 来激活,并通过系统管理模块 SMM 来保护基本代码和关键数据的安全性。同时在文献[25]中,他们还提出了一种基于 Hypervisor 的虚拟机系统 VMs 完整性测试代理 HIMA,可以实现客户系统关键事件的动态监视和客户内存的保护,在程序完整性测试上通过对加载到内存的代码和数据段进行哈希计算来确认完整性;在内存保护上,HIMA 通过访问权限限制来保护客户内存,并使用测试虚拟域内存地址的哈希方法来确保页映射中发生的安全问题。Wu 等人[26]研究了基于 Hypervisor 的系统控制和监视机制,利用 Hypervisor 来进行客户系统的安全保护,提出了 BMCS (behavior monitoring and controlling system)的模块来完成系统中的行为监控。Xu 等人[27]提出了一种基于 VMM 的 OS 内核保护模型 UCON,通过基于事件的策略持续而实时地检测系统。

3.2 针对特定攻击的安全研究

随着虚拟机的广泛应用,目前针对虚拟机的漏洞攻击也有很多种,主要体现在 VMBR 攻击[15]、内存错误等隐蔽通道攻击[5,28]、网络攻击等。有很多安全研究人员针对这些攻击进行了研究,并提出了相关的解决方法。

针对 VMBR 的攻击,Rhee 等人[29]利用一些安全策略,通过监视内核的内存访问来防御动态数据内核 Rootkit 攻击,Ri-

ley 等人[30]提出了通过内存影子来检测内核 Rootkit 攻击。Gebhardtd 等人[31]提出了利用可信计算来防御 Hypervisor 的 Rootkit 攻击。

针对虚拟机系统中存在的网络方面的威胁,如拒绝服务攻击(DoS),Lakshmi 等人[32]提出了一种新的 I/O 虚拟架构,为每个 VM 配置一个虚拟网卡,VM 可以通过自身的网卡驱动与虚拟网卡直接进行通信,然后通过 VMM 监视每个 VM 的数据流,在防御诸如 DMA 的无控制漏洞和 DoS 攻击等威胁的同时,也可以提高网络性能。

隐蔽通道是较难解决的安全问题之一,因为存在的隐蔽通道通常是用户和系统不可知的传输通道,如基于 CPU 负载的隐蔽通道[33],攻击者利用 CPU 的负载传输私密数据流,既能很隐蔽地传输数据,又能成功地避免检测。Salaun[5]研究了虚拟机 Xen 上可能存在的隐蔽通道,从 XenStore 的机制、共享协议、驱动加载、数据传输等方面分析了可能存在的隐蔽通道。隐蔽通道的建立和数据传输通常是需要"同伙的存在",即接收者和发送者的存在。Cheng 等人[34]根据这一特征,在 Chinese wall 的安全模型上进行了改进,利用限制冲突集数据传输来防御隐蔽通道。

3.3　可信计算

在前面的介绍中已经提到了,一些研究人员提出用可信计算来保护系统的完整性。Catuogno 等人[35]研究了一个基于 TCB 的可信虚拟域的设计和执行,通过安全策略和 TVD 协议实现可靠性。Berger 等人[36]则通过软件方法设计了基于硬件 TPM 的虚拟 TPM 来保证多个 VM 的可靠性。而 Ruan 等人[37]设计了一个一般的可信虚拟平台架构 GTVP,将控制域分为管理、安全、设备、OS 成员、通信五个域,每个域都完成相应的功能,从而达到了安全、负载均衡和易用等目的。程川[38]提出了一种基于 Xen 的信任虚拟机安全访问机制,为用户提供了一种有效的安全访问敏感数据的模式。其核心思想是利用虚拟机的隔离性,为数据信息应用提供一个专用的隔离环境,同时利用可信计算技术保证该虚拟平台配置状态的可信性。

3.4　安全应用

中间层 VMM 的存在使得一些传统的安全技术能得到更好的利用,因此,一些研究人员利用传统的安全技术如入侵检测技术来提升系统的安全性。Jansen 等人[39]提出了通过虚拟化来提高系统的安全性和独立性。首先在安全主域配置入侵检测系统,通过对客户机的用户命令所获取的信息和内核内存所获取的信息比较来进行入侵分析;然后通过设置保护模块获取客户机系统调用,进行进程等事件管理,实现完整性保护。张志新等人[40]提出了基于 Xen 的入侵检测服务,通过在 VMM 层设置入侵检测系统,使得这个入侵检测系统位于监控所有对操作系统的入侵事件的最佳位置,并处于一个独立于操作系统之外的受保护的空间内,增强了入侵检测系统的独立性和检测能力,是传统的基于主机和网络入侵检测系统优点的完美结合。

3.5　尚存在的问题

通过上文的分析可以发现,在国内外针对虚拟机系统的安全研究已陆续出现很多,针对不同角度的安全研究都存在,从整体分析来说,尚且存在如下一些问题:

a)没有从整体安全上进行设计,只是从单一的一方面进行了研究,如 sHype[20]只是针对明确数据流,没有考虑到隐蔽通道等安全。

b)一些研究设计过于复杂。在实施上存在问题,如 Terra 架构[14],虽然作者的设计理念十分突出,但是至今没能设计出合适的实现平台。

c)忽略了性能的因素。出于安全的考虑,通过策略来进行系统的完整性保护,如 UCON 保护模型[27],但是在 Linux 系统中,由于资源众多,将存在 50 000 种策略状态,那么在实际中将严重影响系统的性能。有些研究人员针对存在的一些系统复杂性进行了改进,如 Payne 等人[41]提出了分层的访问控制模型,在很大程度上简化了访问控制模块中的主客体关系链。

d)忽略了安全模块自身的安全,一旦安全模块自身被攻击,那么相关的安全将得不到保障,如 HIMA[25]、BitVisor[23]。

4　结束语

本文旨在进行虚拟机系统的安全分析,总结目前已有的研究成果,并指出其中存在的问题。首先以虚拟机 Xen 为例,介绍了虚拟机的架构和关键技术,并从安全的角度对虚拟机中的这些特征和存在的漏洞进行了分析,然后系统地介绍了虚拟机环境中存在的攻击模型,分析了目前存在的一些攻击方式,并针对这些攻击方式提出了相应的防御方法。其次还对目前针对虚拟机安全的研究现状进行了概括总结,主要体现在安全 Hypervisor、安全虚拟机架构、特定攻击安全研究、可信计算等几个方面。同时,本文还分析了目前研究存在的一些问题。在后续研究中,笔者将在前人研究的基础上进行安全虚拟机管理器的研究,设计一个安全可靠的虚拟机管理器架构。

参考文献:

[1] BINU A, KUMAR G S. Virtualization techniques: a methodical review of Xen and KVM[C]//Proc of the 1st International Conference on Advances in Computing and Communications. Berlin: Springer-Verlag, 2011: 399-410.

[2] WANG Xi, CHENG Chuan. Access control using trusted virtual machine based on Xen[C]//Proc of International Conference on Applied Informatics and Communication. Berlin: Springer-Verlag, 2011: 94-101.

[3] 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.

[4] 陈康, 郑纬民. 云计算: 系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337-1348.

[5] SALAUN M. Practical overview of a Xen covert channel[J]. Journal in Computer Virology, 2010, 6(4): 317-328.

[6] PRICE M. The paradox of security in virtual environments[J]. Computer, 2008, 41(11): 22-28.

[7] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 22-28.

[8] IDC. New IDC IT cloud services survey: top benefits and challenges [EB/OL]. (2009-11-15). http://blogs.idc.com/ie/?p=730.

[9] BARHAM P, DRAGOVIC B, FRASER S, *et al*. Xen and the art of virtualization[C]//Proc of the 19th ACM Symposium on Operating Systems Principles. New York: ACM Press, 2003: 164-177.

[10] ZHANG Xiao-tao, DONG Yao-zu. Optimizing Xen VMM based on Intel® virtualization technology[C]//Proc of International Conference on Internet Computing in Science and Engineering. Washington DC: IEEE Computer Society, 2008: 367-374.

[11] BRATUS S, LOCASTO M E, RAMASWAMY A, *et al*. Traps, events, emulation, and enforcement: managing the Yin and Yang of virtualiza-

tion-based security[C]//Proc of the 1st ACM Workshop on Virtual Machine Security. New York:ACM Press,2008:49-58.

[12] LIU Dong-xi,LEE J,JANG Ju-lian,*et al*. A cloud architecture of virtual trusted platform modules[C]//Proc of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Washington DC:IEEE Computer Society, 2010:804-811.

[13] ALSHAWABKEH M,MOFFIE M,AZMANDIAN F,*et al*. Effective virtual machine monitor intrusion detection using feature selection on highly imbalanced data[C]//Proc of the 9th International Conference on Machine Learning and Applications. Washington DC:IEEE Computer Society, 2010:823-827.

[14] GARFINKEL T,PFAFF B,CHOW J,*et al*. Terra:a virtual machine-based platform for trusted computing[C]//Proc of the 19th ACM Symposium on Operating Systems Principles. New York:ACM Press, 2003:193-206.

[15] KING S T,CHEN P M,WANG Yi-min,*et al*. SubVirt:implementing malware with virtual machines[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC:IEEE Computer Society,2006: 314-327.

[16] WEN Yan,HUANG Min-huan,ZHAO Jin-jing,*et al*. Implicit detection of stealth software with a local-booted virtual machine[C]//Proc of the 3rd International Conference on Information Sciences and Interaction Sciences. Washington DC:IEEE Computer Society, 2010:152-157.

[17] ZHANG Shi-bin,XU Chun-xiang,LONG Ya-xing. Study on terminal trusted model based on trusted computing[C]//Proc of International Conference on Internet Technology and Applications. Washington DC: IEEE Computer Society, 2011:1-4.

[18] WANG Zhi,JIANG Xu-xian. HyperSafe:a lightweight approach to provide lifetime hypervisor control-flow integrity[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC:IEEE Computer Society, 2010:380-395.

[19] MITRE Corporation. Common vulnerabilities and exposures list[EB/OL]. 2009-03-16(2011). http://cve. mitre. org/cve/.

[20] SAILER R,VALDEZ E,JAEGER T,*et al*. sHype:secure hypervisor approach to trusted virtualized systems, RC23511[R]. New York: IBM Research,2005.

[21] SAILER R,JAEGER T,VALDEZ E,*et al*. Building a MAC-based security architecture for the Xen open-source hypervisor[C]//Proc of the 21st Annual Computer Security Applications Conference. Washington DC:IEEE Computer Society, 2005:276-285.

[22] JANSEN B,RAMASAMY H V,SCHUNTER M. Policy enforcement and compliance proofs for Xen virtual machines[C]//Proc of the 4th International Conference on Virtual Execution Environments. New York:ACM Press,2008:101-110.

[23] SHINAGAWA T,EIRAKU H,TANIMOTO K,*et al*. BitVisor:a thin hypervisor for enforcing I/O device security[C]//Proc of ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. New York:ACM Press,2009:121-130.

[24] AZAB A M,NING Peng,WANG Zhi,*et al*. HyperSentry:enabling stealthy in-context measurement of hypervisor integrity[C]//Proc of the 17th ACM Conference on Computer and Communications Security. New York:ACM Press,2010:38-49.

[25] AZAB A M,NING Peng,SEZER E C,*et al*. HIMA:a hypervisor-based integrity measurement agent[C]//Proc of the 25th Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society,2009:461-470.

[26] WU Qing-bo,WANG Chun-guang,TAN Yu-song. System monitoring and controlling mechanism based on hypervisor[C]//Proc of IEEE International Symposium on Parallel and Distributed Processing with Applications. Washington DC: IEEE Computer Society, 2009: 549-554.

[27] XU Min,JIANG Xu-xian,SANDHU R,*et al*. Towards a VMM-based usage control framework for OS kernel integrity protection[C]//Proc of the 12th ACM Symposium on Access Control Models and Technologies. New York:ACM Press,2007:71-80.

[28] WU Jing-zheng,DING Li-ping,WANG Yong-ji,*et al*. Identification and evaluation of sharing memory covert timing channel in Xen virtual machines[C]//Proc of the 4th International Conference on Cloud Computing. Washington DC: IEEE Computer Society, 2011:283-291.

[29] RHEE J,RILEY R,XU Dong-yan,*et al*. Defeating dynamic data kernel rootkit attacks via VMM-based guest-transparent monitoring[C]//Proc of International Conference on Availability, Reliability, and Security. 2009:74-81.

[30] RILEY R,JIANG Xu-xian,XU Dong-yan. Guest-transparent prevention of kernel Rootkits with VMM-based memory shadowing[C]//Proc of the 11th International Symposium on Recent Advances in Intrusion Detection. Berlin:Springer, 2008:1-20.

[31] GEBHARDT C,DALTON C I,BROWN R. Preventing hypervisor-based Rootkits with trusted execution technology[J]. Network Security,2008,2008(11): 7-12.

[32] LAKSHMI J,NANDY S K. I/O virtualization architecture for security[C]//Proc of the 10th IEEE International Conference on Computer and Information Technology. Washington DC:IEEE Computer Society, 2010:2267-2272.

[33] OKAMURA K,OYAMA Y. Load-based covert channels between Xen virtual machines[C]//Proc of the 25th Annual ACM Symposium on Applied Computing. New York:ACM Press,2010:173-180.

[34] CHENG Ge,JIN Hai,ZOU De-qing,*et al*. A prioritized Chinese wall model for managing the covert information flows in virtual machine systems[C]//Proc of the 9th International Conference for Young Computer Scientists. Washington DC:IEEE Computer Society, 2008: 1481-1487.

[35] CATUOGNO L,DMITRIENKO A,ERIKSSON K,*et al*. Trusted virtual domains:design, implementation and lessons learned[C]//Proc of International Conference on Trusted Systems. [S. l.]: Springer, 2010:156-179.

[36] BERGER S,CACERES R,GOLDMAN K A,*et al*. vTPM:virtualizing the trusted platform module[C]//Proc of the 15th USENIX Security Symposium. Berkeley:USENIX Association, 2006:305-320.

[37] RUAN An-bang,SHEN Qing-ni,YIN Yuan-you. A generalized trusted virtualized platform architecture[C]//Proc of the 9th International Conference for Young Computer Scientists. Washington DC: IEEE Computer Society, 2008:2340-2346.

[38] 程川. 一种基于 Xen 的信任虚拟机安全访问设计与实现[J]. 计算机与数字工程, 2010,38(3):109-111.

[39] JANSEN B,RAMASAMY H V,SCHUNTER M,*et al*. Architecting dependable and secure systems using virtualization[M]//Architecting Dependable Systems V. Heidelberg:Springer-Verlag, 2008:124-149.

[40] 张志新,彭新光. 基于 Xen 的入侵检测服务研究[J]. 杭州电子科技大学学报,2008(6):91-94.

[41] PAYNE B D,SAILER R,CACERES R,*et al*. A layered approach to simplified access control in virtualized systems[J]. ACM SIGOPS Operating Systems Review,2007,41(4):12-19.