doi:10.11959/j.issn.1000-436x.2015236

云计算中虚拟机计算环境安全防护方案

闫世杰[1]，陈永刚[2]，刘鹏[3]，闵乐泉[1]
（1. 北京科技大学 自动化学院，北京 100083；
2. 国家信息中心，北京 100045；3. 中国标准化研究院，北京 100088）

摘 要：提出了一种虚拟机计算环境的安全防护方案，该方案采用虚拟机内外监控相结合的方式对虚拟机的计算环境进行持续、动态的监控和度量，可对虚拟机进行反馈控制，保障虚拟机计算环境的安全，提升虚拟机的动态适应能力。对比现有安全防护案，该方案充分考虑了云计算中虚拟机效率损耗问题，安全性和执行效率较高，适用于虚拟计算环境。

关键词：云计算；虚拟机；计算环境；主动监控
中图分类号：TP393 **文献标识码**：A

Security protection mechanism of virtual machine computing environment under the cloud computing

YAN Shi-jie[1], CHEN Yong-gang[2], LIU-Peng[3], MIN Le-quan[1]
(1. College of Automation Engineering, University of Science and Technology Beijing, Beijing 100083,China;
2. State Information Center, Beijing 100045, China; 3. China National Institute of Standardization, Beijing 100088, China)

Abstract: A protection mechanism for the computing environment of virtual machine was proposed, this scheme combined inside and outside monitoring mechanism to measure and monitor the computing environment of virtual machines, and it could continually and dynamically monitor and measure the virtual machines. This scheme could also use the feedback control mechanism to ensure the security of the virtual machines computing environment and enhance the dynamic adaptability of virtual machines. Comparing with the existing virtual machine security mechanisms, proposed scheme fully considers the computational loss of the cloud virtual machines, which has a high security and efficiency, and it is suitable for the virtual computing environment.

Key words: cloud computing; virtual machine; computing environment; proactive monitoring

1 引言

作为一种新型的计算模式，云计算在当前信息技术革命中扮演着重要的角色，下一代移动互联网、大数据处理及分析、物联网及智慧城市等新一代信息技术无不与云计算有着密切的关系[1~3]，云计算已经成为各国争相抢占的新技术制高点。

从云计算的实践来看，从其诞生起，云安全问题摆在了云的提供者和应用者面前。随着云计算的不断发展，安全问题日益成为制约其发展的重要因素[4,5]。根据 IDC 公司 2012 年一项调查，有 85.7%的参与者在考虑是否采用云计算服务时，最关心的问题是云安全问题。IBM 公司一项调查显示出同样结果，77%的被调查者认为云计算技术有很大的安全性风险。TechTarget 公司针对中国企业的云安全调查显示，企业对于云安全的认同度不高，约 40%的用户拒绝使用云计算服务模式。而 Amazon、Google 等云计算发起者不断爆出各种安全事故更加剧了人们的担忧。

由于云计算更依赖于虚拟化技术，通过使用虚拟化技术使云计算成本更低、效益更好，同时还具备良好的动态扩展性，但是虚拟化同时导致了一系列的安全问题，在虚拟机环境中，相比传统系统，虚拟机监控器的引入，使虚拟机系统的安全问题变得更复杂[6~8]。传统系统的安全性几乎等价于操作

收稿日期：2015-03-01；修回日期：2015-05-20

系统的安全性，而在虚拟机环境中，首先要确保虚拟机监控器的安全，同时也要确保每一台虚拟机中的安全性。当前国内外学者对虚拟机和虚拟机监控器的安全有诸多的研究，主要通过虚拟机的监控方式来保障虚拟机的安全。文献[9,10]采用虚拟机外监控方式对虚拟机进行监控，但是虚拟机外监控方式要在特权虚拟机和客户虚拟机之间进行大量的上下文切换，带来了巨大的计算开销，这对云计算平台是一个极大的负担，同时外监控方式主要基于完整性度量进行，该度量过程偏于静态，缺乏动态适应性，而且监控机制和虚拟机分离之后无法进行细粒度的度量。文献[11,12]采用虚拟机内监控方式对虚拟机进行监控，将监控机制和虚拟机结合在一起进行监控，一定程度上克服了虚拟机外监控计算开销巨大的缺点，但是一旦虚拟机出现安全问题很容易出现监守自盗的问题，该机制的安全性远不如外监控。

因此，为了更好地保障虚拟机计算环境的安全，本文在参考虚拟机内监控和外监控的机制基础之上，提出了一种虚拟机的计算环境保护方案，该方案采用虚拟机内外监控结合方式，对虚拟机的计算环境进行监控和度量，同时根据监控和度量的结果对虚拟机进行动态反馈调整，与传统的虚拟机防护方案相比，本文提出的方案充分考虑了虚拟机计算资源的损耗问题，同时具有较高的安全性和执行效率以及动态适应性，适用于虚拟计算环境。

2　虚拟机计算环境描述及防护方案流程

2.1　虚拟机计算环境描述

根据云计算平台中虚拟机的类型，虚拟机可以分为两类：特权虚拟机和普通用户虚拟机。普通虚拟机由特权虚拟机进行创建和管理，因此普通节点的外部监控和反馈可以由特权虚拟机进行，普通虚拟机内部同时对自身进行监控和度量，而特权虚拟机可以对普通虚拟机集体监控。特权虚拟机和普通虚拟机的计算环境可以形式化描述如下。

2.1.1　普通虚拟机

普通虚拟机的计算环境由 3 个基本要素构成：虚拟机原始标识、虚拟机上下文环境和虚拟机的外部输出，具体描述如下。

1) 虚拟机原始标识

普通虚拟机的原始标识包括 2 个要素：虚拟机的 id，虚拟机镜像的摘要值 ih，其中，ih 是一个 n+1 维向量，$ih=\{\alpha,\gamma[1],\cdots,\gamma[n]\}$，虚拟机操作系统镜像的摘要值为 α，虚拟机其关键进程的摘要值为 $\gamma[1],\cdots,\gamma[n]$，因此虚拟机的原始标识用二元组 $PI=(id,ih)$ 进行描述。

2) 虚拟机上下文环境

虚拟机上下文环境由关键进程的摘要 δ、应用程序的摘要值 $H(H=(h_1,h_2,\cdots,h_n))$，虚拟机的通信协议 $C=\{c_1,c_2,\cdots,c_n\}$ 组成，因此虚拟机的上下文环境可以描述为三元组 $VE=(\delta,H,P)$。

3) 虚拟机的外部输出

普通虚拟机的外部输出由特权虚拟机进行度量和监控，包括虚拟机通信的源地址、目的地址、通信协议的端口号以及通信过程中蕴含的操作序列，定义 $OM=(Sr,Dr,Con)$，其中，Sr 代表源地址，$Dr=\{po_1,\cdots,po_2\}$ 代表通信协议试图访问的端口号，$Con=(p_1,p_2,\cdots,p_n)$ 为通信协议运行权限。

综上所述普通虚拟机的计算环境可以用以三元组 (PI,VE,OM) 描述。

2.1.2　特权虚拟机

特权虚拟机由 4 个基本要素构成：虚拟机的原始标识、虚拟机的上下文环境、虚拟机的外部输出以及普通虚拟机的反馈列表，其中，虚拟机的原始标识、虚拟机的上下文环境、虚拟机的外部输出与普通虚拟机描述类似，在此不做赘述，特权虚拟机担负着对普通虚拟机外部输出的度量和反馈，其度量节点列表描述如下

$$VN=(n_1,n_2,\cdots,n_n)$$

其中，$n_1,n_2,\cdots,n_n$ 为其度量的虚拟机列表，n_i 中保存特权虚拟机对普通虚拟机的反馈策略。特权虚拟机的计算环境可以用四元组 (PI,VE,OM,VN) 描述。

2.2　虚拟机计算环境防护流程

虚拟机计算环境防护流程如图 1 所示。

1) 首先普通虚拟机完成自身的初始启动度量，将虚拟机原始标识传给特权虚拟机，特权虚拟机将该结果和其存储的原始标识对比，如果一致则认为该虚拟机镜像没有被篡改，否则，认为该虚拟机镜像被篡改，将其隔离。

2) 完成初始启动度量之后普通虚拟机执行自身的动态内监控机制，特权虚拟机根据普通虚拟机的外部输出完成外监控，因为一个虚拟机如果出现安全问题其首先表现为外部输出异常，然后综合内监控和外监控的结果判断该普通虚拟机的计算环境是否安全。

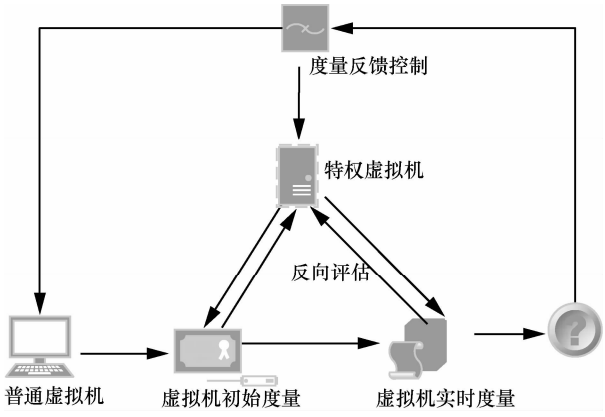


图 1 计算环境保护流程

3) 普通虚拟机也要根据特权虚拟机的外部输出判断特权虚拟机是否值得信赖，给定一个阈值 t，如果有大于 t 个普通虚拟机认为特权虚拟机有安全问题，那么就可以申请系统管理员重建一个特权虚拟机。

4) 通过普通虚拟机和特权虚拟机的相互制约，以及外监控和内监控的相互结合，最大程度地保障虚拟机计算环境的安全。

3 虚拟机的监控度量及反馈

3.1 虚拟机的初始监控度量

普通虚拟机在启动之前，特权虚拟机需要对其原始标识进行度量，以确定虚拟机镜像和虚拟机关键信息没有被篡改，保障普通虚拟机在启动过程的安全。因此给虚拟机的原始标识 $PI=(id,ih)$，给定 $ih=\{\alpha,\gamma[1],\cdots,\gamma[n]\}$，那么虚拟机操作系统镜像的摘要值为 α，虚拟机其关键进程的摘要值为 $\gamma[1],\cdots,\gamma[n]$，设 α' 和 $\gamma'[1],\cdots,\gamma'[n]$ 为存储在特权虚拟机上操作系统和关键进程的摘要值。那么在该虚拟机启动之前需要向特权虚拟机提交 $PI=(id,ih)$，然后特权虚拟机计算

$$I=(\alpha\wedge\alpha')\wedge\sum_{i=1}^{n}\gamma'[i]\wedge\gamma[i]$$

如果 I 取值为 0，则认为虚拟机被篡改过，将阻止虚拟机的启动，否则认为虚拟机原始镜像文件没有被篡改，该虚拟机可以启动。

3.2 普通虚拟机的实时监控度量

给一个普通的用户虚拟机 UV，该虚拟机的监控度量分为 2 部分，自身的内监控及特权虚拟机对其的外监控，内监控和外监控通过对该虚拟机的实时度量完成。设特权虚拟机节点为 PV，设 $T(UV_i,t)$ 为该虚拟机的监控实时度量值，其中该虚拟机的度量时间窗是 t，虚拟机的度量时间窗可以提高行为虚拟机度量的准确性和动态适应性，通过时间窗考察该虚拟机一段时间内的信任值。时间窗反映了虚拟机的信任度具有随时间变化而衰减的特性。

本文认为 $T(UV,t)$ 应该包括对该虚拟机内监控的度量值以及外监控度量值，其中外监控度量值由特权虚拟机完成。该虚拟机的计算环境是否安全需综合考虑该虚拟机的内监控度量值和外监控度量值，因此 $T(UV,t)$ 可以描述为

$$T(UV_i,t)=\frac{a_1}{n}\sum_{i=1}^{n}M_{\text{in}}(UV)+\frac{a_2}{n}\sum_{i=1}^{n}M_{\text{out}}(UV)$$

其中，$M_{\text{in}}(UV)$ 代表对虚拟机 UV 在时间窗 t 内的度量值，$\sum_{i=1}^{n}M_{\text{in}}(UV)$ 表明在 t 时间内对 n_i 完成了 n 次内部度量，同理 $M_{\text{out}}(UV)$ 表示对 UV 一次外部监控度量分析，$\sum_{i=1}^{n}M_{\text{out}}(UV)$ 表明在 t 时间内对 UV 的 n 次外监控度量。

考虑到对虚拟机度量是随时间衰退的，不失一般性，内部监控度量和外部监控度量的衰退是类似的，在此描述内部度量的计算过程，设 t 时间内 UV 的 n 次内监控度量值为 $\{t_1,t_2,\cdots,t_n\}$，设 t_1 为距离现在最久的一次节点的度量值，则 $M_{\text{in}}(UV)$ 和 $M_{\text{out}}(UV)$ 可以定义为

$$M_{\text{in}}(UV)=\begin{cases}\dfrac{t_i e(i)}{i}, & i\neq 0\\ 0, & i=0\end{cases}$$

类似地，设 t 时间内 UV 的 n 次的外监控度量值为 $\{t_1',t_2',\cdots,t_n'\}$，那么有

$$M_{\text{out}}(UV)=\begin{cases}\dfrac{t_i' e(i)}{i}, & i\neq 0\\ 0, & i=0\end{cases}$$

设衰减函数为 $e(i)$，$e(i)\in[0,1]$，$g(i)$ 可以对不同时刻的可信度量合理加权。根据行为随时间衰减的规律，新发生的行为应该具有更多的权重，衰减函数定义如下

$$e(i)=\begin{cases}1, & i=n\\ e(i-1)=e(i)-\dfrac{1}{n}, & 1\leqslant i\leqslant n\end{cases}$$

虚拟机每一次内部度量值 t_i 通过虚拟机的上下

文度量可得，其计算过程如下。

给定 $VE=(\delta,H,P)$，其中，$H=\{h_1,h_2,\cdots,h_n\}$，节点的通信协议 $C=\{c_1,c_2,\cdots,c_n\}$，节点 t_i 计算函数分为 2 个子函数，进程度量函数 E_h 和节点通信协议度量函数 E_p，所以内部监控函数描述如下。

定义 1　内部监控度量计算函数。给定 $H=\{h_1,h_2,\cdots,h_n\}$ 为虚拟机应用程序的摘要值集合，特权虚拟机的预期配置为 $H'=\{h_1^{'},h_2^{'},\cdots,h_n^{'}\}$，定义 E_h 为进程度量函数，描述如下

$$E_h=\frac{1}{n}\sum_{i=1}^{n}h_i\wedge h_i^{'}$$

设特权虚拟机允许运行的通信协议 $\{c_1',c_2',\cdots,c_n'\}$，$C=\{c_1,c_2,\cdots,c_n\}$，定义 E_c 为通信协议度量函数，则 E_c 描述如下

$$E_c=\frac{1}{n}\sum_{i=1}^{n}c_i'\wedge c_i$$

内部监控度量函数描述如下

$$ti=\alpha_1E_h+\alpha_2E_c\cdot$$
$$(\alpha_1\frac{1}{n}\sum_{i=1}^{n}hi\wedge h_i'+\alpha_2\frac{1}{n}\sum_{i=1}^{n}c_i'\wedge c_i)\wedge(\delta\wedge\delta')$$

其中，α_1、α_2 为用户定义的权重系数，$\alpha_1+\alpha_2=1$，δ' 为特权虚拟机保存的关键进程的摘要值。

定义 2　虚拟机外部监控度量函数。给定虚拟机的外部输出 $OM=(Sr,Dr,Con)$，其中，$Dr=\{po_1,\cdots,po_2\}$，$Con=(pr_1,pr_2,\cdots,pr_n)$，恶意通信存在一些共性，比如蠕虫的网络攻击以及拒绝服务攻击的特性等，恶意通信内容及操作序列使通信协议也会出现异常执行状态；某些端口的非正常访问，已禁止的通信协议的执行；远程协助的突然运行等。外部监控度量主要虚拟机的恶意指数，用 $M[i]$ 表示虚拟机通信进程的恶意指数。$M[i]$ 通过一个三元组 $\{pr,p_i,np\}$ 进行计算，pr 表示虚拟机的通信协议试图获取的权限，p_i 为特权虚拟机设定的权限，np 表示进程试图扫描其没有权限访问端口的次数。

定义 E_p 为进程度量函数，其描述如下。

定义 $\|M[i]\|=\sqrt{|pr_i^2-p_i^2|+np^2}$ 进行归一化之后为 $\|M[i]\|'=\dfrac{\|M[i]\|}{pr_i^2+p_i^2+np^2}$，设 Sr' 为特权虚拟机中保存的源地址，那么 t_i' 可以计算如下

$$t_i'=(Sr'\wedge Sr)\wedge(\sum_{i=1}^{n}\frac{\|M[i]\|'}{n})$$

定义 3　特权虚拟机的反馈函数。特权虚拟机的监控由全体普通虚拟机合作完成，给定特权虚拟机 PV，普通虚拟机的集 $\{UV_1,\cdots,UV_n\}$，特权虚拟机的外部输出 $OM=(Sr,Dr,Con)$，设虚拟机 UV_i 对特权虚拟机的监控度量值为

$$mt_i=\frac{1}{n}\sum_{i=1}^{n}(PV\cdot Dr\cdot po_i\wedge UV\cdot Dr\cdot po_i)$$

设全体虚拟机对该特权虚拟机的监控度量值为

$$MT=\frac{1}{n}\sum_{i=1}^{n}mt_i$$

给定设定一个阈值 η，如果 $MT>\eta$，那么就认为该特权虚拟机是符合安全策略的，否则将向系统管理员申请更换特权虚拟机。

4　实验仿真

本文的仿真实验主要验证所提出的虚拟机计算环境保护方案的有效性。此实验中共有 100 个 Domain 参与，除 Dom0 外，还有 99 个 DomU，剩余的 DomU 分别标记为 Dom1~Dom99。本文主要和文献[10,11]中的方案进行对比，文献[13,14]中的方案采用监控关键程序的状态完成对木马的防御，而本文基于内监控和外监控联合度量反馈完成对木马的防御。

实验所在的服务器参数如下，服务器有 16 个 4 核频率为 2.40 GHz、型号为 E5620 的 CPU，256 GB 的物理内存。Xen 的版本为 4.1，Dom0 运行的操作系统是 CentOS 5.4 版本，而 Dom1~Dom9 全部运行 Ubuntu 8.1，所有的 Domain 都运行 Linux2.6.4 版本的内核。剩余的虚拟机运行 Window7 系统。本文在 Xen 系统中设计了如图 2 所示的实验场景，在 Dom1 中植入特洛伊木马程序，Dom2 中装有一个破解工具，它们通过 Xen 中的域间通信机制进行通信，然后通过虚拟机通信过程将木马扩散。由于传统的 Xen 框架中允许 DomU 的用户通过底层 Hypervior 进行相互通信和操作，因此 Dom2 中破解工具可以通过特洛伊木马程序获取 Dom1 中登录框(LoginBox)输入的用户名和密码。本文通过采用虚拟机静态监控和动态监控度量相结合，内监控和外监控相结合的方式保护虚拟机的计算环境。

本文提出的虚拟机计算环境带的保护功能是

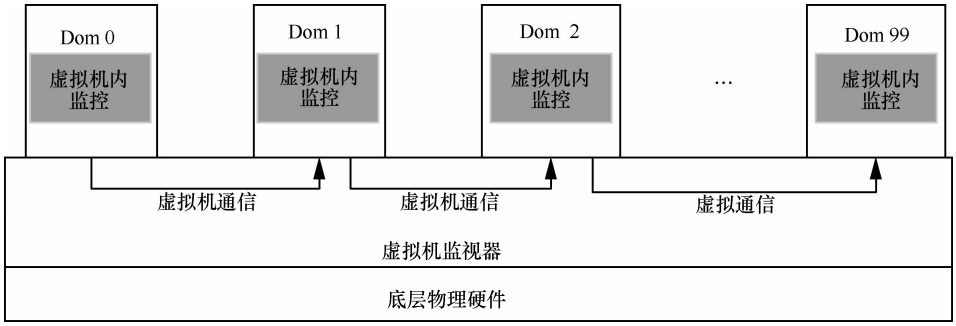


图 2 虚拟机计算环境保护场景

在虚拟机内部状态和外部输出装填有问题时，能及时对某些恶意的虚拟机进行隔离，从而保证整个虚拟计算环境的可信，本文采用有效控制率 *TR* 反映对虚拟机控制成功率，*TR* 主要反映了本文方案在应对恶意攻击时的反应能力。

设在 Δt 时间内，对一虚拟机内外监控度量值中符合安全策略的有 $\alpha(t)$ 个，不符合的有 $\beta(t)$ 个，设虚拟机群体中不符合安全策略的虚拟机的比率为 μ，那么 *TR* 可以描述如下

$$TR=\frac{\alpha(t)}{\mu(\alpha(t)+\beta(t))}$$

对于所有的虚拟机整体而言，本文的方案能否有效保障虚拟机计算环境的安全，可以通过 *TR* 有效反映出。图 3 和图 4 分别反映了本文方案在面对木马攻击时的运行状态。

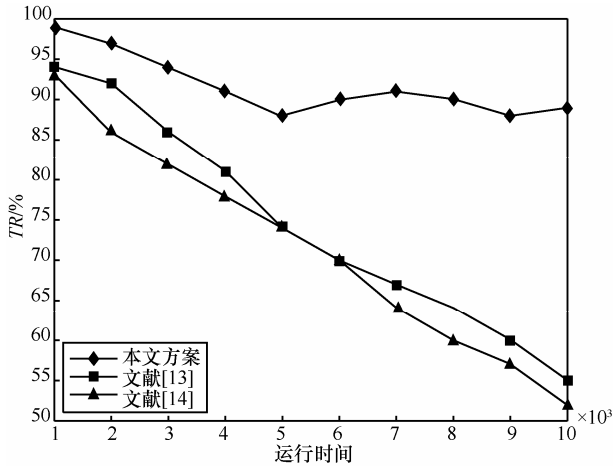


图 3 面对 NE 木马时稳定性对比

从图 3 可以看出，本文提出的方案在面对 NE 木马时，相对其他方案，整个虚拟机的运行态势有较好的运行稳定性，可以保证大部分虚拟机的正常运行。

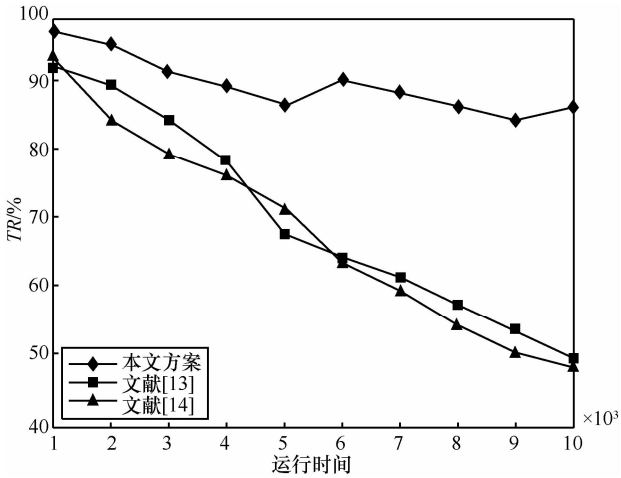


图 4 面对反虚拟机攻击时稳定性对比

从图 4 直观对比可见，采用本文机制之后，虚拟机虽然不能移除所有可能的恶意节点，但至少能保证大部分节点有效运行。图 5 反映了虚拟机的计算资源的损耗率。

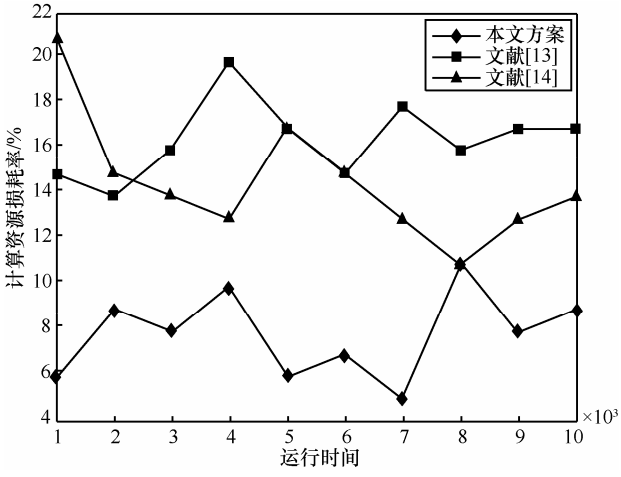


图 5 虚拟机计算资源损耗对比

从图 5 可以看出，本文方案计算资源的消耗要小于传统的方案，因此具有更好的环境适应性。

5　结束语

为更好地保护云计算中虚拟计算环境的安全，本文综合了虚拟机内监控和外监控的特点，创造性地描述了虚拟机的计算环境，采用对虚拟机计算环境动态度量和静态度量相结合，虚拟机内监控和外监控相结合的方式保障虚拟机计算环境的安全，同时特权虚拟机由所有的普通用户虚拟机进行外监控，从而防止特权虚拟机被攻击的情形下影响普通虚拟机的安全性。与传统的虚拟机防护方案相比，本文提出的方案具备较好的运行稳定性，计算资源损耗较低，具有良好的环境适应性。

参考文献：

[1] MELL P, GRANCE T. The nist definition of cloud computing (draft)[J]. NIST Special Publication, 2011, 800:145.

[2] 张亚勤, 沈寓实, 李雨航. 云计算 360 度[M]. 北京: 电子工业出版社, 2013.
ZHANG Y Q, SHEN Y S, LI Y H. Cloud 360 An In-depth Look at Cloud Era by Microsoft Experts[M]. Beijing: Publishing House of Electronics Industry, 2013.

[3] 国家信息技术服务标准工作组. 中国云服务白皮书[R]. 北京: 2013.
Information technology service standards. White Paper of China Cloud Service[R]. Beijing, 2013.

[4] 胡乐明, 冯明, 唐宏. 云计算安全技术与应用[M]. 北京: 电子工业出版社, 2012.
HU L M, FENG M, TANG H. Cloud Security Technology and Application[M]. Beijing: Publishing House of Electronics Industry, 2012.

[5] 王舒榕. 基于云计算平台的安全性及信任模型研究[D]. 南京: 南京邮电大学, 2011.
WANG S R. The Security and Trust Model Study Based on Cloud[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2011.

[6] ARMBRUST M, FOX A, GRIFFITH R, *et al*. Above the Clouds: A Berkeley View of Cloud Computing[R]. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[7] MURRAY D G, MILOS G, HAND S. Improving xen security through disaggregation[A]. Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, ACM[C]. 2008.

[8] HIRANO M, SHINAGAWA T, EIRAKU H, *et al*. Introducing role-based access control to a secure virtual machine monitor: security policy enforcement mechanism for distributed computers[A]. Asia-Pacific Services Computing Conference[C]. 2008.2008.

[9] KING S T, CHEN P M. Backtracking intrusions[J]. ACM Transactions on Computer Systems (TOCS), 2005, 23(1):51-76.

[10] PAYNE B D, CARBONE M, SHARIF M, *et al*. An architecture for secure active monitoring using virtualization[A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. 2008.

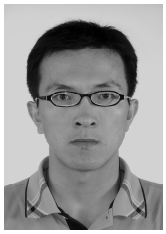
[11] SHARIF M, LEE W, CUI W, *et al*. Secure In-VM monitoring using hardware virtualization[A]. 16th ACM Conference on Computer and Communications Security. ACM[C]. 2009.

[12] WANG Z, JIANG X, CUI W, *et al*. Countering kernel rootkits with lightweight hook protection[A]. 16th ACM Conference on Computer and Communications Security. ACM[C]. 2009.

[13] ERNST M D, PERKINS J H, GUO P J, *et al*. The daikon system for dynamic detection of likely invariants[J]. Science of Computer Programming, 2007, 69(1-3):35-45.

[14] BALIGA A, GANAPATHY V, IFTODE L. Detecting kernel-level rootkits using data structure invariants[A]. IEEE Transactions on Dependable and Secure Computing[C]. 2010.

作者简介：



闫世杰（1979-），男，山西交城人，北京科技大学博士生，主要研究方向为网络空间安全、知识安全、信息安全管理、风险评估等。

陈永刚（1979-），男，河南郑州人，博士，国家信息中心工程师，主要研究方向为信息安全、密码学、风险评估等。

刘鹏（1982-），男，河北廊坊人，博士，中国标准化研究院工程师，主要研究方向为信息安全管理和风险评估等。

闵乐泉（1951-），男，北京人，北京科技大学教授、博士生导师，主要研究方向为细胞神经网络(CNN)模板的稳健性设计、基于 CNN 的图像处理、混沌密码学等。