doi:10.3969/j.issn.1000-436x.2014.z2.013

云计算环境下可信虚拟机管理模型

周振吉，吴礼发，洪征，赖海光，郑成辉
（解放军理工大学 指挥信息系统学院，江苏 南京 210007）

摘 要：为了解决云计算环境下虚拟机管理存在的管理域特权过于集中和用户策略易被恶意篡改等问题，提出了一种可信虚拟机管理模型。模型首先对虚拟机管理域进行了细粒度的划分，赋予管理员和用户不同的管理特权，防止管理员随意访问用户的数据；利用可信计算技术建立可信通道分发用户策略，防止管理员恶意篡改用户策略。安全性分析与实验测试表明，该模型可以有效保护用户数据和用户策略的安全性。

关键词：云计算；可信计算；虚拟机管理
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0094-12

Trusted virtual machine management model for cloud computing

ZHOU Zhen-ji, WU Li-fa, HONG Zheng, LAI Hai-guang, ZHENG Cheng-hui
(Institute of Command Information System, PLA University of Science and Technology, Nanjing 210007, China)

Abstract: For virtual machine in cloud computing, the authorization of manager domain is too centralized to be secure, and the strategies of tenants can be easily falsified. In view of the two problems, a trusted virtual machine management Model for cloud computing infrastructure is proposed. The model provides fine grained manager domain of virtual machine in which both managers and tenants are strictly constrained when they operate on other tenant domains. The sensitive code and data in tenant virtual machine cannot be accessed or falsified without permission. The model creates a trustable tunnel between tenant and system domain, and distributes tenant strategies using the tunnel in a secure way. Security analysis and experimental results show the model ensures the security of tenant data and tenant strategies effectively.

Key words: cloud computing; trusted computing; virtual machine management

1 引言

云计算的核心安全问题是信息的拥有者不能控制进行信息处理的计算机硬件[1]。用户不能确保自己在云基础设施的数据不被提供商非法使用。因此，为了实现云计算安全，必须提高云基础设施管理的可信性。

云基础设施是云计算平台的核心，主要负责管理物理主机、虚拟机、任务和用户等，并给上层服务提供一个良好的访问接口[2]。其中，虚拟机管理是云基础设施管理的重要部分，主要根据用户和系统的需求创建、启动、迁移、停止、删除虚拟机。云基础设施平台通过虚拟机管理在满足用户需求的同时，实现计算资源的最优化。

虽然虚拟机可信度量与证明模型能够保证用户虚拟机在运行过程中的可信性，但是恶意的管理员仍然可以通过滥用管理层的特权来访问用户数据[3]。

现有的云计算环境下，虚拟机管理主要采用混合管理的方式[4,5]，即用户通过向虚拟机管理域发送策略来配置用户域，管理员通过调用管理域的调度操作来管理虚拟机。这种管理方式没有实现用户虚拟机间的真正隔离，管理员和用户的恶意行为会威胁到其他用户虚拟机的安全。在虚拟机管理过程中，现有云基础设施主要存在以下 2 个问题。

收稿日期：2014-07-01
基金项目：江苏省自然科学基金资助项目（BK2011115, BK20131069）
Foundation Item: The Natural Science Foundation of Jiangsu Province (BK2011115, BK20131069)

1) 管理域特权过于集中。在云计算环境中，用户通过虚拟机管理域实施自己的安全策略并控制用户域，管理员根据系统需求通过虚拟机管理域实施用户虚拟机的启动、调度和迁移操作。管理员和用户的恶意攻击和误操作都有可能破坏其他用户数据的机密性和完整性[1]。因此，需要一种能够有效约束管理域特权的方法。

2) 用户策略易被恶意篡改。云计算是一种外包的服务模式，用户通过提交策略实施云服务。但是在现有的虚拟机管理模型中，恶意管理员可以通过篡改用户策略绕过用户原有的安全防护[6]，用户很难保证自身策略的可信性。因此，需要一种可信的用户策略分发和实施方法。

针对上述问题，本文提出了云计算环境下可信虚拟机管理模型(TVMM, trusted virtual machines management model)。首先，根据管理域和不同角色的特权要求，对虚拟机管理域进行了细粒度的划分，赋予管理员和用户不同的管理特权。管理员和用户只能受限地访问其他用户域，无法随意窥视或篡改用户虚拟机上的代码和敏感数据，从而保证了用户数据的安全性。针对用户策略易被恶意篡改的问题，模型提出了基于可信计算技术[7]的用户策略保护方法，用户使用可信计算技术与虚拟机建立可信通道，并利用该通道安全的分发用户策略。最后，对原型系统的有效性进行了安全性分析和实验测试。

2　相关工作

云基础设施平台使用虚拟机将底层的硬件资源转变为统一的虚拟资源，能够实现物理资源的高效管理与共享。但在提高分布式系统物理资源利用率的同时，虚拟机的使用也给用户数据和业务安全带来了新的威胁。用户迫切需要云服务提供商能够紧密结合业务环境，提供更加可信的虚拟机管理服务。当前，对可信虚拟管理平台的研究主要在现有成熟虚拟化平台的基础上附加可信性增强技术来实现，代表性的技术有 Terra[8]、CIVIC[9]、TVDc[10]和 NoHype[11]等。

由 Garfinkel 等人[8]提出的 Terra 方案，是目前最为典型的可信虚拟机管理平台。Terra 系统基于 VMware GSX Server[12]实现，通过附加的底层可信虚拟机监控器将单一的通用平台划分成可信虚拟机和普通虚拟机 2 个隔离域。可信虚拟机监控器一方面提供了闭合运行环境，确保操作系统和应用程序实现远程可信证明；另一方面提供了用户与虚拟机应用之间的可信交互路径，确保通信无法被监听和攻击。

怀进鹏等人[9]在集成多种虚拟机技术的基础上，提出了虚拟机管理平台 CIVIC。CIVIC 通过构建层次化的运行视图，可以为用户提供独立、隔离的计算环境，支持对硬件资源和软件资源的统一管理功能，同时使得动态、异构的硬件资源对应用程序透明。CIVIC 的不足之处在于：仅实现了虚拟机之间的协作信任管理和访问控制安全增强，缺乏对平台本身的可信验证。

为了同时满足对计算资源的有效聚合和可信协同需求，IBM 公司提出了可信数据中心[10]方案。TVDc 由若干相互隔离的可信虚拟域[13,14](TVD, trusted virtual domain)构成，TVD 包括协作完成一种应用服务的若干虚拟机。TVD 通过基于强制访问控制策略的资源安全隔离措施，保证了属于某个 TVD 的资源无法被其他 TVD 中的虚拟机访问；同时利用软硬件 VLAN 技术，通过构建 TVD 可信虚拟子网保证跨物理机的虚拟机可信组合。

斯坦福大学的 Keller 等[11]从提升虚拟机监控器(VMM, virtual machine monitor)安全性的角度出发，提出了采用硬件替代传统 VMM 虚拟化软件层的 NoHype 方案。NoHype 着眼于物理资源在各个虚拟机之间的安全分割，以硬件保护的方式保证处理器、物理内存的安全隔离，并在设备虚拟化的基础上实现 I/O 的安全共享。目前，完全基于硬件实现的 NoHype 方案尚未实现，还处于深入探索阶段。

综上所述方案均通过虚拟机来实现不同可信度的应用及其系统组件的安全隔离，通过完整性度量技术保证虚拟机及其存储的可信。但在云计算环境下，虚拟机管理域的可信性增强机制仍需进一步研究。

3　研究背景

3.1　可信虚拟域

由于虚拟化和云计算技术的大力推广，TVD 得到了广泛的应用。TVD 由分布式虚拟处理单元(VPE, virtual processing element)、存储单元和网络通信介质组成，有明确的网络边界并遵循统一的安全策略。TVD 域内各个 VPE 之间可以安全通信，而不同 TVD 域之间，只有在策略明确允许的情况下才能进行通信，否则默认相互隔离，并且域间即使通信也会受到策略的严格控制。为了保证虚拟域

的统一安全性，VPE 在加入 TVD 时必须满足一定的安全需求。基于 TVD 技术构建的数据中心称为可信虚拟数据中心 TVD，一个典型的 TVDc 架构如图 1 所示[10]。

图 1 中作为 VPE 的用户虚拟机（HostA 和 HostB）部署在 2 个平台上。TVD 架构主要包含 2 个组件：TVD Master 和 TVD Proxy。TVD Master 主要负责 TVD Policy 的部署，而 TVD Proxy 主要负责执行 TVD Policy。每一个 TVD 下运行虚拟机(VM, virtual machine)的主机上都有一个 TVD Proxy。如果承载 VM 的平台属于多个 TVD，那么该平台每个 TVDc 都有一个 TVD Proxy。

3.2 BAN 逻辑

BAN 逻辑[15]是基于信念的模态逻辑，是使用最为广泛的安全协议形式分析方法，主要用于认证协议的安全性分析，可以发现安全协议设计中的缺陷和漏洞。

基本符号如下：

$P|\equiv Q$：P 相信 Q；

$P \lhd Q$：P 曾收到过 Q；

$P|\sim Q$：P 曾发送过 Q；

$P|\Rightarrow Q$：P 有权控制 Q；

$\#(X)$：X 是新鲜的；

$P \xleftrightarrow{K} Q$：P 与 Q 的会话密钥为 K；

$|\xrightarrow{K} P$：P 的公钥为 K。

主要逻辑推理规则如下。

1) 消息含义规则。对于公开密钥，消息含义规则为

$$\frac{P|\equiv|\xrightarrow{K} Q,\ P \lhd \{X\}_{K^{-1}}}{P|\equiv Q|\sim X} \tag{1}$$

表示 P 相信 K 是 Q 的公钥，K^{-1} 为 Q 的私钥，若 P 收到经 Q 的私钥加密的消息 X，则 P 相信 Q 发送过消息 X。

2) 管辖权规则。管辖权规则如下

$$\frac{P|\equiv Q|\Rightarrow X,\ P|\equiv Q|\equiv X}{P|\equiv X} \tag{2}$$

表示 P 相信 Q 可以控制 X，且 P 相信 Q 相信 X，则可推得 P 相信 X。

3) 临时值校验规则。临时值校验规则如下

$$\frac{P|\equiv \#(X),\ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X} \tag{3}$$

表示若 P 相信 X 为新值，且 P 相信 Q 曾发送过 X，则 P 相信 X。

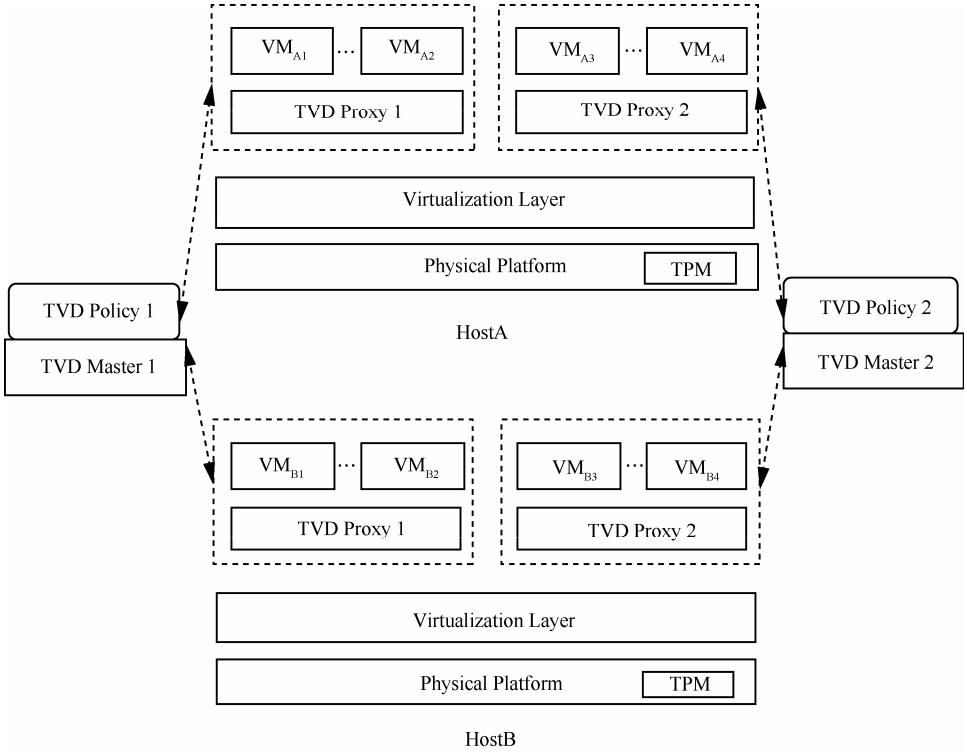

图 1 TVDc 架构

4) 接收消息规则。接收消息规则如下

$$\frac{P \mid\equiv \mid \xrightarrow{K} P,\ P \lhd \{X\}_K}{P \lhd X} \tag{4}$$

表示 P 相信 K 为 P 的公钥，且 P 收到用 K 加密的消息 X，则可推得 P 收到过 X。

5) 新鲜性规则。新鲜性规则如下

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,\ Y)} \tag{5}$$

表示若 P 相信 X 是新鲜的，则 P 相信 X 与 Y 的组合也是新鲜的。

6) 会话密钥规则。会话密钥规则如下

$$\frac{P \mid\equiv \#(K),\ P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \xleftrightarrow{K} Q} \tag{6}$$

表示若 P 相信密钥 K 是新鲜的，且 P 相信 Q 相信 K 中的必要元素 X，则 P 相信 P 与 Q 的会话密钥为 K。

4　可信虚拟机管理模型

4.1　问题分析

基于现有的云基础设施，国际标准化组织分布式管理任务组(DMTF, distributed management task force)提出了传统虚拟机管理模型[4]，如图 2 所示。

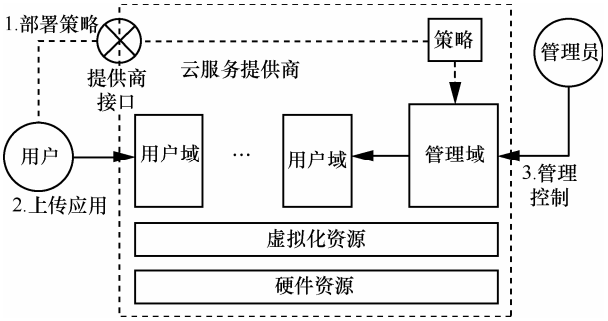

图 2　传统虚拟机管理模型

传统虚拟机管理模型主要包括 3 个交互实体：即用户、云服务提供商和管理员。云服务提供商拥有所有的硬件资源、虚拟化资源以及运行于其上的用户域以及管理域。硬件资源包括各种计算、网络和存储设施，虚拟化资源包括虚拟机、云数据库和虚拟专网等，用户域负责运行用户的应用，管理域一方面负责管理底层的硬件和虚拟化资源，另一方面负责管理用户域。

当使用云服务时，用户首先通过云服务提供商接口向管理域提交自己的策略，管理域根据用户策略创建相应的用户域，用户域启动后用户上传自己的应用，在运行过程中管理员通过管理域按照特定的调度算法对所有的资源进行管理控制。

从上述工作流程中可以看出，虚拟机管理主要有 2 个方面的挑战。1) 管理域的安全性。在云计算环境中，管理员通过虚拟机管理域启动、调度和迁移的用户虚拟机，恶意攻击和误操作都有可能破坏用户数据的机密性和完整性。因此，需要一种约束管理域特权的方法。2) 策略的可信性。用户将策略提交后，恶意的用户或者管理员可以通过篡改策略中的安全规则来访问用户资源，因此，必须能够可信的分发和实施用户的策略。

4.2　管理域划分

在虚拟机执行过程中，传统的管理域拥有以下 6 种特权[16]，如表 1 所示。

然而，这样的管理域特权过于集中，不符合最小特权原则。而且云计算这种共享托管的服务环境中，管理域有多个用户和管理员共同使用，恶意用户或管理员可以通过一些特权操作危害合法用户的虚拟机的安全。因此，基于云计算服务特征，结合虚拟机管理域特权，本节提出了一种新的管理域划分方法 CloudDom，如图 3 所示。

表 1　管理域特权操作

特权	说明
虚拟机管理 (B)	创建、启动、停止和销毁虚拟机
虚拟机控制 (C)	挂起、恢复、调度和迁移虚拟机
虚拟机通信 (I)	设置事件通道和虚拟 I/O 共享内存
虚拟机内省 (P)	映射虚拟机内存和虚拟 CPU 寄存器
状态查询 (R)	查询虚拟机状态信息和主机的物理参数
主机配置 (L)	配置物理主机中断控制器和编程时钟源

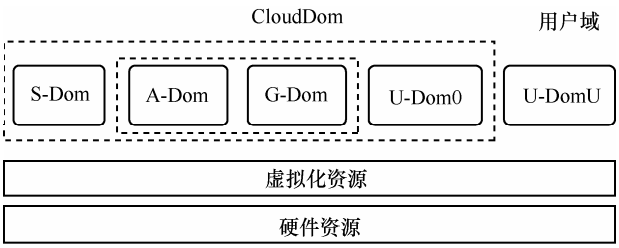

图 3　CloudDom 结构

CloudDom 将原有的管理域划分为系统域(S-Dom)、系统管理域 (A-Dom)、监控域 (G-Dom) 和用户管理域 (U-Dom0) 4 个部分，其中系统域、监控域和虚拟化资源组成了系统的系统可信计算基(TCB, trusted computing base)，每个部分根据虚拟机管理需求赋予不同的特权。

1) 系统域。管理底层的硬件资源并按需求创建与销毁虚拟机。系统域一个主要功能就是管理底层的硬件资源，包括时间片调度、内存和 I/O 配额等，为上层提供一个良好的接口，因此，该域拥有主机配置、状态查询和虚拟机内省的特权。系统域另一个主要功能就是创建、启动、停止和销毁虚拟机，因此，授予该域虚拟机管理特权。最后，系统域负责执行虚拟设备的后端驱动，因此，必须为系统域保留对所有域的虚拟机通信特权。

2) 系统管理域。负责按照特定的需求控制用户虚拟机的运行。系统管理域由系统域创建，负责运行管理员的相关程序和命令，它可以读取主机的状态，然后根据平台的硬件状态和虚拟机信息，按照一定的迁移算法和安全策略对平台进行调度，实现资源的优化使用。因此，该域拥有控制虚拟机、读取虚拟机信息和配置硬件的特权。为了检验用户虚拟机的合规性，系统管理域按照合约向系统域请求创建监控域，并委托监控域检验用户虚拟机，监控域将检验结果返回系统管理域，所以系统管理域拥有与监控域通信的特权。系统管理域不能任意读写用户管理域和用户域的敏感信息，从而确保用户虚拟机的隐私和安全性。

3) 监控域。监控用户域的合规性。通常情况下，管理员需要具有检查用户合规性的能力。例如，管理员希望可以通过检查用户虚拟机来确保用户不滥用其云基础设施托管恶意软件。因此，系统域根据云服务提供商和用户的策略创建监控域，并作为系统 TCB 的一部分。管理员可以在监控域上运行特定的程序来检查用户的虚拟机。用户利用可信计算技术来验证监控域上只运行可信代码，从而保证了用户隐私安全。因此，监控域拥有与用户域和用户管理域通信、内省和查询的特权。

4) 用户管理域。负责控制用户自己的虚拟机。用户管理域不仅负责管理用户虚拟域，还负责通过监控域完成一些针对用户虚拟机的安全服务，如基于内存反省的虚拟机监控、入侵检测和存储加密等，而在传统的云中，这些服务由管理域部署实施。因此，用户管理域拥有执行虚拟机控制、通信、内省和状态查询等特权。

综上所述，CloudDom 及其特权如表 2 所示，其中 B 表示虚拟机管理特权，C 表示虚拟机控制特权，I 表示虚拟机通信特权，P 表示虚拟机内省特权，R 表示状态查询特权，L 表示主机配置特权，“—”表示没有特权。

4.3 模型结构

结合上面提出的 CloudDom，本节提出了一种可信虚拟机管理模型 TVMM。该模型引入一个可信第三方来验证系统域是否可信，然后利用嵌入在硬件中的可信平台模块(TPM, trusted platform module)建立起可信通道，最后把用户策略安全的分发到系统域，从而保证策略的可信性，TVMM 模型的结构如图 4 所示。

TVMM 模型共有 4 个参与交互的实体，即用户、云服务提供商、管理员以及可信第三方。一个虚拟机节点启动后首先向可信证明代理注册，验证虚拟机节点身份的可信度，可信度量模块则向可信证明代理证明系统域的可信性。当使用云服务时，用户首先通过可信第三方的策略分发模块与系统域建立起可信的连接，然后提交用户策略，系统域根据这个策略创建策略代理、监控域、用户管理域和用户域，最后用户上传自己的应用。在 TVMM 模型运行过程中，管理员只能通过监控域来检查用户的合规约性，有效保证了用户的隐私和安全性。

TVMM 主要功能组件包括上下文感知访问控制模块、可信度量模块、可信证明代理模块、策略分发模块、策略管理模块、策略代理模块、虚拟机控制模块、资源管理模块和可信管理模块 9 个部分，其主要功能如下。

1) 上下文感知访问控制模块。约束云管理员的权限。上下文感知访问控制模块将管理角色的访问操作与其上下文（如空间、时间和平台可信等级等）建立起联系，动态地约束云管理角色的权限[17]。

表 2 CloudDom 及其特权

管理域	Hardware	S-Dom	A-Dom	G-Dom	U-Dom0	U-DomU
S-Dom	L, R	—	B, I, P, R	B, I, P, R	B, I, P, R	B, I, P, R
A-Dom	—	—	—	C, I, R	C, R	C, R
G-Dom	—	—	—	—	I, P, R	I, P, R
U-Dom0	—	—	—	—	—	C, I, P, R

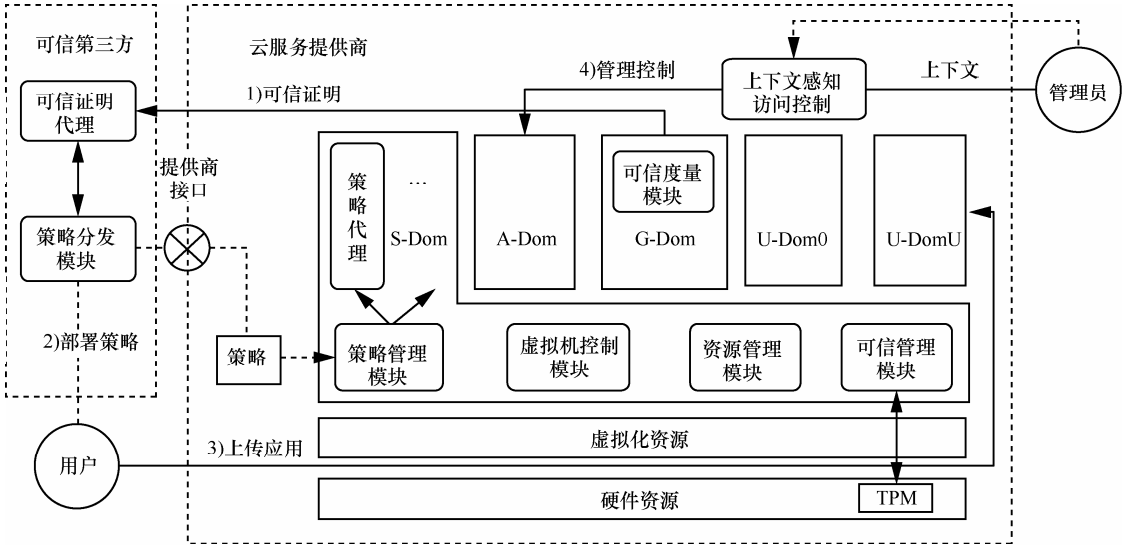

图 4　TVMM 模型的结构

2) 可信度量模块。负责度量系统的可信性并向可信证明代理模块报告。可信度量模块部署在监控域中，主要用来监控系统域在运行过程中的可信性，如果发生改变则实时地向可信证明代理模块汇报[18]。

3) 可信证明代理模块。负责获取云服务的可信度。可信证明代理模块通常由可信第三方维护，保存可信节点并将其配置信息记录到数据库中。在系统域运行过程中，如果可信度量模块检测到异常则向其发送度量记录，可信证明代理模块调整节点的可信度，并通知用户，用户根据需求选择是否继续使用服务。

4) 策略分发模块。负责建立起与系统域的安全连接并分发用户策略。当虚拟机向可信证明代理注册成功后，策略分发模块通过底层的 TPM 模块与系统域建立安全连接，用户使用虚拟机之前首先通过该安全连接分发自己的策略。

5) 策略管理模块。负责根据用户策略建立策略代理实例。用户分发自己的策略到系统域之后，策略管理模块创建一个新的用户策略代理，然后将策略发送给这个代理。如果用户重新改变了自己的策略，则策略管理模块负责更新操作。

6) 策略代理模块。负责执行相应虚拟域的用户策略。策略代理模块与每个用户对应，每个用户在系统域都运行着一个与之对应的策略代理实例，当用户关闭所有虚拟机并注销以后，策略代理实例也随之结束。

7) 虚拟机控制模块。负责执行虚拟机的创建、删除、启动、停止和迁移等操作。虚拟机控制模块负责根据系统和用户的需求创建和启动虚拟机，当用户注销后通过该模块停止和删除虚拟机。

8) 资源管理模块。提供虚拟化网络和存储服务。在云计算环境下，用户虚拟机需要访问其他的虚拟机和加载一些网络文件，资源管理模块负责对这些操作进行封装，虚拟机访问这些资源受到用户策略的控制。

9) 可信管理模块。负责完成所有基于 TPM 的可信操作。可信管理模块是对 TPM 的软件包装，主要完成 2 个工作：一是对平台进行完整性度量并将结果保存到 TPM 的配置寄存器中；二是生成受到 TPM 保护的密钥，用来建立一个连接到可信第三方的可信通道。

4.4　工作流程

虚拟机管理模型的工作流程主要包括可信通道建立和用户策略分发，具体步骤如下。

1) 可信通道建立。恶意管理员可以监听、篡改和重放网络数据。因此，必须在策略管理模块和策略分发模块之间建立一个可信通道。可信通道建立协议如图 5 所示。

图 5 中 $Cert_S$ 和 $Cert_T$ 分别为系统域 S 和可信第三方 T 的证书，SK_S 和 SK_T 分别为 S 和 T 的签名私钥，PK_S 和 PK_T 分别为 S 和 T 的签名公钥。M_S 为系统域的完整性信息。N_S 和 N_T 分别为 S 和 T 产生的随机数。SIG_S 和 SIG_T 分别为 S 和 T 产生的消息签名，SIG_S 为 $\{N_S|N_T|M_S\}_{SKS}$，SIG_T 为 $\{N_S\}_{SKT}$。K 为

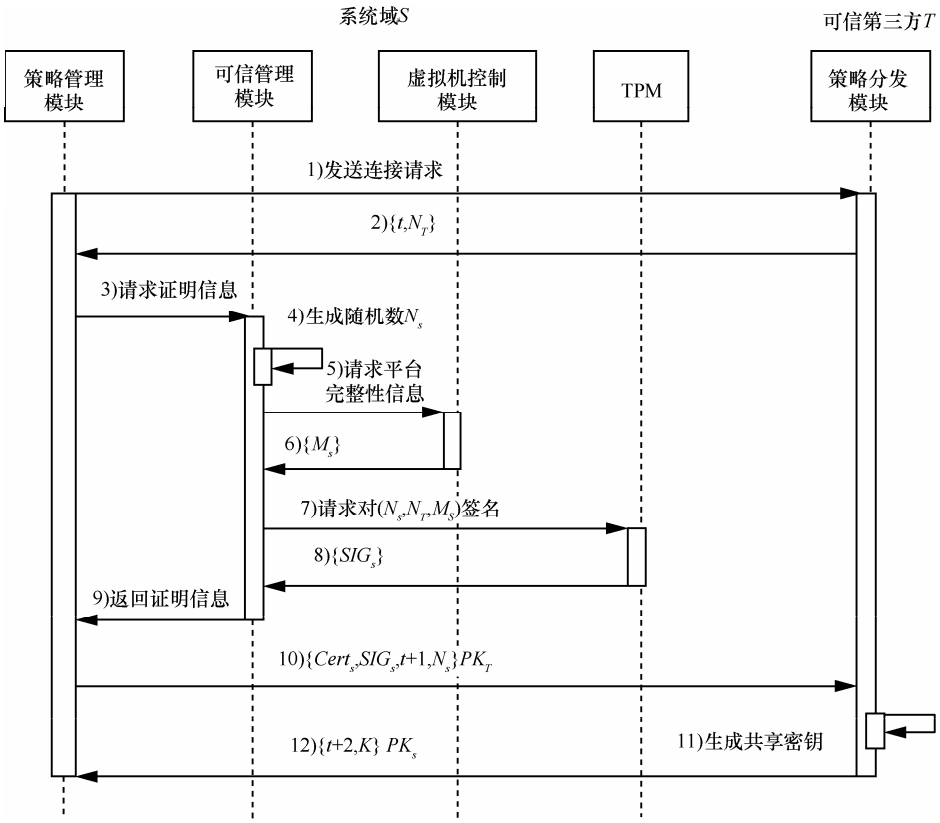

图 5　可信通道建立协议

S 与 T 之间产生的共享密钥。t 为当前时间戳。

该协议始终从虚拟域的策略管理模块发起。首先，策略管理模块向策略分发模块发送服务请求（第 1 步），策略分发模块选择一个随机数 N_T 并和时戳 t 一起发送给策略管理模块作为响应消息（第 2 步），策略管理模块收到策略分发模块的应答消息后向可信管理模块请求证明信息（第 3 步），可信管理模块首先生成一个随机数 N_S（第 4 步），然后通过虚拟机控制模块收集自身平台完整性信息 M_S（第 5~6 步），虚拟机控制模块调用 TPM 对(N_S, N_T, M_S)签名记为 SIG_S（第 7~8 步），策略管理模块得到证明信息($Cert_S$, SIG_S, t+1, N_S)后将其发送给策略分发模块（第 9~10 步），策略分发模块验证策略管理模块的可信性，如果验证成功，则根据随机数生成 N_S 共享密钥 K（第 11 步），最后将 K 发送给策略管理模块（第 12 步），系统域和可信第三方之间的通信均使用该密钥加密。

2) 用户策略分发。可信通道建立以后用户就可以将自己的策略分发到系统域中，随后系统域根据用户策略提供服务。详细的用户策略分发协议如图 6 所示。

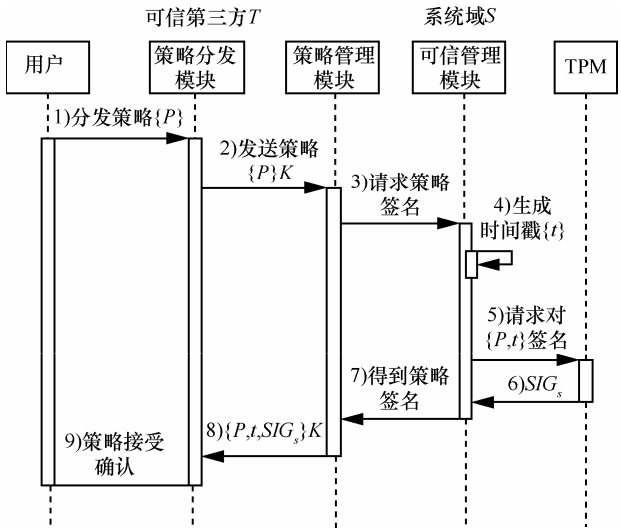

图 6　用户策略分发协议

系统域和可信第三方建立完成后，用户根据需求通过策略分发模块分发策略 P（第 1 步），策略分发模块使用系统域和可信第三方之间的共享密钥 K 加密 P，然后将加密后的策略发送给策略管理模块（第 2 步），策略管理模块调用可信管理模块对策略进行签名（第 3 步），为了防止重放攻击，可信管理模块生成时间戳 t（第 4 步），然后调用 TPM

的私钥对{*P*, *t*}进行签名（第 5 步），策略管理模块得到签名后用共享密钥 *K* 加密（第 6~7 步），然后将加密后的策略签名返回给策略管理模块（第 8 步），最后用户得到策略分发成功的确认信息（第 9 步）。

4.5　安全性分析

可信通道建立以后，可信第三方 *T* 与系统域 *S* 之间共享密钥 *K*，用户策略在分发过程中使用 *K* 进行加密，因此用户策略分发协议的安全性依赖于可信通道建立协议中协商的共享密钥的安全性。本节将系统域 *S* 与可信第三方 *T* 的通信报文（第 10 步和第 12 步）编号为 Message 1 和 Message 2，并对其进行相应的协议理想化处理，然后采用 BAN 逻辑对可信通道建立协议进行安全性分析验证。

1) 协议理想化

Message 1:

$$S \to T\text{: } \{Cert_S,\ \{N_S,\ N_T,\ M_S\}_{SK_S},\ t+1,\ N_S\}_{PK_T}$$

Message 2:

$$T \to S\text{: } \{\{t+2,\ K\}_{PK_S}\}_{SK_T}$$

2)初始化假设

① $T \mid\equiv S \mid\Rightarrow Cert_S$

② $S \mid\equiv T \mid\equiv K$

③ $T \mid\equiv \#(t)$

④ $T \mid\equiv \#(N_T)$

⑤ $S \mid\equiv \#(t)$

⑥ $S \mid\equiv \#(N_S)$

⑦ $T \mid\equiv \mid\xrightarrow{PK_T}T$

⑧ $T \mid\equiv \mid\xrightarrow{PK_S}S$

⑨ $S \mid\equiv \mid\xrightarrow{PK_S}S$

⑩ $S \mid\equiv \mid\xrightarrow{PK_T}T$

⑪ $S \mid\equiv T \mid\Rightarrow K$

3) 协议的安全目标

① $T \mid\equiv S \ni Cert_S$

② $T \mid\equiv T \xleftrightarrow{K} S$

③ $S \mid\equiv K$

4) 系统域身份认证

由 Message 1 利用接收消息规则(4)可以推出

$$\frac{T \lhd \{Cert_S,\ \{N_S,\ N_T,\ M_S\}_{SK_S},\ t+1,\ N_S\}_{PK_T},\ T \mid\equiv \mid\xrightarrow{PK_T}T}{T \lhd \{Cert_S,\ \{N_S,\ N_T,\ M_S\}_{SK_S},\ t+1,\ N_S\}}$$

由消息含义规则(1)可以推出

$$\frac{T \lhd \{Cert_S,\ \{N_S,\ N_T,\ M_S\}_{SK_S},\ t+1,\ N_S\},\ T \mid\equiv \mid\xrightarrow{PK_S}S}{T \mid\equiv S \mid\sim \{Cert_S,\ N_S,\ N_T,\ M_S,\ t+1,\ N_S\}}$$

由新鲜性规则(5)和临时值校验规则(3)可以推出

$$\frac{T \mid\equiv S \mid\sim \{Cert_S,\ t+1\},\ T \mid\equiv \#(t+1)}{T \mid\equiv S \mid\equiv Cert_S}$$

又由管辖权规则(2)可以推出

$$\frac{T \mid\equiv S \mid\equiv Cert_S,\ T \mid\equiv S \mid\Rightarrow Cert_S}{T \mid\equiv Cert_S}$$

结合 $T \mid\equiv S \mid\sim \{Cert_S\}$，从而推出：$T \mid\equiv S \ni Cert_S$，验证了 *S* 的身份。

5) 会话密钥的协商

由消息含义规则(1)可以推出

$$\frac{T \lhd \{N_S,\ N_T,\ M_S\}_{SK_S},\ T \mid\equiv \mid\xrightarrow{PK_S}S}{T \mid\equiv S \mid\sim \{N_S,\ N_T,\ M_S\}}$$

由临时值校验规则(3)可以推出

$$\frac{T \mid\equiv S \mid\sim \{N_S,\ N_T,\ M_S\},\ T \mid\equiv \#(N_T)}{T \mid\equiv S \mid\equiv N_S}$$

由接收消息规则(4)可以推出

$$\frac{T \lhd N_S,\ T \mid\equiv \#(N_T)}{T \mid\equiv \#(N_S,\ N_T)}$$

又由会话密钥规则(6)可以推出

$$\frac{T \mid\equiv S \mid\equiv N_S,\ T \mid\equiv \#(N_S,\ N_T)}{T \mid\equiv T \xleftrightarrow{K} S}$$

从而验证了 *T* 相信与 *S* 的共享密钥为 *K*。

由 Message 2 利用消息含义规则(1)和接收消息规则(4)可以推出

$$\frac{S \lhd \{\{t+2,\ K\}_{PK_S}\}_{SK_T},\ S \mid\equiv \mid\xrightarrow{PK_T}T}{S \mid\equiv T \mid\sim \{t+2,\ K\}_{PK_S},\ S \lhd \{t+2,\ K\}_{PK_S}}$$

由接收消息规则(4)可以推出

$$\frac{S \lhd \{t+2,\ K\}_{PK_S},\ S \mid\equiv \mid\xrightarrow{PK_S}S}{S \lhd \{t+2,\ K\}}$$

由临时值校验规则(3)可以推出

$$\frac{S \lhd \#(t+2),\ S \mid\equiv T \mid\sim \{t+2,\ K\}}{S \mid\equiv T \mid\equiv K}$$

又由管辖权规则(2)可以推出

$$\frac{S \mid\equiv T \mid\Rightarrow K,\ S \mid\equiv T \mid\equiv K}{S \mid\equiv K}$$

从而验证了 *S* 相信共享密钥 *K*，因此用户策略分发协议的安全性也得到了保证。

5 实现与分析

基于上节给出的虚拟机管理模型 TVMM，借助 TVD 技术，本节实现了一个虚拟机管理原型系统，然后使用 6 组攻击实例对原型系统的有效性进行了验证。

5.1 原型系统结构

图 7 给出了基于 TVMM 的虚拟机管理原型系统的总体架构。该系统采用 TVDc 方式构建，包括一个用于管理数据中心的内部网络 VDC，一个用于提供网络存储服务的 NFS 网络，以及用于管理虚拟机的 TVDmgn 网络和虚拟机之间的通信的 TVDdata 网络。底层的虚拟化平台基于 Xen 虚拟机，管理中心 VDC Admin、网络存储 Raw NFS 和访问控制 VDC Agent 分别使用 OpenStack 中的 Horizon、Swift 和 Keystone 组件[19]实现。

本原型系统主要实现了 4 个模块：TVD Master 模块、TVD Proxy 模块、TVD Proxy Factory 模块和 vNet 模块。其中，TVD Master 模块负责部署用户策略，TVD Proxy 模块负责管理用户策略，TVD Proxy Factory 负责管理 TVD Proxy 实例，vNet 模块负责管理虚拟机之间的通信。系统主要实现了 TVD 创建、VM 加入、VM 退出以及 TVD 销毁 4 个功能，具体过程如图 8 所示。

1) 创建 TVD。创建 TVD 的工作流如图 8(a)所示，TVD Proxy Factory 根据用户策略创建 TVD Proxy 实例（第 1)步），并保存返回的 TVD Proxy 实例编号 *PID*（第 2)~3)步），然后调用 vNet 模块创建隔离的虚拟网络（第 4)步），最后返回虚拟网络编号 *NID*（第 5)步）。

2) VM 加入。VM 加入的工作流如图 8(b)所示，VM 从 TVD Proxy Factory 模块获取 TVD 代理号 *PID*（第 6)~7)步），然后向 TVD Proxy 模块发起加入申请（第 8)步），TVD Proxy 模块根据策略验证 VM 是否符合能够加入该 TVD（第 9)步），如果验证成功，则将 VM 加入 TVD 虚拟网络中（第 10)步），最后返回虚拟网络编号 *NID*（第 11)步）。

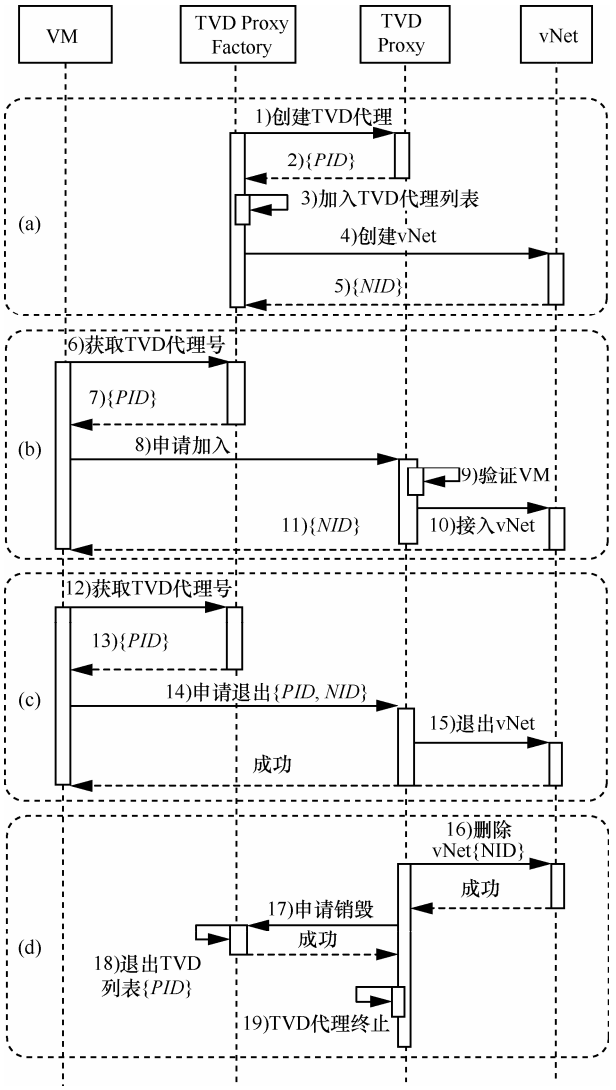

图 8 TVMM 原型系统工作流程

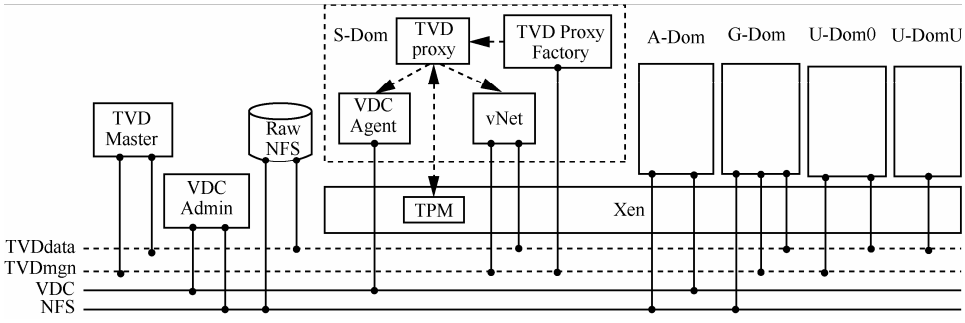

图 7 TVMM 原型系统架构

3) VM 退出。VM 退出的工作流如图 8(c)所示，首先，VM 从 TVD Proxy Factory 模块获取 TVD 代理号 *PID*（第 12)~13)步），然后向 TVD Proxy 模块发起退出请求（第 14)步），TVD Proxy 模块根据 *NID* 调用 vNet 断开 VM 的网络（第 15)步）。

4) TVD 销毁。TVD 销毁的工作流如图 8(d)所示，当检测到所有 VM 均退出 TVD 以后，TVD Proxy 调用 vNet 模块删除虚拟网络（第 16)步），然后向 TVD Proxy Factory 模块申请销毁（第 17)步），TVD Proxy Factory 模块从保存的 TVD Proxy 列表中删除该 TVD Proxy 编号（第 18)步），最后 TVD Proxy 终止运行（第 19)步）。

5.2　实验及分析

4.5 节对 TVMM 策略分发的安全性时进行了分析，表明了 TVMM 可以保证用户在分发策略时的安全，本节通过实验测试系统在保护用户数据机密性和完整性方面的有效性。

本实验假设基于硬件的安全机制（TPM）和 VMM 是安全的，忽略针对系统 CPU、TPM 的物理攻击。攻击者可以在任何时候读取、删除、篡改、伪造和篡改任何存储设备和通信链路的数据。根据虚拟机环境下攻击者通常攻击虚拟 CPU、物理内存、网络存储、网络和虚拟机镜像[20]，设计了 5 组攻击实例，如表 3 所示。

表 3　虚拟机攻击实例

攻击实例	攻击目标	说明
AT(1)	虚拟 CPU	调用特权操作读写虚拟 CPU
AT(2)	物理内存	调用特权操作映射物理内存
AT(3)	外部存储	访问虚拟机磁盘和主机磁盘
AT(4)	网络	监听虚拟机和主机网络
AT(5)	虚拟机映像	调用虚拟机迁移操作读写虚拟机映像

通常云基础设施普通使用 Xen 作为虚拟机管理程序，Xen 实现了 DMTF 提出的传统虚拟机管理模型。本节将 TVMM 与 Xen 以及相关工作中列举的 Terra 和 TVDc 进行对比（CIVIC 缺乏对平台本身的可信验证，而 NoHype 完全基于硬件实现，因此这 2 种模型不予对比）。

通过测试，得到 TVMM 与已有模型有效性测试对比结果如表 4 所示，其中“√”表示可以保证该安全属性，“—”表示不能保证该安全属性。

表 4　TVMM 与已有模型有效性测试对比结果

攻击实例	Xen	Terra	TVD	TVMM
AT(1)	—	√	—	√
AT(2)	—	√	—	√
AT(3)	—	—	√	√
AT(4)	—	—	√	√
AT(5)	—	—	—	√

1) AT(1)。每个虚拟机都有一个或多个虚拟机 CPU(vCPU)，这些 vCPU 用来保存虚拟机运行过程中的 CPU 寄存器的值。Xen 和 TVDc 的虚拟机管理域拥有读写 vCPU 的特权。AT(1)攻击调用虚拟机内省读操作可以破坏 vCPU 的机密性，调用虚拟机内省的写操作可以破坏 vCPU 的完整性。Terra 的可信虚拟机和 TVMM 的系统域和监控域在虚拟机运行过程中拥有这个特权，而这 2 个域是系统 TCB 的一部分。AT(1)通过系统管理域和用户管理域均无法调用虚拟机内省操作，因此，恶意攻击者无法破坏 vCPU 的机密性和完整性。

2) AT(2)。物理内存中保存虚拟机运行过程中所有代码和数据信息。Xen 和 TVD 的虚拟机管理域拥有通过虚拟机内省读写其他用户域的特权，AT(2)攻击调用虚拟机内省读操作可以破坏物理内存的机密性，通过虚拟机内省的写操作破坏物理内存的完整性。Terra 的可信虚拟机和 TVMM 的系统域和监控域在虚拟机运行过程中拥有这个特权，用户域和用户管理域没有虚拟机内省的特权，只能访问自己域对应的物理内存，这部分内存是独享的，攻击者无法通过这部分内存操作破坏其他域的机密性和完整性。虽然系统管理域在管理过程可以创建监控域，但是只能获取部分授权的物理内存，因此，恶意攻击者无法破坏物理内存的机密性和完整性。

3) AT(3)。Xen 的管理域和 Terra 的可信虚拟机负责运行外部存储驱动，其他用户域通过与管理域通信获取外部存储文件。AT(3)攻击通过读取、篡改存储内容来破坏外部存储内容的机密性和完整性。在 TVD 和 TVMM 中，系统管理域、用户管理域和用户域并不直接控制底层的外部存储驱动，所有外部存储中的文件均已使用用户的密钥进行加密 (Linux 下使用 dm-crypt 机制[21]，Windows 下使用 bitlocker 机制[22])，在运行过程中，只有系统域才能获得用户密钥，因此，无论

是通过其他域读写文件还是直接访问外部存储器，攻击者均无法破坏外部存储的机密性和完整性。

4) AT(4)。Xen 的管理域和 Terra 的可信虚拟机负责运行虚拟网络驱动，用户域之间经管理域进行通信。AT(4)攻击通过监听和篡改用户域的网络数据破坏网络内容的机密性和完整性。在 TVD 和 TVMM 中，系统域负责运行虚拟网络驱动，而其他域采用可信虚拟域的方式组织，限制了管理域、用户管理域和用户域的访问范围。当系统域与其他物理实体通信时，所有的报文都是经过加密的，并且数据使用前都进行了完整性检验，只有在虚拟域运行过程中才能解密网络报文。因此，无论是通过监听虚拟网络还是直接监听物理网络，攻击者均无法破坏网络内容的机密性和完整性。

5) AT(5)。虚拟机映像是特殊的外部存储文件，虚拟机通过加载映像运行虚拟机实例。AT(5)攻击将 Xen、Terra 和 TVDc 中虚拟机迁移到一台自己控制的虚拟主机，通过新的主机来操纵虚拟机映像，完全绕过了原来的安全防护。在 TVMM 模型中，只有系统域才能加载虚拟机映像，用户管理域和用户域只能在这些虚拟机之上运行自己的应用。虽然系统管理域可以迁移虚拟机到其他主机上，但是这些主机都经过了可信第三方的认证，恶意攻击者无法完全控制，保证了虚拟机映像的安全。

通过以上的测试分析可以看出，相比传统虚拟机管理模型 Xen 和现有的可信虚拟机管理模型 Terra 和 TVDc，TVMM 模型可以有效保证虚拟 CPU、物理内存、网络存储、网络和虚拟机镜像的安全，为用户提供可信的云计算环境。

6 结束语

针对云计算环境下基础设施管理的特点和需求，本文提出了一种可信虚拟机管理模型 TVMM。模型对虚拟机管理域进行了更细粒度的划分，赋予不同的管理特权，解决了管理域特权过于集中导致的安全性问题。模型使用可信计算技术建立起可信通道，通过该通道分发用户策略，保证了用户策略在云端的可信性。

云计算平台由多个用户共享使用，策略配置不当容易造成策略冲突。攻击者可以通过冲突的策略绕过安全防护，任意访问用户的隐私数据。因此，下一步的重点是研究形式化检测模型策略冲突的方法，并且设计相应的冲突消解策略。

参考文献：

[1] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报, 2011, 22(1), 71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1), 71-83.

[2] 黄瑛, 石文昌. 云基础设施安全性研究综述[J]. 计算机科学, 2011, 38(7): 24-30.
HUANG Y, SHI W C. Survey of research on cloud infrastructure security[J]. Computer Science, 2011, 38(7): 24-30.

[3] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing[A]. Proc of the Workshop on Hot Topics in Cloud Computing[C]. 2009.

[4] Architecture for Managing Clouds[EB/OL]. http://www.dmtf.org/sites/default/ files/standards/documents/DSP-IS0102_1.0.0.pdf.

[5] ABBADI I, RUAN A. Towards trustworthy resouce scheduling in clouds[J]. Information Forensics and Security, IEEE Transactions on, 2013, 8(6) : 973-984.

[6] JOSHUA S, THOMAS M, HAYAWARDH V, *et al*. Seeding Clouds with Trust Anchors[R]. Network and Security Research Center, 2010.

[7] Trusted Computing Group - TCG Architecture Overview, Version 1.4 [EB/OL].http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14

[8] GARFINKEL T, PFAFF B, CHOW J, *et al*. Terra: a virtual machine-based platform for trusted computing[J]. ACM SIGOPS Operating Systems Review, 2003, 37(5):193-206.

[9] 怀进鹏, 李沁, 胡春明, 基于虚拟机的虚拟计算环境研究与设计[J]. 软件学报, 2007, 18(8):2016-2026.
HUAI J P, LI Q, HU C M. Research and design on hypervisor based virtual computing enviroment[J]. Journal of Software, 2007, 18(8):2016-2026.

[10] BERGER S, CACERES R, PENDARAKIS D E, *et al*. TVDc: managing security in the trusted virtual datacenter[J]. Operating Systems Review, 2008, 42(1):40-47.

[11] KELLER E, SZEFER J, REXFORD J, *et al*. NoHype: virtualized cloud infrastructure without the virtualization[A]. Proc of the 37th Annual International Symposium on Computer Architecture[C]. 2010.

[12] VMware GSX server[EB/OL]. https://www.vmware.com/products/gsx/.

[13] GRIFFIN J, JAEGER T, PEREZ R, *et al*. Trusted virtual domains: toward secure distributed services[A]. Proc of the First Workshop on Hot Topics in Systems Dependability[C]. 2005.

[14] BUSSANI A, GRIFFIN J, JANSEN B, *et al*. Trusted Virtual Domains: Secure Foundations for Business and It Services[R]. IBM

Research, 2005.

[15] ABADI M, TUTTLE M R. A semantics for a logic of authentication[A]. Proc of the Tenth Annual ACM Symposium on Principles of Distributed Computing[C]. 1991.

[16] BARHAM P, DRAGOVIC B, FRASER K, *et al*. Xen and the art of virtualization[A]. Proc of the Nineteenth ACM Symposium on Operating Systems Principles, 2003.

[17] ZHOU Z J, WU L F, HONG Z. Context-aware access control model for cloud computing[J]. Journal of Grid and Distributed Computing, 2013, 6(6):1-12.

[18] ZHOU Z J, WU L F, HONG Z, *et al*. DTSTM: dynamic tree style trust measurement model for cloud computing[J]. KSII Transactions on Internet and Information Systems, 2014, 8(1): 305-325.

[19] Openstack open source cloud computing software[EB/OL]. https:// www. openstack.org/.

[20] KAUFMAN L M. Can public cloud security meet its unique challenges [J]. IEEE Security and Privacy, 2010, 8(4): 55-57.

[21] Dm-crypt: a device-mapper crypto target[EB/OL]. http://www.saout.de/misc/dm-crypt/.

[22] Help protect your files using Bitlocker drive encryption[EB/OL]. http:// windows. microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption/

作者简介：

周振吉（1985-），男，江苏连云港人，解放军理工大学博士生，主要研究方向为虚拟化安全，云计算安全。

吴礼发（1968-），男，湖北蕲春人，博士，解放军理工大学教授、博士生导师，主要研究方向为网络安全。

洪征（1979-），男，江西南昌人，博士，解放军理工大学副教授，主要研究方向为网络安全。

赖海光（1975-），男，贵州平坝人，博士，解放军理工大学副教授，主要研究方向为网络安全。

郑成辉（1977-），男，河南光山人，硕士，解放军理工大学讲师，主要研究方向为网络安全。