云计算中动态完整性传递模型研究

姜 路，鹤荣育
（解放军信息工程大学，郑州 450000）

摘 要：针对云平台中虚拟机动态完整性难以保证的问题，基于完整性度量机制，提出了一种虚拟机间动态完整性传递模型。该模型在虚拟机监视器中设计了一个验证模块，验证输入者及输入数据的完整性，保证了虚拟机之间在传输数据或指令时的动态完整性，且传递的消息完整性也得到验证。基于无干扰理论对模型可信性进行了证明，最后用两组实例验证了该模型的可用性。实验结果表明，该模型对不可信输入和不可信平台都有较好的抵御能力。

关键词：云计算；可信计算；动态完整性；信任链；无干扰
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2014)05-1503-04
doi:10.3969/j.issn.1001-3695.2014.05.053

Research of dynamic integrity-transmit model in cloud

JIANG Lu, HE Rong-yu
(*PLA Information Engineering University, Zhengzhou* 450000, *China*)

Abstract: For the problem of VM's dynamic integrity supporting, and using integrity measurement mechanisms, this paper proposed a dynamic integrity-transmit model in-VMs. The model designed a verification module in virtual machine monitor to verify the importer's and the input data's integrity. Thus the VM's instant integrity would be ensured and the input data's integrity be verified as well. Using non-interference theory it proved the model's credibility. Finally, it validated two examples of the availability of the model. Experimental results show that the model can against untrusted input or untrusted platform.

Key words: cloud computing; trusted computing; dynamic integrity; trust chain; non-interference

0 引言

随着云计算的发展与广泛应用，云安全越来越受到业界的关注。云计算通过虚拟化技术在一台计算机上模拟出多个隔离的计算环境，这些隔离的虚拟计算环境被称为虚拟机。云计算平台中的虚拟机需要严格隔离，以保证云平台安全。为保证各虚拟机可信与可控，需要保证各虚拟机的完整性。可信计算[1~3]给云安全带来了全新的解决方案，把可信计算应用到云计算已经越来越成为业界的热点[4]。通过对可信计算技术的虚拟化能够构建可信云平台[5,6]。可信云平台通过 TPM 的虚拟化，为虚拟机建立虚拟机的完整性。

可信云平台基于虚拟 TPM(vTPM)[7]度量与报告机制，保证启动时，信任链从可信平台模块(TPM)[3]中的 CRTM 扩展到 vTPM 到每个虚拟机。但由于 vTPM 在系统启动后，就不再不断检查系统的完整性，所以它只能保证虚拟机的静态完整性。

仅确保虚拟机静态完整性对虚拟机安全来说远远不够，一个安全虚拟机必须能够抵御来自其他虚拟机的通信与数据流通中带来的威胁。强隔离不能正确控制程序间通信和数据流通，也不能有效地进行访问控制[8]。尽管一个虚拟机的资源被隔离在一个安全的隔离区，但后门程序还是可以通过向其注入非法输入，从而影响该程序的完整性。如果此程序从网络上获取输入，那么输入很可能被窃听或者被操作系统层恶意软件更改。

在信任的传递方面，很多学者在各个级别作了很多研究。在 TCG 规范中[1]，规定信任是从可信度量根 CRTM 一直延续到应用软件，形成一条完整的信任链。但在云计算平台中，由于应用了虚拟化技术，可信的传递已经受到了传统平台上传递的限制。当信任链传递到虚拟机监视器的时候，再继续传递到客户虚拟机将是一个挑战性工作，并且在虚拟机之间不存在信任链，不能保证虚拟机通信时可信。文献[9]提出了基于无干扰模型的信任链传递模型，指出只有在不存在非预期干扰的情况下，TCG 规定的信任链传递才是有效的，并提出了形式化的模型及证明。但其具体实现的方法并没有给出详细的方案。

文献[10]设计的 SecureBus 致力于在进程级别检测输入的可信性，SecureBus 位于进程与操作系统内核之间，并做到对上层进程和下层内核的通明性。然而 SecureBus 只是针对于普通平台，在云平台上的应用还有待进一步研究。

文献[11]提出了基于进程级别的系统的可信条件，从可信定义出发，证明了一个系统运行时的可信条件。然而运行时的可信方案也没有给出。文献[5]提出了一种 TCTVM 模型，给出了信任链从虚拟机监视器到用户虚拟机的解决方案，并给出了面向用户的 vTPM。但运行时的可信没有给出，在模型 TCTVM 中也没有考虑虚拟机之间的相互干扰问题。

本文在 TCTVM 模型基础上，针对虚拟机的动态完整性问题，提出了虚拟机间信息传递完整性模型。此模型通过在虚拟

收稿日期：2013-07-02；**修回日期**：2013-08-05

作者简介：姜路(1990-)，男，安徽蒙城人，硕士研究生，主要研究方向为云计算、虚拟机隔离(849148146@qq.com)；鹤荣育(1966-)，河南遂平人，教授，硕导，主要研究方向为信息安全、云计算.

器监视器中添加虚拟机输入验证模块(input authentication module for virtual machine, IAMV),使虚拟机在启动后能够保证其完整性。

1 IAMV 研究

1.1 IAMV 模型设计

针对云平台在启动后就不能保持即时可信的问题,本文提出虚拟机输入验证模型(IAMV)。该模型的设计目标如下:

a)以虚拟机域为对象,简化虚拟机之间的干扰。虚拟机接收到的数据、指令等,一律视为输入。在虚拟机相互通信时,建立一条信任链。

b)在平台启动时建立信任链之后,虚拟机域之间仍然有信任链的传递,能够保持可信的实时性。

c)虚拟机之间的通信应该都经过 IAMV,即在虚拟机之间不存在直接的指令、共享内存等通信方式。虚拟机与底层的 Xen 交互时也需要经过 IAMV。

d)IAMV 应该对上层的虚拟机透明,即客户虚拟机应该能在不作任何改动的情况下兼容 IAMV。

IAMV 模型如图 1 所示,此平台在虚拟机监视器中加入了一块输入验证模块 IAMV,负责虚拟机之间传递数据时验证完整性。平台的可信性是由 TCG 标准信任链保证,完整性从底层的硬件 TPM 一直传递到 Xen 监视器中。各个客户虚拟机利用了 TPM 的虚拟化技术[7],为每一个客户虚拟机提供一个虚拟 TPM(vTPM)。

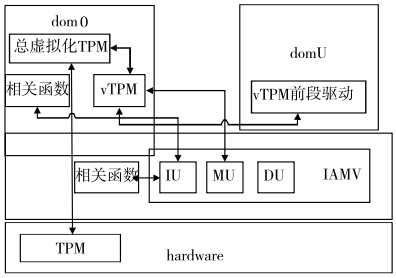

图1 IAMV模型

IAMV 按照功能可划分为四个单元模块,分别是信息库单元(database unit,DU)、截取单元(intercept unit, IU)、度量单元(measure unit, MU),如图 2 所示。

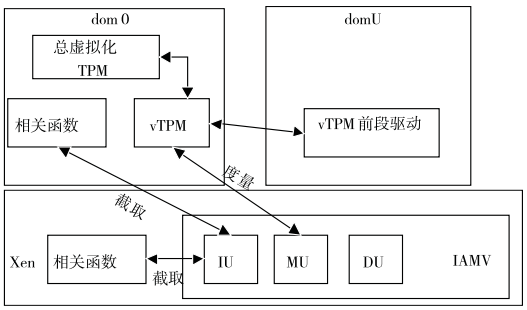

图2 IAMV结构

1)信息库单元 DU

DU 是一个数据库。在 IAMV 启动时,为 DU 在特权 1 的权限上开辟一定的空间,且 DU 为空。在各个域创建的时候,IU 会把每个域的信息在 DU 中注册。其中包括虚拟内存、虚拟 CPU 等信息。这些信息中最重要的是关于域的边界信息。当一个 VM 的信息有更改的时候,IU 单元会把相应更改更新到 DU 中。DU 只有提供给 IU 的接口,只能供 IU 访问和修改。在 IU 对操作进行判断的时候,需要比对 DU 中的信息来确定一个操作是否越界,即此操作是否在该域的范围之内。当系统掉电的时候,DU 会销毁其中的信息。

2)截取单元 IU

IU 是 IAMV 中最活跃的单元,也是 IAMV 的门户。其功能主要是利用钩子函数,把需要 IAMV 截取的指令都传递到 IAMV 中来。这些指令主要包括两类:a)关于域的边界有改变指令,比如域的创建与销毁,域边界的扩张域缩小;b)域中的越界指令,即域中对域以外的内容的访问与修改。在域创建时,IU 能够截取到域创建的指令,在 MU 处理通过之后将该域的信息在 DU 中注册。IU 能够区分一个指令是否越域,如果是 IU 就能够拦截这个指令并交给 MU 来处理,如果该指令没有越域,则指令能够正常执行。IU 的钩子函数主要分布在 dom0 和 Xen 中,与 dom0 的创建域和管理域的函数相关联;在 Xen 中,与关于域间通信的函数相关联。

3)度量单元 MU

MU 是 IAMV 的核心处理单元。经过 IU 的判断,需要继续处理的指令将由 MU 来度量其完整性。在域创建的时候,MU 还负责度量域代码的功能,MU 利用物理 TPM 的度量功能来进行此次度量。对于指令的度量,度量的功能是借用 vTPM 的。在平台中,每一个 VM 都有自己的 vTPM,当一个 VM 的一个越域指令发送给 MU 之后,MU 就给此 VM 的 vTPM 发送一个度量的指令,借助 vTPM 的功能来度量这个指令和此 VM 的完整性。由所在 VM 的 vTPM 来度量有很高的效率,且能减轻物理 TPM 的负担。vTPM 将度量值与标准值比对,如果与标准值相同,说明此 VM 和指令都可信。如果有一项与标准值不同,vTPM 会给出不可信的结果。在判断完成后,vTPM 将结果发给 MU。MU 接收到可信的结果会执行该指令,否则 MU 将终止该指令的执行,并将此指令的错误信息返回。

1.2 动态完整性传递

在平台启动时,平台会建立一条信任链,一直从硬件 TPM 延伸到 vTPM,再到虚拟机上的应用程序[1~3]。然而只有启动时的可信还是不够的,恶意软件能够在运行时通过其他方法寄生到虚拟机中去。它可能通过一个数据的输入,或者通过一段代码的共享,从而进入另一虚拟机,影响另一个虚拟机的可信。所以在运行时度量虚拟机的完整性、输入数据的完整性是很有必要的。

虚拟机完整性传递过程如图 3 所示。图中输入者虚拟机用 VM_1 表示,被输入者虚拟机用 VM_2 表示。为了表示方便,把设置在 Xen 中的钩子函数省去,表示为虚拟机直接与 IAMV 的交互。图中虚箭头指示了从表面上看数据的流向,而实箭头则表示数据的真实流向以及验证过程。假设输入 D_0 的完整性已经被验证过,产生此数据的虚拟机 VM_0 的完整性也已验证过。VM_1 接收数据 D_0 且产生数据 D_1,D_1 是 VM_2 的输入数据,I_1 为中间过程中的完整性度量值,$H(\ )$ 为 hash 函数。验证过程如表 1 所示。

表 1 完整性传递过程

步骤	验证过程	数据
a)	IAMV→VM_1	D_0
b)	VM_1	$I_1 = H(H(D_0) \| \| H(VM_1) \| \| H(D_1))$
c)	VM_1→IAMV	$D_1, I_1, H(D_0), H(VM_1)$
d)	IAMV	验证 D_1, I_1
e)	IAMV→VM_2	D_1

a)VM_1 接收数据 D_0,产生输出数据 D_1,且产生 D_0 的虚拟机已被验证,其状态可信。所以 D_0 不会影响 VM_1 的完整性。

b)由虚拟机 VM_1 的 vTPM 计算出 I_1。这其中要计算 VM_1 的 hash 值,就利用 TPM 对当前的 VM_1 进行运算。

c)VM_1 把 D_1、I_1、$H(D_0)$、$H(VM_1)$发送给 IAMV。

d)IAMV 接收到这些数据后,判断 D_1、VM_1 是否可靠。如果不可靠则不发送 D_1。

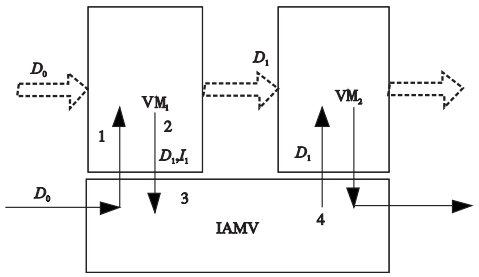

图3　动态完整性传递过程

如果 IAMV 验证通过了 D_1、VM_1,就把 D_1 发送给 VM_2。还要明确的是 IAMV 并不能监测攻击,对于针对 VM 漏洞的攻击,例如缓冲溢出攻击,IAMV 也是无能为力。可信计算并不能保证程序运行在没有错误的环境下[8]。然而,当一个 VM 的输入和输入者已经被验证可信时,IAMV 却能保证 VM 运行时的完整性以及它产生的输出的完整性。

上述验证方法可以适用于 domU 与 domU 之间的通信,也可以验证 domU 与 dom0 之间的通信。对于传统的虚拟机之间的通信方式,例如超调用、中断、事件通道等,IAMV 都能通过验证代码的完整性保证输入的可信。对于共享内存、授权表、或者共享文件的数据交流方式,IAMV 需要在共享内存建立的时候就保证其可信,具体细节则不在本文的研究范围之内。

2　IAMV 的可信性

信息流的无干扰思想于 1982 年提出,此后便有很多基于信息流无干扰模型的理论研究出现[12~14]。本文依据无干扰理论提出此框架的模型,并对其进行验证,借用 Rushby[15] 的模型并作了一定的修改。由于研究的对象是虚拟机,本文简化了动作序列,改为输入序列,并且对于非预期的、对研究系统有干扰的动作序列一律视为非法的输入序列。

2.1　基本符号与定义

根据可信的概念,输出和状态符合预期,定义一个域的模型。这里所说的域,即一个虚拟机,包括虚拟机管理器提供的虚拟硬件、客户操作系统、上层应用等。为了简化模型,研究的重点是域与域之间的干扰,而不考虑域中的程序之间的干扰,且假设域中使用了较强的可信技术手段,已经保证进程的单步隔离性、输出隔离性、状态转移可信等[9]。以域作为一个系统定义如下。

定义 1　一个系统 $M=(S,A,O,F)$应包含如下元素:

S:系统状态集合,包含一个初始状态 s_0,元素用小写字母"$s,t\cdots$"表示。

A:系统输入集合,用"$a,b\cdots$"表示输入集中的元素;用"$\alpha,\beta\cdots$"表示输入序列;空输入用 Λ 表示;输入之间的连接用。表示;输入序列的集合用 A^* 表示;定义合法输入集合 A_+,A_+ 的补集为非法输入 A_-。

O:系统运行输出结果集合。

F:函数集。

a)单步函数。$\text{step}:S\times A\to S$,系统状态经过执行单个输入后到达下一个状态。

b)系统运行函数。$\text{run}:S\times A^*\to S$,系统在运行一个输入序列后的状态变迁。

c)结果输出函数。$\text{output}:S\times A\to O$,表示系统在当前状态下执行输入后产生的结果。

定义 2　定义状态集合 S 上的二元关系"~"为等价关系。

定义 3　函数 $\text{clear}(\alpha):A^*\to A^*$ 归纳定义为:$\forall a\in A,\forall\alpha\in A^*$,有

$$\text{clear}(\Lambda)=\Lambda$$

$$\text{clear}(a\circ\alpha)=\begin{cases}a\circ\text{clear}(\alpha) & \text{if } a\in A_+\\ \text{clear}(\alpha) & \text{otherwise}\end{cases}$$

此函数的作用是去除输入序列中的非法输入,从而使输入都是有意义的输入队列。

定义 4　形式化定义系统运行可信性:$\forall\alpha\in A^*$,$\forall a\in A$ 有下式成立

$$\text{output}(\text{run}(s_0,\alpha),a)=\text{output}(\text{run}(s_0,\text{clear}(\alpha)),a)$$

运行可信性表明,系统并不受非法输入的影响,输出还能保持预期。

定义 5　定义系统的无干扰性:$\forall s\in S,\forall\alpha\in A^*$

$$\text{run}(s,\alpha)\sim\text{run}(s,\text{clear}(\alpha))$$

系统的无干扰性表明,系统的状态能够在非法输入的影响下,保持预期的状态。

定义 6　定义输出一致性。$\forall s,t\in S,\forall a\in A$,满足下式:

$$s\sim t\to\text{output}(s,a)=\text{output}(t,a)$$

则称系统 M 有输出一致性,即系统的两个状态等价,那么在相同的输入下有相同的输出。

定理 1　系统 M 满足无干扰性和输出一致性,则能推出系统满足运行可信性。

证明　因为 M 具有无干扰性:

$$\text{run}(s,\alpha)\sim\text{run}(s,\text{clear}(\alpha))\tag{1}$$

因为 M 具有输出一致性:

$$s\sim t\to\text{output}(s,a)=\text{output}(t,a)\tag{2}$$

把 s_0 代入式(1)得

$$\text{run}(s_0,\alpha)\sim\text{run}(s_0,\text{clear}(\alpha))\tag{3}$$

由式(2)(3)可得

$$\text{output}(\text{run}(s_0,\alpha),a)=\text{output}(\text{run}(s_0,\text{clear}(\alpha)),a)$$

从而 M 满足运行可信性。证毕。

定义 7　定义系统 M 的单步无干扰性,$\forall s\in S,\forall a\in A_-$ 有下式成立:

$$s\sim\text{step}(s,a)$$

系统的单步无干扰性表明,系统在非法输入前后的状态是等价的。

定义 8　定义系统 M 的单步隔离性,$\forall s,t\in S,\forall a\in A_-$ 有下面关系成立:

$$\text{若 } s\sim t,\text{则 } \text{step}(s,a)\sim\text{step}(t,a)$$

单步隔离性表明,两个等价系统状态在非法输入的影响下,还是等价的。

2.2　IAMV 模型的形式化

系统的运行过程可以看成是在一系列输入序列作用下造成的状态转移。为简化问题,模型仅考虑单处理器系统的情况,即系统只能对输入一个一个串行地执行。因此可以理解系统的运行就是系统处理一个个输入,在输入的作用下状态转移并输出结果的过程。

定义 9　系统可达状态,即系统通过运行能够到达的状态。若 $\exists\alpha\in A^*$,使得 $s=\text{run}(s_0,\alpha)$,则称 s 是系统可达状态。

定义 10　定义系统可信状态。系统可达状态 $s=\text{run}(s_0,\alpha)$,若满足下式

$$\text{output}(s,a) = \text{output}(\text{run}(s_0,\text{clear}(\alpha)),a)$$

则称系统可达状态 s 为可信状态。可信状态依据可信的定义，从状态和输出两个方面对预期进行判断，若状态和输出都符合预期，则说明该可达状态 s 可信。

定理 2 若系统具有无干扰性、输出一致性，则系统的每个可达状态都是可信状态。

证明 由系统的无干扰性，$\forall s \in S, \forall \alpha \in A^*$

$$\text{run}(s,\alpha) \sim \text{run}(s,\text{clear}(\alpha)) \tag{4}$$

设可达状态为 s_1，则存在 $\alpha_1 \in A^*$ 使得 $s_1 = \text{run}(s_0,\alpha_1)$，把 s_0、α_1 代入式(4)得

$$\text{run}(s_0,\alpha_1) \sim \text{run}(s_0,\text{clear}(\alpha_1))$$

即

$$s_1 \sim \text{run}(s_0,\text{clear}(\alpha_1))$$

由输出一致性，对于 $\forall a \in A$：

$$\text{output}(s_1,a) = \text{output}(\text{run}(s_0,\text{clear}(\alpha_1)),a)$$

从而可达状态 s_1 是可信状态。证毕。

定义 11 可信系统。当系统满足下面两个条件时，称该系统为可信系统。

1）系统的初始状态 s_0 是可信状态。

2）系统的每个可达状态都是可信状态。

该定义是可信系统的充分条件，可作为判断系统是否可信的条件。

定理 3 若系统具备以下三个条件，则系统是可信系统。

1）系统从可信根开始运行。

2）系统具有无干扰性。

3）系统具有输出一致性。

证明 要证明系统可信，只要证明系统满足定义 11 的两个条件即可。

根据条件 1）系统从可信根开始运行，可知系统的启动状态由设计者的密码技术和物理方法保证，是一种无条件的可信。所以 s_0 是可信状态。

由定理 2 易知由条件 2）3），可以得出系统的每个可达状态都是可信状态，这里不再赘述。

2.3 可信性验证

要证明 IAMV 模型的可信性，只要证明了定理 3 的三个条件即可。

证明 在 dom0 创建 domU 时，假设 dom0 是可信基的一部分，所以 dom0 和创建过程都是可信的。且架构给域 domU 提供了 vTPM，确保了 domU 的启动可信，这就保证了系统从信任根开始运行。条件 1）满足。

由于本文设计的架构，对所有的输入都有一个对完整性检查的过程，所以能够对输入鉴别 $a \in A_+$ 或者 $a \in A_-$。对于输入 a 是非法输入，在 Xen 中的组件 IAMV 会采取禁止输入的方式来解决。所以此架构对输入序列 α 和 $\text{clear}(\alpha)$ 是有一样的效果的。即有 $\text{run}(s,\alpha) \sim \text{run}(s,\text{clear}(\alpha))$，架构满足系统无干扰性。条件 2）满足。

由于系统对于非法输入采取的是禁止输入的方式，所以对于状态 $\text{run}(s,\alpha)$ 和 $\text{run}(s,\text{clear}(\alpha))$ 是相同状态，所以在它们会有相同的输出，即满足输出一致性。条件 3）满足。

由此证明构建的系统是可信的。

3 实验及结果分析

为验证模型的可用性，实验通过两个小组实验来分别验证模型对非法情况的处理。实验环境为 Fedora 10，Linux 内核版本为 2.6.32.26，虚拟机监视器为 Xen 4.0。硬件环境：计算机为 ASUA K43SJ，Intel Core i5-2410M，RAM 2.00 GB。

实验 1 目的在于验证 IAMV 对输入的验证情况。用 Xen 监视器创建虚拟机 dom_1、dom_2。在 dom_2 中编写应用程序 Hello World，程序代码如下：

```
fd = open("hello.txt",O CREAT |O RDW R, \
        S IRUSR|S IWUSR);
if(fd){
  write(fd, "hello world!"
  strlen("hello world!"));
  close(fd);
}
```

把它保存在文件夹/home/piano/code/sys_file 中，其对应的度量值为：0c772110d4f010ce3442f95e827e173789409bbd，并把此度量值保存在 DU 中。在 dom_1 中调用 Hello World 函数，在没有窜改其代码的情况下，能够正常调用。

把 Hello World 的代码稍作修改如下：

```
fd = open("hello.txt",O CREAT |O RDW R, \
        S IRUSR|S IWUSR);
if(fd){
  write(fd, "HELLO WORLD!"
  strlen("hello world!"));
  close(fd);
}
```

即把"hello world"改为"HELLO WORLD"，更改后度量值为：2b0b56af6dbd91fc0ad2cfd035c451da7e202134，再次在 dom_1 调用 Hello Wrold 函数，MU 将此度量值与 DU 中的值比对，则不能成功调用，并出现错误信息："传输数据或代码不可信！

实验 2 目的是在输入没有被窜改的情况下，平台状态的可信性。当在 dom_1 中调用 dom_2 中的 Hello World 函数时，IAMV 不仅验证了函数的完整性，还要验证 dom_2 的完整性。如果平台状态在一个可信的状态，即规定的关键部分的度量值与 DU 中存储的对比值相同，则调用能够顺利进行，反之则不能。

实验 2 把 Hello World 函数的源码放置在 dom_2 的/sbin 目录下。而这个目录下是 IAMV 检测的内核关键位置，在虚拟机运行中不允许有改动。再次通过 dom_1 调用 Hello World 函数，调用不成功，返回信息为：输入者平台存在风险！

由以上两组实验表明，IAMV 模型对输入数据以及输入数据的平台有一定的验证性，在一定程度上保证了云平台计算环境的安全。

4 结束语

本文在简要介绍了完整性度量机制、可信技术虚拟化、以及前人研究成果的基础上，提出了一种虚拟机间完整性传递模型，使虚拟机之间在传输数据或指令时能够保证虚拟机即时的完整性，且能够保证传递的消息内容的完整性。对此模型进行了完整性证明，表明此系统是可信的。

由于可信并不等于安全，保证了可信并不能抵制恶意软件的攻击。接下来的工作主要有：a）应用适当的策略对虚拟机关键资源进行访问控制；b）对虚拟机中的恶意软件进行动态监测；c）考虑虚拟机在运行期间可能存在的对其他虚拟机的干扰；d）优化系统结构，减少系统安全漏洞。

参考文献：

[1] TCG specfication architecture overview [EB/OC]. https://www.trustedcomp-utinggroup.org.

[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学：信息科学，2007，37(2)：129-150.

（下转第 1510 页）

5 结束语

根据以上的分析可知,基于身份的认证加密方案是安全的,所以该政府内网中的电子公文交换模型在发送者加密、接收者解密、私钥分发等方面均保证了完整性和安全性。并且该 IBE 方案的加密速度比一般的 IBE 加密要快,就保证了电子公文传送的效率。同时提出了一种新的私钥共享方案,解决了 IBE 方案的密钥托管问题。通过对比分析可知,该私钥共享方案效率和安全性都较高,使得该系统应用更方便。

参考文献:

[1] 官盱玲. 电子公文应用的不安全因素及对策[J]. 江西行政学院学报,2004,6(4):84-86.

[2] 陈晓辉. 电子公文:能走多远——我国电子公文档案管理五大问题剖析[J]. 档案与建设,2012(8):10-13.

[3] 张晓芳. 电子公文系统的安全性研究[J]. 数字技术与应用,2013(2):175.

[4] 丁惠春. PKI 及其在电子政务中的应用研究[D]. 西安:西北工业大学,2005.

[5] 苏锐丹. 电子政务安全工程若干关键技术研究[D]. 西安: 西安电子科技大学,2010.

[6] 姜岚, 王宏滨. PKI/CA 技术在电子政务中的应用[J]. 黑龙江科技信息,2010(12):68- 69.

[7] 蔡谊, 沈昌祥. PKI 技术在电子政务中的应用[J]. 计算机应用研究,2002,19(10):11-13,16.

[8] 程程. PKI 技术在电子政务中的应用研究[D]. 重庆:重庆大学,2004.

[9] 杨硕,周乐,陈茂兴. PKI 技术及其在电子政务中的应用[J]. 电子科技大学学报:社科版,2007,9(4):35-54.

[10] LYNN B. Authenticated ID-based encryption cryptology, ePrint Archive Report 2002/072[R]. 2002.

[11] 徐丽娟. 基于身份密码体制的研究及应用[D]. 济南:山东大学,2007.

[12] 王璐. 身份密码的密钥管理研究[D]. 武汉:华中科技大学,2011.

[13] 胡亮,刘哲理,孙涛,等. 基于身份密码学的安全性研究综述[J]. 计算机研究与发展,2009,46(9):1537-1548.

[14] 王皓. 基于身份密码体制的研究[D]. 济南:山东大学,2012.

[15] 刘学. 基于身份的密码体制密钥管理研究[D]. 济南:山东大学,2012.

[16] 龙宇, 徐贤, 陈克非. 两个降低 PKG 信任级的基于身份的门限密码体制[J]. 计算机研究与发展,2012,49(5):932-938.

[17] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proc of FOCS'87. New York:ACM Press, 1987.

[18] 侍伟敏. PKI_IBE 关键技术的研究及应用[D]. 北京:北京邮电大学,2006.

[19] 滕曰, 王首道, 林宇, 等. PKI、IBE 、CPK 对比分析[J]. 科技信息:科学教研,2008(18):402- 403.

[20] 石艳荣,贺永强. PKI 和基于身份加密的比较[J]. 微计算机信息,2008(3):16-18.

[21] 杨斌. IBC 和 PKI 组合应用研究[D]. 郑州:解放军信息工程大学,2009.

[22] YU Jia, KONG Fan-yu, HAO Rong. Publicly verifiable secret sharing with enrollment ability[C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington DC: IEEE Computer Society,2007:194-199.

[23] 李大伟. 基于身份加密的秘密共享及其应用研究[D]. 南京:南京邮电大学, 2011.

[24] DEHKORDI M H, MASHHADI S. New efficient and practical verifiable multi-secret sharing schemes [J]. Information Sciences: an International Journal, 2008,178(9):2262-2274.

(上接第 1506 页)

[3] 沈昌祥,张焕国,王怀民,等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2):139-166.

[4] 虚拟化与云计算小组. 虚拟化与云计算[M]. 北京:电子工业出版社,2009.

[5] 武少杰. 云计算下虚拟环境安全的关键技术研究[D]. 郑州:解放军信息工程大学,2012.

[6] 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):109-113.

[7] 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.

[8] OPPILGER R,RYTZ R. Does trusted computing remedy computer security problems? [J]. IEEE Security & Privacy,2005,3(2):16-19.

[9] 张兴,黄强,沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.

[10] ZHANG Xin-wen, COVINGTON M J, CHEN Song-qing. *et al*. SecureBus:towards application-transparent trusted computing with mandatory access control[C]// Proc of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM Press,2007:117-126.

[11] 张兴,陈幼雷,沈昌祥. 基于进程的无干扰可信模型[J]. 通信学报, 2009, 30(3): 6-11.

[12] 赵佳,沈昌祥,刘吉强,等. 基于无干扰理论的可信链模型[J]. 计算机研究与发展, 2008, 45(6): 974-980.

[13] 张兴,黄强,沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.

[14] 张帆, 陈曙, 桑永宣,等. 完整性条件下无干扰模型[J]. 通信学报, 2011,32(10):78-85.

[15] RUSHBY J. Noninterference, transitivity, and channel-control security policies,CSL-92-02[R]. [S. l.]:Computer Science Laboratory, SRI International, 1992.