计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170465
54(10):2284-2295,2017

一种可信虚拟机迁移模型构建方法

石 源 张焕国 吴福生
(武汉大学计算机学院 武汉 430072)
(空天信息安全与可信计算教育部重点实验室(武汉大学) 武汉 430072)
(yuanshi@whu.edu.cn)

A Method of Constructing the Model of Trusted Virtual Machine Migration

Shi Yuan, Zhang Huanguo, and Wu Fusheng
(*School of Computer Science, Wuhan University, Wuhan* 430072)
(*Key Laboratory of Aerospace Information Security and Trusted Computing* (*Wuhan University*), *Ministry of Education*, *Wuhan* 430072)

Abstract The security migration of virtual machines (VMs) is one of the important requirements to ensure the security of cloud environment. For trusted VMs that contain vTPM (virtual TPM), the security migration of vTPM is also need to consider. At present, there are some researches on the security migration of trusted VMs. However, due to the non-uniform model of trusted VMs, the solution of the migration model cannot be applied to all migration schemes, so there are some limitations that there are no uniform security model and test method for the migration of trusted VMs. Regarding the issues above and referring to the common security issues in virtual machine migration and the relevant specifications for trusted computing and cloud, we analysis the security requirements of trusted VMs. Based on the requirements analysis, we propose a migration framework of trusted VMs that abstracts the participation components of trusted migration and describes the key steps and states in the migration process. Then the labeled transition system (LTS) is used to model the behavior and security attributes of the trusted migration system, and we construct a dynamic state transition tree of migration system based on the model of migration components in the system. The migration model of the migration system is constructed based on the modeling of the process components. We prove that our model can be applied to the consistency test of trusted migration protocol, and the comparison with other related work shows that the model is more fully considering the security attributes in trusted migration.

Key words trusted virtual machine; virtual machine migration; security protocol; labeled transition system; security model

---

收稿日期:2017-06-11;**修回日期**:2017-07-31
基金项目:国家自然科学基金项目(61332019);国家"九七三"重点基础研究发展计划基金项目(2014CB340601);国家"八六三"高技术研究发展计划基金项目(2015AA016002)
This work was supported by the National Natural Science Foundation of China (61332019), the National Basic Research Program of China (973 Program) (2014CB340601), and the National High Technology Research and Development Program of China (863 Program) (2015AA016002).
通信作者:张焕国(liss@whu.edu.cn)

摘　要　虚拟机的安全迁移是保障云环境安全可信的重要需求之一.对于包含虚拟可信平台模块(virtual TPM, vTPM)的可信虚拟机,还需要考虑vTPM的安全迁移问题.目前,已有一些针对可信虚拟机的安全迁移的研究,但是由于研究可信虚拟机的模型不统一,导致迁移模型解决问题的方案不能适用所有的迁移方案,存在一定的局限性.针对可信虚拟机的迁移缺乏统一的安全模型及测试方法的问题,参考虚拟机迁移中普遍存在的安全问题以及可信计算和云的相关规范,从整体系统层面对可信虚拟机的迁移进行安全需求分析;提出一种可信虚拟机迁移框架,将可信迁移的参与组件进行了抽象并描述了迁移协议中的关键步骤和状态;以标号迁移系统LTS为操作语义描述工具对可信迁移系统进行进一步的描述,以系统中迁移进程组件的建模为基础构建出动态的迁移系统状态迁移树;分析了LTS模型可以用于可信迁移协议的一致性测试,并通过与其他相关工作的比较说明了模型在考虑安全属性方面的完备性.

关键词　可信虚拟机;虚拟机迁移;安全协议;标号迁移系统;安全模型

中图法分类号　TP309

随着云计算与可信计算技术的兴起与发展,可信虚拟化技术得到了广泛的研究与应用.虚拟化技术为云平台实现资源抽象、隔离以及资源的按需分配提供技术支撑,可信计算技术为增强虚拟化安全提供了新的途经.在可信云虚拟化架构中,可信虚拟机(virtual machine, VM)是系统资源虚拟化的直观体现,也与云用户密切相关.

虚拟机动态迁移是构建可信云平台的重要需求之一.目前与可信计算关联最紧密的虚拟化技术是虚拟可信平台模块(virtual TPM, vTPM),它是TPM虚拟化的一种实现方式,为运行在主机上的多个虚拟机提供可信计算功能.我们把包含vTPM的虚拟机简称为可信虚拟机,其基于内核虚拟机(kenerl-based virtual machine, KVM)的基本结构如图1所示.在可信虚拟机的动态迁移过程中,为使迁移前后系统的安全状态保持同步,需将虚拟机和与对应的vTPM实例一起迁移.这时,主要考虑被迁移vTPM实例内存状态在源主机的加密存储与目的主机的安全恢复,及迁移过程中虚拟机与vTPM实例数据的机密性和完整性保护.

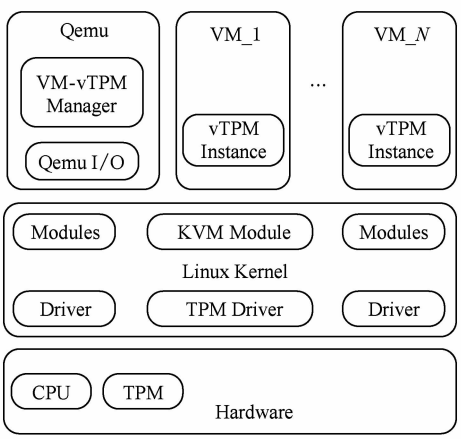


Fig. 1　vTPM architecture on KVM

图1　基于KVM的vTPM架构

目前对于可信虚拟机迁移的研究主要集中在如何安全地构建可信迁移平台并实现虚拟机与vTPM的安全迁移,这些研究为将vTPM应用于真实的云平台提供了理论和实践基础.作为一种特殊的虚拟机,可信虚拟机的迁移不仅依赖于虚拟机的动态迁移技术,还涉及了可信计算的相关理论,因此属于理论与实践结合较为紧密的一项技术.由于动态迁移技术成熟,而可信计算理论尤其是可信虚拟化技术还在发展阶段,存在一些尚未解决的关键问题,因此,将原始的动态迁移技术应用于vTPM虚拟机的迁移就存在着"技术与理论脱节"的问题.

具体来说,vTPM实例与虚拟机都能够通过动态迁移技术实现迁移,但是对于迁移的流程是否安全、vTPM隐私性是否得到保障以及迁移前后的vTPM虚拟机的可信程度是否等价等问题,都没有统一的测试评估标准,因此可信虚拟机迁移的测试评估理论研究是一个刻不容缓的问题.所以现有的可信虚拟机迁移的研究还存在3方面问题和挑战:

1)可信虚拟机的迁移缺乏明确统一的标准,使得现有迁移模型不够完整,难以形成明确的分析目标和依据,无法有效地对迁移模型进行安全分析和评估;

2)现有的大部分迁移方案仅仅只关注可信迁移中的某个问题,而平台环境又不尽相同,这也就导致部分安全分析和解决方案的通用性不强;

3)目前对于可信虚拟机迁移模型缺乏通用的建模方法,对于其安全需求缺少抽象的形式化描述,导致对于可信虚拟机的静态安全以及迁移过程的机

密性、完整性等动态安全属性缺少综合的理论分析研究,不利于在 vTPM 虚拟机与云环境结合之后对可信虚拟机迁移的可信性进行准确的评价.

因此,本文针对可信虚拟机动态迁移缺乏统一的理论模型和测试方法的问题,提出了一种可信虚拟机迁移模型的构建方法,主要工作有 3 方面:

1) 基于可信迁移的相关研究工作,分析可信虚拟机迁移的安全需求,这样首先明确了评估可信迁移的主要内容以及分析的目标和依据,在此基础之上从抽象的角度定义了参与可信迁移主要的相关实体,从而构建一个完善且易于描述的可信迁移模型架构;

2) 对可信虚拟机的迁移流程进行抽象描述,并对可信虚拟机迁移的行为特征进行推导,从动态的角度建立可信迁移模型,再以标号迁移系统(labeled transition system,LTS)为语义描述工具,对可信迁移协议进行形式化说明,以便完整反映可信迁移时组件的交互过程以及系统的状态变迁过程;

3) 分析了本文模型的用途和使用范围,证明了用它来对可信迁移系统或协议进行一致性测试可行性,并针对本文模型相对抽象的特点,证明简化了部分非关键流程的协议模型依然可以用来测试.

1 相关工作

对于可信虚拟机的安全迁移问题,在 vTPM 这一概念被提出时就得到关注[1],目前国内外也有许多学者以协议模型或具体实现的方式对可信虚拟机迁移展开研究.

文献[1]首次提出了 vTPM 的实现方法,在迁移协议中加入了数据完整性保护机制以确保迁移数据的安全,可实现相同配置平台间虚拟机的动态迁移,但文中研究建立在一个非常重要的假设上:迁移的目的主机是可信的,这就使其真正的可信性还需进一步研究. 因为是最早提出的 vTPM 的方案,所以还未考虑其在真实云环境的应用场景,随着 vTPM 和虚拟机技术的发展,迁移模型需要作出相应的调整,尤其是出于实际应用的考虑,相应的安全需求和解决方案都要考虑到更多的细节. 文献[2-3]在分析已有 vTPM 设计方案及相关迁移协议的基础上,提出了迁移过程中的安全需求,然后针对这些需求,设计了一种新的密钥体系,实现了可信虚拟机的安全迁移;文献[4]提出一种可信虚拟机及其 vTPM 实例的安全迁移协议,但该协议中的迁移操作采用的是"挂起-传输-恢复"模式,并不是真正意义上的动态迁移;文献[5]提出一个安全增强的迁移协议,在源主机与目的主机的认证过程中加入随机数,以阻止截获迁移数据的攻击者对其他平台进行重放攻击;文献[6]提出的实例对迁移协议解决了作为独立域运行的时序问题;文献[7]针对可信虚拟机迁移的整个流程中存在的攻击隐患,提出了相应的改进协议,并通过分析验证了新协议抵御各类攻击的能力.

对于普通虚拟机迁移的安全研究相对比较成熟,文献[8]通过实验验证了虚拟机动态迁移的安全问题主要源于 3 个层次:虚拟机监控器(virtual machine monitor, VMM)层、数据层和迁移模块层,攻击者可能利用虚拟化或迁移组件的漏洞获得系统权限或虚拟机的隐私信息[9],还可能利用迁移流程中的认证等协议的缺陷[10]获取传输信道的数据. 文献[11]基于目前主流的 KVM 虚拟化环境,分析了迁移流程中可能存在的诸多安全问题,并基于混合随机变换编码机制提出了一种安全迁移模型. 上述工作虽然是针对普通虚拟机的安全分析和建模,但其中涉及虚拟机动态迁移的安全问题在可信虚拟机迁移中也可能存在,因此,对普通虚拟机的迁移安全研究对于我们分析可信虚拟机的迁移以及建模工作有一定的指导意义.

上述可信虚拟机迁移方案中,或是提出一种概述性的可信虚拟机架构和迁移方法,没有明确的模型建立依据和目标,或是针对 vTPM 迁移、密钥迁移等问题提出的非通用的迁移方案,需要针对特定平台设计新的迁移架构或 vTPM 密钥体系,虽然考虑到虚拟机迁移的灵活性,但失去了通用性,适用范围有限. 因此,本文更关注于从理论角度更加抽象和通用地描述一个可信虚拟机迁移系统或协议,结合可信虚拟机迁移的安全需求建立对可信迁移的进行动态的模型描述,以便对可信迁移系统进行评估和测试.

2 可信迁移安全需求分析

可信虚拟机迁移系统包含大量相关联的实体,为了便于对复杂的迁移系统进行描述,首先应该从较高的层级分析可信迁移有哪些必要的安全需求,在此基础之上抽象地按照逻辑功能定义一些参与可信迁移主要的相关实体,从而构建一个完善且易于描述的可信迁移模型架构.

虽然可信虚拟机的迁移没有明确的规范,但是我们可以根据以往的虚拟机迁移的安全分析[8,11]、可信计算组织(Trusted Computing Group, TCG)制定的可信计算的相关规范[12-13]以及云计算安全联

盟(Cloud Security Alliance, CSA)发布的《云安全指南》[14]来从可信虚拟机迁移的功能性和安全性2方面定义迁移实体的交互规则和安全规范.图2从层级划分的角度描述了可信虚拟迁移整体的安全需求.可以看出:可信迁移所包含的内容非常丰富,根据现有的研究我们发现,基于不同的硬件平台和虚拟化架构会产生不同的可信迁移模型并导致模型在局部设计上存在一定的差异,例如在没有使用物理TPM的平台上就不存在TPM密钥迁移的问题,但是从安全性的角度来看,基于硬件TPM保护可信虚拟机的隐私信息还是非常有必要的,而且现有的技术条件也支持云环境中基于TPM密钥的迁移[15].

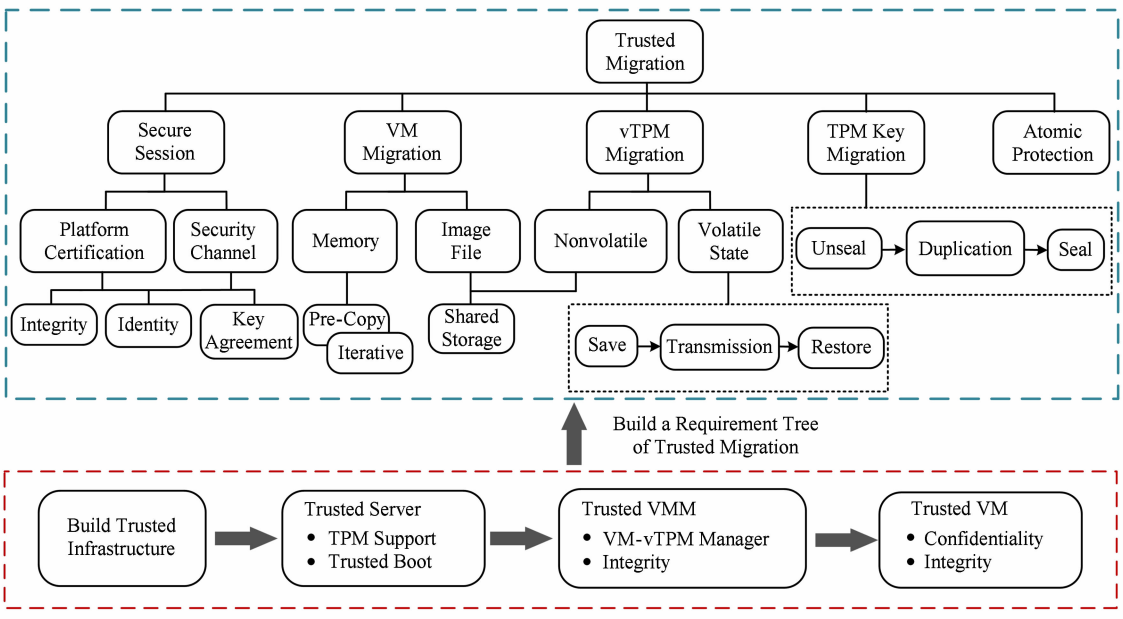


Fig. 2　The security requirements for the migration of trusted VMs

图2　可信虚拟机迁移安全需求说明

根据图2中的安全需求说明,可信迁移是建立在可信的系统架构之上,系统应包括采用支持TPM和可信启动的可信服务器、构建可信的VM-vTPM管理环境以及支持可信虚拟机等特性.上述保障系统迁移环境的安全技术涉及了从硬件层到虚拟化层的众多问题,不可能针对每个层级进行细致的抽象,因此这些都不是本文讨论的重点.本文主要是针对可信虚拟机的迁移流程进行描述,因此我们主要从系统流程中抽取最基本的安全行为和状态,从动态安全的角度,对这些行为和状态进行建模和分析.根据可信虚拟机的特点,其迁移根据流程主要涉及4个方面的安全需求:

1) 建立安全会话.云平台通常包含大量主机,在2台主机之间迁移虚拟机之前,首先要在两者之间建立安全会话.建立会话的过程涉及了许多安全协议,例如迁移双方通过的身份认证及密钥协商建立一个安全的加密信道,随后为了确保对方环境的安全,还要验证主机或者系统软件的完整性;为了抵抗认证和密钥协商过程中可能存在的攻击,本文假设存在一个可信的第三方,该可信第三方包含CA的作用,负责存储和管理主机的证书、软件的度量基准值等.

2) vTPM数据保护.可信虚拟机包含了vTPM设备及其隐私信息,为了保障其使用过程的安全,需要在虚拟机读写vTPM时进行动态的加解密[15].上面提到的vTPM设备和密钥都是属于非易失性的数据,可以直接通过安全信道传输,但是vTPM设备内存这类特殊的易失性的数据,需要采用额外的技术手段[15]进行处理以便进行迁移.

3) 数据安全传输.安全数据的传输是建立在安全会话的基础之上,出于性能的考虑,通常加密vTPM的密钥并非TPM的内部密钥,而是由TPM封装保护的一个外部密钥,那么在迁移vTPM和密钥时自然要考虑到TPM密钥的迁移,这就涉及到TPM2.0中的duplication机制[12].

4) 原子性保护.迁移无论成功与否,迁移虚拟机所拥有的数据和状态都应该是唯一的,迁移成功要删除源主机的所有虚拟机的数据,迁移失败则要将目的端的数据删除,防止产生虚拟机和vTPM隐私信息泄露的安全问题.

3 可信迁移系统描述

3.1 可信虚拟机迁移模型的逻辑构成

可信迁移系统内部包含大量可信虚拟机迁移相关的软件和硬件实体,这些实体涉及的系统层次不同但又相互依存,不可能对所有的迁移相关的实体进行建模.因此,首先要对迁移系统的架构进行进一步的抽象,本文基于现有的迁移系统,然后根据第 2 节提出的可信虚拟机迁移的安全需求,将需求中所提的一些必要组件和流程体现在新的迁移框架中.本文主要是针对可信虚拟机的迁移流程进行描述,所以迁移框架主要体现的是抽象的迁移组件之间的交互.

为了能够抽象出可信迁移中的组件进程,建立不同组件之间的交互关系,我们从逻辑上将可信迁移系统抽象为 4 个主要部分:迁移源主机(source host, SH)集群、目的主机(destination host, DH)集群、可信第三方(trusted third party, TTP)、共享存储服务器集群(shared storage host, SSH),如图 3 所示:

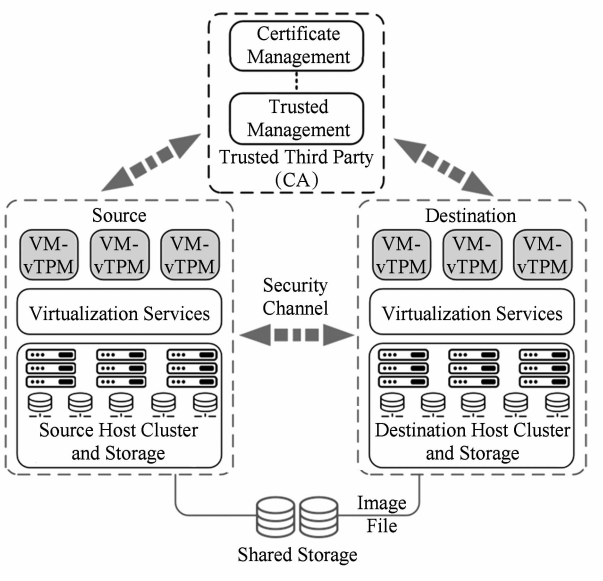


Fig. 3 The basic framework for the migration of trusted VMs

图 3 可信虚拟机迁移基础框架

我们对图 3 进行说明:

1) 迁移主机集群.包括迁移源主机集群和目的主机集群,这里是从迁移系统的逻辑角度来对主机集群进行划分,实际上这些主机都是等价的,都是参与可信虚拟机迁移的主体.迁移双方通过共享服务器以及安全信道来交互数据.

2) 可信第三方.为迁移双方的相互认证提供相应的证书和可信证据(主机、vTPM 虚拟机等的完整性信息等)的管理.

3) 共享存储服务器集群.为了提高迁移效率,一些如虚拟机镜像的大型文件都通过共享存储服务器来共享,避免信道传输大量的数据.

图 3 中的 4 个抽象实体通过不断地交互来完成可信虚拟机迁移的操作,多个组件之间存在重复的交互,这种交互影响着迁移系统状态在不断地变化着,下面我们首先给出可信迁移系统和协议流程的抽象描述.

3.2 迁移模型描述

基于 2.2 节中描述的基本框架与逻辑构成,我们将可信迁移系统做抽象定义:

定义 1. 可信迁移系统.它是三元组(M, Ds, As),其中 M 代表参与迁移的主体.其中,M 代表迁移主体集合,包括了所有可迁移虚拟机的主机、可信第三方 TTP 以及共享存储服务器,记为 $M=\{SH, DH, TTP, SSH\}$,这里 $SH=\{SH_1, SH_2, \cdots, SH_n\}$ 表示所有的源主机,$DH=\{DH_1, DH_2, \cdots, DH_n\}$ 表示所有的目的主机;Ds 代表迁移过程中主体之间交互的数据集;As 代表主体之间交互的动作的合集.上述定义中关键属性的具体内容和说明如表 1、表 2 所示:

Table 1 Data Attributes and Definitions of Migration Protocol

表 1 迁移协议中的数据属性和定义

Data Attribute	Definition
$certificate_i$	Certificate used to verify the identity, $i \in N=\{SH, DH\}$
$measure\_loc$	Measurement results of local platform
$secret$	Secret value in communication
vm_state, $vTPM\_state$	Running data and status of VM and vTPM in the downtime of migration
vm_image	Virtual machine image
$vTPM\_image$	vTPM image
$data\_VM$	All the data related to the VM
$data\_vTPM$	All the data related to the vTPM
$measure\_bak$	Reference value of measurement of host or software managed by TTP
$key_{channel}$	Communication key after the key negotiation
key_{vTPM}	The key protected by TPM used to encrypt the privacy of vTPM
$iterative\_memory$	The memory transferred in an iterative way
$flag_{state}$	$flag_{fail}$ and $flag_{success}$ mark the failure and success of migration

Table 2　Action Attributes and Definitions of Migration Protocol

表 2　迁移协议中的动作属性和定义

Action Attribute	Definition
Authentication	Identity authentication, generally through the host and trusted third party interaction to complete
Keyexchange	Key negotiation, to generate a symmetric key for encrypting the transmitted data
Cont	Operation of contrasting data
Seal/Unseal	Seal and unseal operation of TPM
Import	Import the key into the memory of VM

为了更好地对迁移系统的全局状态和原子动作以及对应的状态变迁规则进行描述,下面首先依据上述定义对整个迁移协议的流程进行描述:

1) 建立安全会话

① 身份认证

$DH \rightarrow SH: certificate_{DH}$;

SH, TTP: Authentication($certificate_{DH}, TTP$);

$SH \rightarrow DH: certificate_{SH}$;

DH, TTP: Authentication($certificate_{SH}, TTP$);

② 协商信道 key_{channel}

DH, SH: Keyexchange($secret_{SH}, secret_{DH}, protocol$);

③ 完整性验证

$DH \rightarrow SH$: Encrypt$_{(Key_{\text{channel}})}$($DH.measure\_loc$);

$SH \rightarrow DH$: Encrypt$_{(Key_{\text{channel}})}$($SH.measure\_loc$);

$TTP \rightarrow DH: SH.measure\_bak.$

$TTP \rightarrow SH: DH.measure\_bak$;

SH: Cont($DH.measure\_loc, DH.measure\_bak$);

DH: Cont($SH.measure\_loc, SH.measure\_bak$).

2) 数据传输

① VM-vTPM 传输

$SSH \rightarrow DH: vm\_image, vTPM\_image$;

DH: Create $DH.vm$ and $DH.vTPM$; $SH \rightarrow DH: Iterative\_memory$;

SH: Suspend VM-$vTPM$ and Save $SH.vTPM\_state$;

$SH \rightarrow DH: SH.vm\_state, SH.vTPM\_state$;

DH: Restore VM-$vTPM$;

② 密钥迁移

SH: Unseal $SH.Key_{\text{vTPM}}$;

SH, DH: Duplication protocol;

DH: Import $SH.Key_{\text{vTPM}}$ and Seal $SH.Key_{\text{vTPM}}$.

3) 原子判定

if ($session\ fail \cup key\ import\ fail \cup VM\ restore\ fail \cup vTPM\ restore\ fail$)

$DH \rightarrow SH: flag\_fail$;

DH: Delete $DH.data\_VM$ and $DH.data\_vTPM$;

else

$DH \rightarrow SH: flag\_success$;

SH: Delete $SH.data\_VM$ and $SH.data\_vTPM$.

end if

这里通过将可信迁移的部分安全需求体现在迁移的系统架构中,然后将可信迁移系统抽象描述为4个实体之间的交互系统,一个迁移系统就能够通过交互协议来进行描述,并且其中的关键动作还反映了系统的部分安全需求.基于交互协议中的关键动作和状态,我们就可利用标号迁移系统对其进行进一步地形式化描述.

4　可信迁移系统的运行状态变迁模型

第3.2节已经将可信迁移模型的执行流程以协议的形式进行描述,那么为了进一步对迁移系统的关键动作和状态进行动态的描述,就需要开展对协议实现的动态分析.根据自动机原理,标号迁移系统[16]是由起点、输入标识、终点组成的一个系统转换模型.由于标号迁移系统不完全等同于自动机,它没有固定的初始状态和接受状态,所以在标号迁移系统中,任何一个状态都可以作为初始状态,故标号迁移系统在动态分析密码协议实现的安全中具有一定的优势.因此,我们采用标号迁移系统对可信迁移系统的协议实现进行描述.

4.1　LTS 相关定义

定义 2. 标号迁移系统.一个标号迁移系统是一个二元组$(\mathcal{Q}, \mathcal{T})$.其中,$\mathcal{Q}$是一个非有限状态集合;$\mathcal{T}$是一个三元关系,通常称之为迁移关系,$\mathcal{T} \subseteq (\mathcal{Q} \times Act \times \mathcal{Q})$,这里 $Act \stackrel{\text{def}}{=} \mathcal{L} \cup \{\tau\}$包含了系统所有可观察动作,$\mathcal{L}$是有限标号(动作)集合,它表示系统所有可观察动作,而τ作为外部不可观察的内部动作.

设S是一个$\mathcal{Q}$的二元关系,若$(p, p') \in S$,其中$p, p' \in \mathcal{Q}$,且$(p, \alpha, p') \in \mathcal{T}$,则我们将其记为 $p \xrightarrow{\alpha} p'$,表示系统从状态$p$经过动作$\alpha$到达$p'$状态.其中$\alpha \in \mathcal{L} \cup \{\tau\}$,即动作$\alpha$既可以是可观察的动作也可以是外部不可见的内部动作;$p_0 \in \mathcal{Q}$表示系统的初始状态.

定义 3. 动作迹(trace). $Trace(p) = \{\omega \in \mathcal{L}^* \mid p = \omega \Rightarrow\}$表示状态$p$上的所有可观察动作的迹,$\mathcal{L}^*$表示$\mathcal{L}$上所有迹的集合. $Sub(p) = \{p' \in \mathcal{Q} \mid \exists \omega \in \mathcal{L}^* : \mid p = \omega \Rightarrow p'\}$描述了迹存在性的表示方法,表示$\mathcal{L}$中存在一条从状态$p$到状态$p'$的动作迹$\omega$.

定义 4. 状态收敛. $q\in\mathcal{Q}$, $q\Downarrow$ 表示状态 q 的收敛,那么:

1) 如果 $q\xrightarrow{\tau}q'$,则 $q'\Downarrow$, $q\Downarrow$;

2) 如果 $q\Downarrow$,则 $q\Downarrow\varepsilon$;

3) 如果 $q\Downarrow$ and $(q=s\Rightarrow q')$,则 $q\Downarrow s$.

规则 1 说明了 $\Downarrow$ 可以用于检测一个标号迁移系统是否存在着不可观察的无限序列;规则 2 表示如果 q 在不可观察动作集合 τ 上收敛,那么 q 也在其空序列是收敛的;规则 3 定义了动作迹的可叠加性.

定义 5. 强模拟. 设 $(\mathcal{Q},\mathcal{T})$ 为一个标号迁移系统,并设 S 是一个 $\mathcal{Q}$ 上的二元关系. 一旦 pSq 总有条件成立:

如果 $p\xrightarrow{\alpha}p'$,则存在 q 使得 $q\xrightarrow{\alpha}q'$ 并且 $p'Sq'$,则称 S 为 $(\mathcal{Q},\mathcal{T})$ 上的一个强模拟. 如果存在一个强模拟 S 使得 pSq 成立,则我们说 q 强模拟 p.

定义 6. 扩展的强模拟. 设 $(\mathcal{Q},\mathcal{T})$ 为一个标号迁移系统. $(\mathcal{Q}',\mathcal{T}')$ 也是一个标号迁移系统, S 在 $\mathcal{Q}\times\mathcal{Q}'$ 上是一个二元关系,且 $p,q\in\mathcal{Q}$. 如果 pSq 满足条件:

1) $\mathcal{Q}'\subseteq\mathcal{Q}$, $\mathcal{T}'\subseteq\mathcal{T}$;

2) $p',q'\in\mathcal{Q}'$,且 $\alpha=\alpha'$, $\alpha'\in\mathcal{T}'$.

如果 $p\xrightarrow{\alpha}p'$,则存在 q' 使得 $q\xrightarrow{\alpha}q'$ 并且 $p'Sq'$,则称 S 是四元组 $(\mathcal{Q},\mathcal{Q}',\mathcal{T},\mathcal{T}')$ 上的一个扩展的强模拟.

标号迁移系统的部分相关符号定义如表 3 所示:

Table 3 Partial Symbols and Definitions in LTS

表 3 标号迁移系统的部分符号和定义

Symbol	Definition
$\mathcal{L}$	All the observable action sets of the system
$\mathcal{L}^*$	The set of strings on the $\mathcal{L}$
a,b,c	The element in the collection $\mathcal{L}$
$\omega,s,s_1,s_2,\cdots,s_n$	The element in the collection $\mathcal{L}^*$
ε	Empty sequence
τ	Unobservable internal action in system
$\mathcal{L}_\tau$	$\mathcal{L}\cup\{\tau\}$
$\alpha,\alpha_1,\alpha_2,\cdots,\alpha_n$	The element in the collection $\mathcal{L}_\tau$
$p,q,p_1,\cdots,p_n$	The element in the collection $\mathcal{Q}$
$p\rightarrow q$	$p\xrightarrow{\tau}q$
$p\xrightarrow{\alpha_1\alpha_2\cdots\alpha_n}q$	There are $p_1,p_2,\cdots,p_n$, $0<i<n$, make $p\xrightarrow{\alpha_1}p_1\xrightarrow{\alpha_2}\cdots\xrightarrow{\alpha_n}p_n=q$

4.2 可信迁移组件状态图

任何协议都可以看成多个实体(或称为进程)之间的交互,而每个实体都可以通过标号迁移系统来形式化地描述其行为和状态,例如典型的端到端的通信协议 AB 协议[17]可以将其中的发送方 S 和接收方 R 当成 2 个进程分别描述成 LTS 树,如图 4 所示,根据树形表示可以很容易得到它们的行为和状态转换.

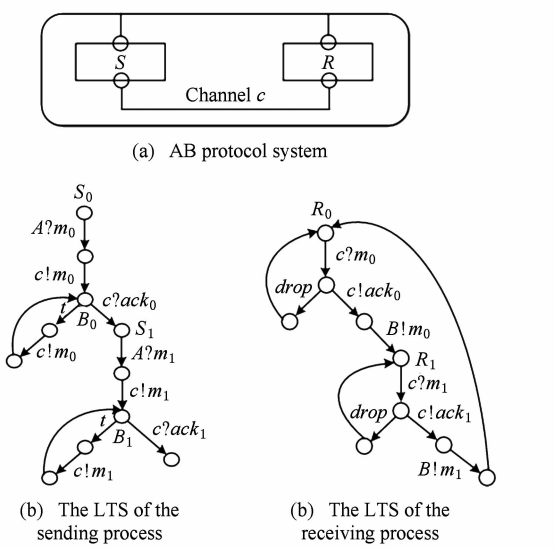


Fig. 4 Process state of AB protocol

图 4 AB 协议进程状态图

根据上述方法,我们首先将 3.1 节中定义的迁移主体作为协议系统中的 4 个进程分别进行 LTS 树建模,将这些进程作为迁移模型的组件,每个组件的 LTS 状态图都可以当成迁移整体架构状态图的一个组成部分. 根据迁移系统的特点,我们将 SH, DD, TTP 和 SSH 之间的通信过程定义为系统的可观察动作,而它们内部组件的处理过程为系统不可观察的内部动作,各组件主要包含交互规则:

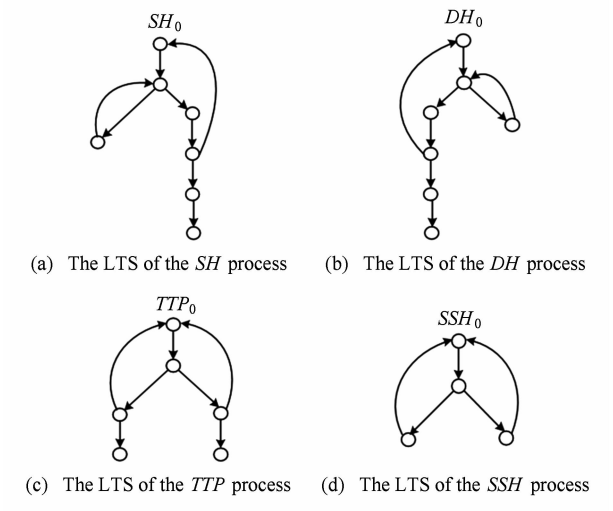
1) SH 负责发起建立安全会话的请求,通过与 TTP 和 DH 交互信息来验证目的主机的当前安全状态. 验证通过之后开始传输迁移数据,并根据传输过程中出现问题与否决定下一步的对剩余迁移数据的处理并进行收尾工作,例如迁移数据成功之后,源主机删除本地所有和迁移虚拟机相关的数据.

2) DH 负责接受迁移的虚拟机,通过与 TTP 和交互信息来验证源主机的安全状态;验证通过之后开始接收迁移数据,并根据传输过程中出现问题与否决定下一步的对剩余迁移数据的处理并进行收尾工作,例如迁移数据失败之后,目的主机删除本地所有和迁移虚拟机相关的数据.

3) TTP 主要负责存储迁移双方的证书以及度量基准值等可信信息,通过与迁移双方交互来提供可信服务.

4) *SSH* 主要负责在源主机和目的主机之间共享虚拟机镜像、vTPM 镜像等容量较大的文件,在迁移这一流程中 *SS* 仅接收源主机和目的主机的请求,并进行相应的处理后返回结果.

根据 4 条规则,我们可信迁移协议中的发送进程 *SH* 和接收进程 *DH* 以及 2 个协调进程 *TTP* 和 *SSH* 进程分别描述成 LTS 树,如图 5 所示:



(a) The LTS of the *SH* process　(b) The LTS of the *DH* process

(c) The LTS of the *TTP* process　(d) The LTS of the *SSH* process

Fig. 5　The process state of trusted migration protocol

图 5　可信迁移协议进程状态图

4.3　可信迁移系统整体状态变迁模型

4.2 节中的进程组件状态图描述的是迁移过程中系统的主要组件的状态变化,为了能够准确反映系统整体的动态属性,比如在可信迁移过程中执行不同关键操作时进程之间相互作用的反馈以及系统在某时刻的整体状态等.因此,有必要根据可信协议整体流程的行为和状态,结合 3.2 节中的各个进程组件的描述刻画出系统运行时的状态变迁图 $LTS(P)$.

在交互行为集的基础上,综合上述组件模型以及变迁规则(见附表 A1),我们就可以进一步刻画出迁移系统运行时的状态变迁图,为了与迁移流程对应,我们将整体的 LTS 树划分为 3 个阶段:

1) 图 6(a)表示系统在建立安全会话阶段的状态变迁图,P_0 表示迁移系统的初始状态,未开始迁移之前的任何异常错误都可能导致系统回到初始状态.系统经过一些安全迁移条件的判别来确认系统是否满足安全会话的条件.

2) 在系统状态满足所有的安全迁移判别条件之后,即建立起迁移主机双方的安全会话达到如图 6(b)所示状态 P_6.在开始内存预拷贝之前,系统还需要根据当前的系统配置和参数进行一些准备工作.

3) 内存预拷贝结束之后开始执行内存的迭代传输,这些都属于系统的内部不可见动作.如图 6(c)所示,在虚拟机所有数据传输结束之后,系统根据虚拟机是否成功恢复运行执行相应的操作,如果迁移失败,系统可能会恢复到迁移之前的状态.

根据可信迁移的相关安全需求和协议规则,图 6 描述了迁移系统在 4 个主要参与实体的影响下的状态变迁关系.因为根据具体的实现和人为的设定,迁移系统的动作的集合是会发生变化的,为了能够通用且准确地测试迁移系统,需要确定迁移过程中通用的可观察状态,即说明系统的状态是收敛,$LTS(P)$不存在状态变迁和内部动作的无穷组合,因此,我们提出命题和证明:

命题 1. 在 $LTS(P)$中存在状态 $P_i, P_j \in \mathcal{Q}$ 且 $i<j$, $\forall Sub(P_i)$,都有 P_j 收敛于某个动作.

证明. 假设 $\exists Sub(P_0)$, $P_i \in \mathcal{Q}(i>0)$,根据定义 2 和定义 3 则有 $\exists \omega \in \mathcal{L}^*$ 使得 $P_0 = \omega \Rightarrow P_i$,说明

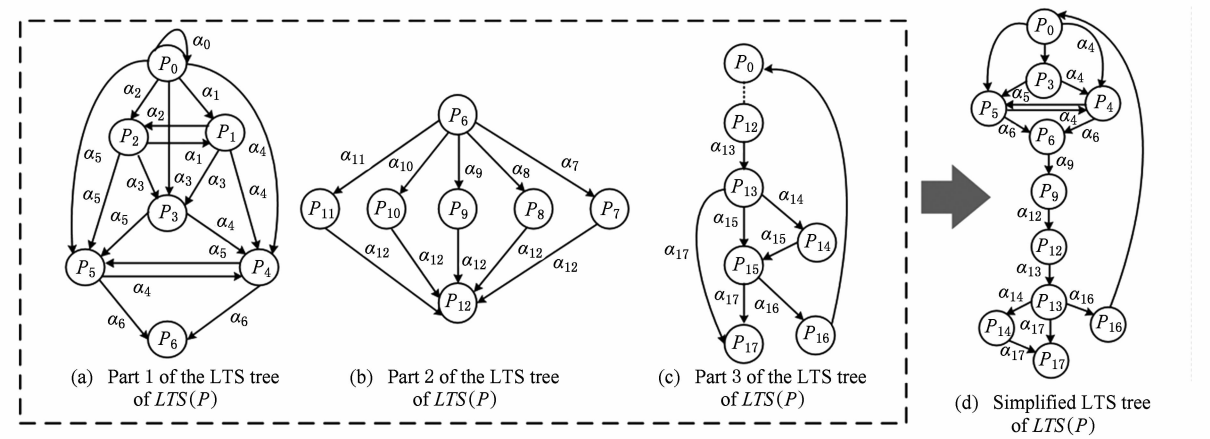


Fig. 6　LTS model of trusted migration system

图 6　可信迁移系统的 LTS 模型

$LTS(P)$中存在一条从状态 P_0 到 P_i 的动作迹 ω，因为在 $LTS(P)$中 P_0 是系统的初始状态，所有显然 $P_0 \Downarrow$，再根据定义 4 可知，如果 $P_0 \Downarrow$ 且存在 P_0 到 P_i 的动作迹 ω，那么 $P_i \Downarrow \omega$. 同理，若 $P_i \Downarrow$，则根据相同的推理规则可以得出 P_i 后续状态也是收敛的某个动作. 命题 1 得证. 证毕.

命题 1 说明了我们定义的迁移系统运行状态是收敛的，即不存在无穷的状态变迁和内部变化，这也满足了具体迁移实现需求，即从迁移初始状态开始，系统能够经过有限的状态变迁，达到预期的收敛状态，不会出现一些无意义的导致系统出现死锁等状态的中间状态. 由此可证明模型的建立是符合需求规则的.

4.4 状态树约减

通常一个系统或协议在实际运行过程中不是一成不变的，这和系统的设计和运行环境都有密切的联系，但是在符合规范的前提下，系统必然有一些必达的运行状态，这些状态之间的路径都是受相关的安全规则所约束的，因此，为了提升测试的效率和可靠性，我们可以对 4.3 中的 LTS 树进行约减.

根据迁移系统的安全需求和各个动作的必要性，我们将一些动作定义为可以约减的动作：1)在真实的云环境中，迁移双方的身份认证实际上是可以由云管理中心的策略来控制实现的，迁移系统本身可以不参与到该流程中，因此状态 P_1，P_2 是可以移除的；2)在迁移双方建立安全会话之后，目的主机可能需要进行一些准备工作，例如从共享服务器获取镜像文件、创建空的 VM 和 vTPM 等，但是这些都不是必须的，因此这些准备工作可能在开始迁移之间已经做好了，因此在状态 $P_7 \sim P_{11}$ 中只有 P_9 是必须保留的，而其他状态可以和 P_9 进行合并；3)在迁移结束阶段，P_{15} 不是必须的，因为在恢复虚拟机运行阶段已包含了验证的逻辑，因此不需要系统主动发起状态检查，除非需要建立特殊的反馈系统提供给云管理中心.

根据上述规则，$LTS(P)$约减树如图 6(d)所示，系统状态从约减之前的 17 种约减为 10 种，$\mathcal{Q} \times \mathcal{Q}$ 上的二元关系从 36 种减少为 19 种. 为了评价约减前后的 LTS 之间的关系，我们引入了最常见的等价关系迹前序 $\leqslant_{tr}$，根据定义 7 以及相关的证明[18-19]，可以推导出：在本文中，由于约减标号迁移树 $LTS(P')$是由 $LTS(P)$经过正确约减得出的，那么它们满足迹前序 $\leqslant_{tr}$，即：

$$P' \leqslant_{tr} P =_{\text{def}} traces(P') \subseteq traces(P).$$

定义 7. 设 $p \in LTS(p)$，$q \in LTS(q)$，若 $LTS(p)$是 $LTS(q)$的子树则两者满足关系 $\leqslant_{tr}$，即有 $traces(p) \subseteq traces(q)$.

5 模型的应用与分析

第 4 节已经讨论了利用 LTS 对可信迁移系统进行建模，并证明其正确性，下面将主要讨论如何利用该模型来对其他的可信迁移系统进行测试，其中涉及了协议一致性测试的工作，我们将结合本文模型进行描述. 为了更好地讨论本文模型，本节最后还将本文的模型与其他相关的工作进行了比较分析.

5.1 协议一致性测试

协议一致性测试主要包含 2 个方面[17]：测试生成和测试执行. 测试生成通过分析协议说明来确定要测试的各个方面，从而产生测试套(测试例集合)；测试执行部分分为测试例的运行提供环境，并分析测试结果，给出测试判决. 本文针对可信迁移系统所描述的 $LTS(P)$即可作为一致性测试中的测试例. 利用第 4 节的 LTS 建模方法，我们可将任意的迁移协议或系统 i 描述成 $LTS(I)$树，我们将其称为测试对象. 通过将本文模型与其他模型进行比较，即将 $LTS(P)$与 $LTS(I)$进行一致性测试，验证协议 i 对应模型所有的与本文定义的可观察动作有哪些是匹配的又有哪些是不在 $LTS(P)$所定义的规则内的. 例如假设 $LTS(I)$对应迁移系统没有考虑 TPM 密钥的迁移，那么其 LTS 树中肯定没有与 $LTS(P)$的 P_{14} 所匹配的状态和路径，那么反过来说明通过本模型确实能够发现其他迁移系统中的缺陷.

根据“一致性”的定义[17]，我们将测试中使用的迁移协议形式化说明集合记为 $MIGSPECS$，将协议实现的集合记为 $MIGIMPS$，它们之间的关系记为 imp，其定义为

$$imp \subseteq MIGSPECS \times MIGIMPS,$$

任何 $(p,i) \in imp$ 或 $p\ imp\ i$ 表示 p 是 i 的一个一致性关系. 对于 $p \in LTS(P)$，$i \in LTS(I)$，$MIGIMPS$ 与 $MIGSPECS$ 的“一致性”关系还可以定义在形式化的系统之上记为 $imp_{\text{LTS}} \subseteq LTS(P) \times LTS(I)$. 为了说明通过一致性测试可以证明协议 LTS 的一致性关系，我们给出命题和证明：

命题 2. 存在一个测试例 $LTS(P)$和一个测试对象 $LTS(I)$，测试套 T 是测试例的一个集合，$\forall i \in LTS(I)$，若 i 能够通过 T，则存在 $imp_{\text{LTS}} \subseteq LTS(P) \times LTS(I)$.

证明. 如果 i 能够通过 T,那么存在 $LTS(P)\in T$,i 能够通过测试例 $LTS(P)$,那么就存在协议说明 $p\in LTS(P)$,使得 i 能够通过 p,根据上述"一致性"的定义,因此就存在协议说明和协议实现之间的一致性关系,即存在 $(p,i)\in imp$,那么对于 $p\in LTS(P)$,$i\in LTS(I)$,就存在 $imp_{\mathrm{LTS}}\subseteq LTS(P)\times LTS(I)$. 命题 2 得证. 证毕.

命题 2 说明了在测试例 $LTS(P)$ 满足一定条件的情况下,可以通过协议的一致性测试来证明测试例与其他协议实现的 LTS 的一致性关系. 需要注意的是,实际测试一般不能证明一致性,而只能证明某些协议实现与协议说明不一致[17]. 由于目前可信迁移系统还没商业化或者开源的实际系统的应用,因此还无法对真实的系统进行测试,但是通过本节的分析已经说明了测试的可行性,后续我们也将基于本文的模型和方法开展对仿真系统中可信迁移系统的测试,为今后真实的平台测试打下良好的基础.

另外,本文可信迁移模型更加抽象,在建模过程中简化了迁移中的部分非关键流程(不影响协议的安全属性),为了说明简化的迁移流程的有效性,我们给出命题和证明:

命题 3. 如果去除可信迁移流程中的非关键部分,且简化前后协议的安全属性具有一致性,那么在分析评估系统的安全状态迁移时,简化的流程可以等价于原系统.

证明. 假设原可信迁移系统是一个标号迁移系统,即为一个二元组 $(\mathcal{Q},\mathcal{T})$,去除部分非关键部分的迁移系统的标号迁移系统为另一个二元组 $(\mathcal{Q}',\mathcal{T}')$,且 S 是在 $\mathcal{Q}\times\mathcal{Q}'$ 上的一个二元关系. $\mathcal{Q}'\subseteq\mathcal{Q}$,$q,q'\in\mathcal{Q}$,$p,p'\in\mathcal{Q}'$,$\alpha,\alpha'$ 分别为 2 个系统的输出标号,$\alpha=\alpha'$(统一为 α). 根据定义 2 可知,一定存在 $p\xrightarrow{\alpha}p'\in\mathcal{T}$ 和 $q\xrightarrow{\alpha}q'\in\mathcal{T}'$. 由于 qSp 与 $q'Sp'$ 成立,根据扩展强模拟的定义 6 可知,标号迁移系统 $(\mathcal{Q}',\mathcal{T}')$ 产生的行为是 $(\mathcal{Q},\mathcal{T})$ 的子集,$(\mathcal{Q}',\mathcal{T}')$ 不会产生 $(\mathcal{Q},\mathcal{T})$ 不具有的行为. 即在用标号迁移系统描述系统状态迁移时,可以用 $(\mathcal{Q}',\mathcal{T}')$ 来替代 $(\mathcal{Q},\mathcal{T})$,故命题得证. 证毕.

5.2　与现有模型对比

本文从抽象的角度概括了可信迁移中的一些安全属性,基于这些属性我们将本文的模型与其他同类工作中的协议或者模型进行对比分析,如表 4 所示. 本文模型基于迁移系统、可信虚拟机的具体实现以及迁移和可信计算相关理论的研究概括总结出更加完备的系统安全属性. 文献[1]首次提出了 vTPM 的概念,为之后的可信虚拟化的发展奠定了基础,但此时可信虚拟机迁移的概念还不够成熟,也没有在真实的系统上实现和应用,因此迁移流程只能考虑到与可信计算相关的细节,无法全面考虑到实际的应用场景的安全需求;文献[2]对一些基于 Xen 的 vTPM 虚拟机迁移方案进行介绍和分析,指出了 vTPM 虚拟机迁移所面临的安全问题,最后设计并实现了 vTPM 虚拟机迁移方案,该方案的安全需求考虑的还是比较全面,但是关键的对于 vTPM 隐私信息的保护和迁移并没有得到有效的解决;文献[3-4]主要是针对 vTPM 密钥树以及相关密钥迁移协议的设计与分析,解决了密钥在云环境中迁移的问题,但是缺少对实际云环境中 vTPM 的安全需求的考虑;文献[6]基于 TPM2.0 的平台设计 vTPM 密钥树以及 VM-vTPM 迁移协议,比较符合目前可信虚拟化的发展趋势,并采用 Ban 逻辑对协议的安全性进行了证明,该方案解决了 VM-vTPM 的状态同步和 vTPM 迁移时序问题,但是没有讨论 vTPM 的非易失性信息的迁移问题;文献[7]分析了现有的 VM-vTPM 方案,并从攻击的角度分析可信虚拟机

Table 4　Comparison Between our Model and Other Related Models

表 4　本文模型与其他相关模型的比较

Module	TTP	Authentication	Integrity Measure	Encrypted Channel	Privacy of vTPM	Volatile State of vTPM	TPM Seal/Unseal	TPM Key Duplication	Atomicity
Ref[1]	No	No	No	Yes	Yes	Yes	Yes	Yes(TPM1.2)	No
Ref[2]	Yes	Yes	Yes	Yes	No	No	No	Yes(TPM1.2)	Yes
Ref[3]	Yes	Yes	Yes	Yes	No	No	No	No	Yes
Ref[4]	No	No	Yes	Yes	No	No	No	Yes(TPM1.2)	Yes
Ref[6]	No	Yes	Yes	Yes	Yes	No	No	Yes(TPM2.0)	Yes
Ref[7]	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Our Module	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes(TPM2.0)	Yes

迁移的安全问题,提出一种改进的 vTPM 虚拟机动态迁移协议,该协议利用基于 TPM 的 TLS 协议进行身份认证,建立安全信道,然后利用基于 TPM 的 vTPM 迁移条件判别方法验证迁移过程中参与实体的完整性,最后在源主机与目的主机间进行数据传输,TPM 可迁移密钥对暂停阶段迁移的数据做加密保护,本文考虑的安全属性较为全面,但是没有对 vTPM 隐私保护相关 TPM 密钥的迁移展开讨论.

本文基于上述研究成果,总结和分析了可信虚拟机迁移的安全需求,并且还考虑了目前可信计算和云平台结合的发展现状,因此,综合来看本文所建模型考虑的安全属性还是较为全面和符合真实应用场景的,能够较完整地体现可信迁移系统的安全需求.

6 总 结

针对可信虚拟机迁移缺少统一的安全分析模型的问题,本文基于虚拟机迁移安全的实践与经验,结合可信计算以及云安全的一些理论知识,抽象出可信迁移中的一些关键的动态安全属性;然后基于标号迁移系统对可信迁移系统的行为和安全属性进行建模,以系统中迁移进程组件的建模为基础构建出动态的迁移系统状态迁移树,并根据相关规则对其进行了约减,以提高测试效率;之后分析了本文模型在协议一致性测试工作的应用场景,并通过理论证明了其有效性;最后将本文模型与其他相关工作进行了比较.在后续的研究中我们将继续完善可信虚拟机迁移模型,首先对安全需求进行进一步的分析,使得模型更加完备;其次,可信迁移中还涉及到很多深层次的协议和理论,随着研究的深入,还应该在模型中考虑到更加细粒度的安全属性;最后,在考虑安全性的基础之上,分析迁移系统的可用性、可靠性等其他属性.

参 考 文 献

[1] Berger S, Goldman K A, Perez R, et al. vTPM: Virtualizing the trusted platform module [C] //Proc of the 15th USENIX Security Symp. Berkeley, CA: USENIX Association, 2006: 305-320

[2] Masti R J. On the security of virtual machine migration and related topics [D]. Zurich: Department of Computer Sciences, Swiss Federal Institute of Technology Zurich, 2010

[3] Liang Xinlong, Jiang Rui, Kong Huafeng. Secure and reliable VM-vTPM migration in private cloud [C] //Proc of the 2nd Int Symp on Instrumentation and Measurement, Sensor Network and Automation. Piscataway, NJ: IEEE, 2013: 510-514

[4] Danev B, Masti R J, Karame G O, et al. Enabling secure VM-vTPM migration in private clouds [C] //Proc of the 27th Annual Computer Security Applications Conf. New York: ACM, 2011: 187-196

[5] Chang Dexian, Chu Xiaobo, Wei Ge. Analysis of the security-enhanced vTPM migration protocol based on ProVerif [C] //Proc of the 5th Int Conf on Computational and Information Sciences. Piscataway, NJ: IEEE, 2013: 1437-1440

[6] Yang Yongjiao, Yan Fei, Mao Junpeng, et al. Ng-vTPM: A next generation virtualized TPM architecture [J]. Journal of Wuhan University: Natural Science Edition, 2015, 61(2): 103-111 (in Chinese)
(杨永娇, 严飞, 毛军鹏, 等. Ng-vTPM: 新一代 TPM 虚拟化框架设计[J]. 武汉大学学报: 理学版, 2015, 61(2): 103-111)

[7] Fan Peiru, Zhao Bo, Shi Yuan, et al. An improved vTPM-VM live migration protocol [J]. Wuhan University Journal of Natural Sciences, 2015, 20(6): 512-520

[8] Rehman A, Alqahtani S, Altameem A, et al. Virtual machine security challenges: Case studies [J]. International Journal of Machine Learning & Cybernetics, 2014, 5(5): 729-742

[9] Xiong Haiquan, Liu Zhiyong, Xu Weizhi, et al. Interception and identification of guest OS non-trapping system call instruction within VMM [J]. Journal of Computer Research and Development, 2014, 51(10): 2348-2359 (in Chinese)
(熊海泉, 刘志勇, 徐卫志, 等. VMM 中 Guest OS 非陷入系统调用指令截获与识别[J]. 计算机研究与发展, 2014, 51(10): 2348-2359)

[10] Wan Tao, Liu Zunxiong, Ma Jianfeng, et al. Authentication and key agreement protocol for multi-server architecture [J]. Journal of Computer Research and Development, 2016, 53(11): 2446-2453 (in Chinese)
(万涛, 刘遵雄, 马建峰. 多服务器架构下认证与密钥协商协议[J]. 计算机研究与发展, 2016, 53(11): 2446-2453)

[11] Fan Wei, Kong Bin, Zhang Zhujun, et al. Security protection model on live migration for KVM virtualization [J]. Journal of Software, 2016, 27(6): 1402-1416 (in Chinese)
(范伟, 孔斌, 张珠君, 等. KVM 虚拟化动态迁移技术的安全防护模型[J]. 软件学报, 2016, 27(6): 1402-1416)

[12] Trusted Computing Group. Trusted platform module library family 2.0 level 00 revision 01.16 [EB/OL]. [2017-05-23]. http://www. trustedcomputinggroup. org

[13] Trusted Computing Group. TCG specifications [EB/OL]. [2017-05-23]. http://www. trustedcomputinggroup. org

[14] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0 [EB/OL]. [2017-05-23]. http://www. Cloudse curityalliance. org/guidance/csaguide. v3.0. pdf

[15] Shi Yuan, Zhao Bo, Yu Zhao, et al. A security-improved scheme for virtual TPM based on KVM [J]. Wuhan University Journal of Natural Sciences, 2015, 20(6): 505-511

[16] Milner R. Communicating and mobile systems: The π-calculus [M]. Cambridge, UK: Cambridge University Press, 1999

[17] Jiang Fan, Ning Huazhong. Automatic test suite generation based on labelled transition system [J]. Journal of Computer Research and Development, 2001, 38(12): 1435-1445 (in Chinese)
(蒋凡, 宁华中. 基于标号变迁系统的测试集自动生成[J]. 计算机研究与发展, 2001, 38(12): 1435-1445)

[18] Xu Mingdi, Zhang Huanguo, Yan Fei. Testing on trust chain of trusted computing platform based on labeled transition system [J]. Chinese Journal of Computers, 2009, 32(4): 635-645 (in Chinese)
(徐明迪, 张焕国, 严飞. 基于标记变迁系统的可信计算平台信任链测试[J]. 计算机学报, 2009, 32(4): 635-645)

[19] Zhao Bo, Dai Zhonghua, Xiang Shuang, et al. Model constructing method for analyzing the trusty of cloud [J]. Journal of Software, 2016, 27(6): 1349-1365 (in Chinese)
(赵波, 戴忠华, 向骁, 等. 一种云平台可信性分析模型建立方法[J]. 软件学报, 2016, 27(6): 1349-1365)

Shi Yuan, born in 1991. PhD candidate at the School of Computer Science, Wuhan University. His main research interests include trusted computing and information security.

Zhang Huanguo, born in 1945. Professor and PhD director of the School of Computer Science, Wuhan University. His main research interests include information security, cryptography, trusted computing, cloud computing, fault tolerance, and computer application.

Wu Fusheng, born in 1974. PhD candidate at the School of Computer Science, Wuhan University. His main research interests include design of cryptographic protocols and security analysis of cryptographic protocols.

附录 A

Table A1　The State Transition of Trusted Migration System

附表 A1　可信迁移系统状态转换

$P \xrightarrow{\mu} Q$	P	Q	μ
α_0	P_0	P_0	
α_1	$P_{0,2}$	P_1	System authenticates the identity information of the destination host
α_2	$P_{0,1}$	P_2	System authenticates the identity information of the source host
α_3	$P_{0,1,2}$	P_3	Source host negotiates the key with the destination host to establish a secure channel
α_4	$P_{0,1,3,5}$	P_4	System verifies the integrity information of the destination host
α_5	$P_{0,2,3,4}$	P_5	System verifies the integrity information of the source host
α_6	$P_{3,4,5}$	P_6	Creates a secure session
α_7	P_6	P_7	Destination host obtains the image files of VM and vTPM from the shared storage server
α_8	P_6	P_8	Destination host creates an empty VM and vTPM
α_9	P_6	P_9	Source host saves the volatile state of vTPM
α_{10}	P_6	P_{10}	System checks the load condition of the destination host
α_{11}	P_6	P_{11}	System checks the running status of the TPMs on both hosts
α_{12}	$P_{7\text{-}11}$	P_{12}	Memory pre-copy
α_{13}	P_{12}	P_{13}	Virtual machine is shut down briefly for performing memory iterative transmission
α_{14}	P_{13}	P_{14}	Execute the TPM duplication protocol to migrate the encryption key
α_{15}	$P_{13,14}$	P_{15}	Verifies the running status of virtual machine
α_{16}	P_{15}	P_{16}	Virtual machine restores fails and performs atomic operations
α_{17}	$P_{13,15}$	P_{17}	Performs an atomic operation and restores the virtual machine to run