一种基于无干扰模型的信任链传递分析方法

张 兴[1),2)] 黄 强[3)] 沈昌祥[1),3)]

[1)](信息工程大学电子技术学院 郑州 450004)

[2)](北京工业大学计算机学院 北京 100022)

[3)](海军计算技术研究所 北京 100036)

摘 要 基于可信计算组织(TCG)的完整性度量只能保证组件没有被篡改,但不一定能保证系统运行可信性.其问题在于,当组件运行时,受其它组件的干扰,出现非预期的信息流,破坏了信任链传递的有效性.文章在分析可信计算平台的信任模型基础上,基于无干扰理论模型,提出了一种分析和判定可信计算平台信任链传递的方法,用形式化的方法证明了当符合非传递无干扰安全策略时,组件之间的信息流受到安全策略的限制,隔离了组件之间的干扰,这样用完整性度量方法所建立的信任链才是有效的.

关键词 可信计算;信任链;无干扰模型;安全策略

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00074

A Formal Method Based on Noninterference for Analyzing Trust Chain of Trusted Computing Platform

ZHANG Xing[1),2)] HUANG Qiang[3)] SHEN Chang-Xiang[1),3)]

[1)](*Institute of Electronic Technology, Information Engineering University, Zhengzhou* 450004)

[2)](*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022)

[3)](*Computing Technology Institute of China Navy, Beijing* 100036)

Abstract The integrity measurement of TCG can only insure that the components of a computing platform are tamper-proofed, which is not enough for avoiding the interference between components at runtime for building the trust chain. The interference of other components results in the unexpected information flow. The trust model of Trusted Computing Platform is analyzed in this paper. Based on the intransitive noninterference model, a formal method of analyzing the trust chain transfer is proposed. It formalized specifies the security policy isolating the interference between components that can make the trust chain valid after integrity measurement.

Keywords trusted computing; trust chain; noninterference; security policy

1 引 言

信任链的建立和传递是可信计算平台的关键.文献[1]将可信计算的思想总结为:首先构建一个信任根,再建立一条信任链,从信任根开始到硬件平台、到操作系统、再到应用,一级认证一级,一级信任一级.从而把这种信任扩展到整个计算机系统,从而确保整个计算机系统的可信.

可信计算组织 TCG(Trusted Computing Group)

收稿日期:2009-07-24;最终修改稿收到日期:2009-11-06.本课题得到国家"九七三"重点基础研究发展规划项目基金(2007CB311100)、国家"八六三"高技术研究发展计划项目基金(2006AA01Z440)资助.**张 兴**,男,1966 年生,博士,高级工程师,研究方向为信息安全、可信计算.E-mail: zhangxing@bjut.edu.cn. **沈昌祥**,男,1940 年生,博士生导师,中国工程院院士,研究领域为计算机体系结构和信息安全. **黄 强**,男,1977 年生,博士,工程师,研究方向为信息安全.

在其系列规范中①②③④⑤描述了可信的定义以及信任的度量、信任传递和系统控制权，TCG 用实体行为的预期性来定义可信：一个实体是可信的，如果它的行为总是以预期的方式，达到预期的目标①. 该定义突出了可信是“实体”的可信，实体的行为按“预期”，其输出结果就是可信. 换句话说，某一实体按照预期方式运行，就是可信的. 所以信任总是与“预期”联系在一起，即“输出”或“结果”与“预期”的一致性. 这个定义抓住了实体的行为特征，得到了广泛的认同，但 TCG 规范所规定的基于装载前度量的可信传递方式[1]并不能保证系统运行时处于可信状态. Ahmad-Reza 团队对那些符合 TCG 规范的产品进行测试，结果表明这些可信计算平台并未达到可信的目标[2].

笔者所在实验室对目前嵌有 TPM 的几种计算机产品进行了验证性的测试，测试产品包括 IBM-T60、HP-NC4200 等，这些产品均声称符合 TPM-1.2 规范. 而测试结果表明：虽然进行了完整性度量，也符合规范所规定的信任链建立过程，但这样的信任链并没有达到系统运行可信的效果，不能防止运行时出现的内存溢出，也不能防止通过隐通道等方式造成的信息泄漏. 其原因是操作系统基于多任务实现，系统组件间依赖性强，存在很多交互通道，隔离性差. 当程序运行时，组件之间出现非预期的信息流，对组件的行为形成干扰，这些干扰现象导致系统组件之间的信任关系难以建立，而且使已经建立的可信链容易受到破坏. 本文围绕系统满足什么条件时，信任链的建立和传递才是有效的这一问题展开研究，这一问题的解决将有助于可信计算平台的设计和验证.

本文第 2 节介绍可信计算平台中的信任链传递的相关研究，同时介绍了非传递无干扰模型；第 3 节进一步分析 TCG 信任链传递存在问题的原因，指出实体间干扰的存在导致了系统运行可信，提出了可信计算平台的信任链传递模型；第 4 节分析了非传递无干扰模型与信任链传递的关系，提出了具有干扰关系的可信计算平台的信任链传递模型，分析了组件干扰与平台信任传递的关系，指出系统域间无干扰也就意味着系统输出的确定性和可预期性，依据无干扰理论给出了一种判定可信计算平台信任链传递关系的有效方法；第 5 节基于虚拟机实现了一个非传递无干扰原型系统，对信任链在可信计算平台上的传递进行了初步验证；第 6 节给出结论和下一步研究重点.

2　相关研究

2.1　TCG 可信计算平台的信任模型

TCG 采用装载前度量的方案，给出了信任链传递和控制权转移的过程（如图 1 所示）①：从可信度量根核心 CRTM（Core of Root Trusted Measurement）开始，依次对各模块进行完整性度量，先对 BIOS 进行杂凑运算，如果与参考值匹配，则度量通过，将控制权转移给 BIOS，信任链也向前扩展了一步，再度量操作系统加载代码，这样逐步建立信任链. 所以信任链（Chain of Trust）就是从底部 CRTM 开始到用户应用程序的链.

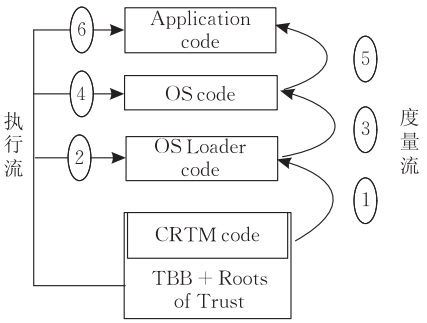

图 1　TCG 信任链传递过程

从这个过程看，虽然信任链建立了，但不能保证系统运行时处于可信状态. 因为，如果系统运行时没有适当的安全策略对各模块、各层之间的信息流进行限制，那么各模块、各层之间可能出现干扰，导致系统运行时可信状态难以传递和保持.

Trent 在文献[3]中指出了这种“装载前度量”完整性检查模式的局限：即装载时刻的可信不等于运行时可信，因为运行后可能被恶意代码篡改，或者代码插入破坏其运行方式. Trent 提出了 PRIMA

① Trusted Computing Group. TCG Specification Architecture Overview[EB/OL]. 2007-08-08. https://www.trustedcomputinggroup.org/groups/TCG_1_2_Architecture_Overview.pdf

② Trusted Computing Group. TPM specification version 1.2. Part 1 Design Principles[EB/OL]. 2007-08-08. https://www.trustedcomputinggroup.org/specs/TPM/Main_Part1_rev94.zip

③ Trusted Computing Group. TPM specification version 1.2. Part 2 TPM Structures[EB/OL]. 2007-08-08. https://www.trustedcomputinggroup.org/specs/TPM/Main_Part2_rev94.zip

④ Trusted Computing Group. TPM specification version 1.2. Part 3 TPM Commands[EB/OL]. 2007-08-08. https://www.trustedcomputinggroup.org/specs/TPM/Main_Part3_rev94.zip

⑤ Trusted Computing Group. TCG PC client specific, implementation specification for conventional BIOS [EB/OL]. 2007-08-08. https://www.trustedcomputinggroup.org/specs/PCClient

方案,在减少度量对象基础上,实现动态运行时的可信,其关键之处在于,作者从信息流观点,基于Clark-Wilson完整性模型提出CW-Lite安全策略模型,利用这一策略模型限制实体之间的信息流动.这一方案说明了可信平台的信任链应该建立在某一安全策略之上,如果系统不加限制,不满足安全策略,那么很难做到动态运行时的可信,信任链的传递也会失效.

另外一个有意义的工作是在TCG之前,IBM Watson实验室开发的安全协处理器IBM 4758①,给出一种逐层验证的可信计算平台体系结构,将平台的代码分为不同信任级别的层,利用棘齿锁(Ratchet Lock)思想,控制程序控制权在不同信任层面、不同的特权要求的代码块之间进行转移,棘齿锁是单向的,即安全级别低的不能再访问安全级别高的,用这种方法保证了完整性级别的用户层不能进行篡改完整性级别的系统操作.

文献[4]基于无干扰理论,提出了基于进程的无干扰可信模型(Non-interference Trusted Model,NITM),利用进程间的干扰性来研究进程运行过程的可信,并基于进程可信构建系统可信模型.同TCG静态可信相比,体现了系统动态运行可信的思想,同时也是对信任链的传递的一种有益探索.

进一步分析文献[3-4]和IBM实验室①的研究成果则可以得到下面的结论,简单地讨论信任链的传递是否有效没有意义,只有当系统本身满足一定的安全策略时,组成系统的各安全域之间的信息流动受到一定安全策略限制,使得组件的运行不受干扰,达到可信目标,这样,用完整性度量方法所建立的信任链才是有效的.本文借鉴文献[3-4]和IBM研究结论①得出:只有满足了无干扰安全策略,信任链才能有效传递下去,即达到系统运行可信,否则安全域之间可能会产生非预期的信息流动,即使通过了信任链的度量,也不能达到系统运行可信的目标.由于以非传递的无干扰模型为基础,为了描述方便,先将文献[5]所提出的模型进行提炼和整理.

2.2 对无干扰模型的研究

信息流的无干扰思想最早由Goguen和Meseguer提出[6],随后出现了多种无干扰安全模型,直到1992年,Rushby对Goguen和Meseguer的无干扰模型进行了改进[5],修正了其中几处错误,使其更合理并容易理解,无干扰模型也趋于成熟.

Rushby的模型[5]采用状态机的方式来描述系统,给出了系统关于传递和非传递无干扰策略安全的定义.Rushby的无干扰模型可以理解为:一个安全域u对安全域v是无干扰的,如果域u发出的动作不影响域v的输出.Rushby无干扰策略模型被成功地运行到BLP、BIBA模型的解释和多级安全系统的安全策略的验证等.

定义1. 系统M由(S,O,D,A)4个要素及一组函数组成,其中:

S为系统状态集合,初始状态$s_0\in S$.

O为系统输出集合.

A为系统操作动作集合,指系统自身发出的控制动作以及输入性质的动作.

D为系统隔离域集合,隔离域中的主体向系统发出操作动作与系统进行交互,并且能够观察到相应的结果.隔离域的划分可以限制系统中的信息流动.

单步状态转换函数$step:S\times A\to S$,$step(s,a)$表示系统发生了内部操作a之后的状态.

输出函数$output:S\times A\to O$,表示从某个系统状态发生操作a带来的结果.

系统运行函数$run:S\times A^*\to S$(A^*表示A的闭包),$run(s,\alpha)$表示系统从状态s经过操作序列α后获得的状态.该函数满足$run(s,\varnothing)=s$且$run(s,a\circ\alpha)=run(step(s,a),\alpha)$.

系统操作与域关系函数$dom:A\to D$,表示系统每个执行操作所属的隔离域.

定义2. 用二元关系符号$\rightsquigarrow$表示两个域间存在信息流的干扰关系,称为干扰关系.用$\not\rightsquigarrow$表示关系$\rightsquigarrow$的补集,称为无干扰关系:$\not\rightsquigarrow=(D\times D)\setminus\rightsquigarrow$.

定义辅助函数$sources:A^*\times D\to P(D)$,其中$P(D)$表示$D$的幂集,它满足

$$sources(\varnothing,u)=\{u\},$$

$$sources(a\circ\alpha,u)=\begin{cases}sources(\alpha,u)\cup\{dom(a),\\ \quad\exists v:v\in sources(\alpha,u)\wedge dom(a)\rightsquigarrow v\\ purge(\alpha,u),\ \text{其它}\end{cases}$$

其中,$v\in sources(\alpha,u)$表示$v=u$或者操作序列α具有一个子序列,该子序列包含域$w_1,w_2,\cdots,w_n$发出的动作,满足$w_1\rightsquigarrow w_2\rightsquigarrow\cdots\rightsquigarrow w_n$,且$v=w_1$,$u=w_n$.

该函数表明:一个在动作序列α发生前产生的动作a是否影响了u,决定于是否存在$v\in sources(\alpha,u)$

① IBM Coprocessor First to Earn Highest Security Validation. http://www-03.ibm.com/press/us/en/pressrelease/2347.wss, 20090414

并且满足 $dom(a)\rightsquigarrow v$. 在此基础上，定义“清除”函数.

定义 3.　函数 $purge: A^*\times D\rightarrow A^*$，满足

$$purge(a\circ\alpha,u)=\begin{cases}a\circ purge(\alpha,u), & dom(a)\in sources(a\circ\alpha,u)\\ purge(\alpha,u), & \text{其它}\end{cases}.$$

该函数从动作序列中清除了那些不干扰域 u 的操作，剩下那些对域 u 直接或间接造成干扰的操作动作.

定义 4.　系统满足无干扰关系的形式化定义

$\forall\alpha\in A^*$，$\forall a\in A$，$\forall d=dom(a)\in D$，满足

$$output(run(s_0,\alpha),a)=output(run(s_0,purge(\alpha,dom(a))),a).$$

定义 5.　若对于系统中任意的域 $u\in D$，状态集合 S 中存在一个等价关系 $\overset{u}{\sim}$，该等价关系满足如下公式：

$$s\overset{dom(a)}{\sim}t\rightarrow output(s,a)=output(t,a),$$

则称 M 具有输出一致性，即两个状态等价则输出相等. 而系统状态总可以用一组客体对象及其取值来表示，Rushby 用以下集合和函数表示状态：

N 表示一组可数的名称集合.

V 表示一组可数的取值集合.

函数 $contents: S\times N\rightarrow V$ 表示名字为 n 的客体对象在系统状态为 s 时的取值.

函数 $alter: D\times S\rightarrow P(N)$ 表示域 u 在系统状态 s 下可以写的客体对象集合.

函数 $observe: D\times S\rightarrow P(N)$ 表示域 u 在系统状态 s 下可以读的客体对象集合.

定义 6.　一个域在某系统状态下所有观察到的对象集合即是它的系统视图，可以用如下函数表示：

$$domview(u,s)=\langle val_1\cdots val_i\cdots val_{|N|}\rangle,$$

$$val_i=\begin{cases}contents(s,n_i), & n_i\in observe(u,s)\\ \varnothing, & \text{其它}\end{cases}.$$

一个域的系统视图指它能够观察到的系统状态的组成部分. 用系统视图的概念，输出一致性还可以表示成：系统的一个内部操作动作造成的输出影响只依赖于发出动作的域的系统视图.

定义 7.　如果下式成立则称为系统 M 具有局部干扰性(locally respects $\rightsquigarrow$)：

$$dom(a)\not\rightsquigarrow u\rightarrow s\overset{u}{\sim}step(s,a).$$

局部干扰性表明，一个域 u 对另一个域 v 无干扰关系的话，则 u 发出的操作对域 v 来说也是不可见的. 局部干扰性保证一个域的系统视图不受那些与其无干扰关系域的动作的影响.

定义 8.　如果下式成立则称为系统 M 具有弱单步一致性(weakly step consistent)：

$$s\overset{u}{\sim}t\wedge s\overset{dom(a)}{\sim}t\rightarrow step(s,a)\overset{u}{\sim}step(t,a).$$

弱单步一致性表明，当一个操作动作发生后，一个域可见的系统状态的变化只依赖其前一状态和发出该动作的域在发出动作之前状态的系统视图.

基于上述定义，文献[5]给出了下面的展开定理(unwinding).

定理 1.　系统满足非传递性无干扰策略的判定定理.

设 M 是一个视图隔离的系统，有一个具有非传递性的 $\rightsquigarrow$ 策略，并且 M 满足：输出一致性、弱单步一致性和局部干扰性，则 M 满足非传递性无干扰策略.

在无干扰模型中，干扰关系分为传递性和非传递性. 传递的无干扰模型给出了系统 M 对由关系 $\rightsquigarrow$ 表达的信息流策略安全的条件，一般表示为，如果 $u\rightsquigarrow v$，$v\rightsquigarrow w$，则 $u\rightsquigarrow w$. 传递性无干扰模型可以用来描述基于格的安全模型(例如 BLP 模型). 非传递的无干扰模型给出了系统 M 对由关系 $\rightsquigarrow$ 表达的信息流策略安全的条件，一般表示为，如果 $u\rightsquigarrow v$，$v\rightsquigarrow w$，但 $u\not\rightsquigarrow w$. 非传递性无干扰模型描述非格的结构.

3　可信计算平台的信任链传递模型

3.1　TCG 可信计算平台的局限性

由可信的定义可以看出，可信的核心内容在于组件行为的可预测性. 组件行为各有不同：对应用程序来说，它的行为包括输出屏幕信息、显示图片、发出声音、创建网络连接等等；对内核来说，它的行为包括产生进程、管理内存、访问控制等等. 这些不同的行为都符合有限状态自动机模型的抽象描述：一个状态确定的系统，其行为是可以预测的，即一个固定的输入队列可以有一个固定的输出队列，也就是这些行为都可以通过信息系统的状态和输出来表现. 而且，从组件外部来看，它们只能通过输出来表现.

因此根据可信的定义，一个初始状态确定、输入确定的有限状态自动机系统是一个可信系统. 但在现实系统中，组件的状态除了取决于自身(通常是代码、堆栈、数据)，还受其所处环境的影响(包括硬件

平台、操作系统、系统中其它的组件的影响),也就是说组件不是一个状态孤立的有限状态自动机,而是一个部分状态受其它关联组件控制的状态机.系统是否可信由其组件和组件之间的交互所决定.这里的组件可以是一个硬件模块、软件模块、应用程序等.组件的可信性可以由图2的模型表示,模型包括4个元素:组件、输入、输出和组件间的干扰.组件运行是否可信,用组件输出是否符合预期来表示,因此一个组件运行可信取决于3个因素:

(1)完整性因素.即组件本身没有被篡改过;

(2)输入因素.组件的输入在允许范围内;

(3)干扰因素.其它组件对其状态没有干扰.

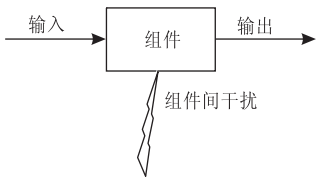

图2 组件间干扰造成运行不符合预期示意

可见:如果组件本身没有被篡改,并且组件间不存在干扰,则组件的输出符合预期,系统中组件的运行是可信的.所以,如果要使信任链传递有效,必须消除组件之间的干扰.

3.2 可信计算平台的信任链传递形式化描述

下面结合无干扰模型,给出可信计算平台的信任链的形式化描述.

可信计算平台用 S 表示,平台由各个组件组成,一个组件可能由更小的组件组成,最小规模的组件可以是一个进程,用 $a_1,a_2,\cdots,a_n$ 表示,即 $S=\{a_1,a_2,\cdots,a_n\}$.

D 表示无干扰模型中的安全域,可以映射到可信计算平台的组件.D 为 S 的真子集.

信任关系可以用一个二元关系表示:$\rightarrow\in D\times D$,$A\rightarrow B$ 表示系统 S 中组件 A 对 B 进行了完整性度量,并且度量成功,组件 A 信任组件 B.易见,这样的信任关系具有传递性、自反性.

因此,系统中信任链可以用下面的式子表示:

$$a_0\rightarrow A_1\rightarrow A_2\rightarrow\cdots\rightarrow A_n,\ A_i\subset D,$$

其中 a_0 表示可信度量根核心 CRTM,表示信任链由 CRTM 开始,注意 $A_i\cap A_k$ 不一定为空,这是由计算平台组件之间复杂的依赖关系所决定的.

基于可信计算技术的装载前度量技术实现的可信链可以这样形式化地描述:

$$digest(A_i,A_k)=expect(A_k)\Rightarrow A_i\rightarrow A_k.$$

如果由组件 A_i 通过摘要运算获得的 A_k 摘要值与预期值 $expect(A_k)$ 相等,则组件 A_i 信任组件 A_k,信任关系将由 A_i 传递至 A_k,系统控制权也转移到 A_k.其中 $digest(A,B)$ 表示组件 A 对组件 B 进行摘要运算的结果,$expect(A)$ 表示组件 A 的完整性预期值.

下面论述 $\forall a,b,c\in S$,如果干扰关系 $\rightsquigarrow$ 是传递性的,则信任链不成立.

若 $A_i\rightarrow A_k$,$a,b\in A_i$,且 $c\in A_k$,则由 $a\rightsquigarrow b\cup b\rightsquigarrow c\Rightarrow a\rightsquigarrow c$.

(1)由于 $a,b\in A_i$,$a\rightsquigarrow b$ 属于组件 A_i 内部程序之间干扰关系,不影响组件之间的信任.

(2)对于 b 和 c 的关系,如果 $b\rightsquigarrow c$,即允许信息流由 $b\rightsquigarrow c$ 实现,这种干扰关系不破坏信任关系.

(3)$a\rightsquigarrow c$ 属于非预期干扰,由 $a\rightsquigarrow c$,意味着有非预期的信息从 A_i 流向 A_k,组件 A_k 的输出必然受到影响,原有 $A_i\rightarrow A_k$ 关系被破坏.这时尽管有 $digest(A_i,A_k)=expect(A_k)$,非预期干扰将导致 $A_i\nrightarrow A_k$.

若组件间的干扰关系具有传递性,各域间通过传递性就可能产生非预期干扰,那么,即使通过了TCG规范规定的完整性度量,输出也不一定符合预期,系统组件的运行是不可信的,系统运行就不可信.因此,非预期干扰能够破坏组件之间的信任关系,导致信任链失效.

由以上推导过程可知,若

$\forall A,B\subset D$;$a,b\in A\cup c\in B$;$a\rightsquigarrow b\cup b\rightsquigarrow c\Rightarrow a\not\rightsquigarrow c$,

则系统将不存在非预期的干扰,称满足以上关系的 $D\times D$ 上二元关系为非传递无干扰关系,记作 $A\xrightarrow{IN}B$.

非传递无干扰关系描述的是一种隔离性要求比较严格的通道控制安全策略,具有非传递无干扰关系的系统组件之间只有直接干扰关系,不存在间接造成的干扰关系.

4 无干扰信任传递判定定理

4.1 非传递无干扰模型与信任链传递的关系

基于以上分析可知,单纯的通过完整性验证实现的信任链传递是否有效无法进行验证.只有当系统具有特定的安全机制,满足一定的安全策略,组成系统的各安全域之间的信息流动受到一定安全策略限制,使得组件的运行不受干扰,这时,用完整性度量方法所建立的信任链才是有效的.

进一步用图 3 表示非传递无干扰关系，其中粗箭头连线表示信任传递关系，细箭头连线表示干扰关系. 可以看出，信任链有两条，分别是

$a_0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3$；$a_0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_4$.

由 $a_3 \rightsquigarrow a_4 \bigcup a_4 \rightsquigarrow a_5 \Rightarrow a_3 \rightsquigarrow a_5 \Rightarrow A_2 \nrightarrow A_3$；

由 $a_7 \rightsquigarrow a_2 \bigcup a_2 \rightsquigarrow a_1 \Rightarrow a_7 \rightsquigarrow a_1 \Rightarrow A_1 \nrightarrow A_4$.

因此，系统中存在的两条信任链均不成立.

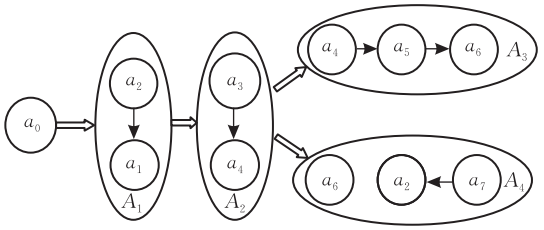

图 3　非传递无干扰关系示意图

因此，可得出 TCG 的信任链传递存在问题，即

$$digest(A_i, A_k) = expect(A_k) \nRightarrow A_i \rightarrow A_k.$$

于是得到下面的具有条件约束的信任链传递模型：

$$A_i \xrightarrow{IN} A_k \bigcup digest(A_i, A_k) = expect(A_k) \Rightarrow A_i \rightarrow A_k \tag{1}$$

模型表示，可信计算平台的组成组件在系统运行时若满足非传递无干扰关系，则信任链能够建立，信任关系能够传递，达到平台可信目标.

4.2　无干扰信任传递判定定理

上述信任链传递模型关键之处是验证系统中是否满足非传递无干扰关系，但从非传递无干扰关系的定义出发很难进行验证，于是，基于定理 1，本文给出无干扰信任传递判定定理，用于判定可观测的系统状态和输出在满足什么条件时，信任链的建立和传递才是有效的.

定理 2.　系统满足非传递无干扰关系的判定定理：

(1) 系统的域满足输出一致性. 即一个内部操作动作造成的输出影响只依赖于发出动作域的系统视图.

(2) 系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联. 即

$$s \overset{dom(a)}{\sim} t \wedge (contents(step(s,a),n) \neq contents(s,n) \vee contents(step(t,a),n) \neq contents(t,n)) \rightarrow contents(step(s,a),n) = contents(step(t,a),n).$$

(3) 系统中，如果一个动作改变了一个客体对象的值，则发出该动作的域一定可以写访问该客体对象. 即

$$contents(step(s,a),n) \neq contents(s,n) \rightarrow n \in alter(dom(a),s).$$

(4) 系统任意两个域间满足如下关系：

$\exists n \in N,\ n \in alter(u,s) \wedge n \in observe(v,s) \rightarrow u \rightsquigarrow v.$

证明.　根据定理 1，只要证明 M 满足输出一致性，弱单步一致性和局部干扰性即可.

输出一致性直接由判定条件(1)得到.

下面证明弱单步一致性，即证明

$$s \overset{u}{\sim} t \wedge s \overset{dom(a)}{\sim} t \rightarrow step(s,a) \overset{u}{\sim} step(t,a).$$

上式可以写成：对 $\forall n \in domview(u,s)$，有下式成立

$$s \overset{u}{\sim} t \wedge s \overset{dom(a)}{\sim} t \rightarrow contents(step(s,a),n) = contents(step(t,a),n).$$

对 n 分 3 种情况讨论：

(1) 若 $contents(step(s,a),n) \neq contents(s,n)$，则由 M 满足判定条件 2，可得

$$contents(step(s,a),n) = contents(step(t,a),n).$$

(2) 若 $contents(step(t,a),n) \neq contents(t,n)$，类似的，由 M 满足判定条件 2，可得

$$contents(step(s,a),n) = contents(step(t,a),n).$$

(3) 若非(1)、(2)两种情况，则必有

$$contents(step(s,a),n) = contents(s,n) \wedge contents(step(t,a),n) = contents(t,n).$$

又由 $s \overset{u}{\sim} t \rightarrow contents(s,n) = contents(t,n)$，可得

$$contents(step(s,a),n) = contents(step(t,a),n).$$

因此弱单步一致性得证.

以下证明局部干扰性，即证明 $dom(a) \not\rightsquigarrow u \rightarrow s \overset{u}{\sim} step(s,a)$，等价于证明其逆否命题：

$$\exists n \in domview(u,s),\ contents(s,n) \neq contents(step(s,a),n) \rightarrow dom(a) \rightsquigarrow u.$$

由判定条件(3)可得

$$contents(step(s,a),n) \neq contents(s,n) \rightarrow n \in alter(dom(a),s).$$

又由 $n \in domview(u,s)$，根据定理中判定条件(4)，立即可得 $dom(a) \rightsquigarrow u$ 成立.　　证毕.

若组件间的干扰关系具有传递性，各域间通过传递性就可能产生非预期干扰，那么，即使通过了 TCG 规范规定的完整性度量，也难以达到系统运行可信的目标. 定理 2 给出了一个计算机系统满足非传递性无干扰关系的形式化规范，也给出了一种判定可信计算平台信任链传递关系的有效方法. 如上所述，系统域间非传递无干扰也就意味着系统输出

的确定性和可预期性，能够确保信任链的建立不受系统中组件间干扰行为的影响.

5 原型实现与验证

我们基于开源的虚拟机监视器(VMM)系统Xen[4,7]，利用虚拟隔离实现了一个满足非传递无干扰的系统.它将应用完全隔离，各应用之间不能直接共享信息，所有隔离域之间的信息交换均通过虚拟机监视器进行.

如图4所示，VMM系统上的设备驱动模型由运行于虚拟机上的前端驱动(虚拟设备)和运行于虚拟机监视器上的后端驱动(实际驱动程序)组成，实现对硬件设备的共享使用.虚拟机间的信息流只能通过可信通道B完成.系统中由不同的虚拟机运行不同安全等级的应用系统，VMM系统上的信任链由图左侧的①和②两步建立(先由硬件平台验证基础软件层VMM，再由VMM对虚拟机整体进行验证).但若使信任链有效，必须确保系统中不存在非预期的干扰，即

$$A \rightsquigarrow B \bigcup B \rightsquigarrow C \Rightarrow A \not\rightsquigarrow C.$$

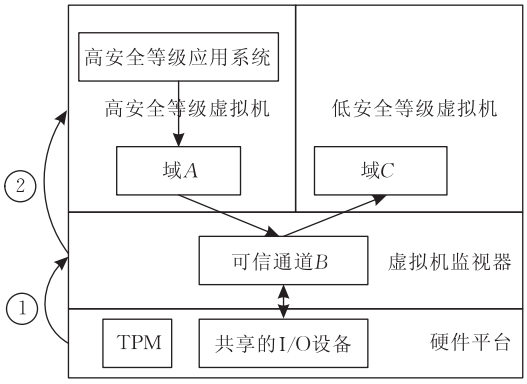

图4 非传递无干扰关系示意图

VMM系统中运行于VMM之上的虚拟机可以对应于无干扰模型的安全域，各个域之间的交互只通过I/O设备进行，因此，只要验证了各虚拟机间通过I/O设备的交互满足非传递无干扰关系，则通过启动阶段针对各虚拟机整体作为文件的完整性验证后，VMM系统建立的信任链是有效的.

依据定理2，该VMM系统的I/O设备驱动程序需满足如下要求：

(1)由输出一致性的定义可知，VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识.

(2)由局部干扰性定义可知，VMM系统中，虚拟I/O设备除其所在的虚拟机外其它虚拟机不能改变它的运行状态，I/O设备驱动与虚拟设备间所传输的数据对其它虚拟机是不可见和不可修改的.该VMM系统的隔离机制确保虚拟机必须采用虚拟设备接口访问后端驱动程序.每个虚拟机能够访问的I/O寄存器被限制，能够禁止未授权的访问.

(3)由弱单步一致性定义可知，对于若干虚拟机共享的客体对象，VMM系统必须具有同步保护机制以防止不同虚拟机对该资源的竞争.

该系统依据非传递无干扰策略模型对传统VMM的虚拟I/O设备体系进行了改造，只要根据应用程序需求，合理划分安全域，各应用安全域的运行不受其它应用程序干扰，依据式(1)描述的信任传递模型，经过完整性验证，系统运行能够达到可信目标.

6 结 论

本文从可信的定义入手，分析了TCG信任链的局限性，指出可信计算平台系统中加载前的完整性度量并不能保证系统运行可信，如果系统没有安全策略限制，讨论信任链传递是没有意义的.然后借鉴Trent的PRIMA方案，基于无干扰模型，用形式化的方法论述了当系统满足非传递无干扰的安全策略时，信任链的建立不受系统中其它安全无关组件与行为的干扰，信任才能有效地传递下去，系统能够建立完整的信任链，实现可信目标.并据此提出了无干扰信任传递判定定理.但是，满足非传递无干扰这一条件对系统限制可能很严格，下一步的研究方向是研究更为实用化和灵活的信任传递模型.

参 考 文 献

[1] Shen Chang-Xiang, Zhang Huan-Guo, Feng Deng-Guo, Cao Zhen-Fu, Huang Ji-Wu. Survey of information security. Science in China Series F: Information Sciences, 2007, 50(3): 273-298(in Chinese)
(沈昌祥，张焕国，冯登国，曹珍富，黄继武. 信息安全综述. 中国科学E辑：信息科学，2007，37(1)：129-150)

[2] Sadeghi Ahmad-Reza, Selhorst Marcel, Stüble Christian, Winandy Marcel. TCG Inside? A note on TPM specification compliance//Proceedings of the 1st Benelux Workshop on Information and System Security. Belgium, 2006

[3] Jaeger Trent, Sailer Reiner, Shankar Umesh. PRIMA: Policy-Reduced Integrity Measurement Architecture//Proceedings of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT 2006). Lake Tahoe, California, 2006: 134-143

[4] Zhang Xing, Chen You-Lei, Shen Chang-Xiang. A non-interference trusted model based on processes. Journal on Communications, 2009, 30(3): 6-11(in Chinese)
(张兴，陈幼雷，沈昌祥. 基于进程的无干扰可信模型. 通信学报，2009，30(3)：6-11)

[5] Rushby John. Noninterference, transitivity and channel-control security policies. Stanford Research Institute, Menlo Park: CSL Technical Report CS-92-02, 1992

[6] Huang Qiang. Study about terminal security architecture based on trusted computing [Ph. D. dissertation]. Naval University of Engineeering, Wuhan, 2007(in Chinese)
(黄强. 基于可信计算的终端安全体系结构研究[博士学位论文]. 海军工程大学，武汉，2007)

[7] Garfinkel Tal, Pfaff Ben et al. Terra: A virtual machine-based platform for trusted computing//Proceedings of the SOSP03. 2003: 193-206

ZHANG Xing, born in 1966, Ph. D., senior engineer. His research interests include security and trusted computing.

HUANG Qiang, born in 1977, Ph. D., engineer. His research interests focus on information security.

SHEN Chang-Xiang, born in 1940, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include computer architecture and information security.

Background

In the process of research on TCG's chain of Trust, the authors analyses different ways of establishing the chain of Trust in a trusted platform. The results obtained from the experiments reveal that the chain of Trust is actually built with integrity measurement as the basis and contradicts the original theory of dynamic behaviors with the results being consistent with expectations. Due to integrity measurement being a static mechanism, it may not be disrupted by the interference resulting from the complicated runtime environment that could destroy the chain. Moreover, the authors analyses the PRIMA scheme proposed by Trent. This model implements security policy CW-Lite to restrict information flows between entities to realize runtime tolerance. Enlightened by this viewpoint, the authors propose a new model to establish trusted chain by utilizing non-interference security policy to guarantee the integrity of the Chain of Trust. This can prevent unexpected information flow between different security domains to achieve real trust in the runtime environment