ISSN 1000-1239/CN 11-1777/TP
45(6): 974～980, 2008

基于无干扰理论的可信链模型

赵 佳[1] 沈昌祥[1,2] 刘吉强[1] 韩 臻[1]
[1](北京交通大学计算机与信息技术学院 北京 100044)
[2](北京工业大学计算机学院 北京 100022)
(04112070@bjtu.edu.cn)

A Noninterference-Based Trusted Chain Model

Zhao Jia[1], Shen Changxiang[1,2], Liu Jiqiang[1], and Han Zhen[1]
[1](*School of Computer and Information Technology, Beijing Jiaotong University, Beijing* 100044)
[2](*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022)

Abstract The traditional information security systems, such as firewall, intrusion detection and anti-virus, are all preventing attacks from the outside. But these methods can't meet the various security requirements. Therefore, experts appeal to solve the problems from the inner. Under this background, TCG proposed the conception of trusted computing. It aims to improve the security on the terminals. At present, trusted computing and its related researches are the focus and trend of information security in inland and oversea. Trusted computing is the foundation of the security, and it may solve the insecure problem caused by the platform of hardware in PC. Trust chain starts from the trust root. TCG introduces the idea of the trusted into the computing environment, but there is still not the formalized uniform description. Trusted computing is still a technology but not a theory, and the basic theory model has not been established. Noninterference theory is introduced into the domain of trusted computing to construct the trusted chain theoretic model. The basic theory of the computing trusted is proposed and a noninterference-based trusted chain model is built from the dynamic point of view, and then the model is formalized and verified. Finally, the process of start up based on Linux operating system kernel is implemented. The implementation provides a good reference for the development and application of the trusted computing theory as well.

Key words trusted computing; trusted computing platform; trusted chain; noninterference theory; trusted root

摘 要 可信计算的相关研究已成为当前国内外信息安全方面的研究热点和趋势之一.可信计算技术也成为构建安全计算机系统行之有效的新技术.目前可信计算理论的发展滞后于技术的发展,针对可信计算中可信链传递缺乏理论模型的问题,将无干扰理论引入到可信计算领域,提出了计算机系统可信的基本理论.从动态的角度建立了基于无干扰理论的可信链模型,并对该模型进行了形式化描述和验证,而且实现了基于Linux操作系统内核的可信启动过程.其实现思路对于可信计算理论的发展和应用具有很好的参考价值.

关键词 可信计算; 可信计算平台; 可信链; 无干扰理论; 可信根

中图法分类号 TP309

收稿日期:2007-05-23;**修回日期**:2008-12-28

基金项目:国家"九七三"重点基础研究发展规划基金项目(2007CB307101);国家"八六三"高技术研究发展计划基金项目(2007AA01Z410,20060101Z4015)

在 Internet 飞速发展的今天,开放的网络环境下的分布式应用越来越普及,为人们的工作生活带来了很大的便利,但同时其中的关键数据的安全处理也给相关的应用以及终端平台(computing platforms)提出了更高的安全需求——应用和终端平台(包括软硬件)需要有一定的"可信度".正是在这种背景下,1999 年成立的可信计算平台联盟[1](2003 年更名为可信计算组织 Trusted Computing Group, TCG)提出了"可信计算"概念,目的就是从终端安全入手,提高终端平台的安全性[2-4].目前,可信计算思想已迅速普及,其相关研究已成为当前国内外信息安全方面的研究热点和趋势之一.可信计算技术也成为构建安全计算机系统行之有效的新技术.

TCG 提出的"可信计算"从行为的角度给出实体可信的定义,强调行为的可预测性和可控性,认为"当一个实体始终沿着预期的方式(操作或行为)达到既定目标,则它就是可信的"[5]."可信计算平台"技术的核心是称为可信平台模块(trusted platform module, TPM)的安全芯片.利用 TPM 来构建可信计算平台,保障硬件平台、操作系统的可信,进而保障应用的可信,可信链的建立和传递是其中的关键技术.TCG 给出了可信链传递的框架和实施机制,但是,各个环节的技术实现还有不少难点需要突破.尤为重要的是由于可信计算思想来源于工程实践,目前针对可信计算的研究大都停留在工程实现层面,缺少严格的理论模型支撑,这必将在一定程度上制约可信计算技术的发展[6-7].

在可信链模型中有一个重要的前提,即系统中存在一个可信根.系统从可信根开始,一级校验一级,一级信任一级,形成一条可信链.根据 TCG 主规范中的描述,可信根被无条件相信是由一系列证书保证的,比如有效性证书(validation certification)、背书证书(endorsement certification)、身份证书(identity certification)、准则证书(conformance certification)等等[8].一个系统的启动过程也就是一条可信链的传递过程,图 1 描述了一个实际系统从加电开始到上层应用的一个可信传递过程.

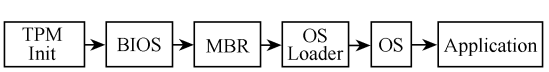

Fig. 1　Transition of trust.

图 1　可信传递过程

由于平台和应用的多样性,应用之间存在着相互的影响,这不仅为可信链的建立和传递带来了困难,而且也难以利用已有的模型准确地刻画该过程.基于信息流的无干扰理论[9]的提出为平台中应用的隔离提供了理论支撑,也为可信链的建立和传递的形式化描述提供了可能.本文将无干扰理论引入到可信计算领域,从动态的角度提出了计算机系统可信的基本理论,建立了基于无干扰理论的可信链模型,并对该模型进行了形式化描述和验证.文章最后给出了可信传递的一种实现方式.

1　相关工作

微软公司在 2002 年提出 Palladium 计划,后改为 NGSCB (next generation secure computing base),即下一代安全计算基[10].该计划强调可信计算在数字产权管理方面的应用.2003 年 9 月,Intel 公司为支持 Palladium 计划推出了 LT 技术(LaGrande technology)[11],包括微处理器、芯片组、I/O 设备及其相应软件,目的是为了保护计算机数据的机密性,并防止恶意软件的攻击.

Stanford 大学的 Garfinkel 等人为可信计算构建了一个灵活的体系结构 Terra[12],Terra 利用可信虚拟机监控器 TVMM(trusted virtual machine monitor)把硬件平台分成多个独立的虚拟机为不同目的的应用提供多种平台支撑.

可信计算在工程实现方面有较大发展,但是,有关可信计算理论模型方面的研究目前较多地集中于如何在信息世界中计算信任的问题上,即如何将社会学中人与人之间的信任关系运用到计算环境中,从而达到信息世界中可信的目的.如基于概率统计的信任模型[13]、基于模糊数学的信任模型[14]、基于主观逻辑的信任模型[15]、基于证据理论的信任模型[16]和基于软件行为学的信任模型[17]等.但这些模型都侧重于社会学中的信任关系,同 TCG 定义的可信还不完全一致,需要进一步完善从而更好地给可信计算提供理论上的保障.

2　信息流的无干扰理论和模型

信息流的无干扰的思想最早在 1982 年由 Goguen 和 Meseguer[18]提出,此后出现了大量基于无干扰思想的信息流模型[19-22].1992 年,Rushby[9]提出了采用状态机的无干扰模型,并给出系统关于传递和非传递无干扰策略是安全的定义,以下沿用文献[9]中的部分术语对该模型进行简要描述.

系统中 M 包括系统状态集 S、动作集 A、输出集 O 和安全域集 D 四个集合,以及这些集合上定义的 4 个函数:

单步状态转换函数 $step: S\times A\rightarrow S$;

系统运行函数 $run: S\times A^{*}\rightarrow S$;

输出函数 $output: S\times A\rightarrow O$;

主域函数 $dom: A\rightarrow D$ 表示系统每个动作所属的域.

在传递无干扰模型中,定义~为安全域 D 上的关系,表示安全域间的干扰关系. 例如 $u, v\in D$,则 $u\sim v$ 可以简单地理解为信息可以从域 u 流向域 v. 为了定义系统 M 在传递的无干扰模型中的安全条件,还要定义一个辅助函数 $purge: A^{*}\times D\rightarrow A^{*}$,对于 $\alpha\in A^{*}$, $v\in D$, $purge(\alpha, v)$ 表示从动作序列 α 中删除所有从不干扰域 v 的域所发出的动作后的动作序列,表示如下:

$$purge(\Lambda, v)=\Lambda$$

$$purge(a\circ\alpha, v)=\begin{cases} a\circ purge(\alpha, v), & \text{if } dom(a)\sim v,\\ purge(\alpha, v), & \text{otherwise,}\end{cases}$$

其中, $dom(a)=v$.

系统 M 对策略~的安全条件是:

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

Rushby 的模型使用了安全域的概念,而在操作系统中域的划分不那么明确,比较抽象. 一般认为,进程才是真实操作系统的主体,因而我们以进程间的信息流动为出发点,借鉴 Rushby 的思想,提出了基于无干扰理论的可信链模型(noninterference-based trusted chain model, NTCM).

3 基于无干扰理论的可信链模型

系统是由多个不同的状态组成的,如果系统从一个可信的初始状态开始,而且所到达的每一个状态都是可信的,那么这个系统就是可信系统. 很容易理解,如果系统中的每个正在运行的进程都满足可信的传递条件,那么就在这些可信的运行进程中传递了可信属性,建立了完整的可信链.

进程最初是在 Unix 等多用户、多任务操作系统环境下为了表示应用程序在内存环境中的执行情况而提出的,它是 Unix 等操作系统中的基本成分,是系统资源分配的基本单位. 本文中我们使用进程的广义定义,抛开操作系统的特定环境,认为进程就是运行的程序,因此在计算机的启动过程中,也就是在操作系统加载之前,计算机系统中的程序也是通过进程来执行的. 进程是一个动态因素,所以本文提出的进程可信将传统的静态意义上的可信扩展为动态可信. 下面我们给出可信系统的形式化的定义.

定义 1. 一个系统可以被描述为一个多元组:

$$M=(P, A, S, O, R_{i\in[1,2]}, F_{j\in[1,6]}),$$

其中:

P 为系统的进程集合,表示为 $(p_1, p_2, \cdots, p_n)$.

A 为系统的动作集合,表示为 $(a_1, a_2, \cdots, a_n)$, α 为 A 中的一个动作序列, $\alpha\in A^{*}$.

S 为系统的状态集合,表示为 $(s_0, s_1, \cdots, s_n)$, s_0 称为系统的初始状态. 如果从初始状态 s_0 开始,经过动作序列 α 后达到另一状态 s,则称 s 是系统的可达状态.

O 为系统的输出结果集合.

系统 M 含有两种关系:

R_1 : $\approx$ 为进程集合 P 上的关系. 当 $p\approx q$ 表示进程 p 的执行会对进程 q 的执行产生影响. 当 $p\not\approx q$ 时表示进程 p 的执行对进程 q 的执行毫不影响.

R_2 : $\overset{p}{=}$ 为进程集合 S 上的一个关于系统状态的观察关系, $s\overset{p}{=}t$ 表示从进程 p 的角度观察,系统状态 s 和 t 是等价的.

系统 M 含有 6 个函数:

F_1: 函数 $step: S\times A\rightarrow S$ 表示系统运行一个动作后的状态变迁.

F_2: 函数 $run: S\times A^{*}\rightarrow S$ 表示系统在运行一个动作序列后的状态变迁. 状态变迁函数具有下述性质:

$$run(s, \Lambda)=s,$$

$$run(s, a\circ\alpha)=run(step(s, a), \alpha),$$

$$run(s, \alpha\circ a)=step(run(s, \alpha), a),$$

其中, Λ 表示一个空的动作序列, $\circ$ 表示动作间的连接操作.

F_3: 函数 $pro: A\rightarrow P$ 表示一个动作所属的进程,即该动作的发出者.

F_4: 函数 $output: S\times A\rightarrow O$,如 $s\in S, a\in A$,则 $output(s, a)$ 表示执行完动作 a 后系统的输出结果.

F_5: 函数 $del: A^{*}\times P\rightarrow A^{*}$,对于 $\forall p\in P$ 和一个动作序列 $\alpha\in A^{*}$, $del(\alpha, p)$ 表示删除动作序列 α 上所有由不干扰进程 p 的进程所发出的动作后剩余的序列. 并且有:

$$del(\Lambda, p)=\Lambda,$$

$$del(\alpha\circ a, p)=\begin{cases} del(\alpha, p)\circ a, & \text{if } pro(a)\approx p,\\ del(\alpha, p), & \text{otherwise.}\end{cases}$$

F_6: 函数 $check: P\times P\to\{\text{true},\text{false}\}$,对 $\forall p, q\in P$,有:

$$check(p,q)=\begin{cases}\text{true, if } run(s_0,\alpha)\overset{p}{=}run(s_0,del(\alpha,p))\\ \quad\Rightarrow run(s_0,\alpha)\overset{q}{=}run(s_0,del(\alpha,q)),\\ \text{false, otherwise.}\end{cases}$$

定义 2～4 是系统中关于进程的几条重要性质.

定义 2. 设 $s,t\in S,a\in A$,当进程 $pro(a)$满足下列条件时,称该进程满足输出隔离性质.

$$s\overset{pro(a)}{=}t\Rightarrow output(s,a)=output(t,a).$$

定义 3. 设 $s,t\in S,a\in A$,称进程 $pro(a)$满足单步隔离性质,当

$$s\overset{pro(a)}{=}t\Rightarrow step(s,a)\overset{pro(a)}{=}step(t,a).$$

定义 4. 称进程 $pro(a)$为可信进程,当其满足如下条件:

$$output(run(s_0,\alpha),a)=output(run(s_0,del(\alpha,pro(a))),a),$$

其中 s_0 为初始状态,$a\in A,\alpha\in A^*$.

从系统微观角度看,任意时刻系统中只可能有一个进程在运行,因此,我们认为如果当前执行的进程是可信的,那么此时的系统状态就可信.下面给出可信状态的递归定义.

定义 5. 可信状态的定义.

1) $\varnothing\in S$ 为可信状态($\varnothing$为空状态);

2) $s=run(\varnothing,\alpha)\in S$ 为可信状态,当且仅当系统正在运行的进程 p 满足结果隔离性质,且 $run(\varnothing,\alpha)\overset{p}{=}run(\varnothing,del(\alpha,p))$成立.

我们认为系统在刚刚加电的瞬间是空状态$\varnothing$,对于一个惟一确定的 TPM,按照 TCG 规范,初始化后的状态 s_0 也应该是惟一确定的,和 TCG 中关于可信根的定义一致,如果 s_0 满足可信状态的定义,即如果 TPM 初始化进程满足结果隔离性质,且 $run(\varnothing,\alpha)\overset{p}{=}run(\varnothing,del(\alpha,p))$成立,那么就称这一特殊的可信状态 s_0 为该系统的可信根,下面的描述都从可信根出发.

定义 6. 当系统满足下面条件时,称系统满足可信传递性质.

$\forall a,b\in A$,且 $pro(a)=p, pro(b)=q$,则对于状态 $s\in S, s=run(s_0,\alpha)$,只要 α 包含动作序列 $a\circ b$,则必有 $check(p,q)=\text{true}$.

$check(\ )$函数体现了进程间可信传递的性质,如果 $check(p,q)=\text{true}$,则根据该函数为真值的条件,可知进程 p 所具有的性质传递给了进程 q,所以,如果系统的动作序列中连续出现了两个进程相继发出的动作,则这两个进程满足可信传递性质.

上面给出了一系列的定义,目的是为了给出一个形式化描述的可信链模型,那么究竟系统满足什么样的条件才能称为是可信的呢,下面我们就给出可信系统的通俗定义.

定义 7. 当一个系统 M 满足下面两个条件:

1) s_0 是可信根;

2) $\forall s\in S$,其中 s 是可达的,且 s 是可信状态,则称系统 M 是可信系统.

定义 7 的描述虽然容易理解,但是无法体现系统的内部联系和可信传递的内在机制,于是我们给出了一个重要定理,这个定理可以更直观地反映出可信在系统中的传递过程.

定理 1. 一个系统 M 当满足下面 3 个条件时:

1) M 从可信根开始运行;

2) M 中的进程满足单步隔离性和输出隔离性;

3) M 满足可信传递性质,

则 M 是可信系统.

证明. 只需证明系统 M 满足定义 7 的两个条件,即可证明 M 是可信系统.

根据可信根的定义,可知 s_0 是可信状态,满足定义 7 的条件 1).

$\forall s$ 是一个系统可达状态,只要证明 s 是可信状态,即可满足定义 7 的条件 2).

设 $s=run(s_0,\alpha)$,对执行序列 α 的长度作归纳法.

归纳基础,当长度为 0 时,系统状态 s_0 是可信状态.

假设长度为 n 时,s 是可信状态,根据可信状态的定义可知,当前执行进程 p 满足:

$$run(s_0,\alpha)\overset{p}{=}run(s_0,del(\alpha,p)).$$

此时,系统执行动作 a,设 $pro(a)=p'$,并进入下一个状态 $s'=run(s_0,\alpha\circ a)$.因此要证明:

$$run(s_0,\alpha\circ a)\overset{p'}{=}run(s_0,del(\alpha\circ a,p')).\quad(1)$$

式(1)左边可得:

$$run(s_0,\alpha\circ a)=step(run(s_0,\alpha),a).$$

式(1)右边可得:

$$run(s_0,del(\alpha\circ a,p'))=run(s_0,del(\alpha,p')\circ a)=step(run(s_0,del(\alpha,p')),a).$$

因为 M 中的进程满足单步隔离性质,所以要证明:

$$step(run(s_0,\alpha),a)\overset{p'}{=}step(run(s_0,del(\alpha,p')),a),$$

即要证明:

$$run(s_0,\alpha) \overset{p'}{=} run(s_0,del(\alpha,p')).$$

下面分情况讨论:

1) $p=pro(a)$:

此时,$p'=p$,由归纳假设即得证.

2) $p\neq pro(a)$:

可以设 b 为动作序列 α 中的最后一个动作,此时出现 $pro(a)=p'$,$pro(b)=p$,且对于状态 $s'=run(s_0,\alpha\circ a)$而言,动作序列中出现了 $b\circ a$,因此由于 M 满足可信传递性质,可知 $check(p,p')=$true,根据验证函数定义和归纳假设前提条件得

$$run(s_0,\alpha) \overset{p'}{=} run(s_0,del(\alpha,p')),$$

由此可知式(1)成立.因此,由归纳法原则,命题成立.

证毕.

定理 1 是对系统动态传递可信的描述,是建立可信链的重要依据.进程是否可信体现在系统中的进程之间的干扰关系.可信根是同 TPM 绑定的,由一系列证书保证,被无条件信任的状态,从可信根出发,系统一级验证一级,在进程中传递可信,形成一条完整的可信链.

从前面的证明过程可以看到,系统的每一个可信状态都是可信链中的一个环节,环环相扣,任意环节出现了错误,都会影响到该环节之后所有节点,但是不会影响该环节之前的节点,也就是说可信链无法传递下去.

4 Linux 的可信启动实例

本文实现了基于 Linux 操作系统内核的可信启动过程.图 2 是系统中的可信终端信任链模型.该模型基于 TPM 硬件的可信度量、密封存储和度量报告的功能,启动过程利用 Grub 引导,装载操作系统内核后,执行 0 号进程 *init*( ),并且在指令/*etc*/*rc*.*d*/*rc* 中选择缺省的运行模式,因为在 Red Hat 中的缺省值为 3,所以执行/*etc*/*rc*.*d*/*rc*3.*d*/目录下的程序.

由于 Grub 引导过程中的 3 个阶段以及操作系统内核执行顺序相对比较固定,因而我们采用较为通用的静态完整性度量方法,在安装 Grub 时,生成各个需要验证的模块的校验值,并且利用 TPM 保护这些校验值.在 Linux 系统加电后,先对 TPM 初始化,进入状态 s_0,根据定义 5 可知 s_0 为系统的可信根.从终端加电到操作系统装载是一个顺序固定的过程,前面的进程执行结束后才会执行下一个的进程,所以这些依次执行的单个进程之间满足单步隔离性质和输出隔离性质.进行静态校验时前一个进程验证后一个进程,如果验证结果和预期的值相同,则表明后一个进程可信,也就是满足可信传递性质,此时才会把系统的控制权交给后面的进程.通过定理 1 可知,本文实现的 Linux 操作系统的启动过程是可信启动过程.

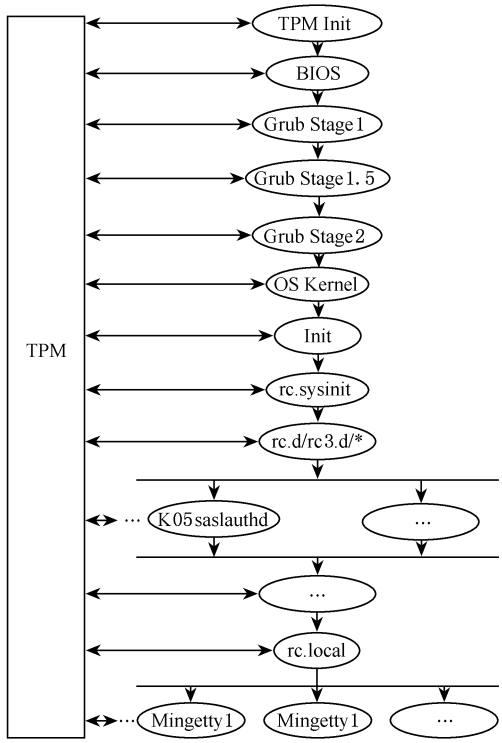

Fig. 2 Trust chain model of a terminal.

图 2 可信终端信任链传递模型

操作系统内核装载之后,我们不仅对文件的内容度量,同时对文件的属性度量,必要时还要对文件的输入值和输出值度量.表 1 给出了在 Pentium Ⅳ 2.40GHz下 Linux 可信启动过程中部分函数的度量耗时,除去文件的 I/O 时间,可信度量大约在系统的启动时间中增加了 9%的额外开销.

Table 1 The Cost of Measuring Process in Trusted Startup on Linux

表 1 可信启动度量各组件耗时列表

Name of Process	Time (μs)
Stage1_5	6999
Stage2	3185
/boot/vmlinuz	32961
/usr/lib/libc.a	58183
⋮	⋮
Total	7.06×10^6

从系统加电开始的整个启动过程中都有 TPM 的参与.只有验证结果和预期的值相同可信链才会传递下去,这为保证系统的安全提供了必要条件.

5 结　论

目前可信计算理论的发展滞后于技术的发展,缺乏可信计算理论模型,一些关键技术有待进一步攻克和完善.本文将无干扰理论引入可信链的建立过程中,从动态的角度建立了从系统加电开始到应用程序的可信链理论模型,由于无干扰理论本身是基于信息流的理论,所以该模型能够有效地发现系统中的隐蔽通道.今后我们研究的重点是如何将终端可信链延伸至网络,建立可信的网络模型.

参 考 文 献

[1] Trusted Computing Group. TPM Main Part 1 Design Principles Specification Version 1.2 [OL]. http://www.trustedcomputinggroup.org, 2003

[2] Chen Youlei. Study on trusted computing model and architecture: [Ph D dissertation] [D]. Wuhan: Wuhan University, 2006 (in Chinese)
(陈幼雷. 可信计算模型及体系结构研究:[博士论文][D]. 武汉:武汉大学, 2006)

[3] Zheng Zhirong, Cai Yi, Shen Changxiang. Research on an application class communication security model on operating system security framework [J]. Journal of Computer Research and Development, 2005, 42(2): 322-328 (in Chinese)
(郑志蓉, 蔡谊, 沈昌祥. 操作系统安全结构框架中应用类通信安全模型的研究[J]. 计算机研究与发展, 2005, 42(2): 322-328)

[4] Zhou Wei, Yin Qing, Wang Qingxian. Abstract security properties in process algebra [J]. Journal of Computer Research and Development, 2005, 42(12): 2100-2105 (in Chinese)
(周伟, 尹青, 王清贤. 进程代数上的抽象安全性质[J]. 计算机研究与发展, 2005, 42(12): 2100-2105)

[5] Trusted Computing Group. TCG Specification Architecture Overview, Version1.2 [OL]. http://www.trustedcomputinggroup.org, 2003

[6] Shen Changxiang, Zhang Huanguo, Feng Dengguo, *et al*. The summary of information security [J]. Science in China, 2007, 37(2): 129-155 (in Chinese)
(沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学, 2007, 37(2): 129-155)

[7] Zhang Huanguo, Luo Jie, Jin Gang, *et al*. Development of trusted computing research [J]. Journal of Wuhan University (Natural Science), 2006, 52(5): 513-518 (in Chinese)
(张焕国, 罗捷, 金刚, 等. 可信计算研究进展[J]. 武汉大学学报(理学版), 2006, 52(5): 513-518)

[8] Trusted Computing Platform Alliance. TCPA Design Philosophies and Concepts Version 1.0 [OL]. http://www.trustedcomputing.org/docs/designv1_0final.pdf, 2001

[9] J Rushby. Noninterference, transitivity, and channel-control security policies [R]. Stanford Research Institute, Tech Rep: CSL-92-02, 1992

[10] Microsoft. Security model for the next generation secure computing base [OL]. http://www.microsoft.com/resources/ngscb, 2003

[11] Intel Corporation. LaGrande Technology Architectural Overview [OL]. http://www.intel.com/technology/security, 2004

[12] T Garfinkel, B Pfaff, J Chow, *et al*. Terra: A virtual machine-based platform for trusted computing [C]. In: Proc of the 19th ACM Symp on Operating Systems Principles. New York: ACM Press, 2003. 193-206

[13] J Patel, W T Teacy, N R Jennings, *et al*. A probabilistic trust model for handling inaccurate reputation sources [C]. Proc of the 3rd Int'l Conf, iTrust 2005. Berlin: Springer-Verlag, 2005. 193-209

[14] Tang Wen, Chen Zhong. Research of subjective trust management model based on the fuzzy set theory [J]. Journal of Software, 2003, 14(8): 1401-1408 (in Chinese)
(唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401-1408)

[15] J Audun. An algebra for assessing trust in certification chains [OL]. http://sky.fit.qut.edu.au/~josang/papers/Jos1999-NDSS.pdf, 1999

[16] Yuan Lulai, Zeng Guosun, Wang Wei. Trust evaluation model based on Dempster-Shafer evidence theory [J]. Journal of Wuhan University (Natural Science), 2006, 52(5): 627-630 (in Chinese)
(袁禄来, 曾国荪, 王伟. 基于 Dempster-Shafer 证据理论的信任评估模型[J]. 武汉大学学报(理学版), 2006, 52(5): 627-630)

[17] Qu Yanwen. Software Behavior [M]. Beijing: Publishing House of the Electronic Industry, 2004 (in Chinese)
(屈延文. 软件行为学[M]. 北京:电子工业出版社, 2004)

[18] J A Goguen, J Meseguer. Security policies and security models [C]. In: Proc of the 1982 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1982. 11-20

[19] J McLean. Security models and information flow [C]. In: Proc of the 1990 IEEE Symp on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1990. 177-186

[20] C O'Halloran. A calculus of information flow [C]. In: Proc of 1st European Symp on Research in Computer Security. Berlin: Springer-Verlag, 1990. 147-159

[21] D Sutherland. A model of information [C]. In: Proc of the 9th National Computer Security Conference. Los Alamitos, CA: IEEE Computer Society Press, 1986. 175-183

[22] J T Wittbold, D M Johnson. Information flow in nondeterministic systems [C]. In: Proc of the 1990 IEEE Symp on Research on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1990. 144-161

Zhao Jia, born in 1980. Ph. D. candidate of Beijing Jiaotong University. Her main research interests include information secure architecture and trusted computing.

赵 佳,1980 年生,博士研究生,主要研究方向为信息安全、体系结构.

Shen Changxiang, born in 1940. Professor and Ph. D. supervisor. Member of the Academy of Engineering. Senior member of China Computer Federation. His main research interests include information security and secure operating system.

沈昌祥,1940 年生,教授,博士生导师,中国工程院院士,中国计算机学会高级会员,主要研究方向信息安全、安全操作系统.

Liu Jiqiang, born in 1973. Associate professor of Beijing Jiaotong University. Member of IEEE. His main research interests include information secure architecture and trusted computing.

刘吉强,1973 年生,博士后,副教授,IEEE 会员,主要研究方向为计算机安全模型.

Han Zhen, born in 1962. Professor and Ph. D. supervisor of Beijing Jiaotong University. Member of IEEE. His main research interests include information secure architecture and computer graphics.

韩 臻,1962 年生,教授,博士生导师,IEEE 会员,主要研究方向为信息安全体系结构、计算机图形学.

Research Background

The traditional information security systems, such as firewall, intrusion detection and anti-virus, are all preventing the attack from the outside. But the traditional preventing methods can't meet the secure requirements, so some exports appeal to solve the problem from the inner. Under this background, in 1999, Trusted Computing Platform Alliance (TCPA), which renamed Trusted Computing Group (TCG) in 2003, proposed the conception of "trusted computing". Its aim is to improve the security from the terminals. At present, the idea of trusted computing is very popular, and the related research work has become the focus and trend of information security in inland and oversea. Noninterference theory is introduced into the domain of trusted computing to construct the trusted chain theoretic model. We propose the basic theory of the computing trusted from the dynamic point of view, and build a noninterference-based trusted chain model, then we formalize and verify the model. Finally, the process of start up based on Linux operating system kernel is implemented. We not only measure the content but also measure the configuration file when it starts up. Its implementation provides a good reference for the development and application of the trusted computing theory as well. The work is supported by the Chinese National Advanced Science and Technology 863 mader grant number (2007AA01Z410, 20060101Z4015) and the 973 Research Foundation under grant number (2007CB307101).