文章编号:1009-3087(2008)06-0150-04

可信计算中完整性度量模型研究

李焕洲[1],林宏刚[2],张 健[3],郭东军[3]
(1.四川师范大学 网络与通信技术研究所,四川 成都 610068;
2.成都信息工程学院 网络工程系,四川 成都 610225;3.四川大学 电子信息学院,四川 成都 610064)

摘 要:为了进一步丰富可信计算完整性验证机制,根据TCG规范中可信传递的思想,提出一种系统完整性度量模型,在执行前度量客体的完整性,防止恶意代码破坏系统完整性,实现信任从前一个实体传递到下一个实体,从而把信任链从运行环境延伸到应用空间。完整性度量模型扩展了现有安全模型的安全属性,它与其它安全模型的结合将能给系统提供更加细致和完善的安全策略。

关键词:可信计算;可信传递;完整性度量
中图分类号:TP309 **文献标识码**:A

Research on the Model of Integrity Measurement to Trusted Computing

LI Huan-zhou[1], *LIN Hong-gang*[2], *ZHANG Jian*[3], *GUO Dong-jun*[3]
(1. Insti. of Computer Network and Communication Technol., Sichuan Normal Univ., Chengdu 610068, China;
2. Dept. of Network Eng., Chengdu Univ. of Info. Technol., Chengdu 610225, China;
3. School of Electronics and Info. Eng., Sichuan Univ., Chengdu 610064, China)

Abstract: In order to enrich further the integrity verification mechanism in trusted computing, a model of integrity measurement was presented based on the idea of transitive trust in the TCG's criterion. In the model, the execute right of an object was defined and specified strictly, and the integrity of the object was measured before execution. The model can prohibit malicious code from compromising the integrity of system and transit trust form one entity to next one, so that the chain of trust can be extended form the BIOS all the way to application layer. The model extended the security attribute of the present security model.

Key words: trusted computing; transitive trust; integrity measurement

TCG[1](trusted computing group)将可信概念引入到计算平台中,试图从系统完整性角度来解决平台的安全性问题。TCG认为:如果从一个初始的"可信根"出发,在平台计算环境的每一次转换时,"信任"可以通过传递的方式保持下去不被破坏,那么平台上的计算环境就始终是可信的,而计算环境的可信事实上就代表了实体的运行可信。完整性度量[2]正是TCG提出的为保证系统安全性和可信性而采用的基本方法之一。在可信链的建立过程中,拥有控制权的实体将控制权转移到下一个实体前都必须对该实体进行可信度量,如果符合某种要求,比如当前度量值和一个事先保存的预期度量值一致,则控制权发生转移,"信任"从前一个实体传递到下一个实体。在TCG规范中,采用了摘要作为可信度量的实现方式,预期度量值(即预期摘要值)是衡量实体是否"按预期方式达到预定目标"的重要依据。

收稿日期:2007-09-07
基金项目:四川省软科学研究资助项目(2006R16-021);四川省应用基础研究资助项目(07JY029-011)
作者简介:李焕洲(1974-),男,副教授.研究方向:计算机取证;可信计算.

TCG规范描述了从平台加电开始,直到运行环境建立,在这个过程中如何对一个欲获得控制权的实体进行度量、验证其完整性。根据TCG规范的描述,所有在此后加载的程序和相关数据都必须在执行之前被度量、被验证,然而,TCG(v1.2)规范只定义了从平台加电到操作系统装载(称之为系统引导)可信传递过程中的完整性度量,并没有描述系统引导后如何对应用程序的完整性进行度量。作者在研究TCG规范中描述的完整性度量方法的基础上,分析了应用程序及其相关客体间的关系,提出一种完整性度量模型,可用于可信传递过程中对应用程序进行完整性度量,把信任链从运行环境延伸到应用空间。

1　完整性度量模型

根据TCG规范对"可信传递"的描述,如果系统启动时的初始状态是可信的,那么在其它任意时刻,只要确保主体所执行代码的完整性没有被破坏即代码完整性特征值与预期完整性度量值相同,就可保证主体所执行代码的安全,从而确保整个系统的完整性。恶意代码破坏系统的完整性须同时具备两个条件:

1) 获得执行机会;

2) 触发了恶意代码的进程具有对其他客体的"写"权限。

现有完整性安全策略主要基于Biba[3]模型或其他各种改进模型[4-11]制定,此类完整性安全策略的实质是把系统划分为不同完整性级别的安全域,防止信息从低完整性级别的安全域流向高完整性级别的安全域,在限制第2个条件方面做了大量的工作,而对第一个条件则很少涉及。作者提出的完整性度量模型针对恶意代码破坏系统的完整性的第一个条件,从访问控制角度,对执行权限进行了严格的定义和描述,把客体的可执行权限以及相关的输入数据作为研究对象,提取客体(还包括相关输入数据,如:脚本文件和相关配置文件)的摘要等作为扩展安全属性,对可执行客体的可执行权限进行严格的定义和描述,度量可执行客体的完整性,防止恶意代码被执行,保护系统的完整性。

1.1　模型定义

定义1　主体(Subject)是一个可以对其它实体施加动作的主动实体。主体可以是用户或其它任何代理用户行为的实体。客体(Object)是一个接受其它实体动作的被动实体,客体可以是一个可识别的资源。一个客体可以包含另外一个客体,需要注意的是,一个实体可以在某一时刻是主体,而在另一时刻是客体,这取决于某一实体的功能是动作执行者还是被执行者。

定义2　系统中被完整性度量的客体构成集合O_p,O_p中所有客体的预期完整性度量值构成集合P,$P=\{p_{o_1},p_{o_2},\cdots,p_{o_i},\cdots,p_{o_n}\mid o_i\in O_p\}$。

定义3　集合$A=\{r,w,e\}$为访问属性集,其中,r为自读方式,w为可读且可写方式,e为执行方式。对$x\in A$,以$rq(s,o,x)$表示主体s对客体o的x访问请求。$O^x_{s_i}$为主体$s_i\in S$,以$x(x\in A)$能访问的客体的集合。

定义4　$\forall o\in O$,$info(o)$表示客体o代表的相关信息。如果$\forall o_1,o_2\in O$,$info(o_1)\neq info(o_2)\Leftrightarrow f_h(o_1)\neq f_h(o_2)$,则称$f_h$为客体特征函数。

定义5　$b\subseteq(S\times O\times A)$表示在某个特定的状态下,哪些主体以何种访问属性访问哪些客体。M为访问矩阵,其中,元素M_{ij}为主体s_i对客体o_j具有的访问权限。

定义6　客体所有的特征值构成集合C,在任一时刻,k客体所有的特征值为C_k,$C_k=\{c_{o,k}=f_h(o)\mid\forall o\in O\}$。

定义7　在任一时刻k,$\forall o_j\in O$,其特征值为$c_{o_j,k}$,$L=\{\text{unmodified},\text{modified},\text{nofound}\}$,$f_c:O\rightarrow L$,$\forall o_j\in O$,$c_{o_j,k}\in C_k$,$p_{o_j}\in P$。

$$f_c(o)=\begin{cases}\text{unmodified iff } c_{o_j,k}=p_{o_j}\wedge o_j\in O_p\\ \text{modified iff } c_{o_j,k}\neq p_{o_j}\wedge o_j\in O_p\\ \text{nofound iff } o_j\notin O_p\end{cases}$$

称f_c为完整性度量函数。

1.2　模型的几个重要公理

1.2.1　恶意代码的作用范围

恶意代码的危害主要表现为对信息系统完整性进行破坏,根据前文对恶意代码作用机制的分析,可以得到以下公理。

公理1　$s_i\in S$,o_i为一带有恶意代码的客体,$o_i\in O$,if请求$rq(s_i,o_i,e)$被允许,则系统被恶意代码入侵。

公理2　带有恶意代码的客体$o_i\in O$被运行一次,系统的破坏范围是$O^w_{s_i}$,系统的机密性破坏范围是$O^r_{s_i}$。

1.2.2　安全公理

为了解释什么样的状态是一个安全状态,什么

样的系统是一个安全系统,模型定义了一组安全公理。

安全公理1 一个系统状态 v 为安全状态,iff $b(S:e) \subseteq O_p$,且 $\forall o_i \in b(S:e), o_k \in f_r(o_i)$ 使得 $f_c(o_k)$ = unmodified。其中,$b(s:x_1,x_2,\cdots,x_n)$ 为 b 中主体 S 对其具有访问权限 x_i 的所有客体的集合。态序列 Z 为一个安全状态序列,iff 对于每一个 $t \in T, z \in Z$ 都是安全状态。

通常情况下,可执行客体的运行还需要其它的相关客体,如需要装载的动态库、读取配置文件/安全策略文件等。如果这些相关客体的完整性被破坏,就不可能保证主体所执行代码的安全,更不可能确保整个系统的完整性,如个人防火墙的安全策略由"高安全性"被非法修改为"低安全性",这虽然也没有破坏可执行客体的完整性,但是却使个人防火墙对终端的防护能力降低,给系统带来极大的安全隐患。基于上述思想,模型在对可执行客体实施完整性度量时,对其相关客体也必须度量其完整性。

定义8 f_r 为定义在 O 上的函数,$o \in O, f_r(o)$ = {o,和 o 相关的其它客体},如:$f_r(o)$ 由"可执行的客体 o"及"执行 o 时需要装载的动态库、配置文件、安全策略文件等客体"组成。

安全公理2 一个系统状态 v 为安全状态,iff $b(S:e) \subseteq O_p$,且 $\forall o_i \in b(S:e)$, $\forall o_k \in f_r(o_i)$ 使得 $f_c(o_k)$ = unmodified。其中,$b(s:x_1,x_2,\cdots,x_n)$ 表示 b 中主体 S 对其具有访问权限 x_i 的所有客体的集合。态序列 Z 是一个安全状态序列,iff 对于每一个 $t \in T, z \in Z$ 都是安全状态。

1.3 完整性度量规则

根据前文所描述的安全公理,可以得到以下完整性度量规则:

定义9 RA 代表请求元素集合。RA = {g,r},其中,g 为请求,r 为撤除。

定义10 R 为请求集 $R = \bigcup_{i=1}^{3} R^i$。其中,$R^1 = RA \times S \times O \times A$ 为请求执行规则。$R^2 = RA \times S \times O_p$ 为请求产生一个新的完整性保护客体,$R^3 = S \times O_p$ 请求删除一个完整性保护客体。

定义11 N = {true,false},$h: O \rightarrow N$,对任意的 $o \in O$,$h(o)$ = true 当且仅当 h 能够证明客体 o 的完整性没有被破坏,称 $h(o)$ 为完整性验证函数。如 $h(o)$ 通过数字签名对 o 的完整性进行验证。

规则1 主体请求对客体"执行"访问。

定义域: $R_k = (g,s_i,o_j,e) \in R^1$

规则:

$$R^1(R_k,v) = \begin{cases} (\text{yes},v) \text{ if } f_c(o_j) = \text{unmodified} \wedge e \in M_{ij} \\ (\text{no},v) \text{ otherwise} \end{cases}$$

规则解释:当完整性度量函数 f_c 检测到客体 o_j 完整性没有被破坏且主体 s_i 的访问属性中有对客体 o_j 的"执行"权限时,主体 s_i 对客体 o_j 进行"执行"访问。

规则2 主体请求增加对客体进行完整性保护。

定义域: $R_k = (g,s_i,o_j,O_p) \in R^2$

规则:

$$R^2(R_k,v) = \begin{cases} (\text{yes},(b,M,f,P \cup \{p_{o_j}\})) \text{ if } s_i \in S_T \wedge h(o_j) = \text{true} \\ (\text{no},v) \text{ otherwise} \end{cases}$$

规则解释:可信主体 s_i 利用完整性验证函数 $h(o)$ 验证客体 o_j 完整性没有被破坏,则把客体 o_j 的预期完整性度量值 p_{o_j} 加入到 P 中,增加对客体 o_j 完整性保护。

规则3 主体请求撤销对客体进行完整性保护。

定义域: $R_k = (g,s_i,o_j,O_p) \in R^3$

规则:

$$R^3(R_k,v) = \begin{cases} (\text{yes},(b,M,f,P^*)) \text{ if } s_i \in S_T \\ (\text{no},v) \text{ otherwise} \end{cases}$$

其中,$P = P^* \cup \{p_{o_j}\}$。

规则解释:只有可信主体 s_i 才能把客体 o_j 的预期完整性度量值 p_{o_j} 从 P 中删除,撤销对客体 o_j 完整性保护。

根据安全公理的描述,不难得到这样的结论:如果一个系统初始安全状态是安全的,即系统中不包含恶意代码,所有可执行代码的完整性都没有被破坏,那么在其它任意时刻,只要确保主体所执行代码的完整性没有被破坏即代码完整性特征值与预期完整性度量值相同,就可保证主体所执行代码的安全,从而确保整个系统的完整性没有被破坏。完整性度量规则给出了具体的操作方法,把预期完整性度量值作为一个执行白名单,在系统运行时,仅当可执行程序是这个白名单的成员且保持完整性才被允许执行,只有拥有特权的可信主体才能增加或减少这个白名单的成员。

2 小 结

根据 TCG 规范对"可信传递"的描述,如果系统启动时的初始状态是可信的,那么在其它任意时刻,只要确保主体所执行代码的完整性没有被破坏即代

码完整性特征值与预期完整性度量值相同,就可保证主体所执行代码的安全,从而确保整个系统的完整性。针对当前安全模型对可执行权限没有专门的定义和描述,对可执行客体没有在运行前进行完整性检测,提出一种完整性度量模型,对可执行客体的可执行权限进行严格的定义和描述,度量可执行客体的完整性,防止恶意代码被执行,保护系统的完整性。该完整性度量模型扩展了当前安全模型的安全属性,它与其它安全模型的结合将能给系统提供更加细致和完善的安全策略。TCG 采用度量组件完整性来描述其是否可信的方法还比较片面,如何全面的描述一个系统的可信,这是作者下一步重点研究的问题。

参考文献:

[1] Trusted computing group. Trusted platform module main specification Version 1.2[S]. 2005.

[2] Sailer R, Zhang X, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture [C]//Proceedings of the 13th Usenix Security Symposium. California: Usenix, 2004:223 - 238.

[3] biba K J. Integrity considerations for secure computer systems[R]. ESD-TR-76-372, Bedford, MA: USAF Electronic Systems Division, Hanscom Air Force Base, 1977.

[4] Oppliger R, Rytz R. Does trusted computing remedy computer security problem[J]. Security & Privacy Magazine (IEEE), 2005, 3(2):16 - 19.

[5] Felten E W. Understanding trusted computing: Will its benefits outweigh its drawbacks[J]. Security & Privacy Magazine(IEEE), 2003,1(3):60 - 62.

[6] Iliev A, Smith S W. Protecting client privacy with trusted computing at the server[J]. Security & Privacy Magazine (IEEE), 2005, 3(2):20 - 28.

[7] Zhao Qinsong. Research on and enforcement of malware-defending technology of secure operating systems[D]. Institute of Software, Chinese Academy of Sciences, Beijing, 2003. [赵庆松,安全操作系统的恶意代码防御技术的研究与实施[D]. 北京:中国科学院软件研究所,2003.]

[8] Shen Changxiang. Trusted computing platform and secure operating systems [J]. Network Security Technology & Application, 2005(04):8 - 9. [沈昌祥. 可信计算平台与安全操作系统[J]. 网络安全技术与应用,2005(04):8 - 9.]

[9] Luo Wanbo, Luo Xiaolan, Chen Wei, et al. Study on the security policy management framework in multi-domain environment[J]. Journal of Sichuan University: Engineering Science Edition,2006,38(2):114 - 117. [罗万伯,罗霄岚,陈炜,等. 多域环境的安全策略管理框架研究[J]. 四川大学学报:工程科学版,2006,38(2):114 - 117.]

[10] Wang Fei, Liu Weipeng, Shen Changxiang. Research of trust transfer of applications model [J]. Computer Engineering and Applications, 2007,43(29):1 - 3. [王飞,刘威鹏,沈昌祥. 应用可信传递模型研究[J]. 计算机工程与应用,2007,43(29):1 - 3]

[11] Zhang Xiaofei, Xu Fang, Shen Changxiang. Research on multilevel security model based on trustworthy state and its application[J]. Acta Electronica Sinica, 2007, 35(8): 1511 - 1515. [张晓菲,许访,沈昌祥. 基于可信状态的多级安全模型及其应用研究[J]. 电子学报,2007,35(8):1511 - 1515.]

(编辑　杨　蓓)

可信计算中完整性度量模型研究

作者： 李焕洲， 林宏刚， 张健， 郭东军， LI Huan-zhou， LIN Hong-gang， ZHANG Jian， GUO Dong-jun

作者单位： 李焕洲,LI Huan-zhou(四川师范大学,网络与通信技术研究所,四川,成都,610068)， 林宏刚,LIN Hong-gang(成都信息工程学院,网络工程系,四川,成都,610225)， 张健,郭东军,ZHANG Jian,GUO Dong-jun(四川大学,电子信息学院,四川,成都,610064)

刊名： 四川大学学报（工程科学版） ISTIC EI PKU

英文刊名： JOURNAL OF SICHUAN UNIVERSITY(ENGINEERING SCIENCE EDITION)

年，卷(期)： 2008，40(6)

引用次数： 0次

参考文献(11条)

1. Trusted computing group Trusted platform module main specification Version 1.2 2005

2. Sailer R. Zhang X. Jaeger T Design and implementation of a TCG-based integrity measurement architecture 2004

3. biba K J Integrity considerations for secure computer systems[ESD-TR-76-372] 1977

4. Oppliger R. Rytz R Does trusted computing remedy computer security problem 2005(2)

5. Felten E W Understanding trusted computing:Will its benefits outweigh its drawbacks 2003(3)

6. Iliev A. Smith S W Protecting client privacy with trusted computing at the server 2005(2)

7. 赵庆松 安全操作系统的恶意代码防御技术的研究与实施[学位论文] 2003

8. 沈昌祥 可信计算平台与安全操作系统[期刊论文]-网络安全技术与应用 2005(4)

9. 罗万伯. 罗霄岚. 陈炜. 李征. 魏雁平 多域环境的安全策略管理框架研究[期刊论文]-四川大学学报（工程科学版） 2006(2)

10. 王飞. 刘威鹏. 沈昌祥 应用可信传递模型研究[期刊论文]-计算机工程与应用 2007(29)

11. 张晓菲. 许访. 沈昌祥 基于可信状态的多级安全模型及其应用研究[期刊论文]-电子学报 2007(8)

相似文献(10条)

1. 期刊论文 陈麟. 林宏刚. 黄元飞. CHEN Lin. LIN Hong-gang. HUANG Yuan-fei 基于可信计算的恶意代码防御机制研究 -计算机应用研究2008,25(12)

根据TCG规范中可信传递的思想,提出一种恶意代码防御机制,对被执行的客体实施完整性度量以防止恶意代码的传播;对客体的执行权限严格进行控制,防止恶意代码的执行,降低恶意代码的传播速度并限制其破坏范围,确保系统的完整性不被破坏.利用可信计算技术设计并实现恶意代码防御机制.

2. 期刊论文 谭良. 徐志伟. TAN Liang. XU Zhi-wei 基于可信计算平台的信任链传递研究进展 -计算机科学 2008,35(10)

信任链传递问题是可信计算的基本问题.阐述了信任链传递在技术与理论方面的最新研究进展.通过分析信任链传递的技术方案、可信测量技术、信任链理论和信任链的可信度度量理论,提出了值得研究的理论与技术方向,包括:以可信静态测量、可信动态测量技术等为代表的信任链传递关键技术,以信任链层次理论模型、信任链传递中的信任损失度量理论和软件的动态可信度度量理论等为代表的基础理论.

3. 期刊论文 王世华. 李晓勇. WANG Shi-hua. LI Xiao-yong 基于策略的计算平台可信证明 -电子学报2009,37(4)

计算平台状态可信证明是可信计算研究的热点问题.基于系统策略的计算平台状态可信证明模型(Policy Based Trustworthiness Attestation Model,PBTAM)可以解决目前计算平台可信证明方法中存在的平台隐私保护等重要问题.PBTAM认为计算平台的状态是否可信与其系统可信传递策略紧密相关,如果证明平台的系统可信传递策略符合质询方的期望,那么该证明平台对于质询方是可信的.PBTAM在可信计算平台技术规范基础上,通过对证明平台的系统可信传递策略进行度量和验证,实现计算平台的可信证明.本文在对实际生产系统应用安装状态采样、统计和分析的基础之上,对PBTAM的性能进行了总结,证明了该模型的实际可行性和有效性.

4. 期刊论文 李晓勇. 沈昌祥. Li Xiaoyong. Shen Changxiang 一个动态可信应用传递模型的研究 -华中科技大学学报（自然科学版）2005,33(z1)

由于终端平台上的应用具有多样性和无序性等特点,系统可信引导的单一链式验证机制并不适用于操作系统到应用之间的可信传递.为此,提出一种动态可信应用传递模型(DATTM),在保持应用装载的灵活性基础上,着重考虑了应用之间的权限隔离问题,最大程度地实现最小特权和按需即知等安全基本原则,进一步改善了系统度量和策略执行的效率和安全问题.

5. 学位论文 赵佳 可信认证关键技术研究 2008

从信息系统安全的角度出发，要考虑应用操作、共享服务和通信三个环节。在“三纵三横两个中心”的信息安全保障技术框架中，认证机制是保障信息系统能以安全、有效的方式被访问的前提。本文将可信计算技术引入到认证领域，建立了终端平台自身的可信认证，平台与平台之间的可信认证机

制，并在此基础上对用户与可信平台之间的身份认证和可信平台与密码管理中心的密钥管理方案以及相关技术展开研究，主要贡献体现在以下几个方面：　　(1)利用可信平台模块TPM(或可信密码模块TCM)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，但是，有关可信计算理论模型方面的研究目前较多的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。这些模型都侧重于社会学中的信任关系，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。本文遵循可信计算组织TCG规范中对可信根和可信传递的定义，应用无干扰理论，从动态的角度，提出了计算机系统可信传递的理论，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。　　(2)在信息系统中，终端平台需要向外部实体证明自己，完成网络通信中的身份认证。目前的证明方法一个明显的不足之处是暴露了本地平台(包括硬件和软件)的配置信息，这在一定程度上给攻击者提供了方便，使之更容易遭受各种攻击。本文提出的可信计算远程自动匿名证明方案以属性证书代替平台配置信息，不仅可以有效防止隐私性的暴露，而且为系统升级和备份过程的可信检测提供了很好的思路；利用环签名实现直接匿名证明，避免了可信计算平台与可信第三方的协商过程，在提高执行效率的同时，也增强了安全性；基于可信计算模块及其宿主联合签署的隐藏属性证书实现远程自动匿名证明，不需要额外的零知识证明，实现效率较高。　　(3)安全信息系统要防止由内部泄漏机密信息。加密机制是防止机密信息泄露的有效手段，其中的密钥管理又是加密中的重要环节，无论加密强度多高，密钥的泄露将导致信息系统全盘崩溃。本文采用秘密共享方案管理密钥，基于XTR公钥体制，提出了一种同时间特性绑定的动态秘密共享方案。该方案在同等的安全强度下，将有限域上的求幂运算时间降为原来的三分之一；每个参与者在有效期之外不能参与共享秘密；参与者更新秘密份额时不需要秘密分发者的参与：秘密份额更新过程简单且具有前向安全性；每个参与者只需要维护一个秘密份额就可以实现多重秘密共享。　　(4)对用户与终端平台之间的认证，提出了XTR公钥密码体制下基于身份的数字签名方案。这种方案不需要计算双线性对，在相同的安全强度下，XTR的密钥比RSA的密钥短得多，在参数的选取速度上与RSA相当，比ECC则要快几个数量级。所以本文中提出的签名方案的时间复杂度和空间复杂度都较低。此外，还对签名算法作出了改进，给出了一种基于身份特征的盲签名方案。　　(5)最后基于终端平台实现了可信认证机制原型系统，在Linux 2.6内核下实现了终端可信启动，并且基于Linux操作系统的PAM模块实现了用户认证。根据系统的实际安全需求、安全威胁和安全假设进行配置，对用户采用了双因子USB-Key认证的方式，由USB-Key管理中心统一进行管理。在可信认证机制的原型系统中，用户分为几种不同的角色，根据强制访问控制的要求，建立了二维标识的强制访问控制模型，使得既能防止越权泄露信息，又能控制信息的非授权修改。　　综上所述，本文讨论了信息系统中的可信认证关键技术，对平台自身的可信认证和平台之间的可信认证，以及用户与平台之间的认证及相关技术进行了研究，建立了终端可信认证的原型系统，为高安全等级信息系统可信机制的设计和实现提供了一些新的途径。

6.期刊论文 王飞.刘威鹏.沈昌祥.WANG Fei.LIU Wei-peng.SHEN Chang-xiang 应用可信传递模型研究 -计算机工程与应用2007,43(29)

应用、服务等操作是终端用户日常工作的基础,如何保证它们能够是安全、可信的行为,是当前信息安全研究的一个热点和难点.文章利用可信计算的观点建立终端的应用可信传递模型,能够保证信任在应用环境中的传递.该模型能够不依赖于对病毒特征的检测,彻底地防止恶意代码在应用环境中的感染和传播,从根本上保障应用、服务的可信,保障终端应用环境的可信.

7.学位论文 林宏刚 可信网络连接若干关键技术的研究 2006

当前大部分信息安全系统主要是由防火墙、入侵监测等组成，针对是共享信息资源为中心在外围对非法用户和越权访问进行封堵，以防止外部攻击，而对共享源的访问者源端不加控制，加之操作系统的不安全因素导致系统的各种漏洞，无法从根本上解决安全问题。产生这种局面的主要原因是没有从终端源头对安全问题进行控制，而仅在外围进行封堵，信息安全系统只以接入终端是否通过认证和授权来判断接入终端是否可以接入受保护的网络，而不关心接入终端本身是否安全可信。　　早在上世纪九十年代初，国内著名的信息安全专家沈昌祥院士就提出要从终端入手解决信息安全问题，这是对安全问题的本质回归。近年来，“可信计算”的兴起正是对这一思想的认可。可信计算组织(TCG)制定的可信网络连接(TNC)规范，采用了标准的接口定义了一个公开的标准，将传统的网络安全技术和“可信计算”技术结合，把可信硬件TPM集成到可信网络连接体系结构中，从终端入手构建可信网络，将不信任的访问操作控制在源端。目前可信网络连接的研究虽然取得了重要的成果，这些成果对信息系统安全的发展发挥了重要的作用，但是由于可信网络连接的研究与实践仍处于发展阶段，还存在研究仍停留在工程技术层面、缺乏理论模型支撑，体系结构不完整等问题。本文紧跟可信计算研究趋势，针对可信网络连接发展中所存在的主要问题展开研究。　　论文首先研究了TNC体系结构的基本思想。TNC体系结构立足于终端，对每个试图连接到网络的终端，在待接入终端通过认证和授权的基础上，还检查终端的当前的完整性及其他安全属性是否与组织定义的安全策略一致，从而提供对网络环境更完善的保护。根据组织安全策略，可信的终端将获得访问网络资源的权限，不可信的终端被隔离，有漏洞的终端被补救，更新其组件和配置，确保任何访问网络的终端具有符合组织安全策略的、最新的、恰当的安全配置。　　接着，论文分析了TCG制定的规范中只对可信硬件和系统引导进行了的定义和描述，指出这种方法不适应对应用程序实施完整性度量。研究了恶意代码破坏系统完整性的作用原理和本质，根据TCG规范中可信传递概念，本文提出一种系统完整性度量模型，对客体的执行权限严格的定义和描述，对被执行的客体及其相关其它输入数据实施完整性度量，防止恶意代码的执行，确保系统的完整性不被破坏。并结合模型，利用可信计算技术实现了一个实时的系统完整性度量服务，用于对系统中的应用程序完整性度量，基于该方法把信任链从操作系统延伸到应用。根据“可信传递”的思想，基于TPM提供的可信报告和可信度量机制，提出了远程证明的基本思想。计算机系统可以以TPM为信任根，通过信任传递，将信任延伸到网络。在建立网络连接时，网络中的实体不仅要求对其鉴别身份，证明它们被授权允许访问网络，而且要求通过远程证明机制验证它们运行环境和程序是否可信，使信任在网络环境下传递，把信任链扩展到网络，确保整个网络的可信性。由于可信网络连接规范中只是对远程证明机制的一般功能做了初步的定义，至于如何实现这一功能，则没有进一步研究，本文对TCG规范中描述的远程证明机制中的可信报告传输、可信度量验证和根据可信报告评估系统可信度等问题进行深入系统的研究。为了确保在可信报告在传输过程中的安全，提出一种远程证明传输协议，以保证通信双方身份的真实性、通信数据的机密性、完整性和消息的新鲜性等特性，并对其安全性进行形式化证明；给出了一种验证可信度量和评估待证明系统可信度的方法，该方法分为两步：首先粗粒度判定，质询方根据可信度量验证规则验证可信度量信息,判定待证明系统是否可信，对于判定为不可信的系统，采取隔离措施，拒绝与其进行交互和向其提供服务；然后细粒度判定，对于判定为可信的系统，质询方用可信度衡量待证明系统值得信任的程度，基于层次分析法对终端可信度评估，以值的方式量化表示，从而可以根据该平台的可信级别来实施能够在该级别下实施的操作。　　为确保应用环境的安全可信，对在访问过程中的终端的访问行为实施控制，提出了一种基于可信度的动态访问控制模型，把RBAC模型无缝的集成到TNC体系结构中。在模型中，把可信计算与访问控制有机的结合，将远程证明机制评估终端用户的可信度作为系统在进行用户角色指派时的依据，在RBAC模型中引入了可信度的概念，对传统RBAC模型进行扩展，把用户的可信度作为授权的一个组成部分，直接参与安全决策，并对其进行形式化描述和分析。该模型在区分不同用户可信度的基础上，让用户的可信度参与授权，只有可信度较高的用户才授予较高权限；如果非法用户没有通过远程证明机制的可信度评估，即使他进入系统获得了管理员身份也不能获取管理员的权限。在用户访问过程中，根据用户在系统中完成任务的情况对用户可信度动态调节。模型不仅细化了TNC体系结构中的访问控制粒度，并且在增强系统灵活性的基础上，提供系统安全性。　　最后，在对可信网络连接研究的基础上，结合前面章节研究成果，把可信网络连接理论应用在远程客户端访问企业网络构建的VPN系统中，构建企业可信应用环境。　　论文紧密围绕可信网络连接体系结构的研究开展工作，文中提出的模型和方法，对可信网络连接的研究和实践及信息安全的理论研究将有积极的意义。

8.期刊论文 王丽芳.李旭 可信在网络安全中的应用研究 -移动通信2009,33(8)

文章以可信计算平台为基础,借鉴TCG的可信网络连接技术规范,将活性标签、安全隔离、不对等访问控制、自适应的应用代理技术,应用到安全组网的设计方案中,初步设计出可信网络模型,以实现将终端建立的可信传递到网络,建立用户、平台与网络三者之间的信任关系,以及不同安全等级终端或网络区域之间的可信互连.

9.学位论文 戴月 Windows系统的可信引导 2007

传统网络安全系统，主要以防火墙、入侵监测和病毒防范为主，在防外上有一定的效果，但在保护整个系统上却并非固若金汤。这是因为它不适应目前信息安全主要“威胁”源自内部的状况。而要解决内部安全威胁，就需要建立一个信息的可信传递模式。　　可信传递过程：在计算平台的运行控制传递过程中，可信根确定其下一级执行代码的真实性和完整性是否被篡改，如果没有，系统将运行控制权传递到下一级可信执行代码，系统的可信范围就从可信根扩大到下一级；同理，这种系统运行代码控制权不断往下传递，从而实现系统可信范围的延伸。　　本文主要关注可信传递过程中的可信引导部分，并以Windows平台和NTFS文件系统为试验环境，研究了Windows环境下可信引导的实现方案。　　Windows系统下的可信引导过程：系统加电自检后进入OS静态验证模块，分别验证MBR，操作系统加载程序和操作系统内核静态部分，如果通过验证，将控制权交给MBR，进入正常引导过程，否则显示出错信息进入可信恢复。　　Windows系统下的可信引导过程主要是对操作系统各类文件进行完整性校验。而可信引导发生在文件系统加载之前，因此引导过程的大量工作是定位解析NTFS文件。本文的重点工作是实现了在NTFS文件系统加载前，对NTFS文件的解析定位。　　Windows可信引

导工作流程中，大部分功能模块都涉及到对控制权的转移并且要求准确定位结束位置，且由于代码需要加载到内存的绝对位置。为了更好并准确的控制程序流程和结束位置，相关代码由汇编语言完成。

10.学位论文 方艳湘 基于虚拟机监视器的可信计算平台研究 2006

TCG从行为可预测性的角度给出实体可信的定义，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”。TCG规范通过可信根、可信传递、可信度量、可信报告等手段的实施达到系统可信的目的。　　目前可信终端的研究仍停留在工程技术层面，缺乏理论模型支撑。TCG提出的可信计算平台规范定义了终端需要提供的可信计算功能。但是如何实现这些功能，仍然需要在构建理论模型，摸清机理的基础上，进行详细的研究。　　可信终端体系结构研究还不成熟。目前对可信终端体系结构的研究主要集中在对主流操作系统的改进上。由于主流操作系统在设计时不是以可信计算为目标，难以从根本上满足可信计算的需要。因此，仅仅通过对主流操作系统改造来满足可信计算的要求是难以实现的。　　本文紧紧围绕上述两个问题展开研究。在对可信计算目标进行形式化分析的基础上，提出了一个基于隔离主域的可信终端模型。在该模型的指导下，设计了一个基于虚拟机监视器的可信计算平台，并且对平台实现的关键技术展开了研究与实践工作。主要包括以下3个方面的成果：　　(1)针对可信计算对强隔离性的需要，提出了一个基于隔离主域的内核模型。并对模型如何应用于实际系统进行了分析，论证了虚拟机体系结构是最理想的实现方式。在此基础上，设计了一个基于虚拟机监视器的可信计算平台体系结构。该结构秉承了虚拟机监视器强大的隔离性、良好的应用兼容性等优点。　　(2)分析了过程完整性及其存在的问题，论述了验证操作系统启动过程完整性的重要性，设计并实现了客户Linux系统的可信启动过程。通过可信启动过程验证虚拟机系统客户Linux系统的内核启动到登陆界面出现之前的过程完整性，确保这一阶段可信链被正确传递，为随后的应用提供一个可信的运行环境。
(3)分析了基于Windows平台的可信度量中的需求和技术难点，设计并实现了一种基于Windows终端的可信度量系统。该度量系统通过在终端系统上运用静态数据度量结合动态环境完整性保护的方式来确保系统的完整和可信。文章最后分析了该度量系统带来的安全增强作用及其对终端平台的性能影响。