基于可信计算平台的静态客体可信验证系统的设计与实现*)

谭 良[1,2] 周明天[2]

(四川师范大学四川省软件重点实验室 成都 610066)[1]

(电子科技大学计算机科学与工程学院 成都 610054)[2]

摘 要 在安全操作系统中,通常采用了多种访问控制模型来保证静态客体的内容的机密性和完整性。但是,传统的访问控制政策不能保证静态客体内容的真实性。因此,安全操作系统中的客体并不可信。本文首先分析了操作系统中客体的类型,总结了安全操作系统中对静态客体的处理存在的问题,提出可信静态客体的概念并分析其特点。为了保证可信静态客体内容的真实性,提出了基于TPM的静态客体可信验证系统。该系统将生成可信静态客体的映像文件,映像文件记录某可信静态客体的来源、各次处理行为和内容变化的签名并存于TPM中。最后对该可信验证系统进行了安全和性能分析。分析表明,该可信验证系统可以保证可信静态客体内容的真实性,为进一步建立可信计算环境提供了基础。

关键词 安全操作系统,客体,可信操作系统,可信静态客体,可信动态客体,可信客体,可信计算平台

Design and Implementation of the Trusted Authentication System for the Static Object Based on the TPM

TAN Liang[1,2] ZHOU Ming-Tian[2]

(School of Comp. Sci. & Engn., Univ. of Electronic Sci. & Tech. of China, Chengdu 610054)[1]

(College of Electronic Engineering, Sichuan Normal University, Chengdu 610066)[2]

Abstract Generally, the security operating system makes use of the multi-mixed access control policies to guarantee the confidentiality and integrity of the static object, but the traditional access control policies still have some deficiencies in accessing the object, and can't guarantee the authenticity of the object. So the object in the security operating system isn't trustworthy. In this paper, the object types in the operating system, which are sorted into the static object and the dynamic object, are analyzed, and some problems for accessing the object in the security operating system are pointed out. Based on that, the conception of the trusted static object, the trusted dynamic object and the trusted object is put forward, and the characters of the trusted object, the relationship between the secure object and the trusted object are addressed. Finally, some requirements for the trusted object, which need to be resolve in the trusted operating system, are presented and discussed. All of these are the foundation for our future works.

Keywords Security operating system, Object, Trusted operating system, Trusted static object, Trusted dynamic object, Trusted object, TPM

1 引言

在浩瀚的网络中,蕴涵着无穷的信息。在今天的互联网上,围绕着客体的内容正在形成一个价值链,内容的创建、管理、访问等这一切共同构造了互联网中的数字财富、数字价值,数字内容的平台和协议、权限的管理、认证、数据等一切东西紧密结合在一起,形成数字内容的相关服务。另外,交互电视、数字动画、网络游戏等新的内容形式还在层出不穷。特别是网络游戏在中国更是突飞猛进,营业额预计2006年达到83.4亿元人民币。网络游戏还带动传统业务如媒体出版、IT产业、通信业务收入的增长,并带来经济总量的成长,成为技术推动型的数字内容产业的重要组成部分。围绕数字内容形成的产业,包括通信网络、各种媒体、计算机、软件技术等,正在形成一个庞大的市场,而在市场与商业的驱动下,数字内容已进入一个迅速发展的阶段。

操作系统是数字内容管理的基础软件系统。在安全操作系统中,数字内容作为一般静态客体被保护和管理。为了保证静态客体内容的机密性和完整性,安全操作系统采用多种安全模型和控制框架对内容的访问实施控制,并在访问控制框架和安全模型方面均取得了丰硕的成果。在访问控制框架方面有:基于政策描述语言的FAM(Flexible Authorization Manager)[1]和企业间多协调框架[2]、基于安全属性的GFAC框架[3]、基于统一模型的数据库FMP[4]、RBAC[5]和Flask[6]框架。在安全模型方面,最重要和最知名的安全模型包括:BLP[7]、HRU[8]、BIBA[9]、Lattice Model of Information Flow[10]、Chinese Wall[11]、DTE[12]等等。但是,纵观安全操作系统将近40年的发展历史,可以发现安全操作系统的主要应用范围仍然是在国防和军事领域,在商用和民用领域尚未有成熟的安全操作系统出现。迄今为止,在国际上,安全操作系统的实际应用并不成功,在实际应用中发挥作用的操作系统绝大部分不是安全操作系统。究其本质,一方面,安全操作系统还存在不完善的地方;另一方面,随着数字内容相关服务

*)基金项目:国家863宽带VPN项目863-104-03-01课题资助;2003年度四川省科技攻关项目03GG007-007支持。谭 良 博士,主要研究方向为信息安全、中间件;周明天 教授,博士生导师,主要研究方向为网络计算、信息安全、分布并行处理。

的发展，要求不仅要保证静态客体内容的安全性，即机密性和完整性，而且要保证客体内容的可信性。另外，随着可信计算技术的兴起[13~19]，可信操作系统逐渐成为研究热点。操作系统的可信不是凭空而来的。可信性的建立不仅需要对操作系统自身和可能降低系统可信性的执行代码进行一致性度量，需要对用户登录进行可信验证，对登录的内部合法用户的行为进行监管，而且需要对操作系统中的客体内容的可信性进行检查和监督。否则，会影响用户对可信操作系统的信任。

本文首先分析了操作系统中客体的类型，总结了安全操作系统中对静态客体的处理存在的问题，提出可信静态客体的概念并分析其特点。为了保证可信静态客体内容的真实性，提出了基于 TPM 的静态客体可信验证系统。该系统将生成可信静态客体的映像文件，映像文件记录某可信静态客体的来源、各次处理行为和内容变化的签名并存于 TPM 中。最后对该可信验证系统进行了安全和性能分析。分析表明，该可信验证系统可以保证可信静态客体内容的真实性，为进一步建立可信计算环境提供了基础。

2 可信静态客体

2.1 客体的分类

在操作系统中，存在着许多客体，如文件、目录、共享内存、消息、信号量、管道、存储器、缓冲器、磁盘和外部设备等。在安全操作系统中，为了不同安全政策的实施，可以对这些客体进行不同的分类。例如，在 OSR 模型[20]中，将除用户外的所有客体划分为五个种类：进程、文件目录、进程间通信、设备和系统控制数据。“系统控制数据”包括系统时钟、主机名和域名等在整个系统范围内起作用的数据。“文件目录”表示系统中文件和目录的集合。因此，为了便于研究客体的可信性，我们将客体分为静态客体和动态客体。

定义 1 在逻辑上只能作为主体行为对象的客体称为静态客体。

分析定义 1 可知，静态客体只能作为主体行为的受体。一旦主体拥有权限，客体只能完全“接受”主题的行为，客体没有根据自身的实际情况与主体的访问进行协商的权利。当然，这类客体也不能验证主体的身份。显然，文件目录、设备和系统控制数据属于静态客体。

定义 2 将在逻辑上既可以作为主体的行为对象，也可以对其它客体或主体施以行为的客体，称为动态客体。

分析定义 2 可知，在逻辑上，动态客体不仅作为行为的受体，而且也可以对其它主体或客体施以行为。因此，动态客体既具有静态客体的特征，又具有一般主体的特征。

2.2 安全操作系统对静态客体的处理存在的缺陷

目前，设计和开发出来一系列的安全操作系统，典型的有 Multics、Mitre 安全核、UCLA 数据安全 Unix、KSOS 和 PSOS、LINUS IV、Xenix、System V/MLS、TUNIS、ASOS、DTOS(Distributed Trusted Operating System)、Flask7、SE-Linux8，以及国内的 SUNIX、COSIX V2.0、LIDS、SoftOS、SecLinux 等[20]。值得注意的是，大部分安全操作系统在处理客体时，没有区分具体的客体类型，将不同类行的客体采用同一方法标识和处理。在传统的访问控制技术条件下，部分主体在访问某类静态客体的时候需要验证客体的身份和完整性。例如，在 Windows 操作系统中，有许多动态链接库(DLL，Dynamic Link Library)。DLL 文件是 Windows 的基础，因为所有的 API 函数都是在 DLL 中实现。DLL 没有程序逻辑，由许多功能函数构成，它并不能独立运行，一般由进程加载并调用。当作为主体的进程调用某 DLL 文件中的功能函数时，如果主体不对该 DLL 文件进行身份认证和完整性检验，则黑客或攻击者可以采用如下两种方法实施攻击[22]：(1)用一个伪造的 DLL 文件替换原 DLL 文件；(2)伪造一个接口相同但包含恶意代码的功能函数供主体调用。该主体均不能辨别这两种情况。显然，传统的访问控制技术不能办到，因为传统的访问控制技术只能在授权条件下解决能不能访问的问题。

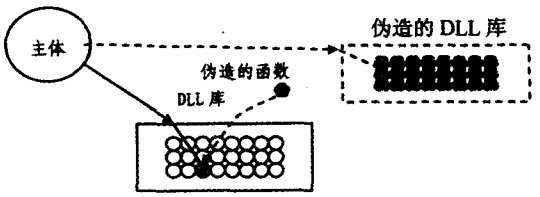


图 1 主体访问伪客体

2.3 可信静态客体的基本概念及其特点

定义 3 如果静态客体的内容是安全的、可信的，则该客体是可信静态客体。

分析定义 3 可知，可信静态客体具有如下特征：

- 内容机密性(confidentiality)：是指防止信息泄露给未授权的用户；
- 内容完整性(integrity)：是指防止未授权用户对客体内容的修改；
- 内容可信性(creditability)：客体内容的可信性研究的是客体内容的真实性(authenticity)。

与安全操作系统中静态客体的机密性和完整性相比，可信静态客体内容的机密性和完整性没有什么不同。不同的是，可信静态客体不仅强调客体内容的机密性和完整性，而且更强调客体内容的可信性，即真实性。在现实世界中，内容的真实性是通过内容与现实的一致性或言语的证据来考察的。内容真实性的考察是一项困难的工作，需要花费大量的人力和物力来进行调查研究或取证。但是，在计算机世界中，实现内容的真实性不能像现实世界一样去考察。对于内容监管来说，一个普遍有效和可以实施的方式是下面描述的方法[21]：

客体内容的真实性＝客体来源的真实性 ＋ 处理内容行为的可信性＋内容变化的可信性。简单地说，在计算机世界中，判断内容是否可信，首先判断信息来源是否可信。如果信息来源可信并真实，那么对信息进行处理的行为本身也必须是可信的；即使行为可信，也不一定表明内容进行增加、删减或修改一定是正确的。但是，如果行为监控充分细致，这种增加、删减和修改也是有可信来源的，包含在行为的输入条件中，那么便满足了内容变化的可信要求。

3 基于 TPM 的静态客体可信验证系统的设计与实现

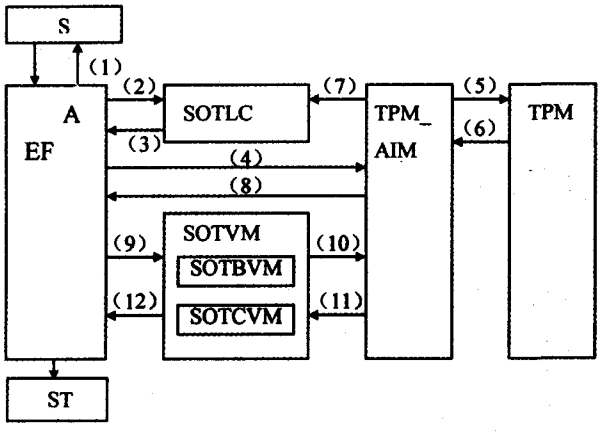
3.1 TPM 简介

TPM 是可信计算技术的核心，是一个含有密码运算部件和存储部件的小型片上系统。通过 LPC 总线与 PC 芯片集结合在一起，将重要的数据信号线或重要的存储区域严密保护起来，这样用人为的物理探头或一般的光探测技术就很难窥探到里面的数据。TPM 在封装时可用一信号探测的方式防拔除。如有人拔除，则会触动一根预先埋好的信号线，其上的信号将发生变化，从而激发一个硬中断，系统将直接跳到自毁灭中断处理程序中，从而将自己内部的数据全部销毁，整个系

统也就自动毁灭，无法复原。因此，TPM 是一个具有较强的密码计算能力和存储能力、完全可信的“信任根”。

3.2 基于 TPM 的静态客体可信验证系统的体系结构

基于 TPM 的静态客体可信验证系统(the Trusted Authentication System for the Staic Object Based on TPM：TASSOBT)将主体对静态客体的可信访问分为五部分：访问控制实施、静态可信客体标记缓冲区、静态客体可信验证模块、TPM 应用程序接口和 TPM。如图 2，用 AEF(Access-control Enforcement Facility)表示访问控制实施部分；用静态客体可信标记缓冲区(Static Object Trusted Label Coach：SOTLC)存储静态客体的可信标识；用静态客体可信验证模块(Static Object Trusted Verify Module：SOTVM)来验证对处理静态客体行为的可信性和静态客体内容变化的可信性，包括可信静态客体行为验证模块(Static Object Trusted Behavior Verify Module：SOTBVM)和可信静态客体行为验证模块(Static Object Trusted Content Verify Module：SOTCVM)；TPM 访问接口模块(TPM Access Interface Module：TPM_AIM)提供对 TPM 的访问接口，包括存储控制接口、密码运算接口等；TPM 用来存储可信静态客体的映像文件和提供密码运算。



(1)主体访问请求；(2)搜索 SOTLC；(3)返回 SOTLC 的结果；(4)请求 TPM_AIM；(5)搜索 TPM 中的静态客体的可信标识；(6)返回静态客体的可信标识；(7)将静态客体的可信标识存入 SOTLC；(8)将静态客体的可信标识返回给 AEF；(9)请求 SOTVM 模块；(10)SOTVM 请求 TPM_AIM 模块；(11)TPM_AIM 模块将处理结果返回 SOTVM 模块；(12)SOTVM 模块将处理结果返回给 AEF；(13)主体对客体施以操作。

3.3 基于 TPM 的静态客体可信验证系统的工作原理

3.3.1 对主体的要求

在操作系统中，主体要访问可信静态客体，它必须首先成为 TPM 的合法用户。主体在注册时，应将表 1 所示的用户身份信息、证书信息及私钥信息存放在 TPM 内部的 Flash 中，并防止非法用户对这类数据的读取。

表 1 用户信息表

用户名	用户 ID	证书	私钥
U_1	U_ID_1	C_1	PK_1
U_2	U_ID_2	C_2	PK_2
U_3	U_ID_3	C_3	PK_3

3.3.2 可信静态客体的可信标识

在安全操作系统中，在实现主体对客体的常用访问方法中，一种常用方法是访问控制列表(Access Control Lists)，又称为 ACLs。在这种实现方法中，每一个客体与一个 ACL 相对应：指明系统中的每一个主体获得对此客体访问的相应授权，如读、写、执行等等。为了识别可信静态客体，并启动静态客体可信验证系统对该客体进行验证，可以在 ACLs 中定义可信标识，使得原 ACL 项由一个三元组变成了一个四元组(*Type*，*ID*，*TC*，*Perm*)组成，分别描述如下：

- *Type*：用户或组的标志；用来表明此可信标识项是指定用户还是指定组的；
- *ID*：用户或组的 ID；用来表明此可信标识项所指定的用户或组的 ID 号；
- *TC*：可信标识；用来表明此可信标识项所指定的用户或组对此客体访问时是否需要可信验证系统的验证，如果 *TC*=1，表示需要；如果 *TC*=0，表示不需要；
- *Perm*：存取权限；用来表明此可信标识项所指定的用户或组的对此客体的访问权限。

3.3.3 可信静态客体的映像文件

可信静态客体的映像文件用来记录主体对客体访问证据，存储在 TPM 内部的 Flash 中，并防止非法用户对这类文件的读取。对于内容监管来说，可以利用 TPM 的密码运算功能和存储功能来保证静态客体的可信性。在静态客体的映像文件中，主要记录的内容应该满足：

- 可信静态客体属主的身份，创建该客体的时间。记录该内容的目的是为了验证客体来源的真实性；
- 当前主体的身份、对该客体的访问行为以及行为发生时间。记录该内容的目的是为了验证处理内容行为的可信性；
- 对变更过后的静态客体进行签名。记录该内容的目的是为了验证内容变化的可信性；
- 映像文件的签名。某个主体一旦完成对静态客体的所有行为后，应用属主的证书对该映像文件进行签名。记录该内容的目的是保证映像文件的完整性。

3.3.4 可信验证系统的工作流程

在 TPM 中注册成功的合法用户，在对可信静态客体进行访问时，需要进行可信验证，保证客体真实性。具体过如下：

(1)主体发出对客体的访问请求。

(2)根据访问控制列表和安全属性，判断主体是否可以访问客体：如果不能，则转到(9)；如果能，则转到下一步。

(3)从 SOTLC 中查询该静态客体可信标识。如果有，就跳转下一步；否则，通过 TPM_AIM 在 TPM 查询客体的可信标识。如果在 TPM 查找到该客体的可信标识，说明该客体是可信客体。将该客体的可信标识存入 SOTLC 中，并将该可信标识返回 AEF，转到下一步；否则，转到(9)。

(4)AEF 查找该客体的属主，用属主的证书验证该客体的身份和完整性。如果为真，则转移到下一步；如果为假，则转移到(9)。

(5)AEF 调用 SOTVM 模块，并通过 SOTVM 模块打开存储在 TPM 中该客体的映像文件：将主体的信息写入映像文件并对这些信息进行签名。

(6)主体访问客体。

(7)AEF 调用 SOTVM 模块，在映像文件记录主体对客体的行为，并对该行为记录进行签名。

(8)AEF 判断主体对客体访问是否结束。如果未结束，

(下转第 300 页)

当系统规模 P 不变，只增加问题规模 W，由于并行效率增长得比 W 慢，从而使得效率增加。因此，可以让 W 和 P 同步增加，以保持效率不变。结论符合适合于可扩放问题的 Gustafson 定律，说明本文给出的计算加速比、效率新方法是简捷有效的。

结束语 本文构建的 Beowulf-T 机群系统是由若干独立的微机和可扩展的星型结构以太网组成，上述实验从资源可扩展性方面表明该系统具有高可用性和高可扩展性。另一方面，机群环境下通讯技术问题、并行程序设计环境问题、负载平衡问题以及全局资源管理与使用等，将是我们下一步研究的内容。

参考文献

1 陈国良. 并行计算-结构. 算法. 编程 [M]. 北京：高等教育出版社，2004
2 李继民，马力，王凤先. PC 机群系统的关键技术[J]. 河北大学学报(自然科学版)，2002，22(1)
3 熊盛武，王鲁，杨婕. 构建高性能集群计算机系统的关键技术[J]. 微计算机信息，2006，22(1-3)
4 黄淑玲. 可扩展并行计算的应用与研究 [J]. 电脑知识与技术，2005. 12
5 黄铠，徐志伟. 可扩展并行计算-技术、结构与编程[M]. 北京：机械工业出版社，2000

(上接第 255 页)

转到(6)；否则，用该客体的属主证书对变更后的客体进行签名，然后进入下一步。

(9)访问结束。

4 安全和性能性分析

(1)自身的安全性。用户信息、密钥或特征码正这些在认证过程中需要的重要信息存储在 TPM 中，防止了非法用户读取敏感信息。

(2)可信验证系统既可以保证主体在访问可信静态客体的时候需要验证客体的身份和完整性，又可以保证客体内容的真实性，解决了安全操作系统对静态客体的处理存在的缺陷。

(3)系统的工作效率。鉴于丰富的计算资源和较高的传输速率，TASSOBT 的主要开销在于内部的计算时间以及与 TPM 的通信时间。选用 SLE66 型号的嵌入式安全模块作为 TPM(通信速率为 38.4k/s)实现 TASSOBT 的计算量和时间花销(包含通信和计算时间)。由于鉴别和签名过程在用 SLE66 型号的嵌入式安全芯片内部，具有较高的安全性，因此可选用速度较快的 HSAH 算法实现鉴别和签名。在 SLE66 型号的嵌入式安全芯片中，鉴别和签名产生的随机数长度均为 160B，HASH 算法选用 SHA. 1。另外，在 TASSOBT 过程中，由于传输的数据量少，通信开销小，通信时间可以忽略；而此过程中，SLE66 型号需要进行 4 次 HASH 运算。对于 SLE66 型号的嵌入式安全模块，一次 SHA. 1 运算化的时间大概是 200ms，所以 TASSOBT 过程所需要的时间开销约为 0.8s。

总结 随着可信计算技术的兴起，可信操作系统逐渐成为人们关注的焦点。在可信操作系统中如何保证静态客体可信成为了一个紧迫的重要课题。随着网络技术的不断发展和 Internet 的日益普及，人们对 Internet 的依赖也越来越强。人们在 Internet 浩瀚的信息海洋中，获取无穷无尽的知识的同时，也会获得一些无用或虚假的信息。随着内容服务的发展，静态客体内容可信的需要越来越强烈。本文首先分析了操作系统中客体的类型，总结了安全操作系统中对静态客体的处理存在的问题，提出可信静态客体的概念并分析其特点。为了保证可信静态客体内容的真实性，提出了基于 TPM 的静态客体可信验证系统。该系统将生成可信静态客体的映像文件，映像文件记录某可信静态客体的来源、各次处理行为和内容变化的签名并存于 TPM 中。为保证静态客体的可信提供了一种解决方案。我们的下一步工作是将 TASSOBT 在 Linux 系统上实现。

参考文献

1 Jajodia S, Samarati P, Subrahmanian V, et al. A unified framework for anforcing multiple access control policies. In: S IGMOD '97, Tucson, AZ, May 1997. 474～485
2 Galiasso P, Bremen O, Hale J, et al. Policy Mediation for Multienterprise Environments. ACSAC, 2000. 100～106
3 Abrams M, LaPadula L, Eggers K, et al. A Generalized Framework for Access Control: an Informal Description. In: Proceedings of the 13th National Computer Security Conference, Gct. 1990. 134～143
4 Bertino E, Jajodia S, Samarati P. Supporting Multiple Access Control Policies in Database Systems. In: IEEE Symposium on Security and Privacy, Oakland, 1996
5 Osborn S, Sandhu R, Munawer Q. Configuring Role-based Access Control to Enforce Mandatory and Discretionary Access Control Policies. ACM Transactions on Information and System Security, 2000, 3(2): 85～105
6 Secure Computing Corporation. DTOS Lessons Learned Report: [Technical Report]. DTOS CDRL A008. Secure Computing Corporation, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota, June 1997. 55113～2536
7 Bell D E, La Padula L J. Secure Computer Systems: A Mathematical Model. MTR 2547-II (AD 771 543). The MITRE Corporation, Bedford, Massachusetts, May 1973
8 Harrison M H, Ruzzo W L, Unman J D. Protection in operating systems. Communications of the ACM, 1976, 19(8): 461～471
9 Biba K J. Integrity considerations for secure computer systems: [Technical Report]. MTR 3153. The Mitre Corporation, April 1977
10 Denning D E. A lattice model of secure information flow. Commun ACM, 1976, 19(5): 236～242
11 Brewer D, Nash M. The Chinese Wall security policy. In: Proceedings of the 1989 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, May 1989. 206～214
12 Boebert W E, Kain R Y. A Pratical Alternative to Hierarchical Integrity Policies. In: Proceedings of 8th National Computing Security Conference, Gaithersburg, October 1985
13 侯方勇，王志英. 可信计算研究[J]. 计算机应用研究，2004(12)：1～4
14 刘鹏，刘欣. 可信计算概论[J]. 信息安全与通信保密，2003(7)：17～19
15 周明辉，梅宏. 可信计算初探[J]. 计算机科学，2004，31(7)：5～8
16 屈延文. 软件行为学[M]. 北京：电子工业出版社，2005
17 林闯，彭雪梅. 可信网络研究[J]. 计算机学报，2005，28(25)：751～758
18 谭良，周明天. CRL 分段-过量发布新模型[J]. 电子学报，2005，33(2)：227～230
19 谭良，周明天. CRL 增量-过量发布新模型[J]. 计算机科学，2005，32(4)：133～136
20 SHAN Zhiyony. Research on the Framework for Multi-Policies and Practice in Secure Operating System [D]. Beijing, P R China: Institute of Software Chinese Academy of Sciences Beijing, 2002
21 屈延文. 软件行为学[M]. 北京：电子工业出版社，2005
22 胡建伟，汤建龙，杨绍全. 网络对抗原理[M]. 西安电子科技大学出版社，2004