基于混合访问控制策略的安全机制的研究*

王建军[1,2]，宁　洪[2]，彭代文[2]

(1. 湖南第一师范学校 信息技术系，湖南 长沙 410002；2. 国防科技大学 计算机学院，湖南 长沙 410073)

摘　要：传统安全内核只实施单一的安全策略。描述了如何在一个安全内核中同时实施机密性和完整性安全策略,满足系统的特殊安全要求。

关键词：安全内核；BLP；CW；机密性；完整性

中图法分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1001-3695(2006)03-0131-02

Research of Security Mechanism Based on Policy of Mixed Access Control

WANG Jian-jun[1,2], NING Hong[2], PENG Dai-wen[2]

(1. *Dept. of Information Science & Technology, Hunan First Normal College, Changsha Hunan* 410002, *China*; 2. *School of Computer Science, National University of Defense Technology, Changsha Hunan* 410073, *China*)

Abstract: Single security policy is implemented in the traditional security kernel. For satisfying the special request of the system, it described a security policy about implementing confidentiality and integrality in the security kernel.

Key words: Security Kernel; BLP; CW; Confidentiality; Integrity

安全开发平台是开发信息安全应用的基础,不仅是要为用户提供开发应用所需的 API,更重要的是,在其内部要产生安全信息系统中的核心元素——密钥和证书。在线为用户提供证书服务时,基于安全开发平台的服务端需要提供多线程支持。在同一时刻,平台内部可能有多个线程为多个用户产生不同的密钥和证书。因此,平台必须提供内部安全机制,保证密钥的内容互不泄漏,证书中的信息不被窜改。

访问控制安全策略是保证平台内部信息安全的主要手段,可以通过实施不同的策略分别保证信息的完整性和机密性。例如 Bell-LaPadula(BLP)[1] 是信息机密性安全策略;Clark_Wilson(CW)[2] 是信息完整性安全策略。

安全内核是一个执行安全策略的机构,通常在安全内核中只实施了机密性策略,用于检查主体对客体的访问权限,并不用于信息的完整性校验,例如 Mach Microkernel,DTOS 等。

根据开发平台的特殊安全需求,需要一个特殊安全内核同时实施机密性和完整性策略,保证开发平台中密钥和证书信息的安全。本文提出了一种实施混合访问控制策略的方案。

1　安全机制的实现

1.1　BLP 机密性策略

BLP 是强制性访问控制策略,主体和客体有对应的安全级别。其安全特性有:

(1) 下读。如果客体的安全级低于主体安全等级,则主体对客体只能读访问。

(2) 上写。如果客体的安全级别高于主体的安全等级,则主体对客体只能写访问。

收稿日期：2005-01-13；修返日期：2005-10-26

基金项目：军队科研基金资助项目(JC03-06-008)

(3) 如果客体和主体的安全级别相等,则主体对客体可读可写。

上述特性保证了信息的单向流动,即信息只能向高安全属性的方向流动。BLP 策略就是通过信息的单向流动来防止信息的扩散,抵御特洛伊木马对系统机密信息的攻击。

BLP 策略的不足:完整性方面控制不够,它重点强调信息向高安全级的方向流动,对信息的完整性保护强调不够,如没有限定拥有权限的主体对客体进行非法修改。

1.2　CW 完整性策略

Clark_Wilson 的基本原则:

(1) Separation of Duty 原则。规定一个任务从开始到结束,将被分给至少两个人完成,防止个人可能造成的欺骗。

(2) Well-formed Transaction 原则。用户不能够任意地处理数据,但是可以通过能够确保数据完整性的方法进行。

CW 策略的三个组成部分:

数据,即客体集合。在 CW 中,系统中的数据被分为两个部分,即完整性约束数据(CDIs)和非完整性约束数据(UDIs)。

过程 IVPs(Integrity Verification Procedure)用于校验数据的完整性,由系统的“安全官员”执行(安全官员不执行 TP);

过程 TPs(Transformation Procedure)是主体对客体的访问方式,使 CDI 从一种约束状态转变为另一种约束状态,保证数据的完整性。该过程由一般用户执行。

完整性策略的三个目标:阻止非授权的修改;保持内部和外部的一致性;阻止授权但非正确的修改。

CW 策略对数据的操作与数据的安全等级无关,主要防止对数据进行非法修改,容易发生信息的泄漏。

1.3　混合安全策略的实施

1.3.1　BLP 策略的实施

在安全开发平台系统的内部,线程是访问的主体,客体是

线程在产生密钥和证书的过程中,由系统生成的对象。在安全内核中,定义了一个对象访问控制列表,简称对象表(Object Table),用于描述对象的状态,包括对象类型、对象句柄、对象的安全等级、生成对象的线程句柄、对象的可使用次数以及对象是否正忙等。安全内核是对象表唯一的访问者,系统产生的每个对象都要在对象表中进行记录。由于篇幅限制,在本文中不详细描述对象表中参数设置的规定和内容。安全内核通过对象表,确保只有产生对象的线程才拥有本对象的访问权限。

对象表中与安全相关的参数如表 1 所示。

表 1 对象表中安全相关的参数

数据项	表示意义
Type	对象的类型
objectHandle	对象句柄,指向对象实体
securityLevel	对象的安全级别
usageCount	能够使用的次数
inUse	对象是否正忙
Owner	产生对象的线程句柄

在本安全内核中,对 BLP 机密性策略进行了灵活实施。

(1) 对象的安全级别在对象初始化时建立,可以改变,其目的是尽可能地减少主体对对象的访问权限,进一步提高对象的安全。

(2) 使用安全状态来表示对象的安全级别,对象允许对其进行何种访问(读、写),由对象的安全状态决定,而并不完全遵照 BLP 的上写下读安全策略。对象的安全状态有: r_w(可读可写),w(只写),r(只读)。

(3) 在开发平台的内部,对对象的访问是通过消息方式完成的。在通常的 BLP 实施中,主体有安全级别。在本安全内核中,线程虽然是访问的主体,但是并没有直接赋予安全级别。安全内核内部定义了一个包含所有消息类型的消息列表,且给每个消息类型分配了一个不变的安全级别(即本消息可执行的行为——读、写)。当线程发消息请求访问对象时,接受访问权限检查的是消息和对象,只有当它们的安全级别关系符合相应安全策略时,访问才可执行。假设一个消息有写权限,如果对象的安全状态是 r_w,则可写,相当于 BLP 中主体的安全级别不大于客体的安全级别。如果对象的安全状态是 r,则不可写,即访问不能进行,相当于 BLP 中主体的安全级别大于客体的安全级别。

安全内核对对象执行机密性策略的步骤为:

(1) 确定发出访问请求的是产生对象的线程。

(2) 确定要访问的对象类型与消息中申明的对象类型是否一致。

(3) 检查对象的可使用次数是否为 0,如为 0,则停止访问,如果不为 0,则将其值减 1。检查对象是否正忙,如果正忙,表示有另一个消息正在访问该对象,本次访问需要等待,如果不忙,则将该值设置为忙状态,允许访问。

(4) 安全内核检查主体发出的访问行为的权限。

图 1 为 BLP 安全策略的实施示意图。

1.3.2 CW 策略的实施

基于 CW 策略的职责分离原则,开发平台的安全内核把对一个对象的完整操作分离为单个独立的行为,并在每次访问行为完成后,执行完整性校验。例如,生成一个证书时,如果行为不分离,系统将把生成一个对象所需的所有信息按证书的格式填好,并完成签名发布。如果某个信息发生了错误,系统不能检测和修改。如果分离为完全独立的单个行为,并对每个行为的结果进行校验,一旦发生错误,便于及时发现和改正。

系统内部的对象分为两种: 受对象表控制的对象,即 CDIs 和不受对象表约束的对象,即 UDIs。对象在创建时,为非约束状态,当安全内核在对象表中记录对象的状态值以后,对象转为约束状态。

TP: 为对对象的访问行为。访问完以后,对象依然受到对象表的安全约束。

IVP: 为对对象访问完后,安全内核执行的校验过程。安全校验的主要目的是防止授权但非正确的修改(需要进行修改的数据是对象表和对象的属性),保证数据的完整性。安全内核提供了一个数据日志,对于读操作,数据日志用于存放读出来的结果;对于写操作,用于记录对象中数据修改前后的值。数据日志中的值用于相关访问行为执行完后的完整性校验。安全内核的校验过程包括两方面: 如果是读数据错误,则要重新执行读操作;如果是写数据错误,非法修改,安全内核要根据日志记录中的数据恢复原值。

系统对 CW 策略也是变通实施的。发出访问请求的是同一主体(产生对象的线程),但是线程通过不同消息调用相应的 TP 去访问对象。系统中的对象是基于面向对象思想实现的,对对象的访问,其实是对对象属性的访问。对属性的访问行为只有读写两种,因此,对每个属性的 TP 程序只有两个,读属性值程序和写属性值程序。对对象属性的访问由对象内部的方法即 TP 完成,线程给对象发出访问请求消息,再由对象调用其内部的方法完成对属性的读写。

要实施 CW 策略,必须保证消息同步。图 2 是 CW 安全策略的实施模型。

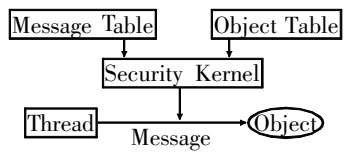

图 1 BLP 策略的实施示意图

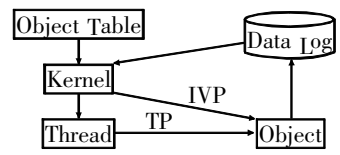

图 2 CW 的实施

1.4 安全内核的设计

基于对象表中描述的对象状态值和数据日志,安全内核针对每个消息执行访问前机密性检查和访问后完整性检查。根据消息管理器提供的消息规则和对象管理器提供的对象安全参数执行安全策略,检查访问行为的权限和对象的完整性。

安全内核的结构和单个消息的安全检查流程如图 3 所示。

函数 Message(messageType, objectHandle, Attribute, Value) 的说明。

messageType 表示要执行何种访问;

objectHandle 表示要访问的对象;

Attribute 表示要访问的属性;

Value 是一个中间变量,用于存放读写对象属性的值。

对于线程发送的每个消息,安全内核都将执行如下过程:

(1) 安全内核先执行 BLP 策略,决定是否执行访问;

(2) 如果允许访问,安全内核根据参数 Attribute 的值,记录数据日志,用于访问完成后的完整性检查;

(3) 执行对对象的访问;

(4) 访问完成后,执行 CW 策略。

对对象的访问有两种情况,即线程通过消息访问对象和内部对象之间通过消息的相互访问。两种访问安全内核都会基于对象表和数据日志进行安全检查。图 4 描述了安全内核对对象的监控作用。

(下转第 135 页)

6　对等模式

模式名称: 对等(Peer to Peer) 。

特点和用途: 对等模式是一种很有前途的安全控制模式, 它主要用于分布式、大规模网络系统的安全控制, 每个安全控制部件都处于平等的地位, 它们具有自主性、移动性、可配置性和通用的配置管理接口, 它们能够自动监测受控对象的安全状态, 自动确定安全控制需求。当需要实施安全控制时, 每个控制部件均可采用查找与匹配算法, 通过中心调度服务器发现其他控制部件, 并向其他控制部件提出自己的协调控制请求, 或接收来自其他控制部件的控制请求, 相互配合完成各自的安全控制任务, 如图 8 所示。

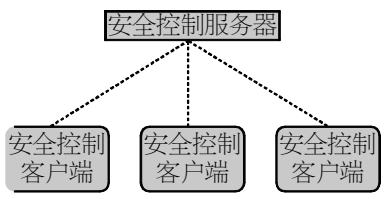

图 7　客户/服务器控制模式

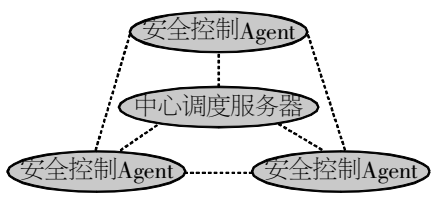

图 8　对等控制模式

解决方案: 对等控制往往采用移动 Agent 技术建立各安全控制部件, 并需要计算机操作系统或虚拟计算环境(如 Java 虚拟机) 的支持, 它们能在网络系统中自由移动, 充分利用网络系统本身的资源。它们自身的安全, 包括完整性和可靠性必须得到保证, 并接受中心调度服务器的生命周期管理。

优缺点: 对等模式是一种崭新的安全控制模式, 它具有可配置、动态灵活的特点, 特别适合于网络结构不固定、安全需求多变的分布式网络系统的安全控制。

7　结论

信息网络是一个复杂的巨系统, 对其进行安全控制是一项系统工程, 为了降低系统分析与设计的难度, 增强安全控制的灵活性、可扩展性和可复用性, 有必要使用一些常用的安全控制模式, 它们与自动控制理论中提出的控制方式[6] 有所不同, 而是融合了信息网络的特点和安全控制需求。对等控制模式应该是未来复杂网络, 特别是网格系统安全控制的潜在方式。

参考文献:

[1]　ndrew S Tanenbaum. Computer Networks(4th Edition) [M]. Prentice Hall, 2003.

[2]　卢昱. 网络控制论浅叙[J]. 装备指挥技术学院学报, 2002, 13(6): 60-64.

[3]　卢昱. 网络控制与控制方式[J]. 装备指挥技术学院学报, 2003, 14(1): 62-65.

[4]　卢昱, 王宇, 吴忠望. 网络控制论系统概念、特性及数学描述[J]. 计算机工程, 2003, 29(21): 128-130.

[5]　卢昱, 王宇, 吴忠望. 基于网络控制论概念的网络控制论系统与分析[J]. 计算机工程与科学, 2004, 26(3): 14-17.

[6]　王雨田. 控制论、信息论、系统科学与哲学[M]. 北京: 中国人民大学出版社, 1986.

作者简介:

王宇(1971-) , 男, 四川简阳人, 副教授, 博士研究生, 主要研究方向为信息网络安全、网络控制; 卢昱(1960-) , 河南洛阳人, 教授, 博士生导师, 国家有突出贡献的中青年专家, 主要研究方向为网络控制论, 信息对抗与网络安全。

(上接第 132 页)

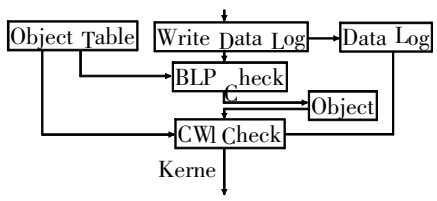

图 3　安全内核的结构和安全检查流程示意图

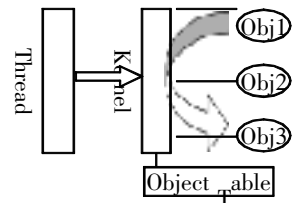

图 4　安全内核安全监控示意图

1.5　系统效率分析

假如系统中产生的对象数为 m, 每个对象的属性平均数为 n 个, 每个属性对应的 TP 为 2 个(读、写) 。假设每个属性仅访问一次, 基于两种方式进行分析。

(1) 如果不把一个完整的访问分离为多个独立的行为, 查找为顺序查找, 发出一个访问消息, 则, 查找对象的平均次数为 $(m+1)/2$, 查找对象属性的平均查找次数为 $(n+1)\times n/2$, 查找属性方法的平均查找次数为 $(2+1)/2$。整个访问所需的平均查找次数为 $((m+1)/2)\times((n+1)\times n/2)\times(2+1)/2$。

(2) 如果把一个完整的访问分离为单个独立的行为, 查找为顺序查找, 发出 n 个访问消息, 则, 查找对象的平均次数为 $n\times(m+1)/2$, 查找对象属性的平均查找次数为 $(n+1)\times n/2$, 查找属性方法的平均查找次数为 $(2+1)/2$。整个访问所需的平均查找次数为 $(n\times(m+1)/2)\times((n+1)\times n/2)\times(2+1)/2$。

第(2) 种方式要完成的平均查找次数为第(1) 种方式的 n 倍。如果 n 较小, 对系统效率的影响是可以接受的。第(1) 种方式虽然效率高, 但是不利于设计完整性检查机制。

2　结束语

基于前述, 通过 BLP 和 CW 两种安全策略结合使用, 可以有效地保证信息的机密性和完整性, 防止非法用户对基于安全开发平台的在线证书服务器的攻击。混合使用该两种策略时, 要注意系统的规模, 对于大的信息系统, 会增加构建系统的复杂度, 降低系统的效率[3] 。由于安全开发平台的规模较小, 因此, 使用 BLP 和 CW 构建安全内核时, 不会对系统效率有太大影响。

参考文献:

[1]　ell, D E L J LaPadulat. Secure Computer Systems[M]. ESD-TR-73-278 (Vol Ⅰ ～Ⅲ) (also Mitre TR-2547) , Mitre Corporation, Bedford, MA, 1974.

[2]　David D Clark, David Il Wilson. The Clark-Wilson Security Model [EB/OL]. URL: www. intel. com/ technology/itj/2003/volume07issue01/art_security/ p05_clr. htm.

[3]　王建军, 宁洪, 陈怀义, 等. 两种模型结合使用的研究与性能分析[J]. 计算机应用研究, 2004, 21(11): 95-96.

作者简介:

王建军(1969-) , 男, 副教授, 硕士, 主要研究方向为信息安全、软件体系结构; 宁洪, 教授, 主要研究方向为数据挖掘、信息安全; 彭代文, 硕士研究生, 主要研究方向为网络信息安全。