一个多策略安全模型的研究与设计

吴 娴 钱培德

(苏州大学计算机科学与技术学院 苏州 215006)

摘 要 信息系统的安全性越来越受到人们的关注。在安全操作系统的研究过程中,提出了许多安全模型。本文研究了在军事部门使用的、保证信息机密性的 BLP 模型和在商业部门使用的、保证信息完整性的 Clark-Wilson 模型。在此基础上,借鉴了 RBAC 模型中的角色概念,提出了一个能够同时保证信息的机密性和完整性的多策略安全模型 MPSM(Multi-Policy Security Model)。文中给出了 MPSM 的设计,讨论了它的机密性控制策略和完整性校验方法,并且介绍了 MPSM 的体系结构和各个子模块的功能。

关键词 安全模型,机密性,完整性,角色

Research and Design of a Multi-policy Security Model

WU Xian QIAN Pei-de

(Department of Computer Science and Technology, Suzhou University, Suzhou 215006, China)

Abstract Today, people pay more attention to the security of information system. In the process of the research of secure operating system, many security models are proposed. This paper studies BLP model that is mainly used in military department for confidentiality purpose and Clark-Wilson model that is mainly used in business department for integrity purpose. Using the idea of role conception in RBAC, we propose a multi-policy security model (MPSM) that supports both confidentiality and integrity of information. We give the design of MPSM and discuss its policies to insure confidentiality and integrity of information. Finally, we introduce the structure of MPSM and functions of its sub-modules.

Keywords Security model, Confidentiality, Integrity, Role

1 引言

人类已经步入了一个信息化的时代,人们的生活空间从人类生活了几百万年的物理空间变换到信息空间(Cyberspace)。在信息空间中,信息安全越来越受到人们的关注。从信息的安全特性角度看,最基本的要保证以下几点[1]:

- 机密性(Confidentiality):防止未经授权的信息泄露。
- 完整性(Integrity):防止未经授权的信息被篡改。
- 可用性(Availability):需要时可被一个授权实体访问和使用,防止拒绝服务。
- 可审计性(Accountability):审计信息必须有选择地保持和保护,以便影响安全的行为可以追溯到责任方。

从 1967 年开始安全操作系统的研究以来[2],根据不同领域安全系统的要求,提出了各种不同的信息安全模型,如以强调机密性为主的 BLP 模型[3]、以强调完整性为主的 Biba 模型[4]和 Clark-Wilson 模型[5],还有 Denning 的基于信息流的格模型[6]、基于角色的访问控制模型 RBAC[7]等。

现今大多数信息系统,不但要求保证信息的机密性,而且要求能够保证信息的完整性。目前,对于这个要求,大多数解决方案是把 BLP 模型和 Biba 模型结合。我们认为,Biba 模型中的约束条件和 BLP 模型中的约束条件有对立的地方,在结合过程中容易造成系统的不灵活。因此,本文在研究了 BLP 模型和 Clark-Wilson 模型后,借鉴 RBAC 中角色的思想,提出了一种对这两个模型的改进方法,构造了一个多策略的安全模型(Multi-Policy Security Model,简称 MPSM)。使用该模型,可以使系统同时支持机密性和完整性约束。在 Linux 操作系统中,使用 LSM 机制实现了 MPSM 安全模型的一个原型。

2 BLP 模型和 Clark-Wilson 模型介绍

BLP 模型在 1973 年由 D. E. Bell 和 L. J. Lapadula 提出,主要应用于军事部门,实现信息访问的机密性控制。BLP 模型是第一个可证明的安全系统的数学模型,被许多系统引用来实现系统的安全性控制[2]。Clark 和 Wilson 于 1987 年提出了 Clark-Wilson 完整性策略,它主要用在商务安全领域,迄今为止被认为是完整性目标、策略和机制的起源,可以有效满足企业信息系统所追求的完整性安全需求[8]。

2.1 BLP 模型[3]

BLP 模型的安全策略由两部分组成:自主安全策略和强制安全策略。

(1) 自主安全策略使用一个访问矩阵表示,访问矩阵第 i 行第 j 列的元素 M_{ij} 表示主体 S_i 对客体 O_j 的所有允许的访问模式,主体只能按照在访问矩阵中被授予的对客体的访问权限对客体进行相应的访问。

(2) 强制安全策略由一个具有偏序关系的安全级别{T, S, C, U, 其中 T > S > C > U}表示。每个主体有一个安全级别,每个客体属于一个访问类,该访问类与一个安全级别相关联。主体有一个当前安全级别,当前安全级别不能超过它的最初安全级别。这样一个主体仅能把它的安全级别改为低于最初分配给它的安全级别。

BLP 模型的安全特性可以归纳为:

(1) 向下读。如果客体的安全级低于主体的当前安全级,则主体对客体只能读访问。

(2) 向上写。如果客体的安全级高于主体的当前安全级,则主体对客体只能写访问。

上述两个特性保证了信息的单向流动,即信息只能向高安全级别的方向流动。BLP 模型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 模型的不足之处是完整性方面控制不够,可能出现的情况是已授权的用户对数据进行非法的修改。

吴 娴 讲师,博士研究生,主要研究方向为操作系统、信息安全;钱培德 教授,博士生导师,主要研究方向为中文信息处理、操作系统。

2.2 Clark-Wilson 模型[5]

Clark-Wilson 模型中控制数据完整性的方法有两个：

(1) 职责分离原则。规定一个任务从开始到结束不能由一个人完成。该任务将分给至少两个人完成，其中一个人执行任务，一个人证明完整性，以防止个人可能造成的欺骗。

(2) 良构事务原则。用户不能任意操作数据，只能用一种能够确保数据完整性的受控方式来操作数据。

Clark-Wilson 模型的三个组成部分如下：

(1) 数据，即客体集合。在 Clark-Wilson 中，系统中的数据被分为两个部分：被约束的数据条目 CDIs 和不受约束的数据条目 UDIs。CDIs 已经具有完整性约束，UDIs 尚不具有完整性约束，如用户通过键盘输入的信息。

(2) 完整性验证过程 IVPs(Integrity Verification Procedure)。该过程用于校验数据的完整性，这是由系统的安全官员执行的。

(3) 变换过程 TPs(Transformation Procedure)。该过程是把 CDI 从一个有效状态转变为另一种有效状态。所谓有效状态是指数据处于被约束的状态。该过程是由一般用户执行，安全官员不执行 TP。TP 可以理解为主体对客体的访问方式。

Clark-Wilson 模型中对数据的操作与数据的安全级别无关，主要是防止对数据进行非法操作，不关注信息的机密性，因此容易发生信息的泄漏。

3 MPSM 安全模型的设计

由上面的分析可知，BLP 模型能实现多级保密功能，但不能保证信息的完整性，也难以处理系统中可信主体泄露敏感信息的问题。另外，在 Linux 等操作系统中，都存在着系统管理员权限过大的问题，违反了安全系统中特权最小化原则。为了兼顾机密性和完整性要求，本文设计的安全模型将 BLP 模型和 Clark-Wilson 模型结合起来，并借鉴 RBAC 的角色-权限的思想，在模型中引入角色的概念。

3.1 角色定义

角色是一组权限的集合，不同的角色具有不同的权限集。在 MPSM 模型中，用一个五元组$\{U, R, P, PA, UA\}$来定义一个角色，其中

U：用户集合，即系统的管理者和使用者。

R：角色集合，在 MPSM 中，角色可以分为：

- 系统管理员(sysAdmin)：负责系统的日常操作，可以添加一般用户。
- 安全管理员(secAdmin)：负责管理系统的安全机制，设置主体和客体的安全级，选择与安全相关的审计规则，可以添加安全管理员。
- 安全审计员(Auditor)：负责监视和记录与安全相关的活动，可以添加审计员。
- 一般用户(user)：系统资源的使用者。

P：权限，包括对文件、设备、存储空间等资源的访问权限。

$PA \subseteq P \times R$：表示权限到角色的映射，这是一个多对多的映射。

$UA \subseteq U \times R$：表示用户到角色的映射，这是一个一对多的映射。

MPSM 模型规定，一个用户不能同时具有一个以上的角色，不同角色的用户，特别是三类系统管理员各司其职，又相互制约，以此来实现三权分立。此外，除了上述几种角色外，还可以根据需要增加其他的角色，以完成系统管理和使用的其他任务。

3.2 机密性控制

在 MPSM 模型中，参考 BLP 模型的定义，机密性控制由以下一组规则组成：

(1) 简单安全规则(ss-property)：

如果 $f_s(S) \geqslant f_s(O)$，则主体 S 拥有对客体 O 的“读”、“写”权限。

(2) * 规则(* -property)：

如果 $f_c(S) \leqslant f_s(O)$，则主体 S 拥有对客体 O 的“添加”权限；

如果 $f_c(S) = f_s(O)$，则主体 S 拥有对客体 O 的“写”权限；

如果 $f_c(S) \geqslant f_s(O)$，则主体 S 拥有对客体 O 的“读”权限。

其中，S 为系统中所有主体的集合，包括操作系统的用户、进程等。O 为系统中所有客体的集合，包括操作系统的资源。f 是一个安全级的映射函数，定义如下：

$$f = S \cup O \rightarrow L$$

在上式中，L 为安全级的集合。$L=\{C, K\}$，C 表示密级，K 表示范畴。假设系统中两个安全级 $L_1=\{C_1, K_1\}$ 和 $L_2=\{C_2, K_2\}$，安全级满足如下规则：

$L_1 < L_2$，当且仅当 $C_1 < C_2$ 且 $K_1 \subseteq K_2$。

主客体的安全级是由系统的安全管理员定义的。对于每个主体，有两个安全级别：f_s 是主体安全级，这是安全管理员授予主体的安全级；f_c 是主体当前安全级，对于活动主体，如进程，f_c 是可以变化的。但是 f_s 和 f_c 之间必须满足 $f_c \leqslant f_s$ 的约束。

这里需要注意的是，简单安全规则和 * 规则中，主体拥有的权限必须属于主体所属角色的权限集，这个检查将会在实施安全性判定之前得到确认。

3.3 完整性校验

对敏感信息，如数字证书，除了机密性控制外，还需要用完整性规则来防止其中的信息被篡改。因此，将系统中的关键任务分离为若干独立的行为，并在每次访问行为完成后执行完整性的校验。

在系统内部，信息被分为两类：受控的数据 CDI 和非受控的数据 UDI。数据被创建或刚刚发生过修改操作之后，是非受控数据。当接受了安全模型的完整性校验后，转换为受控数据。

TP 是那些主体对客体的访问行为，在 MPSM 模型中，TP 需要受到安全级的约束。

IVP 是对数据进行访问之后 MPSM 模型执行的校验过程。校验的目的是防止数据在安全行为中受到非正确的修改，以保证数据的完整性。在这个过程中，需要借助 MPSM 模型的安全审计功能，为数据的完整性检验创建日志。

当然，在对关键任务进行细分后，每个子任务处理的客体将会发生变化，有可能不再是原来那个完整任务面对的客体了。因此，在加入完整性校验的 MPSM 模型中，需要对机密性控制中的客体集合进行更加细粒度的划分，并授予相应的安全级。

4 MPSM 安全模型的实现

我们选择 Linux 操作系统来实现 MPSM 安全模型，以增进 Linux 的安全性。基于 Linux 开发安全操作系统通常有三种方法：虚拟机法、改进/增强法、仿真法[9]。我们借鉴了 LSM 机制[10]，使用改进/增强的方法，将 MPSM 安全模型作

为 Linux 内核的一个模块，在需要的时候以模块方式载入。

4.1 系统结构

用户对客体的访问请求被安全模型的接口处理子模块截获，在对这个请求进行分析后，请求被交给安全仲裁子模块。在仲裁模块中，需要对本次访问进行机密性仲裁，并在访问完客体后进行完整性校验。当然，所有跟安全相关的操作都会被安全审计模块记录。另外，系统还提供了一个安全管理子模块，三类管理员可以借助这个模块进行其管理工作。MPSM 安全模型的总体结构如图 1 所示。

4.2 子模块功能

根据图 1 所示，安全模型包括 4 个子模块，分别是：接口处理模块、安全仲裁模块、安全审计模块和安全管理模块。下面分别介绍这些模块的功能。

(1) 接口处理模块

该模块的主要功能是截获用户访问敏感资源的每一个请求，从中分析出主体和客体的信息，并且为了完成访问后的完整性校验，还需要将请求分解为若干子任务。接口模块将主客体的信息传递给安全仲裁模块进行安全性检查，以决定此次请求是否允许执行，并且将仲裁模块对于该请求的执行结果返回给用户。接口模块的实现对于用户来说是透明的，它的工作与原有操作系统平滑结合，做到接口模块与原有系统的无缝连接。

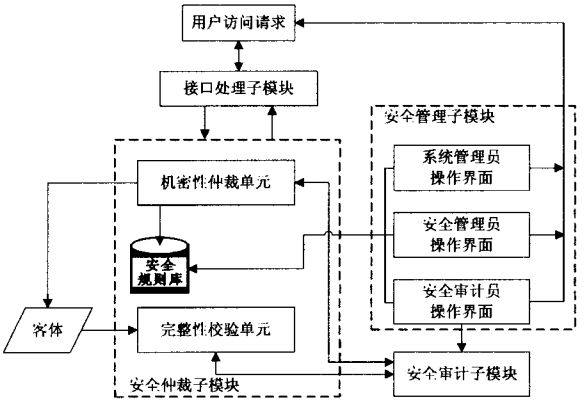

图 1 MPSM 安全模型总体结构图

(2) 安全仲裁模块

安全仲裁模块接收接口模块传递过来的主、客体信息，并且首先根据主体所属的角色，判定此次访问的权限是否属于某个角色。若该权限不属于用户所属角色，则直接拒绝该次访问，并将此次请求记录在安全日志中以便日后追查，只有那些符合角色权限的请求才会被继续执行。安全仲裁模块分为两个主要单元：机密性仲裁单元和完整性校验单元。

仲裁模块首先根据主、客体的安全属性，查询安全规则库，以决定主体是否可以访问客体以及如何访问客体。安全规则库中记录了每个主体和客体的安全标记，以及安全模型中主客体的访问限制规则。访问限制规则按照 MPSM 安全模型中的安全策略制定，基本的安全策略如前所述。为了强化安全措施，可以由安全管理员按实际系统的情况增加一些附加规则。如果允许访问客体，那么此次访问需要被记录在安全日志中，用于访问完成后的完整性检查。

对客体的访问完成后，进入完整性校验单元。这里，由 IVP 根据日志中的数据对客体的读或写访问执行校验。对于读操作，日志存放被读出的结果；对于写操作，日志中存放修改前后的值。经过完整性校验，如果发现读出错，则需要重新读取该数据；如果发现是写出错，则需要根据日志恢复原始值。

由于原先完整的操作已经被分解为若干子任务，因此机密性仲裁和完整性检查可能被多次执行。这里需要注意的是，子任务不对应系统中某个具体的主体，因此我们默认各个子任务的安全级与发出请求的用户的安全级相同。

(3) 安全审计模块

该模块的主要功能一方面是处理机密性仲裁单元中发现的非正常情况，进行事件记录、报警或其他相关事务处理。另一方面，该模块为完整性校验提供依据，为数据的完整性校验创建相关的日志。

(4) 安全管理模块

这个模块为系统的三类管理员提供了操作的界面。其中：

• 系统管理员操作界面的功能是增加和删除用户，定义角色权限、角色用户映射关系，进行系统的日常操作，并对安全管理员的安全属性进行设置。只有系统管理员才有权限进行本模块的操作。

• 安全管理员操作界面的功能是对安全规则库进行建立、增删和修改等操作，定义用户默认的安全属性。只有安全管理员才有权限进行本模块的操作。

• 安全审计员操作界面的功能是负责管理与安全有关的审计信息，包括查询、打印审计信息。当审计信息达到一定规模后，系统还会提示安全审计员进行审计信息的转储。只有安全审计员才有权限进行本模块的操作。

结束语 安全操作系统的研究已经迈入了多策略时期[11]，仅仅在系统中实现一种安全策略已经不能满足现代操作系统对安全性的多方面要求。在研究同时满足机密性和完整性的安全模型解决方案中，大多数模型采用 BLP 模型和 Biba 模型的结合。本文讨论了 BLP 模型和 Clark-Wilson 模型相结合的一种方法，提出了基于这两个模型并引入角色的思想，完成对信息机密性的控制和完整性的检查。MPSM 安全模型使用 LSM 思想在 Linux 操作系统中得到了初步的实现，由于是作为内核的一个安全策略模块，因此对系统的性能不会产生太大的影响。另一方面，受到 LSM 思想的启发，以及随着安全操作系统动态策略时期的到来，我们将进一步研究安全策略管理框架，以此实现对多种安全策略更加灵活和有效的支持。

参 考 文 献

[1] Lampson B W. Requirements and Technology for Computer Security. Washington: National Academy Press, 1991:74-101

[2] 石文昌，孙玉芳. 安全操作系统研究的发展(上). 计算机科学，2002，29(6):5-12

[3] Bell D E, Lapadula L J. Secure Computer Systems: Mathematical Foundations and Model. Bedford, MA: The MITRE Corporation, 1973:74-244

[4] Biba K J. Integrity consideration for secure computer system. Bedford MA: The MITRE Corporation, MTR-2997. 1977

[5] Clark D D, Wilson D R. A comparison of commercial and military computer security policies// IEEE Symp. on Security and Privacy. New York: IEEE Computer Society Press, 1987: 184-194

[6] Denning D E. A Lattice Model of Secure Information Flow. Communications of the ACM, 1976, 19(5):236-243

[7] Sandhu R. Role-based Access Control Models. IEEE Computer, 1996, 29(2):38-47

[8] 卿斯汉，等. 基于 Clark-Wilson 完整性策略的安全监视模型. 软件学报，2004，15(8):1124-1132

[9] 刘文清，等. 基于 Linux 开发安全操作系统的研究. 计算机科学，2001，28(2):52-54

[10] Wright C, Cowan C, Morris J, et al. Linux security modules: general security support for the linux kernel. In Foundations of Intrusion Tolerant Systems (OASIS'03), 2003:213-226

[11] 石文昌，孙玉芳. 安全操作系统研究的发展(下). 计算机科学，2002，29(7):9-12