达到 B 级安全的 PMI 研究与设计*

冷　健[1]，谢冬青[1,2]

(1. 湖南大学 计算机与通信学院，湖南 长沙 410012；2. 中国科学院 软件所 计算机科学重点实验室，北京 100081)

摘　要: 现代软件系统内核采用面向对象的方法,提供对内核数据结构的保护和隐藏,但是内核的安全性设计始终没有到达理想状态。因此,在面向对象的内核设计中引入安全内核模型可以改善内核设计的安全性问题。提出的 BSK 安全模型是一种达到 B 级安全的轻量级安全内核模型,并且将 BSK 内核应用于 PMI 体系结构设计中,设计和实现了达到 B 级安全的 PMI。

关键词: 监控器模型；授权管理基础设施；安全域；安全对象代理

中图法分类号: TP311　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)04-0047-02

Design and Implementation of PMI Based on B-level Security

LENG Jian[1], XIE Dong-qing[1,2]

(1. *College of Computer & Communication, Hunan University, Changsha Hunan* 410012, *China*; 2. *Laboratory of Computer Science, Software Institute, Chinese Academy of Sciences, Beijing* 100081, *China*)

Abstract: The kernel of large-scale software is Object-Oriented and provides protection and concealment to kernel data structures. But the kernel security can not be perfect. The security kernel model can improves kernel security. Presents a model for the lightweight security kernel using B-level security. This model B-level Security Kernel (BSK) is used to highlight security level in the design of PMI architecture.

Key words: Reference Monitor; PMI(Privilege Management Infrastructures); Secure Domain; Secure Object Proxy

现代大型软件系统可以看成对象的集合,这里所说的对象是一种比“类”粒度更大,更方便的单元[1]。它是一种功能集成的单元,具有标准化的公共接口,一旦符合系统体系结构描述的接口特征,即可以重用。对象间的通信和关联可以用节点(表示对象)和弧(表示对象间通信)组成的图来表示[1,2]。对象间通信可以是过程调用、事件广播、管道、过滤器和消息传递机制。基于安全内核的体系结构设计应达到如下目标: 安全策略和安全实施分离,内核设计具有可验证性,安全策略灵活,内核设计简洁,实现性能较好。

PMI[3] (Privilege Management Infrastructures,授权管理基础设施) 建立在 PKI 基础上,与 PKI 相结合,利用属性证书提供实体身份到应用权限的映射,实现对系统资源访问的统一管理。PMI 与 PKI 的主要区别在于: PKI 证明实体身份的合法性; PMI 证明实体具有什么权限,能以何种方式访问什么资源。

PMI 主要由属性证书、属性证书签发机构(AA)、授权策略机构(PA)、用户权限管理机构(UPA)和属性证书发布系统组成。属性证书是一个绑定了实体权限信息的数据结构,它将标志和角色、权限等属性绑定在一起,通过数字签名保证证书的不可伪造性,防窜改。属性证书签发主要负责为用户签发各种属性证书,并负责发布和维护属性证书和属性证书废止列表 ACRL。策略机构负责制定和发布各种策略的制定和设置,如用户策略、角色策略、资源策略和权限策略等。用户权限管理机构是策略机构的一个组成部分,主要负责用户权限策略的制定、为用户分配权限和申请属性证书。发布系统主要采用 LDAP 标准协议存储各种属性证书和属性证书废止列表信息,为应用系统提供应用接口。

在 PMI 体系结构中引入安全内核可以保障 PMI 体系结构自身的安全。本文采用 BSK(B-level Security Kernel) 安全内核来设计 PMI 使得 PMI 体系的安全级别可以达到 B 级。

1　BSK 安全模型

安全模型是安全策略形式化的表述,它是安全策略所管理的实体以及构成策略的规则。John McLean[4] 定义安全模型是用来描述一个系统的保密性、可用性和完整性的需求的形式化的表述。其中在安全模型设计中出现较多的是监控器模型。

监控器模型[5] 最早由 J. P. Anderson 提出,用于主体对客体的访问控制(图 1)。监控器模型仅仅是一种思想,以安全机制的形式体现在安全内核的设计中。它满足完全性、独立性和可验证性。完全性是监控器必须在每次主体对客体访问时都被激活; 独立性是监控器和授权数据库必须受到保护以防止未授权的修改; 可验证性是监控器必须是小巧的、良好组织的、简单的和可理解的,对其是否能够正确执行功能可以全面地分析、测试和验证。

监控器模型包括认证识别子系统、审计子系统和授权数据库。认证识别子系统负责鉴别每个实体(主体)的身份,这是整个模型安全的基础。授权数据库帮助监控器完成访问控制,即决定主体是否有权访问客体,通常是采用访问控制列表(ACL)完成授权。审计是一种信任机制,它是安全策略的一个

收稿日期: 2004-05-13; 修返日期: 2004-07-12

基金项目: 国家自然科学基金资助项目(60373085)

重要部分。监控器的活动通过审计记录下来。

BSK 内核采用消息传递和安全检查的机制。如图 2 所示，BSK 内核采用前面介绍的监控器模型并且进行扩展，主要是授权数据库采用访问控制矩阵(ACL) 并且分离成面向对象(Object ACL) 和面向(对象) 属性(Attribute ACL) 的两个授权库。BSK 安全内核包含的对象分为三类: 安全域(Secure Domain, SD) 、安全对象(Secure Object, SO) 和安全对象代理(Secure Object Proxy, SOP) 。安全域是包容其他对象的对象，是定义好的安全置信区域，是实施安全策略和安全机制的原子单元。安全对象是完成具体功能和操作的执行单元。安全对象代理是安全域间完成通信的对象，主要完成安全域间的安全通信代理。安全域间的通信通过安全对象代理监控。安全对象代理类似看门狗，对进出安全代理对象的数据流进行分析和控制，这样可以通过对信息流流量的分析来检测隐蔽通道。安全内核用于监控外界对安全核的访问。外界访问安全域中的对象必须严格遵循监控器模型安全机制。

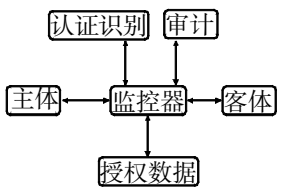

图 1 监控器模型

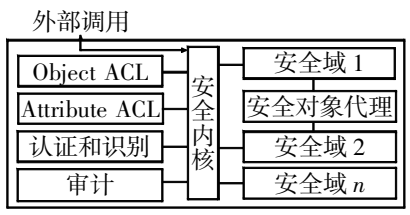

图 2 BSK 安全内核模型

2 PMI 授权管理模型

基于角色的授权管理是把对用户的授权分成两部分，用角色来充当用户权限的中介。用户与角色之间以及角色与权限之间就形成多对多的关系，一个用户可以拥有多类角色，一类角色可以被多个用户所拥有; 同理，一类角色可以包含多种类型的权限，而每一种类型的权限可以被多类角色所拥有。

本文采用基于角色的统一授权策略，主要包括:

(1) 用户定义策略，定义需要进行授权的用户身份和范围，采用用户属性证书定义用户所属的用户组;

(2) 资源定义策略，定义需要区分访问权限的资源类型，采用角色分配证书定义用户组、资源与角色的映射关系;

(3) 权限定义策略，定义信息网内对应用资源的不同权限的操作类型，采用角色规格证书定义角色、资源与权限的映射关系;

(4) 角色定义策略，定义角色类型及其层次策略;

(5) 授权管理策略，包括授权策略公共规则、授权策略特殊规则和授权策略自主规则。

在这些策略的统一授权管理下，由用户与资源确定角色，再由角色和资源确定该用户的权限类型，然后得出权限控制的结果。授权管理策略定义了用户定义策略、资源策略、角色策略和权限策略之间的映射关系。通过用户属性证书、角色分配证书和角色规格证书便可以得到某一用户对某一资源的访问权限。

如图 3 所示，本文给出应用系统利用 PMI 提供的授权管理功能进行访问权限控制的逻辑结构。主体是一个实体，客体是主体试图访问的系统内其他实体(数据、应用等) 。策略实施点(PEP) 介于访问者与目标之间，负责截获请求并向策略决策点申请授权，执行授权决策的决策结果。策略决策点(PDP) 负责与 PMI 的属性发布系统交互，根据接收到的授权请求，取得用户属性证书，按照具体策略计算权限，得到用户的访问权限。

权限控制过程描述:

(1) 访问者发出对某个目标的访问请求，被策略实施点截获。

(2) 策略实施点对请求进行处理，根据用户信息，请求操作和目标信息等形成决策请求，发给策略决策点。

(3) 策略决策点将权限请求送到访问控制服务器。

(4) 访问控制服务器根据用户身份证书从属性证书发布点取得用户属性证书，计算用户权限，并将权限信息发回到策略决策点。

(5) 策略决策点根据用户的权限，对决策请求进行判断，最后将决策的结果返回给策略执行点。该结果只是允许或拒绝。

(6) 策略执行点根据决策结果执行访问或者拒绝访问。

属性证书的发布有两种模式: ①推模式，当主体要求访问资源时，由主体直接提供其属性证书，即主体将自己的属性证书推给应用服务器，这种方式使用应用服务器不需要查找用户的属性证书，可以提高服务器的性能。②拉模式，是授权机构发布属性证书到统一属性证书发布点。当主体需要属性证书时，由应用服务器从该发布点拉回属性证书。

AA 属性证书签发机构是 PMI 体系的核心，它相当于 PKI 体系中的 CA 认证机构。对于一个大型的分布式企业应用系统，也需要根据应用系统的分布情况设立 AA 机构，构成分布式授权体系，其结构如图 4 所示。

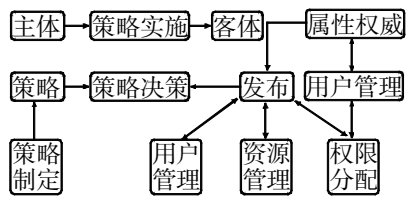

图 3 PMI 权限控制模型

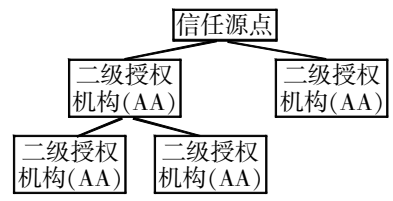

图 4 分布式授权体系

信任源 SOA，即 Source of AA，是最高级别的授权机构，是整个授权管理体系的源节点，主要负责授权管理策略的管理、应用授权受理、AA 中心的设立审核及管理、授权管理体系业务的规范化等。

AA(包括 SOA) 通过发行权限委派证书(属性证书的一种) 来对下一级 AA 进行授权，各级 AA 属性权威可以设立相应的策略机构 PA 和用户权限管理机构 UPA，为本级 AA 属性权威制定与本级 AA 的授权策略，各级 PMI 管理员可以使用 UPA 管理本级用户权限。

PMI 属性证书发布系统采用标准的 LDAP 协议。PMI 发布系统支持分布式设计，与 PKI 发布系统相似。

3 结论

基于 PMI 授权管理在存取控制方面不再基于用户身份，而是基于其拥有属性来决定其对某一资源或服务是否拥有访问权。这样应用程序中访问控制规则可以简单地被定义成按属性的有效期来决定访问权。其优点是简单、容易理解，并且更易维护。同时，又是一个可伸缩的方案，可以支持海量用户，又无须对应用程序进行任何改变(假定所有用户都可以被定义成同样的一套属性集合) 。如果使用传统的基于用户访问控制机制，每增加一个新用户，都要求修改每个 (下转第 51 页)

体进行交配。在实际过程中,通过这样处理,有效地提高了算法的收敛速度。

4.3　在学习样本中加入适当的噪音

在计算适应值时,对式(2)中的模型的实际输入输出 x'_i, y'_k 加入随机白噪音 ξ, ξ,这样使求得的模型更接近实际模型,提高了模型的稳定性。

改进后的演化学习算法如图 3 所示。

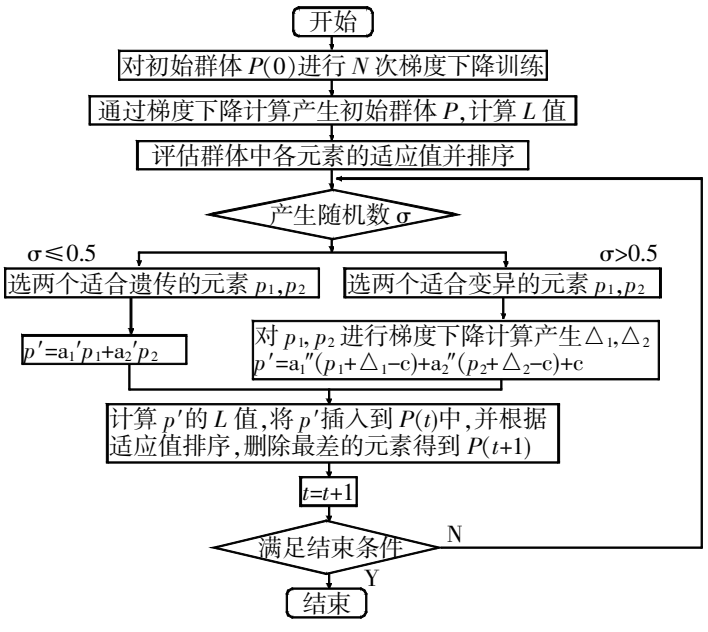

图 3　改进算法示意图

5　模型的应用

笔者提出的这种快速学习的 BP 神经模型,在不少企业的工艺优化中得到了应用。其中,株洲洗煤厂通过应用该模型,优化了其主焦煤的生产工艺,使产品的性能得到了提高。主焦煤的性能指标很多,主要有灰成分(Ad)、挥发成分(Vdaf)、发热量(Qnet. v. ar)、沾结性指数(GR. I)、硫成分(St. d)等。生产的工艺过程也十分复杂,主要流程有:

(1)跳汰洗。主要工艺参数:风量 L_1、水量 L_2、床层厚度 H、跳态频率 f 等。

(2)分级脱水(脱水自动控制,直接产生块精煤)。

(3)煤泥水处理。主要参数:浓缩时间 t_1、搅拌时间 t_2、絮凝剂量 S 等。

(4)浮选和浮精煤脱水(工艺固定)。在洗煤过程中,根据原煤的品种不同,需要选定最优的工艺参数,以保证主焦煤的各项性能指标。其中以 2#原煤为例,性能指标的控制参数为

Ad < 3%; GR. I > 65; st. d < 1%; Qnet. v. ar > 27Mj/kg(要求尽可能高)

通过提取实验样本,用 BP 模型进行拟合,最终优化的工艺参数如表 1 所示。

表 1　指标明细表

L_1	L_2	H	f	t_1	t_2	s
0.42Mpa/cm^3	3T/T	200mm	50Hz	1h	1.8h	0.58%

模型预报的产品主要性能为

Ad: 2.3%; GR. I: 87; st. d: 0.91%; Qnet. v. ar: 29.5Mj/kg

产品的实际性能指标为

Ad: 2.1%; GR. I: 82; st. d: 0.95%; Qnet. v. ar: 28.8Mj/kg

生产实际说明,该种模型具有很好的精度,而且当原煤种类和工序中参数发生变化时,模型通过及时训练,可以产生新的最优工艺参数,使产品的主要性能指标达到要求。

参考文献:

[1] chiffmann W, Joost M, Werner R. Optimization of the Backpropagation Algorithm for Training Multilayer Perceptrons Technical Report [R]. University of Koblenz, Institute of Physics, 1993.

[2] Leonard J, Kramer M A. Improvement of the Backpropagation Algorithm for Training Neural Networks[J]. Computers Chem. Engng, 1990.

[3] Silva F M, Almeida L B. Speeding up Backpropagation[J]. Eckmiller R. AdvancedNeural Computers, 1990.

[4] Yuan Zeng-Ren, Shen Xiao-Hui. A New Method for Faster Backpropagation Learning. Advances in Modeling & Analysis A[M]. AMSE Press, 1995.

[5] 王士同. 神经模糊系统及应用[M]. 北京:北京航空航天大学出版社, 1998.

[6] 潘正君,康立山,陈毓屏. 演化计算[M]. 北京:清华大学出版社, 1998.

[7] 袁曾任. 人工神经元网络及应用[M]. 北京:清华大学出版社, 1999.

作者简介:

许中华(1966-),男,湖南人,讲师,硕士,研究方向为人工智能技术与应用;谭甲凡(1963-),男,湖南人,讲师,学士,研究方向为智能控制系统;杨伟丰(1969-),男,湖南人,讲师,硕士,研究方向为计算机网络通信;孙星明(1962-),男,湖南人,教授,博士,研究方向为智能模型与分布式系统。

(上接第 48 页)应用程序的 ACLs 中。这样会导致 ACLs 在各处分布,或者产生一个集中式的大型 ACLs 以便所有应用程序能够联机访问。从管理角度来说两者都是十分困难的。如果迁移到基于角色的访问流程,可以避免以上操作带来的实施和管理复杂性。

参考文献:

[1] avid Garlan, Mary Shaw. An Introduction to Software Architecture [J]. Advances in Software Engineering and Knowledge Engineering, 1993, (1): 87-128.

[2] Seattle. Proceedings of the First International Workshop on Architectures for Software Systems[C]. Washington, 1995.

[3] ITU-T Rec. X.509 (2000) | ISO/IEC 9594-8 The Directory: Public-key and Attribute Certificate Framework[S].

[4] Carl Landwehr, Constance Heitmeyer, John McLean. A Security Model for Military Message Systems[J]. CM Transactions on Computer Systems, 1984, 2(3): 198-212.

[5] James P Anderson. Computer Security Technology Planning Study Volume II. ESD-TR-73-51[R]. Bedford, MA, USA: Electronic Systems Division, Air Force Systems Command, Hanscom Field, 1972.

[6] John Linn, Magnus Nystrom. Attribute Certification: An Enabling Technology for Delegation and Role-based Controls in Distributed Environments[C]. Proceedings of the 4th ACM Workshop on Role-based Access Control, 1999. 121-130.

作者简介:

冷健(1971-),男,湖南长沙人,博士生,主要研究方向为信息安全理论与技术;谢冬青(1965-),男,湖南益阳人,博士,主要研究方向为信息安全理论。