访问控制技术的研究和进展*)

The Research and Development of Access Control Technology

訾小超　张绍莲　茅　兵　谢　立

(南京大学计算机系　软件新技术国家重点实验室　南京210093)

Abstract　Access Control(AC)is one of the important technologies of System Security and has been widely studied recently because the traditionary AC technologies can't meet with the security commands of contemporary information system. As a result, the traditionary AC technologies have been developed and some new technologies have been put forward. This paper makes the necessary classification for the more-than-ten-year research results of the AC technology, together with the analysis and predication for the development trend of the AC technology in the future.

Keywords　Security technology, Access control, DAC, MAC, RBAC

1　引言

计算机网络的发展与普及使得信息系统的安全问题日益突出,相关的安全技术也成为人们研究的热点。访问控制是实现既定安全策略的系统安全技术,它管理所有资源访问请求,即根据安全策略的要求,对每一个资源访问请求做出是否许可的判断,能有效地防止非法用户访问系统资源和合法用户非法使用资源[1]。美国国防部的可信计算机系统评估标准(TESEC)把访问控制作为评价系统安全的主要指标[2],访问控制对提高系统安全性的重要性是不言而喻的。

计算机信息系统访问控制技术最早产生于六十年代,随后出现了两种重要的访问控制技术:自主访问控制(Discretionary Access Control,DAC)和强制访问控制(Mandatory Access Control,MAC)。它们在多用户系统(如各种 UNIX 系统)中得到广泛的应用,对计算机信息系统的安全做出了很大的贡献。

传统访问控制技术远远落后于当代系统安全的要求,安全需求的发展对访问控制技术提出了新的要求。这主要体现在两个方面:计算机信息系统在各行各业的应用进一步普及,与应用领域有关的安全需求大量涌现,比如公共信息服务系统对信息完整性和可用性的需求要远大于对保密性的需求,传统访问控制技术很难满足这种需求;网络和分布式技术的发展使得访问控制要立足于单位或部门的网络来设计和实施,甚至还要考虑其开放性,以便于协作单位间的系统互连。

为了满足新的安全需求,近年来各国学者对访问控制技术进行了大量研究,一方面对传统访问控制技术的不足进行改进,另一方面研究新的访问控制技术以适应当前计算机信息系统的安全需求。本文主要对近年来的访问控制技术的研究状况及其成果进行总结与分析,展望了未来访问控制技术的发展趋势。

2　传统访问控制技术及其改进方案

要控制用户对资源的访问,必须要明确标示系统中的所有用户和资源。在很多访问控制技术中,用户和资源全部被抽象为主体和客体,主体,即主动实体,导致信息在系统中流动及改变系统状态的用户或进程等;客体,能包含或接受信息的被动实体,如文件、内存块等[2],包括传统访问控制在内的大多数访问控制技术都把资源访问统一为主体对客体的访问加以控制。

2.1　DAC 技术及其改进

传统的 DAC 最早出现在七十年代初期的分时系统中,它是多用户环境下最常用的一种访问控制技术,在目前流行的 UNIX 类操作系统中被普遍采用。DAC 基于这样的思想:客体的主人全权管理有关该客体的访问授权,有权泄漏,修改该客体的有关信息[4]。因此,有些学者把 DAC 称为基于主人的访问控制。

DAC 技术在一定程度上实现了权限隔离和资源保护,但是在资源共享方面难以控制。为了便于资源共

*)本课题得到国家"863"高技术经费资助,课题号:863-301-6-4。訾小超　博士生,研究方向:安全操作系统、访问控制。张绍莲　硕士生。茅　兵　副教授,研究方向:系统安全。谢　立　教授,博导,研究方向:安全操作系统、智能操作系统。

享，一些系统在实现 DAC 时，引入用户组的概念，以实现组内用户的资源共享。

DAC 技术存在明显的不足：资源管理比较分散；用户间的关系不能在系统中体现出来，不易管理；信息容易泄漏，无法抵御特洛伊木马(Trojan Horse)的攻击。特洛伊木马是嵌入在合法程序中的一段以窃取或破坏信息为目的的恶意代码[2]，在自主访问控制下，一旦带有特洛伊木马的应用程序被激活，特洛伊木马可以任意泄漏和破坏接触到的信息，甚至改变这些信息的访问授权模式。

针对 DAC 的不足，一些学者对它提出了一系列改进措施。早在七十年代末，M. H. Harrison，W. L. Ruzzo，J. D. Ullman 就对传统 DAC 做出扩充，提出了客体主人自主管理该客体的访问和安全管理员限制访问权限随意扩散相结合的半自主式的 HRU 访问控制模型，并设计了安全管理员管理访问权限扩散的描述语言[3]。HRU 模型提出了管理员可以限制客体访问权限的扩散，但没有对访问权限扩散的程度和内容做出具体的定义。到了92年，Sandhu 等人为了表示主体需要拥有的访问权限，将 HRU 模型发展为 TAM(Typed Access Matrix)模型[4]，在客体和主体产生时就对访问权限的扩散做了具体的规定。随后，为了描述访问权限需要动态变化的系统安全策略，TAM 发展为 ATAM (Augmented TAM)模型[5]。

上述改进在一定程度上提高了 DAC 的安全性能，但由于 DAC 的核心是客体主人控制客体的访问授权，使得它们不能用于具有较高安全要求的系统，因而这些改进模型几乎没有得到实际应用。

2.2 MAC 技术及其发展

MAC 最早出现在 Multics 系统中，在1983美国国防部的 TESEC 中被用作为 B 级安全系统的主要评价标准之一。MAC 的基本思想是：每个主体都有既定的安全属性，每个客体也都有既定安全属性，主体对客体是否能执行特定的操作取决于二者安全属性之间的关系[2]。

通常所说的 MAC 主要是指 TESEC 中的 MAC，它主要用来描述美国军用计算机系统环境下的多级安全策略[2]。在多级安全策略中，安全属性用二元组(安全级，类别集合)表示，安全级表示机密程度，类别集合表示部门或组织的集合。一般的 MAC 都要求主体对客体的访问满足 BLP(Bell and LaPadula)安全模型的两个基本特性[2]：

·简单安全性：仅当主体的安全级不低于客体安全级且主体的类别集合包含客体的类别集合时，才允许该主体读该客体。

·*-特性：仅当主体的安全级不高于客体安全级且客体的类别集合包含主体的类别集合时，才允许该主体写该客体。

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属性的方向流动，MAC 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保密性的攻击。

MAC 的不足主要表现在两个方面：应用的领域比较窄，使用不灵活，一般只用于军方等具有明显等级观念的行业或领域；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，对高安全级信息的完整性保护强调不够。

为了增强传统 MAC 的完整性控制，美国 Secure-Computing 公司提出了 TE(Type Enforcement)控制技术，该技术把主体和客体分别进行归类，它们之间是否有访问授权由 TE 授权表决定，TE 授权表由安全管理员负责管理和维护。TE 技术在 SecureComputing 公司开发的安全操作系统 LOCK6中得到了应用。TE 技术提高了系统的完整性控制，但维护授权表给管理员带来很多麻烦。为了改进 TE 控制技术管理复杂的不足，TE 发展为 DTE(Domain and Type Enforcement)[7]访问控制技术，它主要通过定义一些隐含规则来简化 TE 授权表，其维护工作也随之大大减少。

Chinese Wall 模型是 Brewer 和 Nash 开发的用于商业领域的访问控制模型，该模型主要用于保护客户信息不被随意泄漏和篡改[8]。Chinese Wall 模型后来被证明也是一种强制访问模型[9]，它的贡献在于对开发商用访问控制技术的尝试。

上述种种改进在一定程度上使得传统的 MAC 技术更加完善，并在商用领域也做出了一定的努力；但从总体上来看，这些模型大都针对具体应用开发，灵活性差，产生的影响不大，只有个别系统采用这些访问控制技术。

3 新型访问控制技术

3.1 基于角色的访问控制 RBAC 及其进展

RBAC(Role_Based Access Control)的概念早在七十年代就已经提出，但在相当长的一段时间内没有得到人们的关注。进入九十年代，安全需求的发展加上 R. S. Sandhu 等人的倡导和推动，RBAC 又引起了人们极大的关注，目前美国很多学者和研究机构都在从事这方面的研究，如 NIST(National Institute of Standard Technology)和 George Mason 大学的 LIST(Laboratory of Information Security Technology)等。NIST 的研究人员认为 RBAC 将是 DAC 和 MAC 的替代者，文[10]给出了民用组织对 RBAC 产品的需求及有关 RBAC 产品的市场调研。从1996开始，美国计算机协会

ACM 每年都召开 RBAC 专题研讨会来促进 RBAC 的研究。图1给出了 RBAC 的结构。

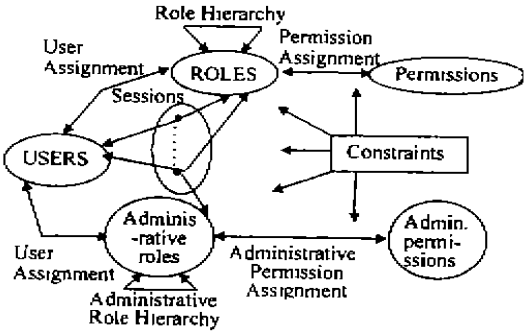

图1 RBAC 原理结构示意图

在 RBAC 中，在用户(user)和访问许可权(permission)之间引入角色(role)的概念。用户与特定的一个或多个角色相联系，角色与一个或多个访问许可权相联系，角色可以根据实际的工作需要生成或取消，而且登录到系统中的用户可以根据自己的需要动态激活自己拥有的角色(见图1中的 sessions)，避免了用户无意中危害系统安全。除此之外，角色之间、许可权之间、角色和许可权之间定义了一些关系，比如角色间的层次性关系，而且也可以按需要定义各种约束(constraints)，如定义出纳和会计这两个角色为互斥角色(即这两个角色不能分配给一个用户)[11]。

与 DAC 和 MAC 相比，RBAC 技术具有显著的优点。首先，RBAC 是一种策略无关的访问控制技术，它不局限于特定的安全策略，几乎可以描述任何的安全策略，甚至 DAC 和 MAC 也可以用 RBAC 来描述[6]，这与 MAC 和 DAC 存在很大区别，DAC 本身就是一种安全策略，MAC 主要是用来描述军用计算机系统的多级安全策略。随着计算机系统在众多行业和部门的普及，访问控制技术的策略无关性显得尤为重要。其次，RBAC 具有自管理的能力，利用 RBAC 思想产生出的 ARBAC(Adminstrative RBAC)模型很好地实现了对 RBAC 的管理[12]。RBAC 的自管理能力具有非常现实的意义。在一个大的系统中，管理众多的用户和文件需要相当大的工作量，由安全管理员集中式管理显然并不理想。同时，RBAC 使得安全管理更贴近应用领域的机构或组织的实际情况，很容易将现实世界的管理方式和安全策略映射到信息系统中，比如现实生活中，一个人担任多方面的职务，在 RBAC 中只要将同一个用户对应多个角色就很容易实现。此外，RBAC 便于实施整个组织或单位的网络信息系统的安全策略，能提高目前一些网络服务(如 Web 服务)的安全性。

与 DAC 和 MAC 相比，RBAC 技术也存在一定的不足。一方面，RBAC 技术还不十分成熟，在角色配置的工程化、角色动态转换等方面还需要进一步研究。此外有关 RBAC 实现技术的研究也需要进一步开展。另一方面，RBAC 比 DAC 和 MAC 复杂，系统实现难度大，再者，RBAC 的策略无关性需要用户自己定义适合本领域的安全策略，定义众多的角色和访问权限及它们之间的关系也是一件非常复杂的工作。

3.2 基于任务的访问控制技术

P. K. Thomas 等人认为传统的面向主体和客体的访问控制技术过于底层和抽象[13]，不便于描述应用领域的安全需要，于是他们从面向任务的观点出发提出了基于任务的授权控制模型 TBAC(Task-based Authorization Control)。该模型不足之处在于"比任何模型都复杂"[14]。

3.3 基于组机制的访问控制技术

1988年，R. S. Sandhu 等人提出了基于组机制的 NTree 访问控制模型[15]，之后这个模型又得到了进一步扩充，相继产生了多维模型 N-Grid 和倒影树模型。Nrree 模型的基础是偏序的维数理论，组的层次关系由维数为2的偏序关系(即 Ntree 树)表示，通过比较组节点在 Ntree 中的属性决定资源共享和权限隔离。该模型的创新在于提出了简单的组层次表示方法和自顶向下的组逐步细化模型。倒影树模型是 NTree 模型的一个特例，一棵倒立的树加上它的倒影就构成了一棵倒影树，倒影树的上半部分负责管理权利分离，倒影部分负责资源共享[16]，倒影树模型解决了组间资源共享问题。

除此之外，在九十年代还出现了一些其它的访问控制技术，如俄罗斯学者提出的基于加密的访问控制技术及 IBM 提出的基于进程间通信(IPC)的访问控制技术等，它们侧重于访问控制实现技术的研究，没有形成太大的影响。

4 访问控制技术的发展趋势

网络技术发展和系统安全需求多样化将会决定未来访问控制技术的发展趋势，具体表现为：

1. 计算机信息系统在不同应用领域的安全需求，将促进与安全策略无关的访问控制技术的研究，其中包括 RBAC 的进一步研究和发展。

2. 分布式和网络技术的发展使得分布式或网络环境下的访问控制技术将成为未来研究的热点。其中不同访问控制技术的统一和互联、协作组织间的网络信息系统访问控制技术、互连网环境下的访问控制技术将成为重要的研究课题。

3. 目前，信息安全受到前所未有的挑战，单一的安全技术很难保证系统的真正安全[14]。与其它安全技术

(下转第41页)

址短缺问题的解决方案。实验室共30余台机器，但是因为能够分配到的IP地址仅有三个，为了使所有机器能够自由地接入Internet，我们使用一台双Pentium® CPU的机器作为NAT router，安装两块Intel Ether Express网卡，分别使用内部地址192.168.5.2和外部地址202.119.37.8；软件使用RedHat Linux 6.0。在具有2.0.*以上版本的内核的Linux发行中，其中内含了ipchains，这是一个简单高效的透明网关的实现，其余30多台机器将网关设置为192.168.5.2即可实现透明访问Internet，利用ipchains的管理功能，还可以实现"黑名单"功能，如拒绝内部网络某些特定IP访问外部地址以及限制所有机器访问外部网络某些不健康的资源。唯一需要注意的是，这样的系统结构导致使用诸如NetBEUI协议工作的软件失效；在访问ftp的时候也需要显式指定使用PASV方式并且在NAT系统上使用对FTP协议的补丁模块。

结束语 在目前中小型网络环境中，NAT方案获得了广泛的应用，其应用领域已经从单纯的解决地址冲突扩展到了负载均衡、多穴路由等领域，而且由于IPv6的实用系统进展缓慢，决定了当前的IP协议体系还需要存在很长一段时间，NAT系统还会继续发展和完善。与此同时，虚拟私用网络(Virtual Private Network，VPN)的需求也在逐渐增强，这将导致IPSec安全体系的广泛采用。相信在IPv6没有普及开来之前，能够实施IPSec安全体系的变形NAT方案将成为对安全性有较高需求的私有网络的首选方案。

参考文献

1 周明天，汪文勇. 网络原理与技术. 清华大学出版社，1993
2 Using IPSec to Construct Secure Virtual Private Networks. IBM Corp，1998
3 Kent S，Atkinson R. IP Encapsulating Security Payload (ESP). RFC 2406，November 1998
4 Kent S，Atkinson R. Security Architecture for the Internet Protocol. RFC 2401，November 1998
5 Srisuresh P，Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663，August 1999
6 Srisuresh P，Tsirtsis G，Akkiraju P，Heffernan A. DNS extensions to Network Address Translators (DNS-ALG). RFC2694，September 1999
7 Hasenstein M. IP Network Address Translation. 1997

(上接第28页)

的结合也将成为访问控制技术的趋势之一，如具有人工智能特性的自适应访问控制技术、与入侵检测系统相结合的访问控制技术等。

参考文献

1 陈爱民，于康友，管海明编著. 计算机的安全与保密. 北京：电子工业出版社，1992. 141～145
2 America Department of Defense. TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA，CSC-STD-001-83，15 Aug 83
3 Harrison M H，Ruzzo W L，Ullman J D. Protection in Operating Systems. Communications of ACM，19(8)：461～471
4 Sandhu R S. The Typed Access Matrix Model. In Proc. of IEEE Symposium on Security and Privacy，Oakland. California，1992. 122～136
5 Sandhu R S，Ganta S. On Testing for Absence of Rights in Access Control Models. In Proc. of IEEE Computer Security Foundations Workshop VI，Franconia NH，1993. 109～118
6 Osborn S. Mandatory access control and role-based access control revisited. In：Proc. of the second ACM workshop on Role-based access control. November 1997. 31～40
7 Badger L. Controlled Execution UNIX. In：Proc. of the 17th National Computer Security Conf. 1994. 66～76
8 Brewer D E，Nash. The Chinese Wall Security Policy. IEEE Symposium on Security and Privacy，1989. 215～228
9 Sandhu R S. Lattice-Based Enforement of Chinese Walls. Comupters & Security，1992，11(8)：753～763
10 Smith Dr. C L，et al. A Survey to Determine Federal Agency Needs for a Role-Based Access Control Security Product. In Proc of the 3rd Int Software Engineering Standards Symposium(ISESS '97)，P222～232
11 Sandhu R S，Coyne E J，et al. Role-Based Access Control Models. IEEE Computer，1992，29(2)：38～47
12 Awischus R. Role based access control with the security administration manager (SAM). In：Proc. of the second ACM workshop on Role-based access control. November 1997. 61～68
13 Thomas R K，Sandhu R S. Task-base Authorization Controls (TBAC). A Family of Models for Active and Enterprise-oriented Authorization Management. In：Proc. of the IFIP WG11.3 Workshop on Database Security，California，August 1997
14 Denning D E. The Limits of Formal Security Models，America National Computer Systems Security Award Acceptance Speech，October1999
15 Sandhu R S. The Ntree：A Two Dimension Partial Order for Protection Groups. ACM Transactions on Computer Systems，1988，6(2). 197～222
16 The Reflected Tree Hierarchy for Protection and Sharing. Information Processing Leters，1989，30(1)