访问控制模型研究进展及发展趋势

李凤华[1,2],苏 铓[1],史国振[3],马建峰[1]
(1.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2.中国科学院信息工程研究所,北京 100195;3.北京电子科技学院电子信息工程系,北京 100070)

摘 要: 访问控制的任务是保证信息资源不被非法使用和访问,冲突检测与消解主要解决不同信息系统安全策略不统一的问题.随着计算机和网络通信技术的发展,先后出现了自主访问控制模型、强制访问控制模型、基于角色的访问控制模型、基于任务的访问控制模型、面向分布式和跨域的访问控制模型、与时空相关的访问控制模型以及基于安全属性的访问控制模型等访问控制模型.本文从理论和应用研究两个角度分析和总结了现有访问控制技术、访问控制策略冲突检测与消解方法的研究现状,提出了目前访问控制模型及其冲突检测与消解研究在面向信息物理社会的泛在网络互联环境中存在的问题,并给出了细粒度多级安全的访问控制模型及其策略可伸缩调整方法的发展趋势.

关键词: 访问控制; 冲突检测; 研究现状; 发展趋势
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2012) 04-0805-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.04.030

Research Status and Development Trends of Access Control Model

LI Feng-hua[1,2], SU Mang[1], SHI Guo-zhen[3], MA Jian-feng[1]
(1. *Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100195, *China*;
3. *Department of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*)

Abstract: The main task of access control is to prevent unauthorized accesses to information resources. Conflict detection and resolution mainly solves problems caused by various security policies among different information systems. With the development of computer and communication technology, several access control models have appeared such as discretionary access control, mandatory access control, role based access control, task-based access control, access control for distributed environment and cross-domain, spatiotemporal attribute based access control and security attribute based access control, etc. The paper analyzes and summarizes the existing domestic and international research situation in the field of access control and conflict detection and resolution from the theoretical research and application aspects, indicates exiting problems in ubiquitous networks for the cyber-physical society, and points out some development trends of fine-grained and multi-level security access control model and scalable method for its policy.

Key words: access control; conflict detection; present status; development trend

1 引言

访问控制技术是信息系统安全的核心技术之一,通过对用户访问资源的活动进行有效监控,使合法的用户在合法的时间内获得有效的系统访问权限,防止非授权用户访问系统资源.该技术兴起于20世纪70年代,最初是为了解决大型主机上共享数据授权访问的管理问题.根据访问控制策略类型的差异,早期的安全策略分为自主访问控制(Discretionary Access Control, DAC)和强制访问控制(Mandatory Access Control, MAC)两种类型.但是,随着计算机和网络技术的发展,DAC、MAC已经不能满足实际应用的需求,为此出现了基于角色的访问控制模型(Role-Based Access Control, RBAC[1,2]).RBAC将用户映射到角色,用户通过角色享有许可.该模型通过定义不同的角色、角色的继承关系、角色之间的联系以及相应的限制,动态或静态地规范用户的行为.作为现在访问控制模型研究的基石,RBAC一直是访问控制领域的研究热点,先后出现了RBAC96[2]、ARBAC97(Administra-

收稿日期:2011-06-08;修回日期:2011-11-20
基金项目:国家自然科学基金(No.61170251);教育部重点项目(No.209156);北京市自然科学基金(No.4102056);新闻出版重大科技工程项目-数字版权保护技术研发工程(No.GXTC-CZ-1015004/05)

tive RBAC97)[3]、ARBAC99[4]、ARBAC02[5]和 NIST RBAC (National Institute of Standards and Technology RBAC)[6]等一系列更加完善的基于角色的访问控制模型.RBAC 的出现基本解决了 DAC 由于灵活性造成的安全问题和 MAC 不支持完整性保护所导致的局限性问题,此后的数年间,访问控制模型的发展呈现出相对稳定的态势.访问控制技术迅速应用于信息系统的各个领域,与信息加密、身份认证、安全审计、入侵检测、系统恢复、风险分析和安全保障等理论和技术有机结合,实现了信息系统安全可靠的存储访问与传输,有效防止了非授权的信息访问和信息泄密[7,8].随着信息技术的发展以及分布式计算的出现,信息的交互从局域网逐渐转向广域网,各种信息系统通过因特网互联、互接的趋势越来越明显.单纯的 RBAC 模型已经不能适应这种新型网络环境的要求,为了保证信息访问的合法性、安全性以及可控性,访问控制模型需要考虑环境和时态等多种因素.在开放式网络环境下,信息系统要求对用户和信息资源进行分级的访问控制和管理,"域"的概念被引入了访问控制模型的研究中,先后出现了基于任务的访问控制模型、面向分布式的访问控制模型和与时空相关的访问控制模型.

泛在计算、移动计算、云计算等新型计算模式的出现推动了互联网的进步,同时也为访问控制模型的研究提出了新的挑战.在具有异构性和多样性特征的网络环境下,访问控制技术向细粒度、分层次的方向发展,授权依据开始逐渐面向主、客体的安全属性,出现了基于信任、基于属性和基于行为等一系列基于安全属性的新型访问控制模型及其管理模型.

2 基于任务的访问控制模型

随着数据库、网络和分布式计算的发展,组织任务进一步自动化,这促使人们将安全问题方面的注意力从独立的计算机系统中静止的主体和客体保护转移到随着任务的执行而进行动态授权的保护上.

1997 年 Thomas 等人采用"面向任务"的观点,提出了基于任务的访问控制模型 (Task-Based Access Control, TBAC),从任务的角度来建立安全模型和实现安全机制,在任务处理的过程中提供了动态实时的安全管理[9~11].该模型能够对不同工作流实行不同的访问控制策略,并且能够对同一工作流的不同任务实例实行不同的访问控制策略,适用于工作流、分布式、多点访问控制的信息处理以及安全工作流的管理.

2003 年,为了满足大型企业对安全信息管理的需求,出现了将 TBAC 和 RBAC 融合的基于任务 - 角色的访问控制模型(Task-Role Based Access Control, TRBAC)[12].随后,文献[13]在 RBAC 模型的基础上深入分析了转授权问题,提出了基于角色和任务的转授权模型 TRBDM(Task and Role-Based Delegation Model),但文献[13]仅是从概念角度引入了转授权的静态责任分离约束和动态责任分离约束,并未给出具体分析和相应的形式化表达.

从 20 世纪 90 年代开始,工作流技术引起了计算机安全领域研究人员的普遍关注.工作流是为完成某一目标而由多个相关任务构成的业务流程,它根据一系列定义的规则,使数据在不同的执行用户间进行传递与执行[14].当数据在工作流中流动时,执行操作的用户在不断改变,用户的权限也在改变,采用传统的访问控制技术已经不能满足动态授权的安全需求.2000 年 Knorr 在研究 Petri 网中工作流的动态访问控制的基础上,提出了利用工作流动态构建访问控制矩阵的方法[15].随后,文献[16]研究了工作流访问控制模型中用户的层次,设计了一种构建典型用户层次的方法,该方法可以直接应用于支持用户层次的 RBAC;文献[17]将 RBAC 应用于可扩展的工作流系统中,在确保工作流系统可扩展的前提下,该模型能够有效增强对授权访问工作流系统用户的安全控制.但是,这些文献缺乏对权责分离问题和工作流访问控制转授权问题的论述.

3 面向分布式和跨域的访问控制模型

随着分布式技术的飞速发展和普遍应用,出现了多种不同形式的分布式系统,协同工作和跨域访问是分布式系统中的两大特点,为此出现了基于团队的访问控制模型等针对分布式系统的访问控制模型.

3.1 基于团队的访问控制模型

基于团队的访问控制(Team-based access control, TMAC)[18]提供了一种以团队为核心,将 RBAC 用于团队协作环境的解决方法.TMAC 旨在解决协作环境中的两个安全需求,首先是混合访问控制模型的需求,该混合模型具有跨对象基于角色的权限,但需要对具有某些角色的个人用户和对象实施基于身份的细粒度访问控制.其次需要区分权限分配的被动概念和基于上下文授权激活的主动概念.Alotaiby 等人对该模型进行了扩展,提出 TMAC04 模型[19],该模型允许特定用户在上下文有限和新权限组织中现有角色的基础上加入团队执行所需的操作.

3.2 分布式基于角色的访问控制模型

一个分布式管理系统有多个不同的管理域,每个域中包含客户、服务器、域安全管理器和外域安全管理器.目标导向类访问控制模型(Object-oriented RBAC, ORBAC)[20]建立在分布式管理系统的基础上,能够完整的实现原始的 RBAC 模型,并且实现了多域访问控制.文献[21]基于 RBAC 提出了分布式基于角色的访问控

制模型(Distributed Role-Based Access Control,dRBAC).该模型利用 PKI 识别信任敏感操作实体的身份和验证委托证书,在跨多个管理域的动态协作环境中实现了资源的访问控制,为域间协作提供了一种可扩展的分布式信任管理和访问控制机制.文献[22]针对在分布式协同操作环境中基于角色的访问控制在利用角色映射的方式时可能存在的安全问题,提出了一种适用于分布式协同操作环境的 RBAC 模型(Role-Based Access Control model for distributed cooperation environment,RBAC-DC),但是该文献并未对模型中的角色层次和角色约束进行论述.为此,文献[23]提出的可约束的分布式 RBAC 模型,定义了适用于分布式远程资源共享服务的主体、角色、分布式角色、权限以及自组织的概念.该模型支持时态约束、势约束和上下文约束,从而能够支持访问控制更多的语义表达,并允许资源提供者和签署机构确定更高级别的安全组织策略.

3.3　基于开放式系统的访问控制模型

文献[24]提出的基于开放式系统的访问控制模型(Open Architecture for Securely Interworking Services RBAC,OASIS RBAC)是一种在开放的分布式环境中用于实现安全互操作的访问控制模型.该模型旨在使自主管理域指定其自身的访问控制策略,为了支持优先级管理,该模型引入了委派的概念,具有特定角色的用户能够利用委派证书授权其他用户.

3.4　基于域的访问控制模型

基于域的访问控制模型也是用于分布式系统间协同工作的模型,主要用于分散的多个管理者之间进行协同工作的多域应用环境.Shafiq 等人提出了基于域的访问控制模型,该模型是一种可以将多域间异构的 RBAC 策略统一应用于全局 RBAC 策略,并在不同的域之间实现资源安全共享的整合框架[25].该整合方法包括混合和消除冲突两个过程,首先将各个协作域的访问控制策略在全局系统中进行综合;之后以一种优化的方法在全局系统中对冲突的部分加以消除.文献[26]通过分析跨域计算网格、P2P 系统以及 WEB 服务等典型的分布式系统,提出了一种策略域访问控制模型(Policy Domain Access Control,PDAC),将分布式系统的节点抽象为一个域,并且为这个定义的域添加策略选择机制,从而使该域能够进行访问控制.但是文献[26]并未对 PDAC 模型的信任评估进行定义和论述.

3.5　使用控制模型

文献[27]提出的使用控制模型(Usage Control,UCON),主要研究传统的访问控制、信任管理、数字版权保护等问题.Park 等人将认证、职责和条件整合到 UCON 中,提出了一种扩展的 UCON,即 $UCON_{ABC}$模型[28].随后,文献[29]利用 Lamport 时序逻辑研究了 UCON 以及 $UCON_{ABC}$的逻辑规范;文献[30]对 UCON 模型进行了形式化分析,提出了使用现行时序逻辑进行 UCON 模型检测的方法;文献[31]通过构造形式化模型的方法得出一些使用控制模型的安全结论,并且分析了关于授权中使用控制模型($UCON_{onA}$)的安全性;文献[32]针对跨域访问过程中的协调性问题,提出了基于 UCON 的跨域访问模型(xDUCON);文献[33]通过对 Web 服务中使用访问控制的研究,将信任的概念引入跨域使用控制模型中;文献[34]将风险评估的方法引入 UCON 的授权机制中,提高了使用访问控制模型的灵活性和安全性.使用控制模型的提出主要是面向分布式环境的访问控制需求,文献[35]提出了一种分布式计算环境下使用控制的实施方案.虽然 UCON 模型在分布式、跨域环境下具有明显的优势,但是该模型的授权管理较为复杂.

4　与时空相关的访问控制模型

4.1　上下文相关的访问控制模型

传统的访问控制模型都是非上下文敏感的,需要复杂而静态的认证基础设施.此外,在某些应用中,与用户的标识相比,访问控制更加依赖于用户的上下文,上下文敏感的访问控制模型[36]应运而生.上下文相关的访问控制模型主要包含基于空间上下文的访问控制模型[37]、Location-aware RBAC[38~40]模型和 GEO-RBAC[41,42]模型.

在无线和移动网络中,有许多基于位置的服务和基于位置的移动应用程序,因而需要位置感知访问控制系统的支持.空间信息在这些模型中被看成是一个关键的上下文信息.文献[40]提出了一个形式化的访问控制模型 SC-RBAC 来保证位置感知应用程序的安全,通过引入空间角色的概念将空间上下文集成到角色中,并引入了逻辑位置域的概念来说明角色的空间边界,可根据用户的当前位置来判断会话中哪些角色是有效的,并为受限的 SC-RBAC 模型确定空间职责隔离限制、基于位置的基数限制和基于位置的时序限制.

Ardagna 提出的基于位置的访问控制模型(Location-Based Access Control)旨在将位置信息整合到普通的访问控制模型中,在进行访问授权时能够考虑用户的位置因素[41].在位置感知的应用程序中,用户经常被分为不同的类别,因此可以对 RBAC 模型加以改进和扩展,使其支持基于位置和空间的访问控制.Ray 等人提出了一种位置感知的 RBAC 模型,将 RBAC 中的组件和位置信息联系起来,并根据位置信息确定一个主体对客体是否具有访问权限[42,43].该模型讨论了 RBAC 中不同组件与位置的关系,但没有考虑到时态和环境对访问控制的影响.

为了给实际的移动应用提供一种完整的可扩展的空间上下文访问控制模型框架,Bertino 等人对基于空间和位置的 RBAC 模型进行扩展,提出了 GEO-RBAC 访问控制模型[41,42],该模型具有两个显著特征:一是利用空间实体来描述客体、用户位置和基于地理位置的角色,角色通过用户的位置进行激活;二是支持物理位置和逻辑位置.针对以往空间数据的访问控制中不能同时支持矢量数据和栅格数据,并且效率较低的问题,文献[43]提出一种面向空间索引树的访问控制模型,该模型为栅格数据和矢量数据提供了更为有效的访问控制方法.

4.2 基于时态的访问控制模型

现有的 RBAC 等访问控制模型对时间约束的支持功能相对简单,对时态对象的存取控制建模能力弱.在绝大多数信息系统中,时间因素无处不在,用户仅在特定的时间段具有特定的角色,因此迫切需要 RBAC 模型能够支持复杂的时间约束建模.

文献[44]提出了一种基于时态特性的访问控制模型(Temporal Role-Based Access Control, TRBAC),将时态约束加入到 RBAC 中.该模型带有时态约束,但是没有考虑对用户 - 角色分配和角色 - 权限分配的时态因素.文献[45]提出的时态模型把模型要素及其关系上的时态约束嵌入到模型中,通过定义新的时态继承机制实现动态基于角色的存取控制,该模型能够有效减少约束规则库中的规则数量,提高存取控制效率;文献[46]将基于时态特征的访问控制模型中的单一主体扩展为多主体,使其更适合现有的复杂网络环境.TRBAC 模型仅对角色增加了时态约束,并未对其他要素增加约束.Joshi 等人提出的通用基于时态的访问控制模型(Generalized Temporal Role-Based Access Control,GTRBAC)是对 TRBAC 的扩展[47],该模型提供了更加广泛的时态约束,并且支持细粒度的基于时态的访问控制策略.文献[48,49]分别提出了基于时态特征的位置感知 RBAC 模型(Temporal and Location-based RBAC,TLRBAC)和基于尺度的时空 RBAC 模型(Role-Based Access Control Model Based on Space,Time and Scale STS-RBAC).

5 基于安全属性的访问控制模型

5.1 基于信任的访问控制模型

Sudip Chakrabony 等在文献[50]中提出了基于信任的访问控制模型 TrustBAC(Trust based access control model).该模型首先为用户划分信任级,然后通过信任级别决定角色.文献[51]将时态的概念引入 TrustBAC 模型中,为诸如在线应用等细粒度访问控制规则的制定提供了更为灵活的方法.文献[52]针对信任的主观性、模糊性与不确定性,建立了包括信任综合评价与信任计算的信任度量化模型.

5.2 基于属性的访问控制模型

基于属性的访问控制(Attribute-Based Access Control,ABAC)针对目前复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题,将实体属性(组)的概念贯穿于访问控制策略、模型和实现机制三个层次,通过对主体、客体、权限和环境属性的统一建模,描述授权和访问控制约束,使其具有足够的灵活性和可扩展性.该机制广泛应用于大型分布式环境[53,54]、Web 服务系统[55~57]、网格计算[58]以及消息共享和管理[59,60]中.文献[61]针对云计算存储服务中服务提供者信任域不同的特点,提出了一种基于属性的细粒度分层访问控制机制 HBAE(Hierarchical Attribute-Based Encryption),并且对约束条件进行了描述.文献[62]则针对云存储基于密文的访问控制问题,提出了一种云存储密文访问控制方法 AB-ACCS,通过控制数据的密文属性进行权限管理,有效地降低了权限管理的难度.

5.3 基于行为的访问控制模型

随着移动互联网和移动计算的广泛应用,多网融合的通信网络系统已是一个异构的、开放的、分布式的和支持移动计算的网络系统.各种网络、信息系统通过 Internet 互联的趋势越来越明显,从而满足了人们日益增长的开放互联的个性化服务需求,这决定了在开放网络环境下传播信息的方式是多样化的.虽然上述部分模型中已考虑了与访问控制相关的时态因素和位置因素,但现有的模型都没有对移动计算下角色所处环境(各种客观因素组成的环境要素,如场所物理位置、网络位置、逻辑位置、硬件平台、软件平台等)对访问控制的影响进行详细分析,故上述模型无法支持开放网络环境下的移动计算.为此,文献[63]提出了“行为”的概念,综合角色、时态状态和环境状态等相关安全信息,提出了基于行为的访问控制模型(Action-Based Access Control,ABAC),文献[64]讨论了该模型中角色、时态状态和环境状态之间的相互关系,并且对行为状态管理函数进行了形式化描述.通过将角色、时间和环境综合考虑,可以使 ABAC 灵活地处理各种信息系统中的访问控制问题.文献[65]基于 ABAC 模型,针对协作信息系统面临的资源授权决策问题,提出了协作信息系统访问控制机制的流程,并给出了相应的安全关联及其产生方法,以及一种安全认证协议.文献[66]给出了一种基于 ABAC 应用于 Web 服务的安全体系结构.

该 ABAC 模型继承了传统访问控制中角色和角色控制的理念,综合考虑了时态和环境约束,而且支持移动计算中接入用户、接入位置、接入的具体业务以及接入平台随机和不可预知的特点,具有更为广泛的应用

范围,该模型能够更加有效地解决网络环境下支持移动计算的信息系统中的访问控制问题.但是行为中角色、时态、环境三者之间的约束关系和管理策略问题还有待进一步研究.

6 策略冲突检测与消解

由于不同信息系统之间的差异,相应的安全策略存在策略不一致、语义不同或相互矛盾的问题,指定的措施或给定的结论之间也存在着相互抵触的情况.这些都有可能造成访问控制的错误裁决,因此,消解访问控制策略的冲突至关重要.访问控制技术的研究提出了大量的检测与消除方法[67,68].文献[68]提出了一种基于 ponder 语言的角色、域和元素的策略冲突检测与消解方法;访问控制策略标记语言 XACML[69,70]基于属性匹配机制定义了策略规则,在传统的分布式环境的访问控制策略的执行中得到了广泛应用.XACML 标准包含了冲突检测算法,能够减少策略冲突对访问请求的影响.文献[71]分析了 XACML 中属性层次操作关联引发的各种规则冲突类型,给出了基于属性层次操作关联的冲突检测算法和基于状态相关性的其他类型冲突检测算法.Bonatti 等[72]针对基于属性的访问控制,将访问控制策略形式化为主体、客体和行为三元组授权集合,用合成代数组合安全策略,利用逻辑设计和局部评估技术来评估代数表达式,从而实现冲突的检测与消解.文献[73]则提出了基于逻辑编程的策略冲突检测与消解方法;文献[74]通过对分布式系统中元素之间的关系进行研究,统一抽象出有向无环图,提出了一种基于有向图的冲突检测方法.文献[75]以有限自动机理论为基础,提出了相应的冲突检测方法.但是上述方法仅仅针对某种特定的安全策略,缺乏扩展性,而且算法复杂度较大.

针对分布式系统节点内的冲突检测问题,文献[76]提出了通过状态转换方式进行冲突检测的方案.为了解决冲突检测机制依赖于管理员的问题,文献[77]提了一种应用于可信可控网络的冲突检测机制.多级安全策略冲突与消除技术由于等级保护环境下信息系统多级、分布的特征而变得更为复杂,国内外在该方面的研究较少.如何在泛在网络环境下结合新型的访问控制策略进行冲突的检测与消解仍需进一步研究.

7 发展趋势

经过了近五十年的发展,访问控制模型的研究取得了丰硕成果.结构化文档[78]等新型网络信息表现方式的出现,加速了信息传播速度,也带来了对象化、细粒度的安全分级数据管理问题;泛在计算、移动计算、云计算满足了人们日益增长的开放互联的个性服务需求,也带来了新的访问控制问题.面向信息物理社会的泛在网络互联环境,基于分布式、不确定、动态交互的分布式计算、移动计算、云计算和泛在计算等计算模式的信息传播与访问方式,现有的访问控制模型不能解决结构化文档的实时动态重组、多级安全和细粒度控制而引起的策略可伸缩调整、策略冲突与消解、结构化文档内容变更轨迹的过程追踪与回溯等新的访问控制安全问题.现有的访问控制模型虽然已逐步考虑了与安全相关的时空因素和环境因素,但是仍然有许多尚待解决的问题.访问控制技术的发展将呈现如下趋势:

(1)如何面向信息物理社会的泛在网络互联环境中分布式计算、移动计算、云计算和泛在计算等计算模式的信息传播与多模式访问方式,研究细粒度多级安全的访问控制模型及其策略;

(2)针对用户移动办公时跨域、跨终端显现/处理设备等环境状态改变和时间状态变更时,研究访问权限的可伸缩性动态调整方法;

(3)研究区域网络边界内部策略和多级互联外部策略冲突与消解方法,研究多级安全策略冲突检测与消解模型;

(4)研究结构化文档内容变更轨迹或访问授权的过程追踪与回溯方法.

参考文献

[1] D F Ferraiolo, D R Kuhn. Role-based access control [A]. In Proceedings of the 15th National Computer Security Conference [C]. Baltimore, USA, 1992, 08. 554 – 563.

[2] R Sandhu, E Coyne, H Feinstein, et al. Role-based access control models [J]. IEEE Computer, 1996, 02, 29(2): 38 – 47.

[3] R Sandhu, V Bhamidipati, Q Munawer. The ARBAC97 model for role-based administration of roles [J]. ACM Transactions on Information and System Security, 1999, 02, 2(1): 105 – 135.

[4] R Sandhu, Q Munawer. The ARBAC99 model for administration of roles [A]. In Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99) [C]. Scottsdale, AZ, USA, IEEE Computer Society, 1999, 12. 229 – 238.

[5] S Oh, R Sandhu, X W Zhang. An effective role administration model using organization structure [J]. ACM Transactions on Information and System Security, 2006, 05, 9(2): 113 – 137.

[6] D F Ferraiolo, R Sandhu, S Gavrila, et al. Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 08, 4(3): 224 – 274.

[7] J Ma, K Adi, M Mejri, et al. Risk analysis in access control systems [A]. In Proceedings of the Eighth Annual International Conference on Privacy, Security and Trust [C]. Ottawa, ON, IEEE Press, 2010, 08. 160 – 166.

[8] C Y Pang, D Hansen, A Maeder. Managing RBAC States with transitive relations [A]. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (ASIACCS'07) [C]. Singapore, 2007, 03. 139 – 148.

[9] R Thomas, R Sandhu. Task-based authorization controls (TBAC): A Family of models for active and enterprise oriented authorization management [A]. In Proceedings of the 11th IFIP WG11. 3 Conference on Database Security [C]. Lake Tahoe, 1997, 08. 166 – 181.

[10] G Coulouris, J Dollimore, M Roberts. Role and task-based access control in the PerDiS groupware platform [A]. In Proceedings of the 3rd ACM Workshop Role-Based Access Control[C]. Fairfax, VA, USA, ACM Press, 1998, 10. 115 – 121.

[11] 邓集波,洪帆.基于任务的访问控制模型 [J].软件学报, 2003, 01, 14(1): 76 – 81.
Deng Ji-bo, Hong Fan. Task-based access control model [J]. Journal of Software, 2003, 01, 14(1): 76 – 81(in Chinese).

[12] O Sejong, P Seog. Task-role-based access control model [J]. Information System, 2003, (28): 533 – 562.

[13] 朱君.角色协同中群体感知和访问控制技术研究[D].广州:中山大学计算机软件与理论博士学位论文.2009.
Zhu Jun. Research on group awareness and access control technology of role cooperation [D]. Guangzhou: Computer Science of Sun Yat-sen University. 2009(in Chinese).

[14] E Bertino, E Ferrari, V Atluri. The specification and enforcement of authorization constraints in workflow management systems [J]. ACM Transaction on Information System Security, 1999, 02, 2(1): 65 – 104.

[15] K Knorr. Dynamic access control through Petri net workflows [A]. In Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00) [C]. Washington, DC, USA, IEEE Computer Society, 2000, 12. 159 – 167.

[16] R Botha, J Eloff. Designing role hierarchies for access control in workflow systems [A]. In Proceedings of the 25th International Computer Software and Applications Conference on Invigorating Software Development (COMPSAC'01) [C]. Washington, DC, USA, IEEE Computer Society, 2001, 10. 117 – 122.

[17] Y Q Sun, X X Meng, S J Liu, et al. Flexible workflow incorporated with RBAC [A]. In Proceedings of the 9th International Conference in Computer Supported Cooperative Work in Design (CSCWD'05) [C]. UK, LNCS 3865, 2005. 525 – 534.

[18] R Thomas. Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments [A]. In Proceedings of 2nd ACM Workshop on Role-based Access Control [C]. New York, US, 1997, 12. 13 – 19.

[19] F T Alotaiby, J X Chen. A model for Team-based access control (TMAC 2004) [A]. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) [C]. IEEE Computer Society, 2004, 04. 450 – 454.

[20] C N Zhang, C G Yang. An Object-oriented RBAC model for distributed system [A]. In Proceedings of the Working IEEE/IFIP Conference on Software Architecture (WICSA'01) [C]. Amsterdam, Netherlands, IEEE Press, 2001, 08. 24 – 32.

[21] E Freudenthal, T Pesin, L Port, et al. dRBAC: Distributed role-based access control for dynamic coalition environments [A]. In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02) [C]. Vienna, Austria, IEEE Computer Society, 2002, 07. 411 – 420.

[22] S Y Liu, H J Huang. Role-based access control for distributed cooperation environment [A]. In Proceedings of 2009 International Conference on Computational Intelligence and Security [C]. Beijing, China, IEEE Computer Society, 2009, 12. 455 – 459.

[23] M C Ma, S Woodhead. Constraint-enabled distributed RBAC for subscription-based remote network services [A]. In Proceedings of the Sixth IEEE International Conference on Computer and Information Technology (CIT'06) [C]. 2006, 09. 01 – 06.

[24] W Yao, K Moody, J Bacon. A model of OASIS role-based access control and its support for active security [J]. ACM Transactions on Information and System Security, 2002, 06, 5 (4): 492 – 540.

[25] B Shafiq, J B D Joshi, E Bertino, et al. Secure interoperation in a multi domain environment employing RBAC policies [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 11, 17(11): 1557 – 1577.

[26] X Wu, P D Qian. Research on policy domain access control model in distributed systems [A]. In Proceedings of Nine International Conference on E-Business and Information System Security [C]. WuHan, China, IEEE Press, 2009, 05. 01 – 06.

[27] J Park, R Sandhu. Towards usage control models: beyond traditional access control [A]. In Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT'02) [C]. Monterey, California, USA, 2002, 06. 57 – 64.

[28] J Park, R Sandhu. The $UCON_{ABC}$ usage control model [J]. ACM Transactions on Information and System Security, 2004, 02, 7(1): 128 – 174.

[29] X W Zhang, J Park, F Parisi, et al. A logical specification for usage control [A]. In Proceedings of the 9th ACM symposium on Access control models and technologies (SACMAT'04) [C]. Yorktown Heights, New York, USA, 2004, 06. 01 – 10.

[30] A Pretschner, J Ruesch, C Schaefer, et al. Formal analyses of usage control policies [A]. In Proceedings of the International Conference on Availability, Reliability and Security [C]. Fukuoka, Japan, IEEE Computer Society, 2009, 03. 98 – 105.

[31] Z G Zhai, J D Wang, Y G Mao. Study and safety analysis on $UCON_{onA}$ model [A]. In Proceedings of the First International Workshop on Database Technology and Applications [C]. Wuhan, China, IEEE Computer Society, 2009, 04. 103 – 106.

[32] G Russello, N Dulay. xDUCON: Coordinating usage control policies in distributed domains [A]. In Proceedings of the Third International Conference on Network and System Security [C]. Gold Coast, QLD, IEEE Computer Society, 2009, 10. 246 – 253.

[33] G P Zhang, W T Gong, J Z Tian. The research of cross-domain usage control model in web services [A]. In Proceedings of the Second International Conference on e-Business and Information System Security [C]. Wuhan, China, IEEE Press, 2010, 03. 01 – 05.

[34] L Krautsevich, A Lazouski, F Martinelli, et al. Risk-aware Usage Decision Making in Highly Dynamic Systems [A]. In Proceedings of the Fifth International Conference on Internet Monitoring and Protection [C]. Barcelona, ESP, IEEE Computer Society, 2010, 05. 29 – 34.

[35] 初晓博,秦宇.一种基于可信计算的分布式访问控制研究 [J].计算机学报,2010,33(1):93 – 102.
Chu Xiao-bo, Qin Yu. A distributed usage control system based on trusted computing [J]. Chinese Journal of Computers, 2010, 33(1): 93 – 102(in Chinese).

[36] M J Covington, W Long, S Srinivasan. Securing context-aware applications using environment roles. In Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. ACM Press, Chantilly, Virginia, USA, 2001, 05. 10 – 20.

[37] 张宏,贺也平,石志国.一个支持空间上下文的访问控制形式模型 [J].中国科学 E 辑 :信息科学,2007,02,37(2):254 – 271.
Zhang Hong, He Ye-ping, Shi Zhi-guo. A formal model for access control with supporting spatial context [J]. Science in China Series F: Information Sciences, 2007, 50(3): 419 – 439.

[38] C Ardagna, M Cremonini, E Damiani, et al. Supporting location-based conditions in access control policies [A]. In Proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS'06) [C]. Taipei, Taiwan, ACM Press, 2006. 212 – 222.

[39] I Ray, L J Yu. Short paper: towards a location-aware role-based access control model [A]. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks [C]. Athens, Greece, IEEE Computer Society, 2005, 09. 234 – 236.

[40] I Ray, M Kumar, L J Yu. LRBAC: a location-aware role-based access control model [A]. In Proceedings of the Second International Conference on Information Systems Security (ICISS 2006) [C]. Kolkata, India, Springer-Verlag, 2006. 147 – 161.

[41] E Bertino, B Catania, M Damiani, et al. GEO-RBAC: A spatially aware RBAC [A]. In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies [C]. New York, ACM Press, 2005, 07. 29 – 37.

[42] M Damiani, E Bertino, B Catania. GEO-RBAC: a spatially aware RBAC [J]. ACM Transactions on Information and System Security, 2007, 02, 10(1): 01 – 42.

[43] 张颖君,冯登国,陈恺.面向空间索引树的授权机制 [J].通信学报,2010,09,31(9):64 – 73.
Zhang Ying-jun, Feng Deng-guo, Chen Kai. Authorization mechanism based on spatial index [J]. Journal on Communications, 2010, 09, 31(9): 64 – 73.

[44] E Bertino, P Bonatti, E Ferrari. TRBAC: A Temporal Role-Based Access Control Model [J]. ACM Transactions on Information and System Security, 2001, 08, 4(3): 191 – 223.

[45] 王小明,赵宗涛.基于角色的时态对象存取控制模型 [J].电子学报,2005,09,33(9):1634 – 1638.
Wang Xing-ming, Zhao Zong-tao. Role-based access control model of temporal object [J]. Acta Electronica Sinica, 2005, 33(9): 1634 – 1638(in Chinese).

[46] C Z Xu, Q X Wang, W M Zhang, et al. Temporal Access Control based on Multiple Subjects [A]. In Proceedings of International Conference on Multimedia Information Networking and Security [C]. HuBei, China, IEEE Computer Society, 2009, 11. 438 – 441.

[47] J B D Joshi, E Bertino, U Latif, et al. A generalized temporal role-based access control model [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 01, 17(1): 04 – 23.

[48] H C Chen, S J Wang, J H Wen, et al. Temporal and location-based RBAC model [A]. In Proceedings of the Fifth International Joint Conference on INC, IMS and IDC [C]. Seoul, Korea, IEEE Computer Society, 2009, 08. 2111 – 2116.

[49] 张颖君,冯登国.基于尺度的时空 RBAC 模型 [J].计算机研究与发展,2010,47 (7):1252 – 1260.
Zhang Ying-jun, Feng Deng-guo. A role-based access control model based on space, time and scale [J]. Journal of Computer Research and Development, 2010, 47 (7): 1252 – 1260(in Chinese).

[50] S Chakraborty, I Ray. TrustBAC: integrating trust relationships into the RBAC model for access control in open systems [A]. In Proceedings of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT'2006) [C]. California, USA, 2006, 07. 49 – 58.

[51] C Z Xu, Y Q Wang, Q Wei, et al. A novel trust model based on temporal historical data for access control [A]. In Proceedings of the International Conference on Computational Intelligence and Security [C]. Beijing, China, IEEE Computer Society, 2009, 12. 446 – 449.

[52] 郎波. 面向分布式系统访问控制的信任度量化模型 [J]. 通信学报, 2010, 31(12): 45 – 54.
Lang Bo. Access control oriented quantified trust degree representation model for distributed systems [J]. Journal on Communications, 2010, 31(12): 45 – 54(in Chinese).

[53] 李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型 [J]. 通信学报, 2008, 04, 29(4): 90 – 98.
Li Xiao-feng, Feng Deng-guo, Chen Zhao-wu, et al. Model for attribute based access control [J]. Journal on Communications, 2008, 04, 29(4): 90 – 98(in Chinese).

[54] 王小明, 付红, 张立臣. 基于属性的访问控制研究进展 [J]. 电子学报, 2010, 07, 38(7): 1660 – 1667.
Wang Xiao-ming , Fu Hong , Zhang Li-chen. Research progress on attribute-based access control [J]. Acta Electronica Sinica, 2010, 07, 38(7): 1660 – 1667(in Chinese).

[55] M Coetzee, J H P Eloff. Towards web service access control [J]. Computers and Security, 2004, 23(7): 559 – 570.

[56] V S Mewar, S Aich, S Sural. Access control model for web services with attribute disclosure restriction. In Proceedings of the Second International Conference on Availability, Reliability and Security [C]. Washington , IEEE Computer Society, 2007, 04. 524 – 531.

[57] B Lang, N Zhao, K Ge, et al. An XACML policy generating method based on policy view [A]. In Proceedings of International Conference on Pervasive Computing and Applications [C]. IEEE Press, 2008, 1. 295 – 301.

[58] R Laborde, M Kamel, S Wazan, et al. A secure collaborative web based environment for virtual organizations [J]. International Journal of Web Based Communities, 2009, 05(2): 273 – 292.

[59] M Pirretti, P Traynor, P McDaniel, et al. Secure attribute-based systems [A]. In Proceedings of the 13th ACM Coference on Computer and Communication Security [C]. New York, ACM. 2006. 99 – 112.

[60] V Goyal, O Pandey, A Sahai, et al. Attribute-based for encryption for fine-grained access control of encrypted data [A]. In Proceedings of the 13th ACM Conference on Computer and Communications Security [C]. New York, USA, ACM Press, 2006. 89 – 99.

[61] G J Wang, Q Liu, J Wu. Hierarchical attribute-based encryption for fine-grained access control in cloud storageservices [A]. In Proceedings of the 17th ACM conference on Computer and communications security [C]. New York, NY, USA, ACM Press, 2010. 735 – 737.

[62] 洪澄, 张敏, 冯登国. AB-ACCS: 一种云存储密文访问控制方法 [J]. 计算机研究与发展, 2010, 47(z1): 259 – 265.
Hong Cheng, Zhang Min, Feng Deng-guo. AB-ACCS: A cryptographic access control scheme for cloud storage [J]. Journal of Computer Research and Development, 2010, 47(z1): 259-265(in Chinese).

[63] F H Li, W Wang, J F Ma, et al. Action-based access control model [J]. Chinese of Journal Electronics, 2008, 07, 17(3): 396 – 401.

[64] 李凤华, 王巍, 马建峰, 等. 基于行为的访问控制模型及其行为管理 [J]. 电子学报, 2008, 10, 36(10): 1881 – 1890.
Li Feng-hua, Wang Wei, Ma Jian-feng, et al. Access control model and Administration of action [J]. Acta Electronica Sinica, 2008, 10, 36(10): 1881 – 1890(in Chinese).

[65] 李凤华, 王巍, 马建峰, 等. 协作信息系统的访问控制模型及其应用 [J]. 通信学报, 2008, 09, 29(9): 116 – 123.
Li Feng-hua, Wang Wei, Ma Jian-feng, et al. Access control model and its application for collaborative system [J]. Journal on Communications. 2008, 09, 29(9): 116 – 123(in Chinese).

[66] F H Li, W Wang, J F Ma, et al. Action-based access control for web services [A]. In Proceedings of Fifth International Conference on Information Assurance and Security [C]. Xi' an, China, IEEE Computer Society, 2009, 08. 637 – 642.

[67] E Lupu, M Sloman. Conflicts in policy-based distributed systems management [J]. IEEE Transactions on Software Engineering Management-Special Issue on Inconsistency Management, 1999, 11, 26(6): 852 – 869.

[68] N Dulay, E Lupu, M Sloman, et al. A policy deployment model for the ponder language [A]. In Proceedings of the IEEE/IFIP International Symposium on Integrated Network Management (IM'2201) [C]. Seattle, 2001. 01 – 12.

[69] OASIS. XACML 3.0 work in progress [S]. 2009, 09.

[70] OASIS. XACML v3.0 administrative policy version 1.0 [S]. 2009.

[71] 王雅哲, 冯登国. 一种 XACML 规则冲突及冗余分析方法 [J]. 计算机学报, 2009, 32(3): 516 – 530.
Wang Ya-zhe, Feng Deng-guo. A conflict and redundancy analysis method for XACML rules [J]. Chinese Journal of Computers. 2009, 32(3): 516 – 530(in Chinese).

[72] P Bonatti, S D Vimercad, P Samarali. An algebra for composing access control policies [J]. ACM Transactions on Information and System Security, 2002, 05(1): 01 – 35.

[73] J Lobo, R Bhatia, S Naqvi. A policy description language [A]. In Proceedings of the sixteenth National Conference on Artificial Intelligence (AAAI – 99) [C]. Orlando, Florida, 1999, 07. 291 – 298.

[74] 姚键,茅兵,谢立.一种基于有向图模型的安全策略冲突检测方法[J].计算机研究与发展,2005,42(7):1108-1114.
Yao Jian, Mao Bing, Xie Li. A DAG-based security policy conflicts detection method [J]. Journal of Computer Research and Development, 2005, 42(7): 1108-1114(in Chinese).

[75] C Basile, A Lioy. Towards an Algebraic Approach to Solve Policy Conflicts [M]. FCS'04, 2004.

[76] X D Dai, X Y Chen, Y L Wang, et al. An improved state transition-based security policy conflict detection algorithm [A]. In Proceedings of the 2010 International Conference on Computational and Information Sciences (ICCIS2010) [C]. Chengdu, Szechwan, China, 2010, 12. 609-612.

[77] 曲延盛,罗军舟,李伟 等.可信可控网络资源控制的冲突检测机制[J].通信学报,2010,31(10):79-87.
Qu Yan-sheng, Luo Jun-zhou, Li Wei, et al. Resource control conflict detection mechanism in trustworthy and controllable network [J]. Journal on Communications, 2010, 31(10): 79-87

[78] 汤帜.新一代结构化版式文档技术[OL]. http://www.ccf.org.cn/resources/2567814757318/tang12242010-12-24-03_32_00.pdf.

作者简介

李凤华　男,1966 年 3 月出生于湖北省浠水县,中国科学院信息工程研究所、博士、博士生导师,主要研究方向为网络安全与可信计算.
E-mail:lfh@iie.ac.cn

苏　铓　女,1987 年 12 月出生于内蒙古赤峰市,西安电子科技大学博士研究生,主要研究方向为访问控制与网络安全.
E-mail:sm1222@163.com

史国振　男,1974 年 6 月出生于河南济源市,北京电子科技学院副教授、博士,研究方向为信息安全和系统软件设计.
E-mail:sgz@besti.edu.cn

马建峰　男,1963 年 10 月出生于陕西省西安市,西安电子科技大学计算机学院院长、博士、教授、博士生导师,主要研究方向为密码学与网络安全.
E-mail:jfma@mail.xidian.edu.cn