基于属性的访问控制研究进展

王小明,付 红,张立臣
(陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 基于属性的访问控制(ABAC)能够解决开放网络环境下资源保护所面临的细粒度问题以及网络系统所面临的大规模用户问题,为未来的开放网络环境提供了较为理想的访问控制策略方案.本文从ABAC理论和应用研究两个方面详细分析和总结了ABAC国内外的现有研究成果,分析了ABAC研究尚待解决的问题及未来研究趋势,为未来开放网络环境中的复杂信息系统访问控制研究提供借鉴和文献参考.

关键词: 安全策略;访问控制;实体属性;形式化模型;ABAC
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 07-1660-08

Research Progress on Attribute-Based Access Control

WANG Xiao-ming, FU Hong, ZHANG Li-chen
(*School of Computer Science and Technology, Shaanxi Normal University, Xi'an, Shaanxi 710062, China*)

Abstract: Attribute-Based Access Control (ABAC) can address the issues of the fine-granularity of resource protection and the user scalability of network systems, and it can provide appropriate strategies for the access control in the open network environment in the future. This paper in detail analyzes and summarizes the existing domestic and international research achievements in the area of Attribute-Based Access Control from two aspects of the theoretical researches and application researches of ABAC, also analyzes the problems waiting to be solved and some research trends in the area of the ABAC research in the future. It may provide some new insights and literature references for the research of the access control of complex information systems in the open network environment in the future.

Key words: security policy; access control; ABAC; entity attribute; formal model

1 引言

访问控制(access control)技术依据预先定义的访问授权策略授予主体(subject)访问客体(object)的权限(right),并对主体使用权限的过程进行有效控制,从而实现系统资源的授权访问,防止非授权的信息泄露,是确保计算系统安全的核心技术之一[1].基于属性的访问控制(Attribute Based Access Control, ABAC)能解决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[2],为开放网络环境提供了较理想的访问控制方案.因此,ABAC已成为复杂计算系统安全领域国内外目前研究的热点.

众所周知,现实生活中的实体可以通过实体特性(组合)来进行有效区分,这种可以对实体进行区分的实体特性称为实体属性(attribute).使用实体属性这个核心概念对主体、客体、权限及授权约束进行统一描述,用属性或属性组来区分不同的实体,用实体属性之间的关系对安全需求进行形式化建模,能够有效解决分布式开放环境下的细粒度访问授权和大规模用户动态扩展问题.但是,传统的访问控制方法并没有把属性概念作为独立要素纳入访问控制策略模型之中进行建模.虽然近年来提出的一些访问控制策略模型用约束(constraint)概念把实体的某些属性纳入到访问控制决策过程之中,但是实体依然用唯一的身份标识来区分,实体属性特征仅仅作为访问控制决策约束参与访问控制决策,这类访问控制策略模型在分布式开放环境下面临的问题是实体属性的语义往往不明确,缺乏统一性;当系统规模增大时,约束规则数量面临爆炸性增长,从而导致访问控制系统效率低下.

ABAC把实体属性(组)概念贯穿于访问控制策略、模型和实现机制三个层次,把与访问控制相关的时间、实体空间位置、实体行为、访问历史等信息当作主体、客体、权限和环境的属性来统一建模,通过定义属性之间的关系描述复杂的授权和访问控制约束,能够灵活地表

收稿日期:2009-03-24;修回日期:2010-01-14
基金项目:国家自然科学基金(No.60773224, No.60970054);教育部科学研究重点项目(No.107106);教育部留学回国人员科研启动基金

达细粒度、复杂的访问授权和访问控制策略,从而增强访问控制系统的灵活性和可扩展性.ABAC 的突出优点是它具备强大的表达能力[3].属性可以从不同的视角描述实体.用属性描述的策略可以表达基于属性的逻辑语义,灵活地描述访问控制策略.如果将传统访问控制中的身份、角色以及资源安全密级等信息抽象化为实体属性,ABAC 则能有效实现传统访问控制模型的功能.

总之,ABAC 能够解决传统访问控制难以解决的细粒度访问控制和面向大规模主体动态授权的问题,并具有很强的灵活性和良好的可扩展性,是未来开放网络环境中较为理想的访问控制策略模型,具有广阔的应用前景.本文从 ABAC 的理论研究和应用研究两个方面详细分析和总结 ABAC 国内外现有研究成果,并对 ABAC 亟待解决的问题及未来研究趋势进行讨论,为未来开放网络环境中的复杂信息系统访问控制研究提供新思路和文献参考.

2　ABAC 基本概念

目前,ABAC 还没有统一的形式化定义.本文借鉴文献[4]对 ABAC 形式化定义如下:

定义 1　ABAC 是一个四元组(S,O,P,E),其中 S,O,P 和 E 分别是由主体属性、客体属性、权限属性和环境属性确定的主体、客体、权限和环境集合.

为描述简便,以下把主体、客体、权限和环境统称为实体(entity).于是,实体共有四种类型:主体类(s),客体类(o),权限类(p)和环境类(e),实体类型全体为$\{s,o,p,e\}$.每一类实体其特征用一组属性变量描述.

定义 2　实体属性是描述实体固有特征的变量.实体属性值是实体属性变量的取值.实体属性变量的取值范围称为该属性变量的域(domain).

定义 3　实体模式是对实体属性的描述,形式表示为 $X(U,D,dom,F)$,其中 X 是实体名,U 为刻画该类实体的属性变量集合,D 为 U 中属性变量的域,dom 为属性变量到属性变量域的指派(assign) $dom:U\rightarrow D$,F 为属性变量值之间的依赖关系,用来对属性之间的复杂关系进行描述.

实体模式通常简记为 $X(x.a_1,x.a_2,\cdots,x.a_n)$,其中 X 为实体名,$x.a_1,x.a_2,\cdots,x.a_n$ 为实体属性变量名,$x\in\{s,o,p,e\}$,x 决定 X 属于哪一类实体;域名及属性向域的指派通常直接说明为属性的类型[5].

定义 4　属性元组是实体模式的实例.对实体模式 $X(x.a_1,x.a_2,\cdots,x.a_n)$,其属性元组形式为 $<x.v_1,x.v_2,\cdots,x.v_n>$,表示各属性值分别为 $v_1,v_2,\cdots,v_n$ 的 x 类实体集合,其中 $x\in\{s,o,p,e\}$.

在开放环境下,实体模式通常是静态、相对稳定的,属性元组是动态、随时间不断变化的.

定义 5　ABAC 授权是一个四元组$(<s.v_1,s.v_2,\cdots,s.v_n>,<o.v_1',o.v_2',\cdots,o.v_m'>,<p.v_1'',p.v_2'',\cdots,p.v_k''>,E)$,表示属性值为 $v_1,v_2,\cdots,v_n$ 的主体对属性值为 $v_1',v_2',\cdots,v_m'$ 的客体在环境属性集合 E 满足条件下,实施属性值为 $v_1'',v_2'',\cdots,v_k''$ 的操作.

定义 6　ABAC 策略形式为 $R(po)\leftarrow G_i,\cdots,G_n,\Psi$,其中 $n\geqslant 1,1\leqslant i\leqslant n$,$G_i$ 是基于属性的授权谓词,Ψ 是环境属性合取式,表示授权约束,符号“,”表示合取.对 G_i 和 Ψ 中的任意变量 var,var 的结构为 $x.a_i$.称 var 为实体属性变量,其全集记为 $X.A$,$G_1,\cdots,G_n,\Psi$ 为策略体,$R(po)$为策略头部,po 是一个常量,标识当前策略.一个系统的 ABAC 策略全集记为 PO.

定义 7　ABAC 访问控制策略评估是在给定的策略评估环境(AAR)下的一个映射 POE:$PO\rightarrow\{$permit, deny, unknown$\}$.

对任意 $po\in PO$,如果 po 的策略体内所有谓词全集 $TP(po)$中的每一个谓词和布尔表达式的值均为真(true),则 $POE(po)$ = permit,表示访问请求可以被授权;如果存在一个或一个以上的谓词或者布尔表达式的值为假(false),则 $POE(po)$ = deny,表示访问请求不可以被授权;如果存在一个实体属性变量 $var\notin X.A$,则 $POE(po)$ = unknown,表示访问请求无法判定.一般情况下,对一个特定的 AAR 和与该 AAR 相关的策略集合 PO,当 AAR 的元素语义明确时,对任意 $po\in PO_{AAR}$,要么 $POE(po)$ = permit,要么 $POE(po)$ = deny,二者有且仅有一种情况成立,表明访问控制策略判定结果是无歧义的.如果存在 $po_i\in PO$,$po_j\in PO$,使得 $POE(po_i)$ = permit,并且 $POE(po_j)$ = deny,则产生了策略冲突,称 PO 为冲突策略集.此时,需要引入冲突消解策略对判定结果进行二次决策.

3　ABAC 理论研究现状

3.1　ABAC 实体属性研究

(1)实体属性描述及绑定.实体属性是 ABAC 策略的核心概念.ABAC 策略规则由属性的布尔函数表达式产生,其属性描述方法的难易程度会对分布、异构环境下的策略执行与合成产生较大的影响.ABAC 起初的研究绝大多数都基于 X.509 属性证书[6].例如,文献[7]在网格计算中利用跨组织域的授权机制构建了一个基于属性证书的 ABAC 系统.文献[8]使用属性证书定义了基于属性的授权模型,但上述模型只能定义服务提供方的授权策略,没有提供访问主体方的属性透露方案.2002 年发布的 X.509 版本(RFC3281)扩展了权限管理体系(PMI),PMI 可以用于属性管理,实现分布环境下的

属性委托,但该方法还不够灵活[9].文献[10]采用基于角色的信任管理语言(RT)来描述分布环境中的授权凭证和访问控制策略,其角色交集、角色行为委托等概念满足了 ABAC 属性及策略表达需求.资源描述框架(RDF)[11]也可描述实体属性,RDF 提供了描述 Web 上信息资源的标准,允许定义任意属性来描述实体,利用统一资源定位(URIs)来引用资源或将这些资源与属性及其属性值相关联,从而解决不同组织域属性之间的语义交互问题.文献[12]提出的 ABAM 模型用属性值元组描述访问矩阵中主体与客体的属性关系,并用关于属性的谓词来描述指令执行条件,证明了 ABAM 模型安全决策的可判定性.在属性绑定方面,主体属性绑定可以利用经数字签名的 SAML 属性声明等凭证实现,同时利用 XML-DSIG 来标记相关属性以保证其完整性.对于客体属性,由于应用场景和资源本身的多样性,还没有一个标准的方法来实现客体属性绑定[13],方法之一是利用通用 XML 数据结构来实现资源元数据与实际数据的融合.

(2)实体属性管理及发现.在 ABAC 中,访问控制决策可能需要来自不同属性权威(AA)的属性信息.具备 ABAC 功能的授权系统 PERMIS、VOMS、Shibboleth 等都能从多个属性权威中获取属性值,实现基于远程属性权威的属性授权策略.但它们限制用户在不同 AA 中只能有一个相同的可供识别的全局用户名,这种命名上的限制不利于保护用户隐私[14].文献[15]针对网格计算中的凭证管理问题进行了深入探讨,其 MyProxy 系统为用户提供了加密的 X.509 凭证代理服务,访问主体可以委托 MyProxy 来获得短期的属性凭证信息.文献[16]为 ABAC 提出了一种属性聚合方案,根据基于名誉的信任评估计算属性提供方的名誉值来确定所获属性的可信度,摆脱了对 AA 的过分依赖.

3.2 ABAC 策略描述与语义互操作研究

对高层应用需求的策略抽象描述语言是 ABAC 研究的关键问题之一.目前 ABAC 策略描述语言可归类为基于逻辑的形式化语言和高层声明式语言[17].文献[18]将策略操作模型化为权限分配集合上的操作.文献[19]使用分层 CLP 中的集合来描述 ABAC 策略,用可计算集合理论中的集合限制理论把访问授权模型化为集合运算.已被工业界广泛支持的可扩展访问控制标记语言(XACML)[20]为 ABAC 提供了利用属性进行访问控制的策略描述语言,并给出了基本的 ABAC 授权框架,是 ABAC 的策略描述语言最理想的选择[21].XACML 还提供了策略冲突处理方案,利用冲突避免算法保证访问控制系统评估结果的确定性,减少了策略冲突对访问请求的影响.但是 XACML 中策略描述元素以及元素关系的复杂性导致策略定义和描述过程复杂化,对用户提出了较高的专业要求.文献[22]利用语义 Web 技术扩展 XACML,将用户、资源和环境属性作为语义背景,提供基于本体的推理引擎完成不同属性之间的语义映射,简化 ABAC 中的属性管理和策略管理.文献[23]利用巴科斯范式(BNF)来定义访问控制策略,提出扩展的 XACML 策略描述语言(A-XACML).文献[17]基于资源属性语义树建立 XACML 策略索引改进传统的遍历匹配,缩小策略检索空间,建立了高效的策略索引结构.

ABAC 访问控制决策所需的属性可能来自不同的组织域,不同组织域间的语义互操作成为 ABAC 研究中需要解决的另一个重要问题.将 ABAC 与语义 Web 技术相结合,可以为实体提供更精确的描述,进而定义更灵活的访问规则,实现语义推理功能,有效解决属性语义互操作问题.文献[24]借助语义和本体的概念保证了 ABAC 模型高效的访问控制决策.文献[25]结合语义 Web 技术,采用描述逻辑推理器(DL)分类用户和资源并证明访问控制策略的一致性.文献[26]利用语义 Web 技术提出了一个有语义感知功能的 ABAC 模型(SABAC).SABAC 模型用 Web 本体语言(OWL)描述资源的元数据和用户的属性并实现属性推理;用 XACML 作为控制策略描述语言,为 Web 服务的访问控制提供可扩展的管理和语义互操作能力.

3.3 ABAC 策略合成与冲突消解研究

开放的分布式异构环境中各组织域可能有不同的资源访问控制策略,需要通过合成多域访问控制策略来实现域间的资源共享或协作.ABAC 策略合成不仅应考虑组织域间不同的安全约束,还应保证合成策略对资源访问判决结果的确定性,避免策略冲突,同时要验证合成策略是否与预期要求相符.现有研究主要利用逻辑代数或函数的方法描述 ABAC 策略合成,检测和消解策略冲突,并验证策略合成结果的正确性及安全性.Bonatti 等[27]提出用合成代数组合安全策略,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,用并、交、差等操作符描述策略合成方式,并利用逻辑设计和局部评估技术来评估代数表达式.但该方案不适于涉及属性值计算的策略合成场景.文献[18]提出用原子策略表达和组合操作符等抽象符号构成的合成代数,将策略描述为主体、客体、行为三元组间的非确定性转换.文献[28]定义了一套较完整的规则关系来分析组织域策略的相似性,实现域间策略自动合成算法,但没有对规则间冲突检测进行分析.文献[29]利用细粒度合成代数(FIA)提供合成策略能力,实现了单一策略的性能证明和多策略的相似性比较等分析功能.Bertino 等[30]基于 FIA 提出了 XACML 策略合成架构并证明了所提出的代数的最小性和完整性,可以处理 XACML 策

略的细粒度合成.文献[5]用属性值计算结构扩展策略合成形式化框架,提出基于属性的策略合成代数模型——ApoCA,并讨论了策略表达式的代数性质.

ABAC策略描述复杂,加之不同组织域的控制策略存在差异,使得合成策略容易发生冲突.如果合成策略的判决冲突不被检测和解决,访问控制将不能保证相关实体的安全授权.对策略规则进行逻辑推理是用于分析策略冲突的基本方法.一些ABAC策略(例如XACML)本身也提供了冲突避免算法.文献[31]提出的policymorph系统可以对检测出的逻辑约束冲突提出消除建议,有助于系统管理者动态评估带逻辑约束的ABAC访问控制策略.文献[32]用描述逻辑(DL)形式化XACML策略,借助已有的DL验证分析工具检测策略中的冗余规则.

3.4　ABAC形式化模型研究

文献[19]利用可计算集合理论中的集合限制理论提出了ABAC的逻辑框架(LABAC),使用CLP中的集合来描述属性和服务.文献[33]提出的基于属性的Web服务访问控制模型具有较强的表达能力,其访问控制决策依据的属性同时包括了主体属性、资源属性和环境属性.文献[12]引入属性到访问控制矩阵中,提出基于属性的访问控制矩阵模型ABAM,该模型支持基于属性的授权和动态权限限制,增强了访问矩阵的表达能力.文献[34]提出基于属性的授权委托模型ABDM,在赋予一个角色委托权限时,要求该角色必须满足属性表达式约束.文献[5]利用受限Datalog和CDB抽象描述了ABAC整体框架和访问控制策略判定过程,其ABAC框架中将系统策略区分为访问策略和元策略,分别抽象为带限制的Datalog规则和映射.文献[35]提出了使用上下文属性来捕获移动环境动态性质的上下文敏感的ABAC模型,适合移动环境下的访问授权.使用控制[36](UCON)利用主体、客体以及系统属性和条件来定义授权规则,将访问授权策略建立在授权、职责和条件三种决策因素上,支持可变属性和持续授权,实质也是一种ABAC模型[37].虽然UCON满足下一代访问控制的需求,但其授权管理结构复杂.文献[38]提出支持时间和使用限制的TMAAC模型,其资源和权限均与属性相关联,通过可量化的授权机制使每个授权对应一个时间周期,主体对资源的访问行为将消耗一定的授权量,以防止授权被滥用.

RBAC通过角色实现用户到权限间的授权,简化了授权管理.但是,单纯的基于角色的访问控制不能完全适用于网络环境下支持移动计算的信息存取管理[39].文献[10]将RBAC和信任管理的思想结合起来,提出了一种ABAC概念模型,对ABAC策略的分散属性、属性授权委托、属性推理、属性值域等具有较强的表达能力.文献[40]在用户到角色赋值过程中引入属性,解决了RBAC中大规模用户的动态角色赋值问题.文献[41]利用X.509属性证书对RBAC模型进行了扩展.文献[42]提出基于属性和规则的角色访问控制模型(GARBAC),根据不同的属性表达式进行用户到角色的赋值.随着用户和资源属性数目的增长,GARBAC中规则数目呈线性增长,与文献[33]中模型的规则数目呈指数级增长相比有性能上的改进.文献[43,44]把实体属性概念引入面向服务的授权和授权责任担保,提出了带权表决授权和承诺-担保授权模型.

3.5　ABAC属性和策略安全交互研究

实体敏感属性保护及系统敏感策略保护是ABAC安全交互研究中的重要课题.ABAC安全交互既要求交互双方能建立一定级别的可信关系,又希望能提交满足策略的属性信息最小集合或以属性隐藏的方式完成交互过程,有时还需要借助可信的第三方在资源提供者和访问主体间执行协调功能.如文献[43]在访问控制中引入第三方担保的思想可以为ABAC属性和策略的安全交互提供借鉴.文献[45]提出ACK策略来加强敏感属性保护.在ACK策略机制中,协商的一方要得知对方是否满足某个属性要求,首先应满足对方对应敏感属性的ACK策略.文献[46]引用ACK策略和信任目标图(TTG)协议来增强协商过程中的安全性,研究了不同类型的推理攻击.文献[47]提出策略库概念隐藏凭证拥有者的身份.文献[48]提出改进的策略库系统,给出了关联属性的形式化定义,建立相关属性的关系模型,在策略库中加入相关性检测器解决概率推理可能导致的资源拥有敏感信息的透露问题.文献[49]提出基于信任和属性的访问控制模型,资源提供方需要询问请求方的受限属性时,必须向其描述自由属性,从而在双方之间建立可信关系.文献[50]以隐藏属性凭证及访问策略的方式进行信任协商,最小程度地透露凭证和访问策略,根据需要实现不同程度的隐私保护.文献[9]提出属性联邦(attribute federation)概念,用户在属性交互时不执行信任协商过程,而是委托属性联邦来完成交互,增加了访问控制对用户的透明性.文献[51]实现了访问控制中用户对可信策略决策点(PDP)的动态选择.用户根据需要定义自己的属性透露规则和隐私保护策略等参数,在物理上分离的PDP中动态选择PDP.

匿名凭证系统能提供用户的属性证明而不透露其身份,对ABAC的隐私保护研究有很大影响.文献[52]利用不经意属性证书(OACerts)机制和基于承诺的不经意封装(OCBE)机制实现了不经意访问控制策略.文献[53]提出可证输入私有策略评估(CIPPE)的概念,利用OACerts和2-SFE实现了策略隐藏的访问控制.但2-SFE函数的输入是属性证书而不是属性信息本身,需要同

时考虑数字签名认证等验证过程,所以该方法效率较低.文献[54]提出利用解决百万富翁问题的"魔法协议"进行属性交换,保护了服务提供方的访问控制策略,并通过可信第三方证明实体的行为,实现了属性交换过程中的欺骗检测.

4 ABAC应用研究现状

(1)ABAC在Web服务中的应用.在Web服务系统中,服务和用户可能在任何时候加入或离开系统,这要求系统的访问控制机制具备动态扩展性[55].Web服务的动态特征还要求访问控制策略考虑上下文等环境信息.文献[33]从授权架构和策略阐述方面探讨ABAC模型在Web服务中的应用,提出了支持传统的MAC和DAC授权的ABAC模型.文献[56]提出了面向Web的访问控制研究应解决的关键问题,包括基于属性的实时动态访问决策和策略合成. Bertino等[8]在提出的基于属性的Web服务访问控制模型中引入了属性值域限制,在访问控制策略中同时考虑了主体和客体属性.文献[57]引入属性透露限制概念扩展了Web服务中的ABAC模型,通过对不同安全级别的属性进行加密以保护属性信息,为Web服务中的联邦安全提供了有效的解决方案.

(2)ABAC在网格计算中的应用.ABAC有足够的灵活性和可扩展性来解决网格计算系统的访问控制问题.文献[58]利用属性授权系统Shibboleth协调组织间的认证,通过组合ABAC模型、隐私管理基础设施和身份联邦为网格计算中的虚拟组织提供了一个安全的协作环境.文献[59]基于XACML标准为电子商务构建了具有ABAC功能的AAI模型,实现了AAI上灵活的单点登录(SSO).文献[60]利用组合认证技术和属性智能加密技术构建了鲁棒性较强的认证和访问控制系统,增强了在策略和角色动态改变时访问控制的灵活性.文献[61]扩展基于角色的信任管理语言,将ABAC应用到CROWN网格项目实现了细粒度的访问控制.

(3)ABAC在信息共享和消息管理中的应用.ABAC在信息共享、信息查询、消息管理等方面也受到越来越多的关注.文献[62]探讨了ABAC在安全信息共享中的应用,利用基于属性的加密(ABE)构建了新的安全信息管理体系.文献[63]提出基于密钥策略的属性加密系统(KP-ABE)为数据的细粒度访问控制提供了加密方案.文献[64]提出的基于密文策略的属性加密系统则将密文与访问策略相关联,而用户的私钥与属性集合相关联,避免了复杂访问控制中存储信息对可信服务器的强烈依赖.文献[21]提出了ABAC在企业基于属性的消息系统(ABM)应用的一种解决方案,提高了ABM系统从企业数据库获取属性的灵活性,同时简化了权限的赋值和管理.

5 ABAC研究趋势

尽管ABAC理论和应用研究已经取得了丰硕成果,但是ABAC研究仍然有许多尚待解决的重要问题.

(1)简洁的策略描述框架.ABAC需要简单易用的策略描述和分析工具,以降低用户描述ABAC策略的难度.

(2)完善的策略合成模型.ABAC策略合成代数模型需要具有方便添加新的策略合成操作符以增强策略合成的能力.同时,还应研究相应的代数操作的普适性.

(3)高效的安全属性交互协议.ABAC需要安全、高效的协商协议来为属性交互服务,同时考虑隐私信息保护等问题,支持凭证中属性的细粒度提交或不经意访问控制.

(4)易理解的通用本体(Ontology).ABAC需要简洁、高效的通用策略描述语言和本体[65],以解决多组织域之间属性描述、策略表达等方面的语义互操作问题.

6 总结

基于属性的访问控制(ABAC)能够解决传统访问控制难以解决的细粒度访问控制和大规模动态授权问题.本文以ABAC策略、模型和属性安全交互为主线,对国内外ABAC理论研究现状进行了系统总结;以ABAC在Web服务、网格计算、信息共享和消息管理中的应用为背景,对ABAC应用研究进行了详细分析,同时对ABAC未来研究趋势进行了展望,为未来开放网络环境中的复杂信息系统访问控制研究提供了新思路和文献参考.

参考文献:

[1] R Sandu, P Samarati. Access control: principles and practice [J]. IEEE Communications Magazine, 1994, 32(9): 40 - 48.

[2] P Bonatti, P Samarati. A uniform framework for regulating service access and information release on the web[J]. Journal of Computer Security, 2002, 10(3): 241 - 271.

[3] R F Han, H X Wang, Q Xiao, et al. A united access control model for systems in collaborative commerce[J]. Journal of Networks, 2009, 4(4): 279 - 289.

[4] 林莉,怀进鹏,李先贤.基于属性的访问控制策略合成代数[J]. 软件学报,2009,20(2):403 - 414.
LIN Li, HUAI Jin-Peng, LI Xian-Xian. Attribute-based access control policies composition algebra[J]. Journal of Software,

2009,20(2):403 - 414. (in Chinese)
[5] 李晓峰,冯登国,陈朝武,房子河.基于属性的访问控制模型[J].通信学报,2008,29(4):90 - 98.
LI Xiao-feng, FENG Deng-guo, CHEN Zhao-wu, FANG Zi-he. Model for attribute based access control[J]. Journal on Communications, 2008, 29(4): 90 - 98. (in Chinese)
[6] B Lang, I Foster, F Siebenlist, et al. A flexible attribute based access control method for grid computing[J]. Journal of Grid Computing, 2009, 7(2): 169 - 180.
[7] M Thompson, W Johnston, S Mudumbai, et al. Certificate-based access control for widely distributed resources[A]. Proceedings of the 8th conference on USENIX Security Symposium[C]. Berkeley: USENIX Association, 1999. 215 - 228.
[8] E Bertino1, A C Squicciarini, I Paloscia, et al. Ws-AC: A fine grained access control system for web services[J]. World Wide Web, 2006, 9(2): 143 - 171.
[9] I Agudo, J Lopez, A Jose. Enabling attribute delegation in ubiquitous environments[J]. Mobile Networks and Applications, 2008, 13(3): 398 - 410.
[10] N Li, J C Mitchell, W H Winsborough. Design of a role-based trust-management framework[A]. Proceedings of 2002 IEEE Symposium on Security and Privacy[C]. Washington: IEEE Computer Society, 2002. 114 - 130.
[11] Resource Description Framework (RDF): Concepts and abstract syntax. world wide web consortium[OL]. February 2004. http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/, 2004-02-10/200903-12.
[12] X W Zhang, Y J Li, D Nalla. An attribute-based access matrix model[A]. Proceedings of the 2005 ACM Symposium on Applied Computing[C]. New York: ACM, 2005. 359 - 363.
[13] Y Eric, W Greg. Assured counter-terrorism information sharing using attribute based information security (ABIS)[A]. Proceedings of the 2005 IEEE Aerospace Conference[C]. Montana: IEEE Computer Society, 2005. 1 - 12.
[14] D Chadwick. Authorisation using attributes from multiple authorities[A]. Proceedings of the 15th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises[C]. Washington: IEEE Computer Society, 2006. 326 - 331.
[15] J Basney, M Humphrey, V Welch. The myProxy online credential repository[J]. Software: Practice and Experience, 2005, 35(9): 801 - 816.
[16] J Lee, H Kim, J S Hong. An attribute aggregation architecture with trust-based evaluationfor access control network operations and management symposium[A]. Proceedings of the 2008 IEEE Symposium on Network Operations and Management[C]. Salvador: IEEE, 2008. 1011 - 1044.
[17] 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)
[18] D Wijesekera, S Jajodia. A propositional policy algebra for access control[J]. ACM Transactions on Information and System Security, 2003, 6(2): 286 - 325.
[19] L Y Wang, D Wijesekera, S Jajodia. A logic-based framework for attribute based access control[A]. Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering[C]. New York: ACM, 2004. 45 - 55.
[20] G Simon, M Tim, A Anne, et al. Extensible access control markup language (XACML)[OL]. OASIS specification, 2005. http://www.oasis-open.org/specs/JHJxacmlv2.0, 2005-02-01/2008-10-28.
[21] R Bobba, O Fatemieh, F Khan, et al. Using attribute-based access control to enable attribute-based messaging[A]. Proceedings of the 22nd Annual Computer Security Applications Conference on Annual Computer Security Applications Conference[C]. Washington: IEEE Computer Society, 2006. 403 - 413.
[22] T Priebe, W Dobmeier, N Kamprath. Supporting attribute-based access control with ontologies[A]. Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES'06)[C]. Washington: IEEE Computer Society, 2006. 465 - 472.
[23] C Ye, J Zhong, Y Feng. Attribute-based access control policy specification language[J]. Journal of Southeast University, 2008, 24(3): 260 - 263.
[24] J Warner, V Atluri, R Mukkamala, et al. Using semantics for automatic enforcement of access control policies among dynamic coalitions[A]. Proceedings of the 12th ACM Symposium on Access Control Models and Technologies[C]. New York: ACM, 2007. 235 - 244.
[25] L Cirio, I F Cruz, R Tamassia. A role and attribute based access control system using semantic web technologies[A]. Proceedings of 2007 IFIP Workshop on Semantic Web and Web Semantics[C]. Berlin: Springer, 2007. 1256 - 1266.
[26] H Shen. A semantic-aware attribute-based access control model for web services[A]. Proceedings of the 9th International Conference on Algorithms and Architectures for Parallel Processing[C]. Berlin: Springer-Verlag, 2009. 693 - 703.
[27] P Bonatti, S D Vimercati, P Samarati. An algebra for composing access control policies[J]. ACM Transactions on Information and System Security, 2002, 5(1): 1 - 35.
[28] P Mazzoleni, E Bertino, B Crispo, et al. XACML policy integration algorithms[A]. Proceedings of the eleventh ACM symposium on Access control models and technologies[C]. New York: ACM, 2006. 219 - 227.
[29] P Rao, D Lin, E Bertino, et al. EXAM: an environment for access control policy analysis and management[A]. Proceedings

of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks[C]. Washington: IEEE Computer Society, 2008. 238 – 240.

[30] P Rao, D Lin, E Bertino, et al. An algebra for fine-grained integration of XACML policies[A]. Proceedings of the 14th ACM Symposium On Access Control Models and Technologies[C]. New York: ACM, 2009. 63 – 72.

[31] M LeMay, O Fatemieh, C A Gunter. PolicyMorph: interactive policy transformations for a logical attribute-based access control framework[A]. Proceedings of the 12th ACM Symposium on Access Control Models and Technologies[C]. New York: ACM, 2008. 205 – 214.

[32] V Kolovski, J Hendler, B Parsia. Analyzing web access control policies[A]. Proceedings of the 16th International Conference on World Wide Web[C]. New York: ACM, 2007. 677 – 686.

[33] E Yuan, J Tong. Attributed based access control (ABAC) for web services[A]. Proceedings of the IEEE International Conference on Web Services[C]. Washington: IEEE Computer Society, 2005. 561 – 569.

[34] C Ye, Z Wu, Y Fu. An attribute-based delegation model and its extension[J]. Journal of Research and Practice in Information Technology, 2006, 38(1): 3 – 17.

[35] J Michael, R Manoj. A contextual attribute-based access control model[A]. Proceedings of 2006 Workshops on the Move to Meaningful Internet Systems[C]. Berlin: Springer, 2006. 1996 – 2006.

[36] J Park, R Sandhu. The UCONABC usage control model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128 – 174.

[37] D Q Zou, L G He, H Jin, et al. CRBAC: imposing multi-grained constraints on the RBAC model in the multi-application environment[J]. Journal of Network and Computer Applications, 2009, 32(2): 402 – 411.

[38] R Yang, C Lin, F Feng. A time and mutable attribute-based access control model[J]. Journal of Computers, 2009, 4(6): 510 – 518.

[39] 李凤华,王巍,马建峰,梁晓艳.基于行为的访问控制模型及其行为管理[J].电子学报,2008,36(10):1881-1889.
LI Feng-hua, WANG Wei, MA Jian-feng, LIANG Xiao-yan. Action-based access control model and administration of actions[J]. Acta Electronica Sinica, 2008, 36(10): 1881 – 1889. (in Chinese)

[40] M A Al-Kahtani, R Sandhu. A model for attribute-based user-role assignment[A]. Proceedings of the 18th Annual Computer Security Applications Conference [C]. Washington: IEEE Computer Society, 2002. 353 – 362.

[41] D Chadwick, A Otenko, E Ball. Role-based access control with X.509 attribute certificates[J]. IEEE Internet Computing, 2003, 7(2): 62 – 69.

[42] Y Zhu, J Li, Q Zhang. General attribute based RBAC model for web services[J]. Wuhan University Journal of Natural Sciences, 2008, 13(1): 81 – 86.

[43] 王小明,赵宗涛,马建峰.基于承诺-担保的访问控制模型[J].电子学报,2003,31(8):1150 – 1154.
WANG Xiao-ming, ZHAO Zong-tao, MA Jian-feng. A promise-assurance-based access control model[J]. Acta Electronica Sinica, 2003, 31(8): 1150 – 1154. (in Chinese)

[44] X Wang, Z Zhao. A service oriented voting authorization model[J]. Chinese Journal of Electronics, 2006, 15(1): 37 – 40.

[45] N Li, W H Winsborough. Towards practical automated trust negotiation[A]. Proceedings of the Third International Workshop on Policies for Distributed Systems and Network[C]. Washington: IEEE Computer Society, 2002. 92 – 103.

[46] W H Winsborough, J Jacobs. Automated Trust Negotiation in Attribute-Based Access Control[A]. DARPA Information Survivability Conference and Exposition[C]. Los Alamitos: IEEE Computer Society, 2003. 252 – 257.

[47] K Irwin, T Yu. Preventing attribute information leakage in automated trust negotiation[A]. Proceedings of the 12th ACM Conference on Computer and Communications Security[C]. New York USA: ACM, 2005. 36 – 45.

[48] H Lu, B Liu. Improved policy database system for protecting possession sensitive attributes in automated trust negotiation [A]. Proceedings of the 2007 Japan-China Joint Workshop on Frontier of Computer Science and Technology[C]. Washington: IEEE Computer Society, 2007. 61 – 66.

[49] J Biskup, J Hielscher, S Wortmann. A trust- and property-based access control model[J]. Electronic Notes in Theoretical Computer Science, 2008, 197(2): 169 – 177.

[50] K B Frikken, M J Atallah, J Li. Attribute-based access control with hidden policies and hidden credentials[J]. IEEE Transactions on Computers, 2006, 55(10): 1259 – 1270.

[51] K Jan, S Rolf, P Günther. A privacy-enhanced attribute-based access control system[A]. Proceedings of 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security[C]. Berlin: Springer-Verlag, 2007. 129 – 143.

[52] J Li, N Li. OACerts: oblivious attribute certificates[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 4 (3): 340 – 352.

[53] J Li, N Li. Policy-hiding access control in open environment [A]. Proceedings of the Twenty-fourth Annual ACM Symposium on Principles of Distributed Computing[C]. New York: ACM, 2005. 29 – 38.

[54] T Takagi, T Komura, S Miyazaki, Y Okabe. Privacy oriented attribute exchange in shibboleth using magic protocols[A]. Proceedings of the 2008 International Symposium on Applications and the Internet[C]. Washington: IEEE, 2008. 293 –

296.
[55] Bo Lang, Nan Zhao, et al. An XACML policy generating method based on policy view[A]. Proceedings of International Conference on Pervasive Computing and Applications[C]. IEEE Press, 2008, Vol 1. 295 – 301.
[56] M Coetzee, J H P Eloff. Towards web service access control [J]. Computers and Security, 2004, 23(7): 559 – 570.
[57] V S Mewar, S Aich, S Sural. Access control model for web services with attribute disclosure restriction[A]. Proceedings of the Second International Conference on Availability, Reliability and Security[C]. Washington: IEEE Computer Society, 2007. 524 – 531.
[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, 5(2): 273 – 292.
[59] S Christian , S Manuel, M Björn, et al. Attribute – based authentication and authorization infrastructures for e-commerce providers[A]. Proceedings of the 7th International Conference on Electronic Commerce and Web Technologies[C]. Berlin: Springer, 2006. 132 – 141.
[60] H Park, D H Lee, J Zhan, Attribute-based access control using combined authentication technologies[A]. Proceedings of 2008 IEEE International Conference on Granular Computing[C]. Hangzhou: IEEE, 2008. 518 – 523.
[61] J P Huai. Distributed access control in CROWN groups[A]. Proceedings of the 2005 International Conference on Parallel Processing[C]. Washington: IEEE Computer Society, 2005. 435-442.
[62] M Pirretti, P Traynor, P McDaniel, et al. Secure attribute-based systems[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2006. 99 – 112.
[63] V Goyal, O Pandey, A Sahai, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2006. 89 – 99.
[64] J Bethencourt, A Sahai, B Waters. Ciphertext-policy attribute-based encryption[A]. Proceedings of the 2007 IEEE Symposium on Security and Privacy[C]. Washington: IEEE Computer Society, 2007. 321 – 334.
[65] J S Kowalik, J Gorski, A Sachenko. New directions in access control[A]. Proceedings of the NATO Advanced Research Workshop on Cyberspace Security and Defense[C]. Netherlands: Springer, 2005. 279 – 293.

作者简介:

王小明　男,1964 年出生于甘肃省天水市,博士,教授,博士生导师.主要研究方向是访问控制、新型无线传感器网络.
E-mail: wangxm@snnu.edu.cn

付　红　男,1984 年出生于重庆市巫溪县,硕士研究生.主要研究方向是访问控制、新型无线传感器网络.
E-mail: fuhong@stu.snnu.edu.cn

张立臣　男,1979 年出生于河北省邢台市,博士.主要研究方向是访问控制、网络信息安全.
Email: zhanglichen@snnu.edu.cn