Web服务访问控制模型研究

颜学雄[1] 王清贤[1] 马恒太[2]

(信息工程大学信息工程学院 郑州 450002)[1] (中国科学院软件所 北京 100080)[2]

摘 要 本文分析了Web服务给访问控制带来的挑战性问题,包括跨域的访问控制、动态授权和标准化问题等。然后,根据访问控制模型的决策依据,对现有的访问控制模型进行了分类研究。介绍了各类模型的基本原理,分析了它们解决Web服务访问控制挑战性问题的能力。最后,对Web服务访问控制模型研究的方向进行了讨论。

关键词 Web服务,访问控制模型,安全

Survey of Web Services Access Control Model

YAN Xue-xiong[1] WANG Qing-xian[1] MANG Heng-tai[2]

(Institute of Information Engineering, PLA Information Engineering University, Zhengzhou 450002, China)[1]

(Institute of Software, Chinese Academy of Sciences, Beijing 100080, China)[2]

Abstract This paper analyzes new challenges, which include access control across multiple security domains, dynamic authorization and standards, for Web Services access control. The paper classifies access control model according to what the model depends to making decision, and then introduces the principles of these models. After analyzing the ability to solve the new challenges, this paper discusses the research directions for Web Services access control model.

Keywords Web services, Access control model, Security

1 引言

以服务为中心的SOA(Service Oriented Architecture,面向服务体系结构)可以大大提升公司或者组织的协作和信息共享能力,其思想可以广泛应用于电子商务、电子政务以及军队信息化建设中的综合信息系统集成。

Web服务是实现SOA的重要手段,是描述一个操作集合的接口,服务请求者使用标准的XML消息,通过网络可以访问这些操作[1]。服务请求者通常通过UDDI[2]发现所需要的服务,根据WSDL[3]文档自动生成所需要的请求程序,并通过SOAP协议[4]和服务提供者进行信息交互。

但是,安全问题影响了Web服务的推广使用,而访问控制是其中非常重要的一个安全问题。

访问控制就是保证资源只授予授权用户、程序和进程等,保护资源免于非法访问。相对于传统的访问控制,Web服务的访问控制存在不少的挑战性问题,其根本原因在于Web服务应用环境是分布式的,需要处理跨域情景下的访问控制。本文对Web服务访问控制的挑战性问题进行了分析,在此基础上,根据访问控制决策的依据,对现有的访问控制模型进行了分类,并分析了这些模型的基本原理和解决挑战性问题的能力。

2 Web服务带来的挑战

Web服务给访问控制带来了新的挑战性问题,主要包括:

问题1 跨域的访问控制

传统的访问控制模型主要是基于单域,也就是请求者和提供者都在同一个管理域内,它们相互"认识"。而Web服务主要应用于不同组织、部门之间的信息集成,跨域的服务请求者和提供者之间可能相互并不"认识",因此这个问题也称为"陌生人"之间的访问控制问题[5,6]。

问题2 动态授权

传统的访问控制模型一般都是由管理员事先按照一定的规则给主体(通常依据主体的身份)指派权限,然后将这些指派关系保存起来(如使用ACL),这种事先指派的授权称为静态授权。在Web服务跨域应用环境下,管理员对于外域主体并不清楚,很难实现这样的静态权限指派,因此需要一种动态授权机制。它包括三个方面的内容:①主体动态获取授权。传统的主体通常是静态获取授权(如使用ACL),而Web服务中主体需要在执行任务时根据一定的规则动态推导出主体的授权。②授权依据的动态性。传统访问控制模型主要依据请求者的身份进行授权。而在Web服务应用环境中,影响授权的因素非常多,如主体的属性、对象的属性和环境的属性等,而且这些因素不断地发生变化。③授权变更。传统访问控制过程中,主体对资源的授权关系比较稳定,授权时间也比较长。而在Web服务访问控制过程中,服务的请求者在执行任务时,由于一些突发因素(如发现请求者可能存在攻击行为),可能需要对主体已有授权进行变更,甚至中止授权。

问题3 标准化问题

Web服务应用于跨域的综合信息系统集成,其各种信息交互都需要建立在标准的基础上,对于Web服务访问控制问题也是如此。

3 Web服务访问控制模型

访问控制就是保证资源只授予授权用户、程序和进程等,保护资源免于非法访问。访问控制模型是对访问控制基本元

颜学雄 博士生,讲师,主要研究领域为Web服务安全;王清贤 教授,博士生导师,主要研究领域为网络信息安全和算法设计与分析;马恒太 博士,副研究员,主要研究领域为信息安全。

素的抽象，主体(Subject)、对象(Object)和权限(Permission)是其中的最基本元素。

从权限管理角度来看，访问控制模型可以分为自由访问控制模型(Discretionary Access Control，DAC)和强制访问控制模型(Mandatory Access Control，MAC)[7,8]。自由访问控制模型中的主体可以自由支配自己的权限(如将权限指派给其他主体等)；强制访问控制模型中的主体不可以随意支配拥有的权限，对主体进行授权时，需要依据主体和对象本身的特性(如机密程度)。

本节根据访问控制决策过程中的主要依据对访问控制模型进行分类，并介绍这些模型基本原理以及在 Web 服务访问控制中的应用情况。

3.1 基于身份的访问控制模型

基于身份的访问控制模型的主要思想就是将权限和主体身份关联起来。最经典的基于身份的访问控制模型就是基于矩阵的访问控制模型[7,9]，即在一个矩阵中，行表示主体，列表示对象，对应的矩阵格表示主体(与行相对应)对对象(与列相对应)的访问权限。

传统的基于身份访问控制模型不适应分布式环境。为了解决这个问题，目前主要有两种方式：一是集中身份管理方式，二是分布式身份联盟方式。

· 集中身份管理

集中身份管理就是使用一个(或多个)可信赖的中心服务器，对所有需要参与访问控制的主体进行集中管理。当一个主体需要访问其他域的服务时，中心服务器对其提供身份证明。目前，身份集中管理方式模型主要包括基于 X.509 身份验证框架[10]的访问控制模型、基于 Kerberos[11]的访问控制模型以及微软的基于.NET Passport[12]的访问控制模型等。

· 分布式身份联盟

分布式身份联盟没有一个可信赖的中心服务器，不同域的用户通过联盟的方式相互认可。在访问之前，跨域的用户之间先建立联盟，当一个主体处于某一个联盟中，它就可以访问联盟中的服务资源。跨域主体身份联盟通过信任网(Web of Trust)的方式实现。典型的分布式身份联盟访问控制模型包括自由联盟工程(The Liberty Alliance Project，LAP)[13]和 PGP 的访问控制模型[14]等。

不管是集中方式还是分布式联盟方式，基于身份的跨域访问控制需要参与者之间交互身份有关的一些信息，如服务的提供者需要请求者的身份验证信息。SAML[15](Secure Assertion Markup Language)提供了参与者之间传递身份验证信息的标准，断言(Assertion)是一种统一的身份验证信息的传输格式。同时，WS-Security[16]对 SOAP 消息进行扩展，在 SOAP 头中传输包括 SAML 断言在内的多种安全信息。

E. Damiani[17]等提出了针对 SOAP 的访问控制模型，该模型依据访问主体的身份等信息进行访问控制决策。E. Bertino[18]等提出了一种依赖于身份管理系统的访问控制模型，依据请求者的身份属性等条件进行访问控制决策。J. V. Bemmel[19]等提出在 Web 服务发现阶段对服务请求者进行身份验证，验证后的请求者得到一个令牌，随后依据令牌进行访问控制决策。

在 Web 服务的分布式应用环境下，通过多个参与者之间交互身份验证信息，可以实现基于身份的访问控制，一些国际标准化组织也制定了相关的标准(如 SAML[15]等)。但是，跨域的 Web 服务访问控制决策仅仅依据请求者的身份信息是不充分的[20]，这个特性决定了基于身份访问控制模型的局限性。

3.2 基于格的访问控制模型

基于格的访问控制模型[21]主要应用于信息流的访问控制，基本原理就是为对象和主体分配标签，表示它们的安全级别。标签之间的信息流动有一些限制规则，标签和信息流动限制规则就构成了一个格。

目前，基于格的 Web 服务访问控制模型实现还比较少。基于格模型的决策依据是请求主体和对象的标签，根据标签中信息流动规则限制访问，这样一种非中心管理方式很适合 Web 服务的分布式特点。基于格模型需要为主体和对象建立一个标签系统，由于 Web 服务应用环境的复杂性，这是一个比较困难的问题。

3.3 基于角色的访问控制模型

基于角色的访问控制模型[22,23]根据请求主体的职务功能和角色进行授权，其管理方式比基于身份的访问控制模型更有效。基本原理包括两个映射：一是主体到角色的映射，当一个主体请求访问时，根据这个映射给主体分配一个角色；二是角色到权限的映射，根据角色对应的权限以及相关的限制规则进行访问控制决策。

R. Wonoboesodo 等[24]将 RBAC 模型应用于 Web 服务访问控制，他们将 Web 服务分为单服务和组合服务的情况进行讨论，基本思想就是针对不同的服务用户，分配不同的角色，然后根据角色进行相应的授权。P. Liu 等[25,26]提出一种 Web 服务业务处理的 RBAC 模型，基本思想就是将参与业务处理的合作伙伴映射到角色，然后根据角色进行相应的授权。F. Xu 等[27]也提出了一个针对 Web 服务的 RBAC 访问控制模型，在该模型下，根据请求者的身份等信息将请求者映射到一个或者多个角色，请求者每启动一个角色就产生一个执行者 Actor，它代表请求者执行有关操作。

基于角色的访问控制模型中，一个关键问题就是如何将请求者映射到相应的角色。以上 Web 服务 RBAC 模型主要还是依赖于请求主体的身份等信息。和基于身份的访问控制模型一样，对于 Web 服务的跨域访问控制来说，单单依靠身份进行主体到角色的映射是不够的。

3.4 基于授权的访问控制模型

基于授权的访问控制模型就是直接依据主体获得的授权来进行访问控制决策。T. Y. C. Woo 等[28,29]首先提出了将授权从其他安全服务中分离出来，单独作为一个研究对象，这就是基于授权的访问控制模型的思想基础，该思想关注的是如何描述请求和策略，并对请求和策略的一致性进行评估。这样，访问控制问题就转化成一个授权问题：一个服务请求是否和策略一致？以后的基于授权的访问控制模型继承并发展了这一思想，T. Y. C. Woo 等[30,31]后来提出将授权作为一个核心的服务，并设计了一种通用语言 GACL 来描述策略和请求。

M. Blaze 等[32,33]进一步对基于授权的访问控制模型进行抽象，提出了信任管理的概念，通过信任证(Credential)来证明主体获得的授权，这样访问控制问题就转化为[34]：请求者递交的信任证是否证明请求满足了策略的要求？

为了解决信任管理的标准化问题，先后出现了 KeyNote[35,36]，SPKI/SDSI[20,37]等描述授权以及授权在主体之间传递的规范。

主体如何获得授权证明(信任证)以及权限在多个主体之间的传递关系，是基于授权的访问控制模型需要重点解决的问题。为了实现跨域授权，常用的方法就是委托(Delegation)。信任证表示主体之间的授权委托关系，主体和对象之间通过多级委托方式在两者之间建立信任链(这就是信任管

理名称的由来),这样就建立了一条跨域访问的渠道。为了规范委托以及相关的一些运算,N. Li[38,39]等提出了一种委托逻辑方法,并对信任管理的信任证查找问题进行了研究[40],提出了相关的算法。

虽然目前还没有基于授权的 Web 服务访问控制模型,但是其思想很容易在 Web 服务访问控制中得到应用。

基于授权的访问控制模型通过信任证得到授权,这些信任证需要事先安排,很难满足 Web 服务访问控制的动态性要求。同时,信任链上的每一个主体都要为自己的委托授权负责,增加了权限管理的难度。

3.5 基于属性的访问控制模型

属性就是主体、对象等实体拥有的某些特性,比如身份、年龄、组关系等。基于属性的访问控制模型依据一些参与实体的属性进行访问控制决策,如请求主体的属性、对象的属性以及环境属性等。

W. Johnston 等[41]提出了一个基于属性的分布式访问控制模型。在该模型中,多个管理实体制定策略,提出对请求主体的属性要求。当一个主体请求资源时,需要递交他的属性证书表明其属性。明确提出基于属性模型概念的是 N. Li 等[42],基本思想就是根据请求主体的属性信息,然后分配相应的角色。同时,他们还建立了基于属性的 RBAC 访问控制框架和相应的 RT(Role-based Trust-management)语言。

E. Bertino 等[18]提出了 Web 服务的基于属性的访问控制模型。作者根据请求主体的身份、地址等属性信息进行访问控制决策。E. Yuan 等[6]给出了表达能力更强的基于属性 Web 服务访问控制模型,访问控制决策依据包括请求主体的属性(如身份、地址等)、资源的属性(如资源的服务能力等)以及环境的属性(如系统负载等)。

文献 [43-45] 针对环境属性(它们称为 Context 或者 Condition)的变化特性,提出了动态授权模型。这些模型根据变化的环境因素动态调整有关的授权。尤其在文献 [44] 的模型中,授权的结果可能改变有关的环境属性,因此更能表达动态授权的思想。

XACML (eXtensible Access Control Markup Language)[46]标准中,充分体现了基于属性的访问控制决策过程,PDP(Policy Decision Point,访问控制决策点)可以依据主体、对象以及环境的属性信息进行授权决策。

跨域的主体和对象之间如何交互相关的属性信息呢?如何对敏感的属性信息(如特殊病人属性信息)进行保护呢?这就是属性的协商问题,称为信任协商[47-50],主体和对象之间通过交互,逐步建立信任关系,完成属性协商。

基于属性的访问控制模型非常适合 Web 服务这样的分布式环境,但是它需要属性系统的支持。属性系统提供属性的定义以及属性证书维护等功能,这给模型实现带来了一定的困难。

4 模型能力综合分析

本节分析各类模型解决 Web 服务访问控制挑战性问题的能力,我们用强、弱和无三个级别来描述解决能力。强表示比较简单地解决了问题;弱表示解决问题比较复杂,或没有提出明确的解决途径;无表示没有解决问题的能力。

针对跨域访问控制问题,无论是采取集中方式还是分布式联盟方式,参与主体的复杂性使得基于身份的访问控制模型处理起来比较困难,因此其处理能力弱。基于格的访问控制模型的决策依据是主体和对象的标签,只要请求主体有相应的标签,就可以很方便实现跨域的访问控制,因此其处理能力强。基于角色的访问控制模型中,将"陌生人"映射到相应的角色是处理的难点,因此它的解决能力也比较弱。基于授权的访问控制模型中,陌生人只要有相应的信任证,就可以得到授权,因此处理能力强。基于属性模型的决策依据是一些属性信息,和请求主体是否陌生人没有关系,因此其处理能力强。

对于基于身份的访问控制模型来说,主体通过自己的身份获取授权,因此并没有动态授权的特性。基于格的访问控制模型中,主体对某一特定对象的授权事先并不知道,根据标签以及信息流动限制就可以推导出主体授权,因此具有主体动态获取授权的能力;但是基于格的访问控制模型的授权依据是事先定义好的标签,不具有依据动态因素调整授权的能力,更没有对授权进行变更的能力。基于角色的访问控制模型中,主体的授权是通过相关的角色而得到,主体到角色的映射需要根据具体应用环境而定,因此对于模型本身来说,主体动态得到授权的能力弱;同时,基于角色的访问控制模型本身并没有对主体到角色映射中的依据因素进行限定,也需要根据具体应用环境而定,因此授权依据的动态性比较弱;在基于角色的访问控制模型中,也没有考虑授权变更问题。基于授权的访问控制模型中,主体需要服务时,递交相关的信任证,然后根据请求和策略推导出主体的授权,这是一种主体动态获取授权方式;基于授权的访问控制模型中的授权依据是主体获得的信任证,信任证一般需要事先获得,因此授权依据不具有动态性;同样,基于授权的访问控制模型没有考虑授权变更问题。基于属性的访问控制模型依据主体等属性信息,动态授权,因此主体具有动态获取授权的能力;基于属性的访问控制模型的授权依据,不单依赖于主体属性,同时依赖对象和环境属性,因此授权依据具有动态性;不过目前的基于属性的访问控制模型并没有考虑到授权的变更问题。

由于 Web 服务应用环境的分布式特点,标准化是 Web 服务应用需要重点考虑的问题,其中也包括 Web 服务访问控制方面的标准化问题。基于身份的访问控制模型试图从集中管理方式和分布式联盟方式来进行标准化;基于格的访问控制模型一直没有一定的标准;基于角色的访问控制模型目前已经有相关的标准,但是这个标准没有很好说明多域情况下的访问控制问题;基于授权的访问控制模型已经有了不少的规范文档[20,36];而 XACML[46]可以看成是基于属性访问控制模型的一个标准。

综合以上的分析,现有模型在解决 Web 服务访问控制挑战性问题的能力情况,如表 1 所示。

表 1 Web 服务访问控制模型能力

	基于身份	基于格	基于角色	基于授权	基于属性
问题 1	弱	强	弱	强	强
问题 2.a	无	强	弱	强	强
问题 2.b	无	无	弱	无	强
问题 2.c	无	无	无	无	无
标准化	弱	无	弱	强	强

结束语 本文总结了 Web 服务给访问控制带来的挑战性问题,包括跨域访问控制问题、动态授权和标准化问题。同时,在分析各类访问控制模型原理的基础上,综合分析了它们解决 Web 服务访问控制挑战性问题的能力。

从现有模型的分析可以看出,跨域的访问控制已经得到比较好的解决,只是在实现这些模型的时候,还需要复杂的工作要做,如基于格模型需要建立相关的标签系统,基于授权模型需要信任证系统的支持,基于属性模型需要属性证书系统的支持,这些工作具体实现还需要考虑其它因素,如信任模型

等。

对于动态授权，还没有一个模型能够完全适应，主要的问题就是没有相关的授权调整能力。可能的处理方式就是对现有模型进行扩展（如基于角色模型根据属性进行有关映射等），增加相应的动态授权处理能力。同时，可能需要设计一种新的动态授权模型，该模型可以结合现有的模型，一起解决Web服务访问控制问题，如文献[43]中的模型就体现了这样的思想。

标准化是影响Web服务访问控制实现的一个重要问题。目前，虽然有了一些标准，但是Web服务访问控制还需要很多支撑技术，如PKI技术。随着Web服务访问控制技术研究的深入和其他有关标准的出台，需要尽快对Web服务访问控制有关标准进行研究。

参考文献

[1] Kreger H. Web Services Conceptual Architecture 1.0, IBM Software Group. http://www-3.ibm.com/software/solution/webservices/pdf/WSCA.pdf, 2001

[2] Bellwood T, Clement L, Ehnebuske D, et al. OASIS Specification, UDDI v3.0. http://uddi.org/pubs/uddi_v3.htm, 2002

[3] Chinnici R, Gudgin M, Morea J-J, et al. W3C Working Draft, Web Services Description Language (WSDL) Version 2.0 Part1: Core Language. http://www.w3.org/RT/2004/WD-wsdl20-200403026, August 2004

[4] Gudgin M, Hadley M, Mendelsohn N, et al. W3C Recommendation, SOAP Version 1.2 Part 1: Messaging Framework. http://www.w3.org/TR/2003/REC-soap12-part1-20030624/, June 2003

[5] O'Neill M, Allam-Baker P, Cann S M, et al. Web Services Security[M]. McGraw-Hill, 2003

[6] Yuan E, Tong J. Attributed-based Access Control(ABAC) for Web Services[C]//IEEE International Conference on Web Services(ICWS'05). 2005:561-569

[7] Sandu R S, Samarati P. Access Control-Principles and Practice [J]. IEEE Communication, 1994,32(9): 40-48

[8] Kraft R. Research and design issues of access control for network services on the Web[C]//The 3th International Conference on Internet Computing(IC2002). June 2002,3:542-548

[9] Lampson B W. Protection[C]. //5th Princeton Symposium on Information Science and Systems. 1971:437-443

[10] Union I T. ITU-T recommendation X.509 (08/97) - information technology - open systems interconnection - the directory: Authentication framework[S], Aug. 1997

[11] Kohl J, Neuman C. The Kerberos Network Authentication Services. RFC1510, September 1993

[12] Microsoft Passport Service. http://www.passport.net/

[13] The Liberty Alliance Project. http://www.projectliberty.org/

[14] Zimmerman P. The Qficial PGP User's Guide[M]. Cambridge :MIT Press , 1995

[15] Cantor S, Kemp J, Philpott R, et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML), V2.0. OASIS Standard, March 2005

[16] Nadalin A, Kaler C, Monzillo R, et al. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard, February 2006

[17] Damiani E, Vimercati S D C, Paraboschi S. Fine Grained Access Control for Soap E-Services[C]. WWW10, May 2001

[18] Bertino E, Squicciarini A C, Mevi D. A Fine-grained Access Control Model for Web Services[C]//2004 IEEE International Conference on Services Computing(SCC'04). 2004:33-40

[19] Bemmel J V, Wegdam M, Lagerberg K. 3PAC: Enforcing Access Policies for Web Services[C]//IEEE International Conference on Web Services(ICWS'05). 2005:589-596

[20] Ellison C M, Frantz B, Lampson B, et al. SPKI certificate theory. RFC 2693, Sept. 1999

[21] Sandhu R S. Lattice-based Access Control Models[J]. IEEE Computer, Nov. 1993:9-19

[22] Sandhu R, Ferraiolo D, Kuhn R. The NIST Model for Role-based Access Control-Towards A Unified Standard[C]//The 5th ACM Workshop on Role Based Access Control. July 2000

[23] Ferrailo D F, Barkley J F, KuhnD R. A Role based Access Control Model and Reference Implementation Within A Corporate Intranet[J]. ACM Transactions on Information and System Security, 1999, 2(1)

[24] Wonohoesodo R, Tari Z. A Role-based Access Control for Web Services[C]//2004 IEEE International Conference on Services Computing(SCC'04). 2004:49-56

[25] Liu P, Chen Z. An Access Control Model for Web Services in Business Process[C]//Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI'04). 2004:292-298

[26] Liu P, Chen Z. An Extended RBAC Model for Web Services in Business Process [C]//IEEE International Conference on E-Commerce Technology for Dynamic E-Business(CEC-East'04). 2004:100-107

[27] Xu F, Lin G, Huang H, et al. Role-based Access Control System for Web Services[C]//The 4th International Conference on Computer and Information Technology(CIT'04). 2004:357-362

[28] Woo T Y C, Lam S S. Authorization in Distributed Systems-a Formal Approach[C]//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, 1992

[29] Woo T Y C, Lam S S. Authorization in Distributed Systems-A New Approach[J]. Journal of Computer Security. 1993(2/3): 107-136

[30] Woo T Y C , Lam S S. A Framework for Distributed Authorization (extended abstract)[C]// Proceeding of 1st ACM Conference on Computer and Communication Security. Fairfax. Virginia, November 1993:112-118

[31] Woo Y Y C, Lam S S. Designing a Distributed Authorization Service[C]//Proceedings of 17th Annual Joint Conference of the IEEE Computer and Communications Societies. INFOCOM (1998), vol2. IEEE Press, 1998:419-429

[32] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management[C]IEEE Symposium on Security and Privacy. Oakland, May 1996

[33] Blaze M, Feigenbaum J, Strauss M. Compliance-checking in the PolicyMaker Trust-Management System[C]//Proc. 2nd Financial Crypto Conference. Anguilla 1998 LNCS 1465, Springer-Verlag, 1998: 251-265

[34] Blaze M, Feigenbaum J, Ioannidis J. The Role of Trust Management in Distributed Systems Security[C] //Secure Internet Programming, LNCS1603, Springer, 1999:185-210

[35] Blaze M, Feigenbaum J, Keromytis A D. KeyNote: Trust management for public-key infrastructures [C]. LNCS1550, 1999:59-63

[36] Blaze M, FeigenbaumJ, Ioannidis J, et al. The KeyNote Trust-Management System. Version 2, RFC2704, Sept. 1999

[37] Clarke D, Elien J E, Ellison C, et al. Certificate Chain Discovery in SPKI/SDSI[J]. Journal of Computer Security, 2001, 9(4): 285-322

[38] Li N. Delegation Logic: A Logic-based Approach to Distributed Authorization[D]. PhD thesis. New York University, September 2000

[39] Li N, Grosof B N, Feigenbaum J. Delegation Logic: A Logic-based Approach to Distributed Authorization[J]. ACM Transactions on Information and System Security(TISSC), February 2003

[40] Li N, Winsborough W H, Mitchell J C. Distributed Credential Chain Discovery in Trust Management[J]. Journal of Computer Security, 2003, 11(1):35-86

[41] Johnston W, Mudumbai S, Thompson M. Authorization and Attribute Certificates for Widely Distributed Access Control [C]//IEEE Int'l Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. 1998

[42] Li N, Mitchell J C, Winsborough W H. Design of A Role-based Trust Management Framework[C] //Proceedings of the 2002 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, May 2002

[43] Ryutov T. The Condition-driven Authorization Model for Distributed System Services[D]. PhD thesis. University of Southern California, August 2002

[44] Wolf R, Keinz T, Schneider M. A Model for Context-dependent Access Control for Web-based Services with Role-based Approach[C]//4th International Workshop on Database and Expert Systems Application(DEXA'03). 2003

[45] Bhatti R, Bertino E, Ghafoor A. A Trust-based Context-Aware Access Control Model for Web-Services[C]. ICWS04, 2004: 184-192

[46] Moses T. eXtensible Access Control Markup Language (XACML), Version 2.0. OASIS Standard, Feb. 2005

[47] Winsborough W H, Seamons K E, Jones V E. Automated Trust Negotiation[C] //DARPA Information Survivability Conference and Exposition. Vol I, IEEE Press, Jan. 2000: 88-102

[48] Winsborouth W H, Li N. Towards Practical Automated Trust Negotiation[C] //Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks(Policy 2002). IEEE Computer Society Press, June 2002:92-103

[49] Winsborough W H, N Li. Protecting Sensitive Attributes in Automated Trust Negotiation [C] //Proceeding of the ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2002

[50] Li Jian-Xin, Huai Jin-Peng, Li Xian-Xian. Research on Automated Trust Negotiation[J]. Journal of Software, 2006, 17(1): 124-133