基于逻辑的访问控制研究

颜学雄 王清贤
(信息工程大学信息工程学院 郑州 450002)

摘 要 描述了访问控制和逻辑的关系,并将访问控制授权判决问题归约成逻辑蕴涵问题;总结了基于逻辑的访问控制的基本逻辑问题,即逻辑基础、可判定性和安全性分析;分析了一些访问控制模型的基本逻辑问题,包括基于身份的访问控制模型、基于信任管理的访问控制模型和基于属性的访问控制模型;指出了结构化属性描述能力和安全性分析是基于逻辑的访问控制需要进一步研究的问题。

关键词 访问控制,逻辑,可判定性,安全性分析
中图法分类号 TP309 **文献标识码** A

Research of Logic-based Access Control

YAN Xue-xiong WANG Qing-xian
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract This paper addressesd the relation between access control and logic, reduced authorization decision to logic containment, and studied the basic logical issues of access control, namely logical foundation, decidability and security analysis. Then, the paper researched the basic issues of some access control models, which include identity based, trust management based and attribute based access control model. Lastly, the paper discussed the research direction of the logic-based access control, which includes structure attribute logic and security analysis.

Keywords Access control, Logic, Decidability, Security analysis

访问控制是网络信息安全的核心问题之一,用于限制用户的行为,或限制代表用户进行各种操作的程序的执行,以阻止引起系统不安全的行为[1]。授权判决(即用户请求是同意还是拒绝)是访问控制的关键问题,授权判决过程必须是可靠的(授权判决同意的用户请求就是合法的用户请求)、完全的(所有合法的用户请求都能够授权判决同意)和可判定的(任意用户请求能否在有限的时间内给出判决结论)。

早期的访问控制思想比较简单,授权判决过程也比较简单,如访问控制矩阵模型[1-3]。随着分布式信息系统的出现和发展,授权判决问题变得越来越复杂,需要有力的理论基础才能够很好解决,同时保证可靠性、完全性和可判定性。逻辑系统(尤其是一阶逻辑)具有很好的可靠性和完全性的特点,很容易被应用来解决访问控制问题[4-6]。

在访问控制思想和技术发展过程中,有很多基于逻辑的模型和语言[7-13]。但是,从逻辑的角度来看,有些模型和语言没有很好地分析可靠性问题和完全性问题;而且,由于很多逻辑系统本身是不可判定的(如一阶逻辑是不可判定的)[14],有些模型和语言也没有考虑授权判决过程的终止性问题;同时,授权后行为给系统安全带来的影响,也很少被系统设计者关注。

本文首先描述了逻辑和访问控制的基本关系,将授权判决问题归约到逻辑蕴涵问题,并从逻辑的角度分析访问控制的基本逻辑问题,即逻辑基础、授权判决可判定性问题和安全性分析。然后,针对这3个基本逻辑问题,分析了现有一些模型的解决情况。最后,总结分析访问控制还需要解决的一些问题,主要包括结构化知识表达能力和安全性分析问题。

1 访问控制和逻辑关系分析

用户为证明其请求的合法性,往往需要递交证明材料。访问控制授权判决就是根据证明材料和访问控制策略,同意或拒绝用户请求。

如果将证明材料描述成逻辑公式 c_i,c_i 不包含任何变量(事实),则所有的证明材料就是事实的集合:

$$Fact=\{c_1,c_2,\cdots,c_m\}$$

如果将访问控制规则描述成逻辑公式集合 P_i,则访问控制策略 $Policy$ 就是规则的集合:

$$Policy=\{P_1,\cdots,P_n\}$$

将用户请求描述成逻辑公式 R,那么访问控制授权判决过程就变成了逻辑蕴涵问题,即在证明材料集合 $Fact$ 和访问控制策略 $Policy$ 的前提下,用户请求 R 是否为真?

$$Fact\cup(\cup Policy)\mid=?\ R$$

因此,在一定条件下,访问控制问题可以归约到逻辑蕴涵问题。从逻辑的角度分析访问控制,需要研究如下3个基本问题:

到稿日期:2008-05-30 本文受国家高技术研究发展计划(863)(No. 2007AA01Z471)资助。
颜学雄(1975-),男,讲师,主要研究方向为Web服务安全、访问控制,E-mail:yangxuexiong@sina.com;王清贤(1960-),男,教授,博士生导师,主要研究方向为网络信息安全。

· 逻辑基础问题

应用逻辑描述访问控制模型，从逻辑的角度分析模型的可靠性和完全性等。同时考虑其知识表达能力，如复杂知识表达能力等。

· 可判定性问题

对于任意用户请求，授权判决都将在有限的时间内给出判决结论(同意或拒绝)。也就是说，访问控制的性质决定了授权判决过程必须是一个可判定的问题。而一些访问控制模型对应的逻辑语言可能是不可判定的(如一阶逻辑[14,15])，因此需要研究基于逻辑的访问控制的可判定性条件。

· 安全性分析

用户得到授权，执行一定的操作后，可能使得用户授权增加，从而导致用户可以执行一些新的操作。这样的系列操作后，用户最终可能得到非管理员期望的授权。任何安全的访问控制系统，必须能够证明不会出现这个情况。

2 现有访问控制机制分析

文献[16,17]分析了一些访问控制模型和机制。本节从逻辑的角度出发，分析和总结一些访问控制模型的逻辑基础和可判定性问题。

2.1 基于身份的访问控制模型

基于身份的访问控制模型将权限和用户身份关联起来，通常使用访问控制矩阵来描述[1-3]，行表示用户，列表示对象，矩阵格表示用户对对象的访问权限。当用户请求某对象的权限时，判决程序通过查找矩阵做出授权判决。

访问控制矩阵可以用一阶逻辑谓词 $access(user,object,action)$ 描述[6,11]，$user$ 表示用户，$object$ 表示对象，$action$ 表示用户对对象的操作权限，则访问控制矩阵就描述成了谓词 $access$ 的基本公式。

授权判决规则可以表示成如下逻辑公式：

$access(user,object,action)\rightarrow request(user,object,action)$

这样，授权判决问题归约成了逻辑蕴涵判决问题：

$\vdash ?\ request(u,o,a)$

定理 1 基于访问控制矩阵的授权判决问题，其归约的逻辑蕴涵问题是可判定的。

证明：根据 Herbrand 定理[15]可以证明定理 1。证明过程略。

基于角色的访问控制模型[18,19]对访问控制矩阵模型加以改进，根据用户的角色进行授权。基本原理包括两个映射：一是用户到角色的映射，当一个用户请求访问时，给用户分配一个角色；二是角色到权限的映射，根据用户角色对应的权限进行授权判决。

用户到角色的映射，用谓词 $rolemap(user,role)$ 描述，$user$ 表示用户，$role$ 表示角色，则所有的用户到角色的映射关系就组成了谓词 $rolemap$ 的基本公式；角色到权限的映射，用谓词 $perminssion(role,object,action)$ 描述，$role$ 表示角色，$object$ 表示对象，$action$ 表示授权，则角色到权限的所有映射就组成了谓词 $perminssion$ 的基本公式。

授权判决规则可以表示成如下逻辑公式：

$(rolemap(user,role)\wedge perminsseion(role,object,action))\rightarrow request(user,object,action)$

这样，授权判决问题归约成了逻辑蕴涵判决问题：

$\vdash ?\ request(u,o,a)$

定理 2 基于角色的访问控制模型的授权判决问题，其归约的逻辑蕴涵问题是可判定的。

证明：根据 Herbrand 定理[15]可以证明定理 2。证明过程略。

2.2 基于信任管理的访问控制模型

基于身份的访问控制模型不能很好地适应分布式信息系统[20](如网格计算)，其主要原因是难以解决跨域用户的授权问题。

Woo 等[7-10]首先将授权从其他安全服务中分离出来，并重点关注如何进行请求描述、策略描述以及请求和策略的一致性评估。Blaze 等[21-23]进一步提出了信任管理的概念，通过信任证(Credential)来证明用户获得的授权，这样访问控制问题就转化为[23]：用户递交的信任证是否能证明请求满足了策略的要求？该类访问控制模型的核心问题是：权限如何在多个主体之间传递？

Blaze 等[21-23]提出的信任管理语言 PolicyMaker 首次完整地给出了信任管理的基本要素的描述，包括请求描述、断言描述(访问控制规则)。然而，在一般情况下，该语言的一致性评估问题是不可判定的[22]。

KeyNote 语言[24,25]是 PolicyMaker 语言的升级版本，用户递交的信任证和本地策略都表示成断言(Assertion)，根据断言对用户请求进行授权判决[22]。

SPKI/SDSI 语言[26,27]可以看成一种信任管理语言，该语言定义了五元组及其推演规则。文献[28]从一阶逻辑的角度对 SDSI/SPKI 语言进行描述，并证明了五元组推演规则的可靠性和不完全性。

文献[29]给出了一个信任管理语言的数学基础框架，用于统一描述基于信任管理的访问控制模型和语言。该框架应用格上的最小不动点理论，基本框架如下：

(1) $p\in Principal$

(2) $u\in Auth$

(3) $m\in AuthMap=Principal\rightarrow Auth$

(4) $l\in License=AuthMap\rightarrow_m Auth$

(5) $a\in Assertion=Principal\times License$

(6) $M_{Assertion}:P(Assertion)\rightarrow_m AuthMap$

$M_{Assertion}(A)=lfp(\lambda m.\lambda p.\bigcup\{l(m)\mid\langle p,l\rangle\in A\})$

(7) $M_{engine}:Principal\times Auth\times P(Assertion)\rightarrow Bool$

$M_{engine}(p,u,A)=u\subseteq M_{assertions}(A)(p)$

(1)和(2)定义主体和授权集合，要求授权集合 $Auth$ 中的元素组成一个格；(3)定义了一个函数，表示对于特定主体得到其他主体的授权情况，由于 $Auth$ 集合是一个格，因此 $AuthMap$ 中的集合元素也组成一个格；(4)定义了一个单调函数，表示特定主体从 $AuthMap$ 集合中得到的授权；(5)定义了断言，表示授权主体对其他主体的授权；(6)是计算所有主体的授权情况，计算将在 $AuthMap$ 集合的最小不动点处停止；(7)定义了授权判决引擎的计算方式，其含义是，如果用户 p 请求的授权 u，比应用(6)计算出的 $\langle p,auth\rangle$ 中的授权 $auth$ 要少，则授权同意。

将该信任管理的框架转换成逻辑描述，如下：

(1)变元：$p\in Principal,u\in Auth$

(2)函数：$f\_auth(u_1,u_2)=u_3,u_1,u_2,u_3\in Auth$

(3)谓词:$assertion(p,u)$,$p\in Principal$,$u\in Auth$

(4)授权策略规则:

(4.1)$assertion(p,u)\rightarrow request(p,u)$

(4.2)$(assertion(p,u_1)\wedge assertion(p,u_2))\rightarrow$
$assertion(p,f\_auth(u_1,u_2))$

Principal 定义了主体集合,*Auth* 定义了授权集合;函数 f_auth 定义授权迭加的运算;*assertion* 表示断言某主体 p 的授权 u;(4.1)表示,如果用户请求的授权 u,得到了有关断言的支持,则授权通过;(4.2)表示用户拥有授权 u_1 和 u_2,可以得到授权 $f\_auth(u_1,u_2)$。这样,基于信任管理的授权判决问题,归约成逻辑蕴涵判决问题:

$\vdash ?\ request(p,u)$

定理 3 如果授权集合形成一个格,授权迭加函数 f_auth 具有最小不动点,则信任管理的判决问题归约的蕴涵问题是可以判定的。

证明:任一信任管理的授权判决问题对应的逻辑程序为 *Instance*,则 *Instance* 中,*Principal* 集合是有穷的,*Auth* 集合有穷且形成一个格。由于函数 f_auth 在集合 *Auth* 上具有不动点,即集合$\{u|u=f_auth(u_1,u_2),u_1,u_2\in Auth\}$是有穷的,因此,逻辑程序 *Instance* 的 Herbrand 域是有穷的。根据 Herbrand 定理[15]可得到该蕴涵问题是可以判定的。

事实上,要求授权组成一个格且授权迭加函数具有不动点,是比较难的。为了解决这个问题,信任管理语言 DL[30,31]以 Datalog[32,33]为基础理论,设计了"says"和"delegates"表达式来表示授权委托。在授权判决过程中,将 DL 语言转换成一般的逻辑程序,由于 DL 基于 Datalog,保证了授权判决问题的可判定性。

2.3 基于属性的访问控制模型

随着信息技术的发展,出现了面向服务体系结构(Service Oriented Architecture,SOA)[34],相应地提出了基于属性的访问控制模型[35-38,14]。属性就是主体、对象等实体拥有的特性,如身份、年龄等。该模型基本思想就是依据参与实体的属性实现授权判决,如用户属性、对象属性和环境属性等。

RT 语言[36,37]以 Datalog 为理论基础,将基于角色的访问控制思想和信任管理结合起来,将用户属性定义为用户角色,并提供了本地角色定义、角色委托和角色组合等描述。RT 语言的用户和角色关系可以使用谓词 $isMember(x,X)$ 来描述,表示用户 x 拥有角色 X。RT 语言可以将授权规则转换成 Datalog 规则,授权判决问题归约成逻辑蕴涵问题,因此具有可判定性。

文献[39]提出了基于属性访问控制模型的逻辑框架。该框架以受限逻辑程序为基础,主要包括 4 种类型、两大类型的集合和 3 种谓词。Ker_a 和 Set_a 用于描述用户属性,Ker_s 和 Set_s 用于描述服务属性。$cando(X,Y,+/-,Z)$表示拥有属性 X,则可以(+)或者不可以(-)访问服务 Y,Z 表示递归的深度;$dercando(X,Y,+/-,Z)$和 $cando(X,Y,+/-,Z)$的基本含义一样,区别在于前者可以出现在递归规则中,而后者不可以;$do(X,Y,+,Z)$的基本含义和 $cando(X,Y,+/-,Z)$一样,区别在于其用于表示最后的授权结果。该逻辑框架将访问控制策略转换成分层限制(stratified constraint)和 flounder-free 的逻辑程序,因此,具有可判定性[40]。

3 待进一步研究的问题

3.1 结构化属性研究

基于属性的访问控制模型思想比较适合分布式环境,其授权判决过程可归结为属性关联推断:在用户表明的属性集合(各种信任证)U、请求资源的属性集合 R、当前环境属性集合 C 的前提下,用户是否可以拥有请求的行为属性 r?

用户属性、资源属性和环境属性等都具有结构化的特征,如用户的身份属性具有颁发者标识、拥有者标识、颁发时间、有效时间等子属性。而逻辑的结构化表达能力有限,目前基于逻辑的访问控制模型或者语言,从表达能力上来说,还缺乏结构化知识的描述能力,文献[36,37,39]也只提供了部分的结构化描述能力,因此需要进行基于逻辑的结构化属性描述及推理能力研究。主要包括 3 个方面的内容:

(1)属性描述:描述具体属性和抽象属性类,以及它们之间的成员关系;

(2)属性关联描述:将属性和逻辑结合,使用逻辑的方法,描述属性之间的逻辑关联关系;

(3)属性逻辑引擎:根据属性描述、属性关联描述的属性,设计属性的逻辑的推理系统,并设计相应的属性逻辑引擎算法。

3.2 访问控制模型安全性分析

文献[41]分析了基于访问控制矩阵模型的安全性,它将一个保护系统抽象成一个配置(Configuration),表示为三元组(S,O,P),S 表示主体,O 表示对象,P 表示访问控制矩阵。如果在执行 P 许可的一系列操作后,得到了 P 授权之外的权限 r,则称从当前配置泄露了权限 r。一个系统是安全的(Safety),则不会出现权限泄露。访问控制的安全性分析的一般问题是不可判定的[41],此后的多篇文章对此问题进行继续研究,提出了可判定的系统安全性分析模型[3,42]。

文献[43]在文献[41]的基础上,对安全性(Security)分析的概念进行了扩展,包括简单安全性(Simple Safety)、简单可用性(Simple Availability)、范围安全(Bounded Safety)、活跃度(Liveness)、互斥性(Mutual Exclusion)和蕴涵性(Containment)。同时,以 RT 语言[36,37]为典型的信任管理语言,对信任管理进行了安全性分析,并研究了这类问题的可判定性和计算复杂性。

归纳来说,访问控制的安全性分析就是分析在一系列合法的授权执行之后,是否会产生非法的授权。从逻辑的角度,对这个问题刻画如下:

(1)对任何用户,管理员对他授权有一个期望,表示为期望授权集合 R^T。

(2)C 表示用户请求时递交的信任证集合,P 表示基于逻辑描述的授权策略,R^0 表示 $C\cup P$ 推导出来的授权集合:

$C\cup P\vdash R^0$

(3)用户在得到授权集合 R^0 后,执行相应的授权操作后,可能会得到新的授权集合 R^1,这个过程称为授权扩展:

$C\cup P\cup R^0\vdash R^1$

显然有 $R^0\subseteq R^1$,多次扩展后的授权集合表示为 R^*,则访问控制系统的安全性命题可以描述如下:

安全性命题 访问控制系统是安全的,当且仅当 $R^*\subseteq R^T$。

如何对安全性分析问题做进一步的刻画，同时证明有关访问控制系统的安全性命题，是今后需要很好研究的问题。

结束语 对于访问控制来说，授权判决是核心问题之一。授权判决的可靠性保证了授权的合法性，完全性保证了合法用户的合法授权，可判定性保证了授权判决过程的可终止性。

很多逻辑理论具有可靠性和完全性，促使了逻辑理论和访问控制问题的结合，从逻辑的角度来看，访问控制需要考虑逻辑基础、可判定性和安全性分析。

基于身份的访问控制模型主要包括基于访问控制矩阵的模型和基于角色的访问控制的模型，可以归约到一阶逻辑的蕴涵问题，具有可判定性。早期的基于信任管理的访问控制语言缺乏较好的理论基础，甚至是不完全的。因此，从逻辑角度看，其可判定性的条件要求比较苛刻。DL 语言则以 Datalog 作为理论基础，具有可靠性、完全性和可判定性。目前，基于属性的访问控制模型或者语言，借鉴了信任管理的思想和理论基础，具有可靠性、安全性和可判定性。

基于属性的访问控制模型思想是今后发展的一个方向，但是还需要研究结构化属性问题，以提供更灵活的策略描述能力。同时，对于访问控制系统自身的安全性分析工作，研究比较少，将是今后的研究重点。

参 考 文 献

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

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

[3] Sandhu R S. The Typed Access Matrix Model[C]// Proceedings of the 1992 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1992: 122-136

[4] Lampson B, Abadi M, Burrows M, et al. Authentication in Distributed Systems: Theory and Practice [J]. ACM Transaction on Computer Systems, 1992, 10(4): 265-310

[5] Abadi M, Burrows M, Lampson B, et al. A calculus for access control in distributed systems[J]. ACM Transactions on Programming Languages and Systems, 1993, 15(4): 706-734

[6] Abadi M. Logic in Access Control[C]// Proceedings of 18th Annual IEEE Symposium on Logic in Computer Science (LICS' 03). 2003: 228

[7] 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

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

[9] Woo T Y C, Lam S S. Designing a Distributed Authorization Service// Proceedings of Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 1998). vol. 2, IEEE Press, 1998: 419-429

[10] 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

[11] Jajodia S, Samarati P, Subrahmanian V S. A Logical Language for Expressing Authorizations[C]// Proceedings of the 1997 IEEE Symposium on Security and Privacy. 1997

[12] Sirer E G, Wang K. An Access Control Language for Web Services [C]// Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies. 2002: 23-30

[13] Koshutanski H, Massacci F. A Logical Model for Security of Web Services[C]// Proceedings of First International Workshop on Formal Aspects of Security and Trust. Italy, September 2003

[14] Boolos G S, Burgess J P, Jeffrey R C. Computability and Logic. Fourth Edition [M], Cambridge University Press, 2002

[15] Richard A N, Ashore. Logic for Applications[M]. New York: Springer-Verlan, 1997

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

[17] Lin C, Feng F J, Li J S. Access Control in New Network Environment[J]. Journal of Software, 2007, 18(4): 955-966

[18] Sandhu R, Ferraiolo D, Kuhn R. The NIST Model for Role-based Access Control—Towards A Unified Standard[C]// Proceedings of 5th ACM Workshop on Role Based Access Control. July 2000: 26-27

[19] Ferrailo D F, Barkley J F, Kuhn D 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)

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

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

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

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

[24] Blaze M, Feigenbaum J, Keromytis A D. KeyNote: Trust Management for Public-key Infrastructures// LNCS1550. 1999: 59-63

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

[26] Ellison C M, Frantz B, Lampson B, et al. SPKI Certificate theory [S]. RFC 2693, Sept. 1999

[27] 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

[28] Li N, Mitchell J C. Understanding SPKI/SDSI Using First-order logic[J]. Journal of Information Security, 2006, 5(1): 48-64

[29] Weeks S. Understanding trust management systems[C]// Proceedings of 2001 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, May 2001: 94-105

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

[31] 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

[32] Lloyd J W. Foundations of Logic Programming[M]. Second Edition. Springer, 1987

[33] Li N, Mitchell J C. Datalog with Constraints: A Foundation for

Trust Management Languages[C]// Proceedings of Fifth International Symposium on Practical Aspects of Declarative Languages(PADL 2003). New Orleans Louisiana, LNCS 2562, Springer, January 2003:58-73

[34] Alonso G, Casati F, Kuno H, et al. Web Services Concepts, Architecture and Applications[M]. Springer, 2004

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

[36] Li N, Winsborough W H, Mitchell J C. Distributed Credential Chain Discovery in Trust Management (extended abstract) [C] //Proceedings of the Eighth ACM Conference on Computer and Communications Security (CCS-8). ACM Press, November 2001:156-165

[37] 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

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

[39] Wang L, Wijesekera D, Jajodia S. A Logic-based Framework for Attribute based Access Control[C]// Proceedings of 2004 ACM Workshop on Formal Methods in Security Engineering. Washington, D. C., October 2004

[40] Chen W, Warren D S. Tabled Evaluation with Delaying for General Logic Programs[J]. Journal of the ACM, 1996, 43(1):20-74

[41] Harrison M A, Ruzzo W L, Uliman J D. Protection in operating systems[J]. Communications of the ACM, 1976, 19(8):461-471

[42] Sandhu R S. The Schematic Protection Model: Its Definition and Analysis for Acyclic Attenuating Systems[J]. Journal of ACM, 1988, 35(2):404-432

[43] Li N, Winsborough W H, Mitchell J C. Beyond Proof-of-compliance: Safety and Availability Analysis in Trust Management[C] //Proceedings of the 2003 IEEE Symposium on Security and Privacy. May 2003

(上接第 20 页)

[17] OASIS. Web Services Security (WSS) TC. http://www.oasis-open.org, 2006.2

[18] OASIS. Security Assertion Markup Language (SAML) V2.0. http://docs.oasis-open.org/security/saml/v2.0, 2005.5

[19] OASIS. eXtensible Access Control Markup Language v2.0 (XACML). http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip, 2005.2

[20] Tian M, Gramm A, Ritter H, et al. A Survey of Current Approaches Towards Specification and Management of Quality of Service for Web Services[J]. PIK Journal, 2004, 3:132-139

[21] W3C Member. Web Services Policy 1.2 - Framework. http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/, 2006.4

[22] Zeng L Z, Boualem B, Ngu Anne H, et al. QoS-aware middleware for Web services composition[J]. IEEE Transactions on Software Engineering, 2004, 30(5):311-327

[23] Al-Masri E, Qusay H. Mahmoud QoS-based Discovery and Ranking of Web Services [J]. IEEE, 2007:529-534

[24] 文黎明,陆菊康. 基于测量目的的 Web 服务 QoS 监控框架[J]. 微电子学与计算机,2006,23(10):93-95

[25] Zhou C, Chia L T, Lee B S. QoS Measurement Issues with DAML-QoS Ontology [C] // Proceedings of the ICEBE'05. 2005:395-402

[26] Park J T, Back J W. Web-based Internet/Intranet Service Management with QoS Support[J]. IEICE Transactions on Communications, 1999: E82-B (1):1808-1816

[27] Araban S, Sterling L. Measuring Quality of Service for Contract Aware Web-Services [C] // Proceedings of the 1st Australian Workshop on Engineering Service-Oriented Systems. 2004: 54-56

[28] 杨胜文,史美林. 一种支持 QoS 约束的 Web 服务发现模型[J]. 计算机学报,2005,28(4):589-594

[29] Feng X Z, Ren Y, Hu J Q, et al. A Model for Service Composition with Multiple QoS Constraints[C]// Proceedings of the International Conference on Computing: Theory and Applications table of contents. 2007:208-213

[30] Tian M, Gramm A, Ritter H, et al. Efficient Selection and Monitoring of QoS Aware Web Services with the WS-QoS Framework[C] // Proc. IEEE/WIC/ACM Int'l Conf. Web Intelligence. IEEE CS Press, 2004:52-158

[31] Hwang S Y, Wang H J, Tang J, et al. A probabilistic approach to modeling and estimating the QoS of web-services-based workflows [J]. Information Sciences, 2007, 177(23):5484-5503

[32] Yoon S, Kim D, Han S. WS-QDL containing static, dynamic, and statistical factors of Web services quality [C]// IEEE Proceedings of the IEEE International Conference on Web Services. IEEE Computer Society Press, 2004:808-809

[33] Zhang J. Trustworthy Web Services-actions for Now[J]. IEEE IT Pro, 2005, 7:32-36

[34] Dobson G. Quality of Service in Service-Oriented Architectures. http://digs.sourceforge.net/papers/qos.html, 2004.9

[35] 冯名正. Web 服务组合关键技术研究[D]. 南京:东南大学,2006

[36] Kim Y, Doh K G. A Trust Type Based Model for Managing QoS in Web Services Composition[C] // 2007 International Conference on Convergence Information Technology. IEEE Computer Society, 2007:438-443

[37] Daniel A, Menasc'ea, Ruana H, et al. QoS management in service- oriented architectures [J]. Performance Evaluation, 2007, 64:646-663

[38] Tian M. QoS integration in Web Services with the WS-QoS framework. Dissertation for Doctor, 2005.12

[39] Wille E, Mehhia M, Leonardi M, et al. Algorithm for IP network design with end-to-end QoS constraints [J]. Computer Networks, 2006, 50:1086-1103

[40] IBM. Use architecture and levels of abstraction to create a better SOA. http://www.ibm.com/developerworks/architecture /library /ar-archserv1/, 2007.9

[41] 胡建强,邹鹏,王怀名,等. Web 服务描述语言 QWSDL 和服务匹配模型研究[J]. 计算机学报,2005,28(4):505-513

[42] 李盛恩,洪晓光. 一种业务流程 QoS 有保障的动态服务组合方法[J]. 计算机科学,2007,34(12):107-110

[43] 曹蓟光,周永丽. 多媒体业务服务质量相关问题的研究[J]. 现代电信科技,2004(11):16-20