doi:10.3969/j.issn.1000-436x.2014.z2.034

基于非合作博弈的访问控制安全机制

张伊璇，何泾沙，赵斌
（北京工业大学 软件学院，北京 100124）

摘 要：访问控制技术是保护计算机系统和网络中的敏感信息和关键资源的一种重要的信息安全技术。但是传统的访问控制方法只能被动地对用户的访问请求进行响应，无法完全适应如今不断动态变化的网络环境。为了提高访问控制中系统应对恶意攻击和威胁的能力，基于博弈论中的非合作博弈方法，设计了一套适用于访问控制模型的安全机制，当访问主体提出访问请求后，对访问主体与被访问客体进行非合作博弈，得到纳什均衡，最终通过纳什均衡与门限的比较决定是否对访问主体进行授权。实验证明了该安全机制的有效性。

关键词：访问控制；非合作博弈；级别—权限—收益表；级别—权限—门限表
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0246-05

Security mechanism in access control based on non-cooperative game

ZHANG Yi-xuan, HE Jing-sha, ZHAO Bin
(School of Software Engineering, Beijing University of Technology, Beijing 100124, China)

Abstract: Access control technology is an important information security technology to protect the sensitive information and critical resources in computer system and network. But traditional access control methods could only respond to access requests of users passively and can't meet the changing dynamic network environment. In order to improve the ability to respond to malicious attacks and threats in access control system, a security mechanism is designed, which is suitable for access control, based on non-cooperative game theory in the game. When the subject makes an access request to the object, there will be a non-cooperative game between them to get Nash equilibrium. Then the security mechanism will compare the probabilities in the Nash equilibrium to the setting thresholds to get the conclusion that whether to authorize the subject or not. Experiment proves the effectiveness of the security mechanisms.

Key words: access control; non-cooperative game; level-permissions-payoffs table; level-permissions-threshold table

1 引言

信息安全是当前的研究热点，访问控制作为一项保护计算机系统和网络中的敏感信息和关键资源免受恶意攻击的重要的信息安全技术，吸引了越来越多的研究者。它允许被授权的主体对某些客体进行访问，同时拒绝向非授权的主体提供服务，通常用于系统管理员控制用户对服务、文件等网络资源的访问。但是随着通信技术的高速发展，当前的网络环境已经从早期相对静态的、面向机构内部或者特定用户群体的、封闭式网络发展成为面向大量外部用户的、可共享的动态开放式网络。而传统的访问控制模型无法完全满足动态网络的安全需求，也无法根据对恶意用户攻击行为的危害大小施以不同程度的惩罚，只能被动承受恶意访问行为带来的损失。

为了使访问控制技术能更好地应对当前网络环境中的未知风险，本文将非合作博弈技术引入其中，设计了一套适用于访问控制模型的安全机制。

收稿日期：2014-10-21
基金项目：国家自然科学基金资助项目（61272500）；北京市自然科学基金资助项目（4142008）；市委、市政府重点工作及区县政府应急项目预启动基金资助项目（Z131100005613030）
Foundation Items: The National Natural Science Foundation of China (61272500); The Natural Science Foundation of Beijing (4142008); Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030)

在本文设计的该安全机制中设置级别—权限—收益表和级别—权限—门限表，当用户提出访问请求后，首先根据用户行为将用户对应到不同级别，再通过级别—权限—收益表获得当前级别下用户请求的各个权限对应的收益，收益包括访问主体的收益以及被访问客体的收益，之后在二者收益的基础上进行非合作博弈，得到访问主体与被访问客体之间的纳什均衡。通过该纳什均衡，可以得到被访问客体将某一权限授予访问主体的概率，再通过授权概率与权限对应的门限之间的比较，决定被访问客体是否将这一权限授予访问主体。

2　相关工作

访问控制是一种限制通过身份验证的合法实体的行为和操作的安全机制，通过对合法用户和服务请求进行授权，保证用户和服务请求的操作遵守该组织的安全策略。传统的访问控制策略分为以下3种：自主访问控制[1]、强制访问控制[2]和基于角色的访问控制[3,4]。其中，自主访问控制是基于身份的一种授权策略，强制访问控制是基于系统中设定的安全规则进行访问，而基于角色的访问控制的基本思想是将访问权限分配给角色，再根据用户的身份分配一定的角色，该用户就具有了该角色的所有权限。在基于角色的访问控制的基础上，又发展出了基于上下文的访问控制[5]和基于属性的访问控制[6,7]。基于上下文的访问控制是将访问请求者所处的环境等上下文因素作为访问控制决策的依据，而基于属性的访问控制是将参与决策的相关实体的属性作为基础进行访问控制的授权。

本文将非合作博弈引入到访问控制中，非合作博弈是一种参与者不可能达成具有约束力的协议的博弈类型，指的是博弈双方之间没有一个具有约束力的协议[8]。非合作博弈研究的是策略选择问题，即博弈方如何在利益相互影响的局势中进行决策，从而使自己的收益最大。在非合作博弈条件下，可能会形成的一种均衡状态，这就是纳什均衡[9]。在纳什均衡中，任何一个博弈方单方面的改变策略，都会造成自己的收益下降（或不变），不会使自己的收益增加，因此每个博弈方都不会轻举妄动去破坏这个平衡。

3　安全机制基础

本文主要是通过非合作博弈方法建立一套安全机制，使访问控制模型具备更好的抵御开放式动态网络中恶意威胁和攻击的能力。其中，级别—权限—收益表与级别—权限—门限表是安全机制的基础，下面分别对它们进行介绍。

3.1　级别—权限—收益表

当访问主体向被访问客体的某些权限提出访问请求后，系统会根据主体的访问参数计算其对应的安全级别，再根据级别—权限—收益表以及收益子表获取各个权限在该安全级别下，带给访问主体与被访问客体的收益。级别—权限—收益如表1所示。

表 1　　**级别—权限—收益表**

级别	权限				
	Q_1	Q_2	…	…	Q_n
J_1	T_{11}	T_{12}	…	…	T_{1n}
J_2	T_{21}	T_{22}	…	…	T_{2n}
…	…	…	…	…	…
…	…	…	…	…	…
J_m	T_{m1}	T_{m2}	…	…	T_{mn}

从表1可以发现，安全机制中共有 m 个安全级别和 n 个权限，分别是 $\{J_1, J_2, \cdots, J_m\}$ 以及 $\{Q_1, Q_2, \cdots, Q_n\}$。而第 i 个安全级别 J_i 和第 j 个权限 Q_j 对应的收益 T_{ij} 代表的是级别—权限—收益表的收益子表，在该收益子表中，访问主体与被访问客体不同的策略选择会带来不同的收益，它们之间的博弈就是在这些收益的基础上进行的。T_{ij} 如表2所示。

表 2　　**收益子表 T_{ij}**

被访问客体	访问主体	
	诚实访问	不诚实访问
授权	$O_income_{per}^{hon}, S_income_{per}^{hon}$	$-O_loss_{per}^{mal}, S_income_{per}^{mal}$
不授权	$-O_income_{per}^{hon}, 0$	$O_income_{den}^{mal}, -S_loss_{den}^{mal}$

3.2　级别—权限—门限表

在安全机制中，当访问主体与被访问客体之间的博弈结束之后，会得到被访问客体选择授权策略的概率，而客体最终是否对主体请求的某一权限进行授权，则要看授权概率与门限比较的结果。如果授权概率大于门限，则授权；否则，不授权。门限是一套可以灵活设置的参数，方便系统根据自身抵御未知风险的能力决定授权尺度的大小。如果系统自身抵御网络中未知风险的能力较强，即系统拥有防火墙、入侵检测系统等识别并抵御恶意攻击和威

胁的措施，则将门限设置为较小的值，可以对更多的访问请求进行授权，有利于吸引更多的用户；如果系统自身抵御网络中未知风险的能力较弱，则将门限设置为较高的值，加大拒绝用户可能的恶意攻击与威胁的概率。级别—权限—门限如表 3 所示。

表 3　　级别—权限—门限表

级别	权限				
	Q_1	Q_2	…	…	Q_n
J_1	R_{11}	R_{12}	…	…	R_{1n}
J_2	R_{21}	R_{22}	…	…	R_{2n}
…	…	…	…	…	…
…	…	…	…	…	…
J_m	R_{m1}	R_{m2}	…	…	R_{mn}

如表 3 所示，安全机制中共有 m 个安全级别和 n 个权限，分别是$\{J_1, J_2,\cdots, J_m\}$以及$\{Q_1, Q_2, \cdots, Q_n\}$。而第 i 个安全级别 J_i和第 j 个权限 Q_j对应的门限 R_{ij}代表在该级别下该权限对应的门限值。

4　基于非合作博弈的安全机制

在访问主体与被访问客体进行博弈的过程中，需要具备 3 项基本要素：参与者、策略空间以及收益。显然，在访问控制中，访问主体与被访问客体就是博弈过程的参与者，并且它们各自的策略空间是天然存在的，对访问主体而言，策略空间是{诚实访问，不诚实访问}，对被访问客体而言，策略空间是{授权，不授权}。参与者不同的策略选择会得到不同的收益，它们的收益体现在级别—权限—收益表中。当博弈过程结束后，会得到被访问客体对访问主体的访问请求授权的概率，通过级别—权限—门限表可以得到某一级别的访问主体请求访问某一权限时的门限值，将授权概率与门限值进行比较，被访问客体最终得到决定是否将该权限授权给该级别的访问主体。其具体流程如图 1 所示。

Step1　访问主体对客体的 p 个权限提出访问请求。

Step2　系统获取主体的访问参数，例如主体 IP 地址、端口号、访问时间、请求的权限个数等。

Step3　通过访问主体的 IP 地址及端口号获取该主体对应的历史记录。

Step4　通过主体的访问参数以及历史记录计算主体对应的安全级别。

Step5　根据级别—权限—收益表获取该级别的主体请求的 p 个权限分别对应的收益子表。

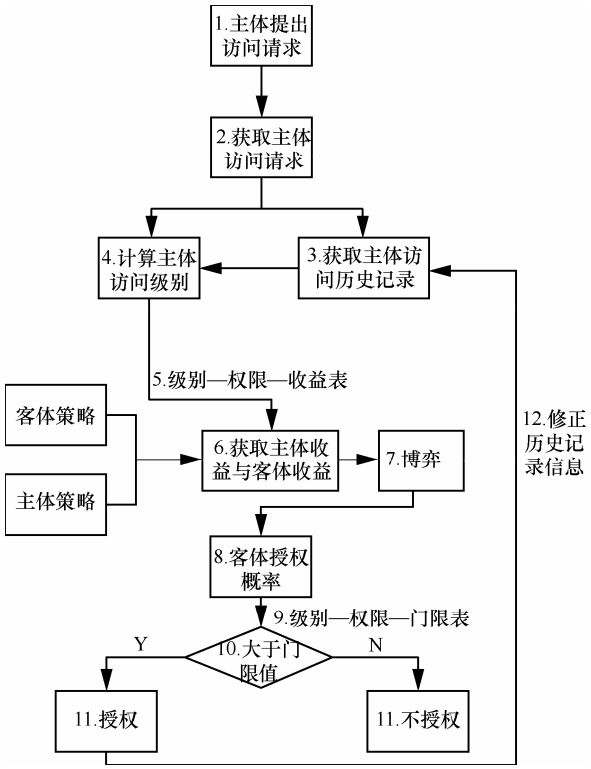


图 1　安全机制流程

Step6　访问主体的策略集合为{诚实访问，不诚实访问}，访问客体的策略集合为{授权，不授权}，根据收益子表获取参与者选择不同访问策略时对应的不同收益。

Step7　主体与客体进行博弈，从而达到纳什均衡。在双方达到纳什均衡的过程中，针对 p 项权限中的每一项权限而言，设客体选择授权与不授权的概率为 $\boldsymbol{P}_o$=(x, 1−x)，主体选择诚实访问与不诚实访问的概率为 $\boldsymbol{P}_s$=(y, 1−y)，通过式(1)~式(3)可以计算出 x 的值。

主体的收益函数为 $E_{subject}$，计算方法如式(1)。

$$\begin{aligned} E_{subject} &= \boldsymbol{P}_o \boldsymbol{P}_{subject} \boldsymbol{P}_S^{\mathrm{T}} = (x,1-x) \cdot \\ &\quad \begin{pmatrix} S_income_{per}^{hon} & S_income_{per}^{mal} \\ 0 & -S_loss_{den}^{mal} \end{pmatrix} (y,1-y)^{\mathrm{T}} \\ &= xS_income_{per}^{hon} y + xS_income_{per}^{mal} \cdot \\ &\quad (1-y) + (1-x)\left(-S_loss_{den}^{mal}\right)(1-y) \end{aligned} \tag{1}$$

$E_{subject}$对 y 求导得到式(2)。

$$\frac{\partial E_{subject}}{\partial y} = xS_income_{per}^{hon} - xS_income_{per}^{mal} + (1-x)\left(S_loss_{den}^{mal}\right) \tag{2}$$

令求导公式为 0，得到 x 的值，如式(3)。

$$x=\frac{S_loss_{den}^{mal}}{S_income_{per}^{mal}+S_loss_{den}^{mal}-S_income_{per}^{hon}} \quad (3)$$

Step8　x 的值即是被访问客体选择对该权限进行授权的概率，通过上一步可以得到客体对主体请求的 p 项权限的授权概率集合$\{x_1, x_2,\cdots, x_p\}$。

Step9　通过级别—权限—门限表得到主体请求的 p 项权限对应的门限值集合$\{R_1, R_2,\cdots, R_p\}$。

Step10　判断集合$\{x_1,x_2,\cdots, x_p\}$中的各项值是否大于集合$\{R_1, R_2, \cdots, R_p\}$中对应的值。

Step11　如果权限概率大于门限值成立，则客体最终授权给主体；否则，不授权。

Step12　根据最终的结果对该主体对应的历史记录进行修正。

5　实验分析

为了验证基于非合作博弈的访问控制安全机制的有效性，运用 Matlab 进行了仿真实验，假设有 10 个访问主体 $S_1, S_2,\cdots, S_{10}$ 与 10 个被访问客体 $O_1, O_2,\cdots, O_{10}$，其中 5 个主体 $S_1, S_2, \cdots, S_5$ 通过传统访问控制方法随机访问客体 30 次，另外 5 个主体 $S_6, S_7,\cdots, S_{10}$ 通过本文提出的基于非合作博弈的访问控制机制随机访问客体 30 次。实验 1 中以较高的初始概率平均值 0.9 选择诚实访问，实验 2 中以较低的初始概率平均值 0.1 选择诚实访问，之后选择诚实访问的概率平均值分别如图 2 和图 3 所示。

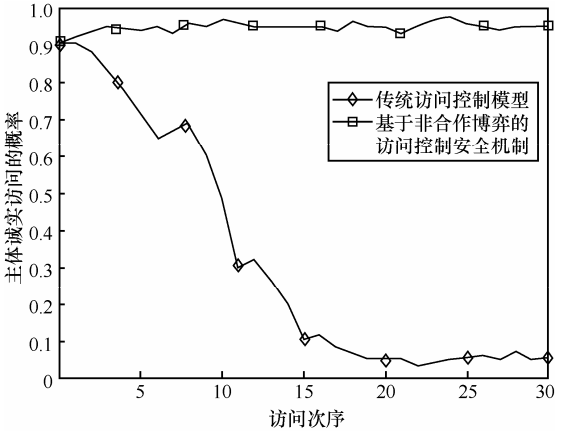


图 2　以较高初始概率开始的主体选择诚实访问的概率

通过图 2 和图 3 可以发现，不论以较高的初始概率还是以较低的初始概率开始，在传统访问控制中，用户选择诚实访问的概率是随机波动的，这是因为不论用户采取什么样的访问策略都不会对他下一次的访问产生影响，因此用户会在提出访问请求时会随机选择访问策略，并且为了获得更大的利益，用户会偏向于恶意访问。而在采用了基于非合作博弈的安全机制的访问控制模型中，用户选择诚实访问的概率是随着访问次数而大体增长的，这是因为在纳什均衡的作用下，如果用户采取了诚实的访问策略，访问结果会反馈到历史信息中，从而使用户的安全等级逐渐提高，获取的收益也在不断变化，用户的访问请求被授权的概率也会随之增长，最终用户会得到更多的访问权限。反之，如果用户在某次选择了不诚实访问，他将会被惩罚，最终被减少得到的访问权限。因此，采用非合作博弈的安全机制后，用户选择诚实访问的概率明显高于传统访问控制模型。所以，本方法可以更好地应对当前网络环境带来的未知风险，提高访问控制中系统抵御恶意攻击和威胁的能力。

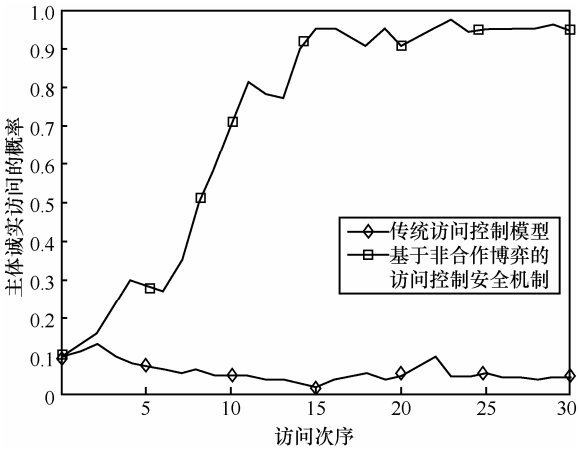


图 3　以较低初始概率开始的主体选择诚实访问的概率

6　结束语

本文基于博弈论中的非合作博弈方法，设计了一套适用于访问控制模型的安全机制，在该机制中，当访问主体提出访问请求后，首先通过主体的访问参数计算主体的安全级别，再通过级别—权限—收益表得到该级别下的主体请求访问的各个权限分别对应的收益子表，在此基础上，访问主体与被访问客体进行非合作博弈，得到纳什均衡，从而得到客体对主体请求的各个权限进行授权的概率，最终通过这些概率与级别—权限—门限表中门限值的设置的比较决定是否对访问主体进行授权。接下来，通过实验证明了该安全机制可以有效提高访问控制中系统应对未知风险的能力。

参考文献：

[1] SNYDER L. Formal models of capability-based protection systems[J]. IEEE Trans on Computers, 1981, 30(3): 172-181.

[2] LAPADULA L J, BELL D E. Secure Computer Systems: a Mathematical Model[M]. MA, USA: Mitre Corporation, 1973.

[3] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[4] FERRAIOLO D, RICHARD D, KUHN. Role-based access control[A]. Proc NIST-NSA National Computer Security Conference[C]. 1992. 554-563.

[5] TONINELLI A, MONTANARI R, KAGAL L, *et al*. A semantic context-aware access control framework for secure collaborations in pervasive computing environments[A]. Proc 5th International Semantic Web Conference[C]. Athens, GA, USA, 2006.473-486.

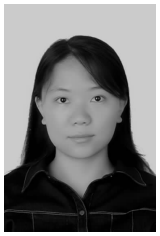
[6] YUAN E, JIN T. Attribute based access control (ABAC) for Web service[A]. Proc 2005 IEEE International Conference on Web Service[C]. Orlando, FL, USA, 2005.561-569.

[7] ZHANG X, LI Y. An attribute-based access matrix model[A]. Proceedings of the 2005 ACM Symposium on Applied Computing[C]. Santa Fe, New Mexico, 2005.45-55.

[8] 郑耿忠, 刘三阳, 齐小刚. 基于非合作博弈的无线传感器网络功率控制研究[J]. 控制与决策, 2011, 26(7): 1014-1018.
ZHENG G Z, LIU S Y, QI X G. Study on power control of wireless sensor networks based on non-cooperative game[J]. Control and Decision, 2011, 26(7): 1014-1018.

[9] 侯剑, 张立卫. 广义纳什均衡问题求解的极小极大方法[J]. 大连理工大学学报, 2013, 53(6): 924-929.
HOU J, ZHANG L W. Minimax method to solve the problem of generalized Nash equilibrium[J]. Journal of Dalian University of Technology, 2013, 53(6): 924-929.

作者简介：



张伊璇（1988-），女，河北深州人，北京工业大学博士生，主要研究方向为网络信息安全、云计算、访问控制等。

何泾沙[通信作者]（1961-），男，美籍华人，北京工业大学教授、博士生导师，主要研究方向为计算机与网络安全、网络测试技术、无线通信技术。E-mail: jhe@bjut.edu.cn。

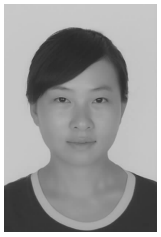
赵斌（1979-），男，山东济宁人，北京工业大学博士生，主要研究方向为网络与信息安全。

（上接第 245 页）

New McEliece variants from moderate density parity-check codes[A]. 2013 IEEE International Symposium Information Theory Proceedings (ISIT)[C]. IEEE, 2013.2069-2073.

[17] SENDRIER N. On the use of structured codes in code based cryptography[A]. Coding Theory and Cryptography III, The Royal Flemish Academy of Belgium for Science and the Arts[C]. 2010.

作者简介：



李泽慧（1990-），女，陕西咸阳人，西安电子科技大学硕士生，主要研究方向为编码理论公钥密码体制、密码学与信息安全。

杨亚涛（1978-），男，河南平顶山人，博士，北京电子科技学院讲师、硕士生导师，主要研究方向为网络安全、可信计算等。

李子臣（1965-），男，河南焦作人，西安电子科技大学教授、硕士生导师，主要研究方向为密码学可信计算、信息安全与密码学等。