

基于任务的访问控制模型*

邓集波⁺, 洪帆

(华中科技大学 计算机科学与技术学院 数据安全与保密实验室,湖北 武汉 430074)

Task-Based Access Control Model

DENG Ji-Bo⁺, HONG Fan

(Laboratory of Data Security and Cryptology, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

+ Corresponding author: Phn: 86-27-87555893, E-mail: dengjb303@163.com

<http://www.hust.edu.cn>

Received 2001-06-22; Accepted 2001-09-18

Deng JB, Hong F. Task-Based access control model. *Journal of Software*, 2003,14(1):76~82.

Abstract: Nowadays, all access control models take a system-centric view of protecting resources, and they don't take the context into account when controlling the permissions. However, with the development of databases, networking, and distributed computing, it causes people to shift the focus on security issues from the protection of individual objects and subjects in isolated computer systems, to the protection of dynamically authorization with different task. In this paper, an access control mechanism called TBAC (task-based access control) is introduced, which models from the tasks in workflow and dynamically manage the permissions through tasks and tasks' status. The TBAC is well suited for distributed computing, information processing activities with multiple points of access, and decision making in workflow and distributed process and transaction management system. The basic concepts of TBAC are introduced and a formalization description and an analysis are given. It is clear that TBAC will be used widely in many fields, such as OA, business, and so on.

Key words: task-based access control; active security model; task; workflow

摘要: 目前的访问控制模型都是从系统的角度出发去保护资源,在进行权限的控制时没有考虑执行的上下文环境。然而,随着数据库、网络 and 分布式计算的发展,组织任务进一步自动化,与服务相关的信息进一步计算机化,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态的主体和客体保护,转移到随着任务的执行而进行动态授权的保护上。介绍了一种称为基于任务的访问控制 TBAC(task-based access control)的访问控制机制。它从 workflow 中的任务角度建模,可以依据任务和任务状态的不同,对权限进行动态管理。TBAC 非常适合分布式计算和多点访问控制的信息处理控制以及在工作流、分布式处理和事务管理系统中的决策制定。介绍了 TBAC 的基本概念,对其模型进行了形式化描述和分析。可以预见,TBAC 将在办公及商业等多种领域中得到广泛的应用。

* Supported by the National High Technology Development 863 Program of China under Grant No.863-301-1-3 (国家 863 高科技发展计划)

第一作者简介: 邓集波(1977—),男,湖南祁阳人,硕士,主要研究领域为访问控制,数据库安全。

关键词: 基于任务的访问控制;主动安全模型;任务; workflow

中图法分类号: TP311 文献标识码: A

目前,许多敏感的信息和技术都是通过计算机来控制和管理.如何确保这些不被人窃取和破坏,即如何使它们安全,是当今计算机技术的研究热点.ISO(国际标准化组织)在网络安全标准(ISO7498-2)中定义了5个层次型安全服务(身份认证服务、访问控制服务、数据保密服务、数据完整性服务、不可否认服务),访问控制是其中的一个重要组成部分.所谓访问控制,就是通过某种途径显式地准许或限制访问能力及范围,从而限制对关键资源的访问,防止非法用户的侵入或者合法用户的不慎操作造成破坏.

近20年来,人们在访问控制的研究方面取得了很大成果,有许多访问控制模型被提出来.20世纪70年代,Harrison, Ruzzo 和 Ullman 提出了 HRU 模型.接着,Jones 等人在1976年提出了 Take-Grant 模型.后来,又有著名的自主访问控制模型(DAC)和强制访问控制模型(MAC)提出来了.这些早期努力的总结参见文献[1].近几年比较热门的访问控制模型是由 Ferraiolo 和 Kuhn 在1992年提出的基于角色的访问控制(role-based access control).Ferraiolo 和 Ravi Sandhu 对此作了许多研究^[2,3].

通过对这些访问控制模型的研究可以看出,它们都是从系统的角度(控制环境是静态的)出发保护资源.其访问控制的原理可以简单地描述为:如果主体对某客体有访问操作请求,而且主体拥有操作权限,那么提供访问操作.我们将它们统称为被动安全模型.这种控制原理比较简单——它没有将执行操作所处的环境考虑在内,这样容易造成安全隐患.例如,在文献[4,5]中描述了一些企图利用这些简单性造成的隐患的行为.此外,在这些安全模型中,不能记录主体对客体权限的使用,权限没有时间限制,只要主体拥有对客体的访问权限,主体就可以无数次地执行该权限.

然而,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,与服务相关的信息进一步计算机化,这促使我们将安全问题方面的注意力从独立的计算机系统中静态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.当前的一个研究热点是 workflow. workflow^[6]是为完成某一目标而由多个相关的任务(活动)构成的业务流程.它的主要特点是使处理过程自动化,对人和其他资源进行协调管理,从而完成某项工作. workflow 所关注的问题是处理过程的自动化.它根据一系列定义的规则,把文档、信息或任务在参与者之间传递,以达到某种目的.

在 workflow 应用访问控制^[7,8]时,传统的访问控制技术显得力不从心.当数据在 workflow 中流动时,执行操作的用户在改变,用户的权限也在改变,这与数据处理的上下文环境相关.采用传统的访问控制技术,如 DAC, MAC, 则难以做到这一点,若采用 RBAC,也需要频繁地更换角色,且不适合 workflow 的运转.因此,有必要采用一种新的访问控制模型.

1 基于任务的访问控制(TBAC)

TBAC 是一种新的安全模型,从应用和企业层角度来解决安全问题(而非已往从系统的角度).它采用“面向任务”的观点,从任务(活动)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动态实时的安全管理^[9-11].在 TBAC 中,对象的访问权限控制并不是静止不变的,而是随着执行任务的上下文环境发生变化,这是我们称其为主动安全模型的原因.具体说来,TBAC 有两点含义.首先,它是在 workflow 的环境考虑对信息的保护问题.在 workflow 环境中,每一步对数据的处理都与以前的处理相关,相应的访问控制也是这样,因而 TBAC 是一种上下文相关的访问控制模型.其次,它不仅能对不同 workflow 实行不同的访问控制策略,而且还能对同一 workflow 的不同任务实例实行不同的访问控制策略.这是“基于任务”的含义,所以 TBAC 又是一种基于实例(instance-based)的访问控制模型.最后,因为任务都有时效性,所以在基于任务的访问控制中,用户对于授予他的权限的使用也是有时效性的.

1.1 TBAC的基本概念

(1) 授权步(authorization step).表示一个原始授权处理步,是指在一个 workflow 中对处理对象(如办公流程

中的原文档)的一次处理过程.它是访问控制所能控制的最小单元.授权步由受托人集(trustee-set)和多个许可集(permissions set)组成,如图 1 所示.其中,受托人集是可被授予执行授权步的用户的集合,许可集则是受托集的成员被授予授权步时拥有的访问许可.当授权步初始化以后,一个来自受托人集中的成员将被授予授权步,我们称这个受托人为授权步的执行委托者,该受托人执行授权步过程中所需许可的集合称为执行者许可集.在 TBAC 中,一个授权步的处理可以决定后续授权步对处理对象的操作许可,我们将这些许可称为激活许可集.执行者许可集和激活许可集一起称为授权步的保护态.

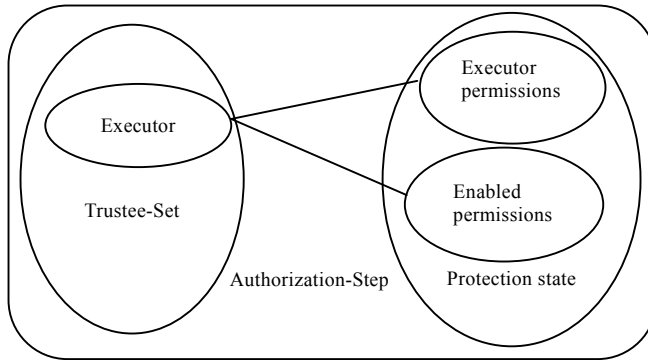


Fig.1 Authorization-Step

图 1 授权步

(2) 授权结构体(authorization unit).授权结构体是由一个或多个授权步组成的结构体,它们在逻辑上是联系在一起的.授权结构体分为一般授权结构体和原子授权结构体.一般授权结构体内的授权步依次执行,原子授权结构体内部的每个授权步紧密联系,其中任何一个授权步失败都会导致整个结构体的失败.

(3) 任务(task).任务是工作流程中的一个逻辑单元.它是一个可区分的动作,可能与多个用户相关,也可能包括几个子任务.例如,一个支票处理的流程包括 3 个任务:准备支票、批准支票和提交支票.在实际工作中,一个任务包含如下特征:(a) 长期存在;(b) 可能包括多个子任务;(c) 完成一个子任务可能需要不同的人.

这里,我们确定任务与授权结构体的联系.授权结构体是任务在计算机中进行控制的一个实例.任务中的子任务,对应于授权结构体中的授权步.

(4) 依赖(dependency).依赖是指授权步之间或授权结构体之间的相互关系,包括顺序依赖、失败依赖、分权依赖和代理依赖.依赖反映了基于任务的访问控制的原则.各种依赖关系的定义见表 1.

总之,一个 workflows 的业务流程由多个任务构成.而一个任务对应于一个授权结构体,每个授权结构体由特定的授权步组成.授权结构体之间以及授权步之间通过依赖关系^[11]联系在一起.表 1 定义了 TBAC 建模中所需的一些符号.

考虑一个支票处理应用,职员必须准备支票,指定一个账户,然后 3 个(分开的)监督者必须批准该支票和账户,最后支票由另一个不同的职员发出(通过凭证区分职员).下面我们利用表 1 中的符号对支票处理的工作流进行模型化,如图 2 所示.在图 2 中,FU1~FU3 分别表示 workflow 单元 1~workflow 单元 3,Au1~Au3 分别表示授权结构体 1~授权结构体 3.其中,workflow 单元 1 由准备支票任务组成,workflow 单元 2 由 3 个不同的人分别执行批准支票的任务,workflow 单元 3 由提交支票组成,授权结构体 1 由一个准备支票授权步组成,授权结构体 2 由 3 个批准支票授权步组成,授权结构体 3 由提交支票授权步组成.

1.2 TBAC 授权

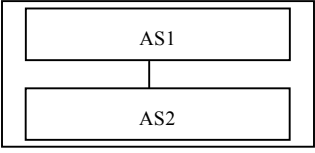
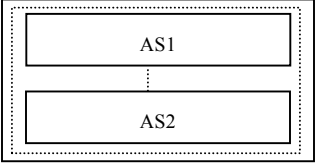
作为一种新的主动访问控制模型,TBAC 的授权与传统访问控制模型的授权有很大的不同.

传统访问控制模型的授权一般用三元组 (S,O,P) 表示,其中 S 表示主体, O 表示客体, P 表示许可.如果存在元组 (S,O,P) ,则表明 S 可在 O 上执行 P 许可.否则, S 对 O 无任何操作许可.这些三元组都是预先定义好并静态地存放在系统中,且无论何时都是有效的.对于用户的权限限制,访问控制是被动的、消极的.

在 TBAC 中,授权需用五元组 (S,O,P,L,AS) 来表示.其中 S,O,P 的意义同前, L 表示生命周期(lifecycle), AS 表示

授权步 P 是授权步 AS 所激活的权限,而 L 则是授权步 AS 的存活期限. L 和 AS 是 TBAC 不同于其他访问控制模型的显著特点.在授权步 AS 被触发之前,它的保护态是无效的,其中包含的许可不可使用.当授权步 AS 被触发时,它的委托执行者开始拥有执行者许可集中的权限,同时它的生命期开始倒记时.在生命期期间,五元组 (S,O,P,L,AS) 有效.当生命期终止,即授权步 AS 被定为无效时,五元组 (S,O,P,L,AS) 无效,委托执行者所拥有的权限被回收.

Table 1 Signal define in TBAC
表 1 TBAC 中的符号定义

	Authorization-Step	Signal	Note
Unit		AS	The primary unit in model
	Normal authorization unit		It consists of one or more AS, among which are order.
	Atomic authorization unit		It consists of one or more AS, among which are atomic.
Dependency	Order dependency	AS1 → AS2	AS2 can be activated only after AS1 has been finished.
	Defeat dependency	AS1 → AS2	AS2 can be activated only after AS1 has defeated.
	Defeat revocation and agent dependency	AS1 $\xrightarrow{\{r,d\}}$ AS2	The d means that AS1's permissions can be surrogated to AS2 when AS1 is aborted, the r means that AS2 and it's permissions are revoked when AS1 is aborted.
	Divided permission dependency	AS1 ↔ AS2	AS1 and AS2 must be executed by different user.
	Graded and divided permission dependency	AS1 $\xleftrightarrow{H/L}$ AS2	AS1 and AS2 must be executed by different user who has different permission. The H means that the grade of AS1's user is higher than the grade of AS2's user. The L means that the grade of AS1's user is lower than the grade of AS2's user.

根据需要,授权步的保护态中的权限集中也可以加入使用次数限制.比如,保护态中的写权限只能使用 3 次,当授权步使用写权限 3 次以后,写权限自动从保护态中的执行者许可集中去除.

另外,授权步不是静态的,而是随着处理的进行动态地改变内部状态.对一个授权步的内部状态,可以用一个状态变迁图来表示,如图 3 所示.授权步的状态变化一般自我管理,依据执行的条件而自动变迁状态,但有时也可以由管理员进行调配.授权步的生命期、许可的次数限制和授权步的自我动态管理,三者形成了 TBAC 的动态授权.

各状态的意义如下:

- (1) 睡眠状态,表示授权步还未生成;
- (2) 激活状态,表示授权步被请求激活,此时授权步已经生成;
- (3) 有效状态,表示授权步开始执行,随着权限的使用,它的保护态发生变化;
- (4) 挂起状态,表示授权步被管理员或因执行条件不足而强制处于挂起状态,它可以被恢复成有效状态,也可能因生命周期用完或被管理员强制为无效状态;
- (5) 无效状态,表示授权步已经没有存在的必要,可以在任务流程中删除.

1.3 TBAC 的形式化定义

TBAC 模型如图 4 所示.下面,我们给出其形式化定义.

定义 1. TBAC 模型由如下单元组成:

- (1) 由 workflow Wf、授权结构体 Au、受托人集 T、许可集 P 四部分组成;
- (2) Wf 是由一系列 Au 组成,Au 之间的关系为

$$Au \times Au \subseteq 2^D, D = \{\text{顺序依赖, 失败依赖, 分权依赖, 代理依赖}\};$$

- (3) Au 与 T 是 1:n 关系, $Au \rightarrow R$, 是一个从 $T = \{R_1, R_2, \dots, R_n\}$ 选择一个执行委托者的函数;

- (4) Au 与 P 是 1:n 关系, $F(Au, R) \rightarrow P, R \in T, P = \{p_1, p_2, \dots, p_n\}$ 为许可集, F 为初始化执行者许可集函数; $G(Au, P1) \rightarrow P2, P1 \subseteq P, P2 = P - P1, G$ 为权限回收函数.

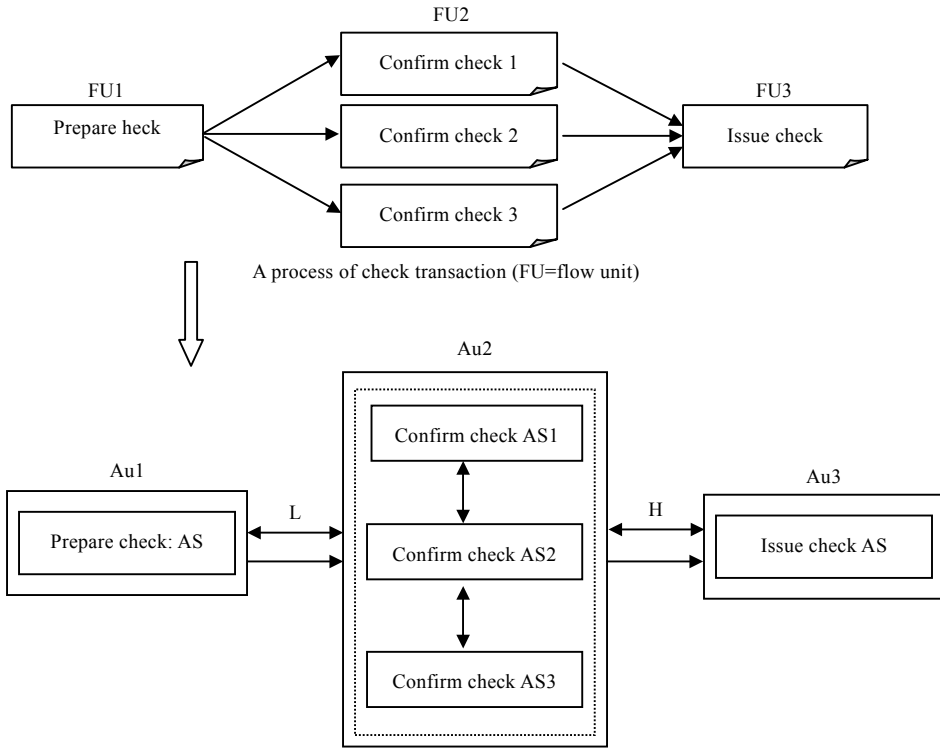


Fig.2 An example of using the symbol to model a workflow
图 2 使用符号模型化 workflow 示例

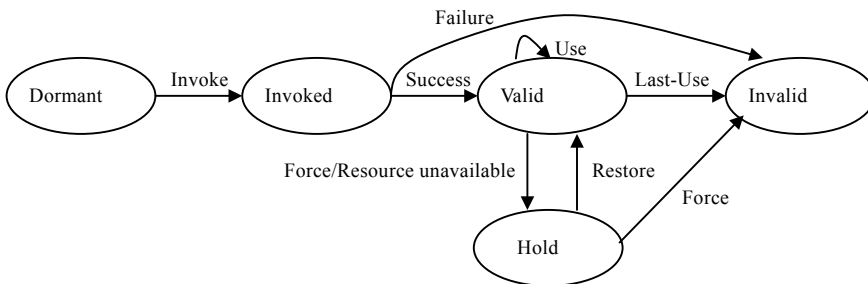


Fig.3 The inner states in a authorization-step
图 3 授权步内部状态

1.4 TBAC安全分析

TBAC 的访问政策包含在 Au-Au,Au-T,Au-P 关系中.Au-Au 的关系决定一个工作流的执行流程,Au-T 和 Au-P 组合决定一个授权结构体的运行.这些组件关系一般由系统管理员直接配置.

通过授权步的动态权限管理,TBAC 支持两个著名的安全控制原则:

- 最小特权原则.在执行任务时只给用户分配所需的权限,未执行任务或任务终止后用户不再拥有所分配的权限;而且在执行任务过程中,当某一权限不再使用时,授权步自动将该权限回收.

- 职责分离原则.有时,一些敏感的任务需要不同的用户执行,如支票处理流程中准备支票和提交支票的职员必须不同.这可通过授权步之间的分权依赖实现.

另外, TBAC 也支持数据抽象原则.例如,权限不局限于操作系统提供典型的读/写/执行权限,它可以抽象为实际工作流的操作权限,如一个银行账户对象的存款/贷款操作.

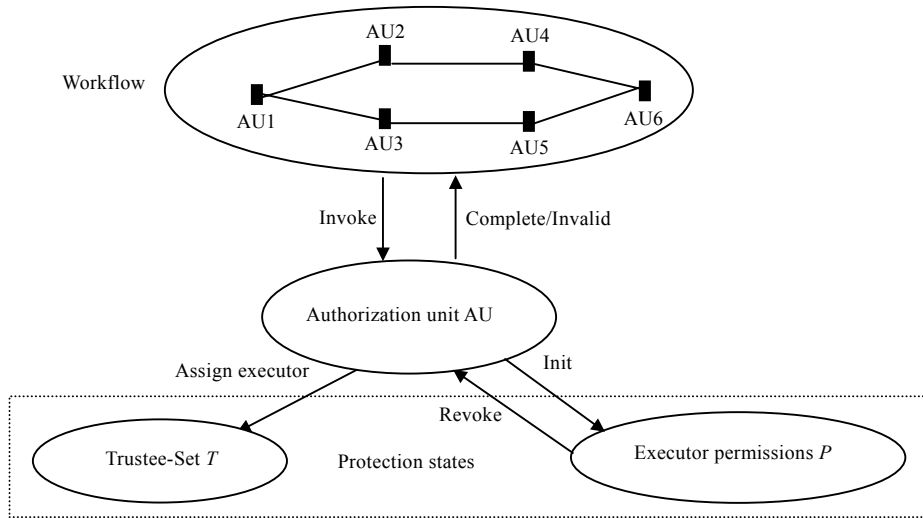


Fig.4 The model of TBAC

图4 TBAC 模型

可以将授权步中受托人集说明为角色集,这样可以将 TBAC 与 RBAC(基于角色的访问控制)结合起来,从而为 TBAC 带来更大的灵活性.

由图2及上述分析可以看出, TBAC 可以把实际应用中的工作流和访问控制所需的各种关系整体地结合在一起,可以清晰地表达复杂工作流的控制机制.可以预见, TBAC 将在办公和商业等各种领域中得到广泛应用.

References:

- [1] Snyder L. Formal models of capability-based protection systems. *IEEE Transactions on Computers*, 1981,30(3):172~181.
- [2] Ferraiolo D, Kuhn R. Role-Based access controls. In: *Proceedings of the 15th NIST-NCSC National Computer Security Conference*. 1992. 554~563.
- [3] Sandhu R, Conyne EJ, Lfeinstein H, Youman CE. Role based access control models. *IEEE Computer*, 1996,29(2):38~47.
- [4] Abrams MD, Eggers KW, La Padula LJ, Olson IW. A generalized framework for access control: an information description. In: *Proceedings of the 13th National Computer Security Conference*. 1990. 135~143.
- [5] Abrams MD, Heaney J, King O, LaPadula LJ, Lazear M, Olson I. Generalized framework for access control: toward prototyping the Orgcon policy. In: *Proceedings of the 14th NIST-NCSC National Computer Security Framework*. 1991. 257~266.
- [6] Shi ML, Yang GX, Xiang Y, Wu SG. WsMS: the manage system of workflow. *Chinese Journal of Computers*, 1999,22(3):325~334 (in Chinese with English Abstract).
- [7] Atluri V, Huang WK. An authorization model for workflows. In: *Proceedings of the 5th European Symposium on Research in Computer Security*. *Lecture Notes in Computer Science Vol 1146*, Springer-Verlag, 1996. 44~64.
- [8] Coulouris G, Dollimore J, Roberts M. Role and task-based access control in the PerDiS groupware platform. In: *Proceedings of the ACM Workshop on Role-Based Access Control*. George Mason University, 1998. 115~121. <http://www.dcs.qmw.ac.uk/research/distrib/perdis/>.
- [9] Thomas RK, Sandhu RS. Towards a task-based paradigm for flexible and adaptable access control in distributed applications. In: *Proceedings of the 1992-1993 ACM SIGSAC New Security Paradigms Workshops*. 1993. 138~142.

- [10] Thomas RK, Sandhu RS. Task-Based authorization: a research project in next-generation active security models for workflows. In: NSF Workshop on Workflow and Process Automation in Information Systems: State-of-the-Art and Future Directions. 1996.
- [11] Thomas RK, Sandhu RS. Task-Based authentication controls (TABC): a family of models for active and enterprise-oriented authentication management. 1997. 11~13.

附中文参考文献:

- [6] 史美林,杨光信,向勇,伍尚广. WfMS: workflow管理系统. 计算机学报. 1999,22(3):325~334.

.....

2003 年机器人、智能系统和信号处理国际会议(RISSP)

征文通知

由国防科学技术大学主办,中国 863 高技术发展计划机器人与自动化主题、IEEE 机器人与自动化协会、中国科学院沈阳自动化所、中国科学院自动化所、中国自动化协会机器人专业委员会和 IEEE 香港联合机器人与自动化和控制系统分会协办,国防科学技术大学电子科学与工程学院、国防科学技术大学机电工程与自动化学院、香港中文大学、香港中文大学工学院与国防科学技术大学电子科学与工程学院智能感知系统联合研究中心承办的 2003 年机器人、智能系统和信号处理国际会议定于 2003 年 5 月 19 日~24 日在湖南省长沙和张家界召开.各国专家在这次交流会上将畅谈近期的一些研究成果,并展望未来的主要研究方向,共同探讨这些领域的交叉点.会议将邀请国际知名专家做专题报告,并选择优秀论文在 Robotics and Autonomous Systems,Int.J. of Soft Computing,Asian J. of Intelligent Control 和 Int.J. of Computation Intelligence 等国际知名专业期刊(SCI 或 EI 收录)编辑专刊和由国际出版社出版英文专著.

一. 征文范围:

信号处理、计算机视觉、模式识别、生物机器人、医疗机器人、网络机器人、遥控机器人、服务机器人、微型机器人、纳米机器人、传感器和驱动器技术、自动控制技术、运动规划、机器智能、智能感知系统、机电系统等领域的理论与技术.

二. 论文提交:

作者必须将一份英文论文(最长 6 页)发到下列电子邮箱: yhliu@nudt.edu.cn,论文要求符合 IEEE 会议论文格式.

三. 截止日期:

论文提交:2003 年 2 月 15 日

接受通知:2003 年 3 月 15 日

论文终稿:2003 年 4 月 15 日

四. 联系方式:

通信地址: (410073)湖南省长沙市 国防科学技术大学 电子科学与工程学院 二系 联合研究中心

联系人: 刘云辉 教授; 王成友 博士

电话: (86)0731-4514427, 0731-4576436

传真: (86)0731-4514427

E-mail: yhliu@nudt.edu.cn

会议网址: <http://www.nudt.edu.cn/znyzzx>; <http://www.acae.cuhk.edu.hk/~icrissp>