一种基于RBAC的UCON管理模型

刘志锋 毛竹林
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 UCON模型作为新一代的访问控制模型,能够通过可变属性对使用实现连续控制,可满足当前开放的网络环境需求。但UCON模型仍存在一些缺陷:不能实现对权限的管理、对权限的委托和对属性来源的管理。为此,在UCON模型的基础上引入角色元素并把角色分为提供者角色和消费者角色,然后把权限分为直接使用权限和需要授权权限,以实现对UCON模型中权限的管理和权限的委托,并通过提供者角色对可变属性的来源进行管理,使UOCN对权限管理更加灵活,属性来源更加可信,从而使UCON的应用范围更加广泛。

关键词 UCON,角色,权限管理,权限委托,属性来源管理
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.028

Administrative Model for UCON Based on RBAC

LIU Zhi-feng MAO Zhu-lin
(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract UCON is a new generation access control model. It can control usage continually by variable attribute to meet the current demand of open network. But there are still some drawbacks in UCON model, that is to say the authority management, authority delegation and attribute source management can not be achieved. So the role elements are introduced and divided into the provider role and the consumer role based on the UCON model. Then the authority is divided into the direct usage authority and the authority to be authorized, in order to achieve the management of authority and authority delegation in the UCON model. And through the role of the provider, the management of the source of variable attributes can be achieved, making UOCN more flexible in management of authority and the attribute source more reliable, so the application scope of UCON is more extensive.

Keywords UCON, Role, Authority management, Authority delegation, Attribute source management

1 引言

随着信息技术的发展,传统访问控制已经很难满足当前开放的网络环境需求。由Sandhu等人[1]提出的使用控制模型(Usage Control,UCON)是一种全新的访问控制方法,包含了传统访问控制[3,4]、信任管理[5,6]和数字版权管理[7]3个方面,并且在定义和范围上超过了这3个方面,被认为是下一代访问控制技术的发展方向[2]。

为了满足现代访问控制需求,对资源实现实时的访问控制,UCON模型引入使用连续性和属性可变性两种新的重要特征。但UCON模型仍存在一些缺陷:使用控制模型定义抽象、实现复杂、不易管理和应用[12-15]。在UCON模型中,研究者主要集中在对消费者主体使用客体的研究,很少关注提供者主体和标识者主体,并且UCON模型也无法自主地把部分权限委托给其他用户,以便后者代替前者完成一些相应任务。一些学者认为,对UCON模型中管理问题的进一步研究是UCON模型成功的关键[2]。

学者们对于UCON模型的管理问题做了相应的研究。Zhang Zhi-yong等人[8]通过研究委托的基本特征,分析它在UCON体系框架中的具体表现,给出了一种新的模型UCOND,但该模型未对权限进行管理。蔡伟鸿等人[9]针对UCON在委托授权以及权限管理方面的不足,提出了基于属性RBAC的带委托性质的使用控制模型EUCON,但是该模型未对EUCON的角色管理和委托授权进行详细描述。Farzad Salim等人[10]定义了一种新的UCON管理模型,解决了属性的管理问题,并且能够对权限进行委托,但是该模型并没有合适的实现方法。鲁柯等人[11]对基于时间特性的RBAC的使用控制模型的管理进行了研究,但是该研究只是将角色引入使用控制模型,通过对角色的管理实现UCON模型的管理,并没有解决角色间权限委托的问题。针对以上不足,本文通过对UCON和RBAC的研究,在UCON模型中引入角色元素,并对权限进行分类,同时对属性来源进行管理,实现UCON模型的管理和委托。

2 问题分析

Sandhu等人[2]提出了UCON核心模型($UCON_{ABC}$),并将主体分为消费者主体、提供者主体和标识者主体,每一种主体都和其他主体有密切的关系,一个主体可以影响其他主体

到稿日期:2015-09-16 返修日期:2016-03-04
刘志锋(1981-),男,博士,副教授,主要研究方向为访问控制、模式识别、可信计算与物联网;毛竹林(1989-),男,硕士生,主要研究方向为访问控制。

的应用决策，并在研究中给出了 $UCON_{ABC}$ 管理三角形[2]。他们利用该模型简单地说明 3 种主体间的关系，但是并没有具体解决管理问题。$UCON_{ABC}$ 管理三角形如图 1 所示，其中消费者主体是一个供应链中客体内容的最后受益者，且消费者被提供者管理。

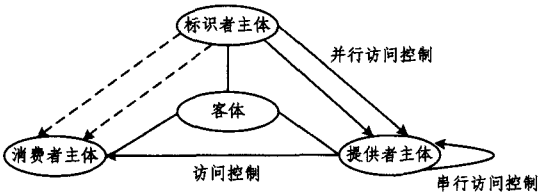

图 1 $UCON_{ABC}$ 管理三角形

(1)消费者主体(Consumer Subjects,CS)：以某种权限访问客体的实体。

(2)提供者主体(Provider Subjects,PS)：提供客体或者客体的某种权限的实体。

(3)标识者主体(Identifiee Subjects,IS)：包含隐私敏感信息的数字客体，可以认为是一类特殊的 CS 或 PS。

在 Sandhu 等人[1]对 $UCON_{ABC}$ 的研究中，虽使用了大量的例子来证明 $UCON_{ABC}$ 模型能够全面完整地描述传统的访问控制、信用管理和数字版权管理，并且实现了传统技术所不能实现的使用控制连续性。然而有些例子只是简单地使用一些属性，并假设这些属性来源于模型外的可信第三方，却不关心这些属性的来源。此外，在这些例子中，对于主客体之间的权限指定也是假设基于可信的第三方，模型本身并不关注这些权限的来源，既没有实现 3 种主体对权限和属性的有效管理，也没能解决权限的委托等问题。为此，本文在 $UCON_{ABC}$ 基础上引入角色元素形成一种新的模型，并把此模型命名为 R-UCON，通过角色管理实现对 UCON 权限的管理及属性来源的管理，以解决 UCON 中权限委托困难的问题，使权限管理更加灵活，更好地适应当前复杂的网络环境。

3 R-UCON 管理模型

R-UCON 在原有的 UCON 模型的基础上加入角色元素，利用角色来实现提供者主体和消费者主体之间的权限管理、属性来源管理，并且通过划分权限实现委托授权的细粒度管理，以确保提供者主体的某些重要权限的安全。

3.1 权限管理

3.1.1 角色引入

在对 UCON 的研究中很少有涉及到管理这一部分的内容，基本都只包含了对消费者主体的研究，只注重消费者主体对客体的使用权限，没有对提供者主体的管理问题进行研究。因此，本文提出 R-UCON 模型，在该模型中角色具有两类属性：提供者角色属性、消费者角色属性，通过不同属性的角色实现权限的管理。用户-角色-权限关系如图 2 所示。

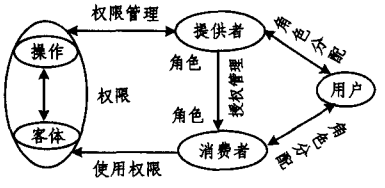

图 2 用户-角色-权限关系

1)提供者角色(Provider Role,PR)：唯一拥有某一客体资源的所有权限。

2)消费者角色(Consumer Role,CR)：使用客体资源的一些权限，受提供者角色管理。

3)授权管理(Authorization Administrate,AA)：提供者角色管理消费者角色的使用权限。

4)用户(User,U)：使用或管理客体资源的实体。

定义 1 访问控制管理模型由以下组件组成。

1)S：主体集合；2)R：角色；3)PR：提供者角色，$PR \subseteq R$；4)CR：消费者角色，$CR \subseteq R$；5)OPS：操作；6)OBS：客体；7)$PRMS$：权限集合，$PRMS = 2^{OPS \times OBS}$；8)$UPRA \subseteq S \rightarrow PR$：用户与提供者角色是一对一的指派关系；9)$UCRA \subseteq S \times CR$：用户与消费者角色之间是多对多的指派关系；10)$PPRA \subseteq PRMS \rightarrow PR$：从权限集合到提供者角色的一对一映射，表示提供者角色所拥有的权限关系；11)$PCRA \subseteq PRMS \times CR$：权限集合到消费者角色集合的多对多映射，表示消费者角色被赋予的权限关系。

此模型中本文考虑以下管理策略。

$creates(r,o,PR)$：创建一个提供者角色，其中 $r \in R, o \in OBS$；$creates(r,o,CR)$：创建一个消费者角色，其中 $r \in R, o \in OBS$；$deletes(r,o,PR)$：删除一个提供者角色，其中 $r \in R, o \in OBS$；$deletes(r,o,CR)$：删除一个消费者角色，其中 $r \in R, o \in OBS$；$assign(u,r)$：分配角色给用户，其中 $u \in S, r \in R$；$addperm(r, perm)$：给角色添加权限，其中 $r \in R$，$perm \in PERM$；$deleteperm(r, perm)$：删除角色权限，其中 $r \in R$，$perm \in PERM$；$auperm(u, perm)$：给用户授权，其中 $u \in S$，$perm \in PERM$。

当用户是提供者主体时就会被赋予提供者角色，并拥有对相应客体的所有权限且能管理这些权限。同时，消费者主体会被赋予消费者角色权限，但其只能使用部分或全部权限并受提供者主体限制。

3.1.2 角色应用分析

与 RBAC 相比，本文采用 UCON 的连续控制能够在使用过程中对消费者主体进行限制。其中，角色的赋予由系统管理，而权限的管理则通过提供者角色管理，形式化表示为：$s \in creates(r,o,PR)$：主体 s 是一个提供者主体角色；$o_i \in creates(r,o,CR)$：主体 o_i 是一个消费者主体角色；$p_i \in PRMS$：p_i 是权限；$re \in OBS$：re 是资源。$allowed(o_i, re, p_i) \rightarrow auprem(s, p_i) \wedge Condition(UCON_{ABC})$，其中，$auprem(s, p_i)$ 表示 s 分配权限 p_i，提供者角色 s 对消费者角色 o_i 赋予不同的权限 p_i。

3.1.3 权限划分

为更好地控制消费者对权限的使用以及实现对客体权限的有效管理，本文把权限划分为可直接使用权限和需要授予权限。权限管理如图 3 所示。

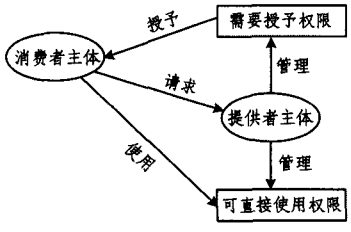

图 3 权限管理

可直接使用权限(DP)：消费者主体能够不经过提供者主体授权就可以对资源进行使用。可直接使用权限根据使用条件的属性不同又可分为无条件使用和有条件使用。例如：所

有用户都可以浏览电子书的前5页，但是后面内容只有付费用户才能阅读。

需要授予权限(NDP)：资源的所有权限都由提供者主体管理，其中有一部分特殊权限，可以根据消费者主体的请求来判定是否授予。例如：提供者主体可以把自己的管理权限部分或全部委托给自己信任的主体，同时提供者主体将会暂时或者永久失去这些权限。这些特殊权限的回收可以利用时间属性实现连续性使用控制，时间属性由系统管理。

定义2 $PRU, CRU, O, PRMS, DP, NDP$ 分别表示提供者角色用户、消费者角色用户、客体、权限集合、可直接使用权限、需要授予权限。

$PRMS \in (DP, NDP)$ 表示权限分为 DP, NDP；$allowed(cru, o, prms) \rightarrow Condition(UCON_{ABC}) \wedge prms \in dp$ 表示只要满足 $UCON_{ABC}$ 中的条件，消费者角色用户就可以使用 DP；$allowed(cru, o, prem) \rightarrow Condition(UCON_{ABC}) \wedge auprem(pru, prem) \wedge prem \in NDP$ 表示只有经过提供者角色用户授权，消费者角色用户才可以使用 NDP。

3.2 属性管理

由于Sandhu在研究时使用的一些例子中只是简单地使用一些属性，并假设这些属性来源于模型外的可信第三方，却不关心这些属性的来源，因此要安全地使提供者角色对不同的消费者角色实施不同的使用权限管理，就要实现对UCON中属性的管理。在UCON中属性分为可变属性和不可变属性，不可变属性是指策略执行后不会改变的属性，而可变属性则随着策略执行改变。

本文通过对属性来源的管理，实现UCON中属性的管理。本文将属性划分为系统属性和用户属性，这两种属性同时包含可变和不可变两种属性，同时规定不可变属性由系统或用户改变，而可变属性只能由提供者角色提供并管理。在同一个系统中，同一可变属性只能由一个主体进行管理，该属性通过策略执行来改变，且可变属性可以进行委托。属性来源管理如图4所示。例如当用户想要浏览电子书的更多内容时，就需要付钱，而对于当前的账户中用户是否有足够的资金，就需要银行给出相应的数值。所有关于资金这一项可变属性的管理，就可以通过银行这个提供者角色来管理。如果在该例子中通过时间属性对授权进行限制，系统就作为提供者角色。通过对属性的划分，明确属性的来源，在系统运行时能够判断出使用的属性是否是可信的。

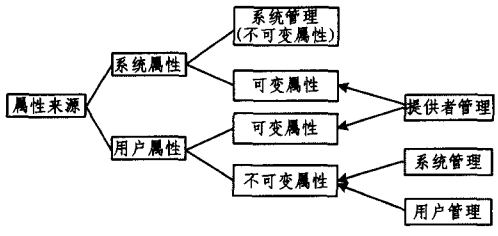

图4 属性来源管理

定义3 $Attfrom(AF)$，$SystemAttr(SA)$，$UserAttr(UA)$，$immutableAttr(IA)$，$mutableAttr(MA)$，$User(U)$，$PRU, System(sys)$ 分别表示属性来源、系统属性、用户属性、不可变属性、可变属性、用户、提供者角色用户、系统。

$SA \supset (MA, IA)$ 系统属性包含可变属性和不可变属性；$UA \supset (MA, IA)$ 用户属性包含可变属性和不可变属性；$AF \supset (SA, UA)$ 属性来源分为系统属性和用户属性；$trusted(ma) \Rightarrow manger(pru)$ 提供者角色用户提供可变属性；$trusted(ia) \Rightarrow manger(u, sys)$ 不可变属性由用户和系统管理。

4 比较和应用

4.1 模型对比

将R-UCON与前文中提到的几种访问控制模型进行对比，结果如表1所列。

表1 对比结果

访问控制模型	角色元素	控制连续性	属性可变性	权限管理	属性来源管理	委托
R-UCON	Y	Y	Y	Y	Y	Y
RBAC	Y	N	N	Y	—	N
UCON	N	Y	Y	N	N	N
EUCON[9]	Y	Y	Y	Y	N	Y
UCOND[8]	N	Y	Y	Y	N	Y
TRUCON[11]	Y	Y	Y	Y	N	N

注：Y表示包含此种特性；N表示不具有此种特性；—表示不存在此种特性。

由表1可得R-UCON比其他模型性能更优：与EUCON模型相比，本模型能对属性来源进行管理；与UCOND模型相比，本模型通过引入角色元素对属性来源进行管理，并且通过角色的运用能够更加灵活地管理权限；与TRUCON模型相比，本模型能够对属性来源进行管理并且能够实现权限的委托。R-UCON模型通过对权限和属性的管理，能实现权限的委托，对于含有隐私敏感信息的主体而言，可以有效地控制这些敏感信息的使用，能够保证自身的隐私信息在使用过程中不被非法使用。

4.2 模型应用

下面将利用本文提出的R-UCON模型来实现电子书阅读网站的权限管理。

电子书阅读网站有3类角色，分别为管理员(manager)、读者(reader)、作者(writer)。管理员分为系统管理员(administrator)和普通管理员(omanager)，他们具有读者管理、作者管理、电子书管理等权限。此外，管理员管理为系统管理员所独有的权限，即不能直接授予权限(NDP)；管理员管理分为添加管理员(addmanager)、删除管理员(deletemanager)；作者管理分为添加作者(addwriter)、删除作者(deletewriter)；读者管理只有删除读者(deletereader)；电子书管理分为添加电子书(addbook)、删除电子书(deletebook)。管理员权限如图5所示。

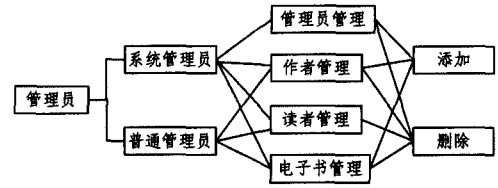

图5 管理员权限

读者具有充值(addvalue)、阅读(view)等权限以及账户属性(rvalue)，该属性为动态属性需要得到网站(Onet)的信任，而网站信任(credit)银行或第三方交易平台提供的消息。

作者具有发布电子书(publish)、修改电子书(alter)等权限，属于不能直接授予权限(NDP)。

电子书(book)分为免费电子书(freebook)和付费电子书(bookfee)，付费电子书具有不可变属性价值(value)。

形式化表示如下。

creates(*adm*,*Onet*,*PR*)：将系统管理员角色设置为网站管理员，为提供者角色；*creates*(*bank*,*value*,*PR*)：将银行设置为提供者角色；*creates*(*writer*,*book*,*PR*)：将作者角色设置为提供者角色；*creates*(*reader*,*book*,*CR*)：将读者角色设置为消费者角色；*addperm*(*adm*,*addmanage*)：给系统管理员添加设置管理员权限；*addperm*(*adm*,*deletemanger*)：给系统管理员添加删除管理员权限；*addperm*(*adm*,*addwriter*)：给系统管理员添加设置作者权限；*addperm*(*adm*,*deletewriter*)：给系统管理员添加删除作者权限；*addperm*(*adm*,*deletereader*)：给系统管理员添加删除读者权限；*addperm*(*adm*,*addbook*)：给系统管理员添加增加电子书权限；*addperm*(*adm*,*deletebook*)：给系统管理员添加删除电子书权限；*addperm*(*reader*,*addvalue*)：给读者添加充值权限；*addperm*(*reader*,*view*)：给读者添加阅读权限；*addperm*(*writer*,*publish*)：给作者添加发布电子书权限；*addperm*(*writer*,*alter*)：给作者添加修改电子书权限。

假设有5个人分别为读者(r)、作者(w)、系统管理员(a)、银行员工(b)、普通管理员(m)。当读者看免费电子书时，可以直接观看，但当读者要看付费电子书时，需要检查其是否有足够的钱，这时需要银行给出证明，银行作为提供者角色给出了属性来源的证明。若要修改电子书，则必须具有修改权限，且该权限必须由作者授权，实现对不同权限的管理。那么根据授权规则，有：

assign(*r*,*reader*)；

allow(*r*,*view*,*freebook*)；

allow(*r*,*view*,*bookfee*)⇒*condition*(*rvalue*>*value*)；

trusted(*rvalue*)⇒*credit*(*b*)；

allow(*r*,*alter*,*book*)⇒*auperm*(*w*,*alter*,*book*).

当普通管理员需要管理管理员权限时，就必须由系统管理员授予该权限，实现权限的委托。那么根据授权规则，有：

allow(*m*,*addmanager*)⇒*auperm*(*a*,*addmanager*)；

allow(*m*,*deletemanager*)⇒*auperm*(*a*,*deletemanager*)

R-UCON模型成功实现了对权限的管理及授权，并实现了对属性来源的管理，使访问控制系统在使用过程中更加灵活可靠。

结束语 R-UCON通过在UCON模型的基础上引入角色元素，并对权限进行划分，实现对权限的管理和委托以及对属性来源的管理。这样，对于含有隐私敏感信息的主体而言，可以有效地控制这些敏感信息的使用，能够保证自身的隐私信息在使用过程中不被非法利用。本文有效地解决了UOCN模型的管理问题，扩充了UCON模型的使用范围，能够实现权限委托。接下来将对R-UCON做进一步的研究，解决其应用问题。

参 考 文 献

[1] Park J, Sandhu R. Towards usage control models: beyond traditional access control[C]// Proceedings of the Seventh ACM Symposium on Access Control models and Technologies. ACM, 2002: 57-64

[2] Park J, Sandhu R. The UCON ABC usage control model [J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 128-174

[3] Wang Y D, Yang J H, Xu C, et al. Survey on access control technologies for cloud computing[J]. Journal of Software, 2015, 26(5): 1129-1150(in Chinese)
王于丁，杨家海，徐聪，等. 云计算访问控制技术研究综述[J]. 软件学报，2015，26(5)：1129-1150

[4] Cai Ting, Chen Chang-zhi. Research for Access Control based on UCON in Cloud Computing[J]. Computer Science, 2014(S1): 262-264(in Chinese)
蔡婷，陈昌志. 云环境下基于UCON的访问控制模型研究[J]. 计算机科学，2014(S1)：262-264

[5] Zhang Guang-hua. Research on Security Models Based on Trust Management[D]. Xi'an: Xidian University, 2014(in Chinese)
张光华. 基于信任管理的安全模型研究[D]. 西安：西安电子科技大学，2014

[6] Guo Jing-jing, Ma Jian-feng, Li Qi, et al. Game theory based trust management method for mobile ad hoc networks[J]. Journal on Communications, 2014, 35(11): 50-58(in Chinese)
郭晶晶，马建峰，李琦，等. 基于博弈论的移动自组织网络的信任管理方法[J]. 通信学报，2014，35(11)：50-58

[7] Lv Jing-hua. Research on Techniques of Usage Control in Mobile Digital Publishing Rights Management [D]. Beijing: Beijing University of Posts and Telecommunications, 2013(in Chinese)
吕井华. 移动数字出版版权保护使用控制技术研究[D]. 北京：北京邮电大学，2013

[8] Zhang Z, Yang L, Pei Q, et al. Research on usage control model with delegation characteristics based on OM-AM methodology [C]// IFIP International Conference on Network and Parallel Computing Workshops, 2007. NPC Workshops. IEEE, 2007: 238-243

[9] Cai Wei-hong. The Research of Access Control Model Based on EUCON [D]. Guangzhou: South China University of Technology, 2012(in Chinese)
蔡伟鸿. 基于EUCON的访问控制技术研究[D]. 广州：华南理工大学，2012

[10] Salim F, Reid J, Dawson E. An administrative model for UCONABC [C]// Proceedings of the Eighth Australasian Conference on Information Security-Volume 105. Australian Computer Society, Inc., 2010: 32-38

[11] Lu Ke, Zhou Bao-qun, Wang Hui-fang. Usage Control Model Based on Timed RBAC and Its Administration [J]. Computer Engineering, 2008, 34(6): 170-172(in Chinese)
鲁柯，周保群，王惠芳. 基于带时间特性RBAC的使用控制模型及其管理[J]. 计算机工程，2008，34(6)：170-172

[12] Shibli M A, Ali A. Extensible Access Control Framework for Cloud based Applications[EB/OL]. http://ais.seecs.nust.edu.pk/project

[13] Jiao D, Lianzhong L, Ting L, et al. Realization of UCON Model Based on extended-XACML[C]// 2011 International Conference on Future Computer Sciences and Application (ICFCSA). IEEE, 2011: 90-93

[14] Masood R, Shibli M A, Bilal M. Usage control model specification in XACML policy language[M]// Computer Information Systems and Industrial Management. Springer Berlin Heidelberg, 2012: 68-79

[15] Colombo M, Lazouski A, Martinelli F, et al. A proposal on enhancing XACML with continuous usage control features[M]// Grids, P2P and Services Computing. Springer US, 2010: 133-146