多域安全互操作的可管理使用控制模型研究*)

洪 帆 崔永泉 崔国华 付 才
(华中科技大学计算机学院 武汉 430074)

摘 要 多域环境的异构、动态和区域自治的特点为安全互操作访问控制研究提出了新的挑战。近来在多域安全互操作访问控制方面做了大量研究,大多在单域内基于角色访问控制的前提下,将外域角色映射到本地角色来实现访问控制,在外域和本地角色的管理上缺乏系统化的统一。本文提出了可管理的使用控制模型,对外域和本地用户角色指派进行统一管理,弥补了原有模型的安全漏洞。该模型提供了足够的灵活性,可以区分外域用户和本地用户,并且对外域用户实施更为严格的控制,同时保留了传统 RBAC 模型的优点。该访问控制模型正在实践中实施。

关键词 访问控制,多域安全,管理模型,使用控制

Administrative Usage Control Model for Secure Interoperability between Administrative Domains

HONG Fan CUI Yong-Quan CUI Guo-Hua FU Cai
(College of Computer Science, Huazhong University of Science and Technology, Wuhan 430074)

Abstract The heterogeneous, dynamic and self-governing in local domain nature of multi-domains environments introduces challenging security issues. Despite the recent advances in access control approaches applicable to secure interoperability between multi-domains, there remain issues that to perform role-based access control model in one domain and implement security interoperability by translating role of foreign domain to local role. Amongst them are the lacks of uniform administration for role of foreign and local domain. In this paper, we present an access control scheme that resolve these issues, and propose a Administrative Usage Control (AUCON) framework which corrects the security shortcoming of previous model and administrates user-role assignment for local and foreign domain with untie method. The AUCON model provides flexible enough mechanism to distinguish user of foreign and local domain and enforces more strict control for foreign user. While retaining the advantages of traditional RBAC model. AUCON model is being implemented in our experiment.

Keywords Access control, Security interoperability between administrative domains, Administrative model, UCON

1 引言

在目前高度动态、异构化、分布式的现代信息系统中,跨越单个管理域的限制,在多个域之间进行安全互操作是一个非常必要的系统需求。因此,对等的多域间安全互操作成为目前一个研究热点问题。Kap 等人提出了安全互操作基于角色访问控制模型(IRBAC2000),它利用动态角色转换的方法,在外域角色和本地角色之间建立了一些关联,从而使得外域角色能够访问本地资源,在基于角色访问控制(RBAC)的安全域之间进行安全互操作[1]。对于跨越多个安全域的系统而言,动态分布基于角色访问控制模型(DRBAC)提供了一个可伸缩的、分散的信任管理和访问控制机制,并提出了第三方委托的概念,可以将角色转换或委托给其他域角色[2,3]。这些模型都侧重于将外域角色转换或者委托给本地角色,从而实现了安全域之间的互操作。然而,它们都缺乏足够的灵活性,在外域和本地的角色之间进行严格的区分,为系统带来了一定的安全隐患。管理互操作基于角色访问控制模型(A-IRBAC2000)引入了进行域间角色转换的安全管理员角色,实施外域到本地的角色转换[4]。但是,该模型定义的先决条件存在安全漏洞,并且在外域和本地的用户角色指派之间不统一,带来了管理的复杂性。

在最近的安全文献中,使用控制(UCON)模型被看作下一代访问控制模型而引发热烈的讨论。它作为一种通用的框架覆盖了传统访问控制、信任管理和数字权限管理等安全领域,并且在定义和范围上都超越了这些领域。在此基础上,本文提出了可管理的使用控制(AUCON)模型。它使用形式化的定义,更加严密地规范了安全管理员实施用户角色指派的过程,并且对外域用户和本地用户的角色指派进行了系统化的统一管理,弥补了 A-IRBAC2000 模型中先决条件的安全漏洞;在实施访问控制的过程中,引入了条件(Conditions)组件,提供了足够的灵活性,可以对外域用户实施更为严格的安全控制。AUCON 模型已经在原型系统中得到应用,并且取得良好的效果。本文第 2 节对相关研究工作进行了总结和回顾;第 3 节中提出了一个可管理的使用控制模型(AUCON)来解决多域安全互操作的访问控制问题;在第 4 节中描述了 AUCON 模型在原型系统中的实施框架。最后引出了本文的结论。

2 相关研究工作和进展

2.1 IRBAC2000 模型

Kap 等人提出了 IRBAC2000 模型,它是一个在多域之间进行安全互操作的策略框架。该框架在外域和本地之间定义了一系列的关联,这些关联形成了一个组合的偏序角色层次,使得外域角色能够映射到本地角色,从而获得对本地资源的

*)本课题得到国家自然科学基金(60403027)、湖北省自然科学基金(2005ABA243)资助。洪 帆 教授,博士生导师,主要研究方向为信息安全、访问控制、网络安全等;崔永泉 博士研究生,主要研究方向为分布式系统安全、访问控制;崔国华 教授,博士生导师,主要研究方向为数据库加密、信息安全;付 才 博士研究生,主要研究方向为分布式系统安全、Ad-hoc 网。

访问权限。

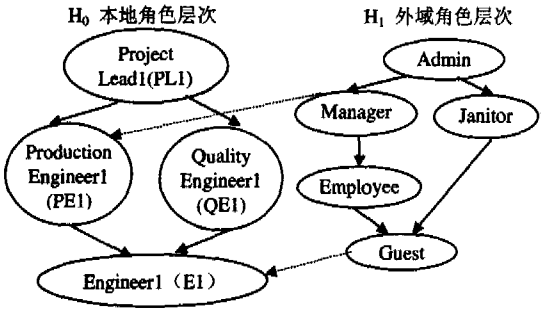

图 1 两个角色层次之间的偏序关系

如图 1 所示，虚线箭头代表外域的角色能够映射到本地角色。为了形式化地说明这个模型，本文用 H_0 代表本地角色集 R_0 中的层次关系，用 H_1 代表外域角色集 R_1 中的层次关系，用 $Manager_{R_1} \mid\!\rightarrow PE1_{R_0}$ 表示 R_1 中的角色 Manager 可以映射到本地的 PE1 角色。

该模型存在一定的安全风险。外域角色经过映射到达本地以后，该模型没有对外域角色进行严格的区分和限制。然而，在实际系统中可能需要根据系统整体的安全警戒级别和系统负载情形对外域角色进行严格的限制，比如限制外域角色访问系统的时间和 IP 地址。

2.2 ARBAC97 管理模型和 A-IRBAC2000 管理模型

在单域环境下，通常利用 ARBAC97 模型对系统内的用户、角色、权限等实施安全管理。使用 ARBAC97 模型的目的就是在保证全局集中安全控制的前提下，分散 RBAC 系统的管理。因为权限和角色是相对固定的，本文只分析涉及用户角色指派的 URA97 模型[5,6]。

URA97 模型中的用户角色指派由 can_assign(x,y,z)来约束，其中 x：管理角色；y：先决条件；z：角色范围。例如，can_assign(PSO1,E1 ∧ ¬ QE1,[PE1,PE1])表示的意义如下：管理角色 PSO1 的一个成员，能够给满足先决条件 E1 ∧ ¬ QE1 的用户指派一个 PE1 的角色，先决条件 E1 ∧ ¬ QE1 表示用户必须是角色 E1 的成员，而且不能是角色 QE1 的成员。从某种意义上来说，先决条件是管理角色的用户库，限定某个管理员只能为符合先决条件的用户指派某一个角色范围内的角色。

受 ARBAC97 模型的启发，A-IRBAC2000 模型引入了先决条件和角色范围来对外域角色到本地角色的映射进行管理。对 R0 域的安全管理员角色 PSO1 来说，就可以定义如下的关系：can_assignT(PSO1, In_domain(R1) ∧ ¬ mapped_to (QE1),[PE1,PE1])。与 URA97 模型中的含义相类似，该关系表示管理员角色 PSO1 的一个成员，能够将来自于 R1 域并且没有映射到 QE1 角色的一个角色映射到 PE1 的角色。

实际上，上述的先决条件是不完备的，存在很大的安全漏洞，因为来自于 R1 域中，不能够被映射到 QE1 角色的角色有很多。比如在图 1 所示的 R1 中，Guest 角色没有被映射到 R0 域中的 QE1 角色，即是 Guest 角色满足该 can_assignT 关系。如果将 Guest 角色映射到 R0 域的 PE1 角色，则带来很大的安全隐患，违背了系统的安全策略。

2.3 UCON 模型

在访问控制研究 30 多年的历史上，也曾经出现过一些非常著名的模型，比如矩阵模型、格模型和 RBAC 模型。这些传统访问控制模型一个共同的局限性就是仅仅关注于访问控制的授权过程。当主体提出访问请求时，系统将根据主体请求的权限，对比主体和客体的安全属性，从而决定该请求是否被允许。而现代信息系统关注的不仅仅是授权。比如，用户需要从某个网站下载某项产品使用手册时，该网站要求用户必须进行注册。这个注册的行为就可以看作是一个义务(oBligations)。义务就是在访问请求执行以前必须由义务主体履行的行为。另外，某些数字音频文件必须要求在特定的设备或者地点播放，这些环境的约束就称为条件(Conditions)[7,8]。在目前高度动态分布式环境下，义务和条件也是决定访问请求是否能够被允许的至关重要因素。

UCON 模型包括了授权、义务和条件组件，提供了一个通用的、统一的框架，可以覆盖传统访问控制、信任管理和数字权限管理这些安全领域，并且在内容和范围上超越这些领域，成为富有潜力的下一代访问控制模型[9,10]。

3 可管理的使用控制模型(AUCON)

3.1 AUCON 模型的核心思想

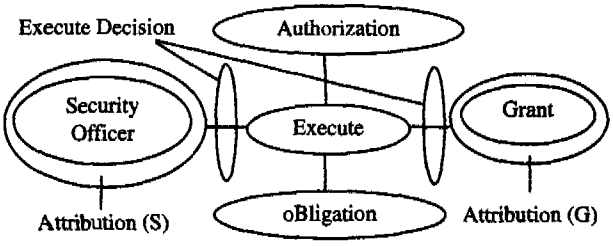

图 2 安全管理员进行用户角色指派的模型

用户需要访问系统，首先要经过安全管理员为用户指派相应的角色。如图 2 所示，安全管理员为用户指派角色的过程中不但需要考虑授权(Authorization)控制，而且相应的义务主体必须履行相应的义务(oBligation)。

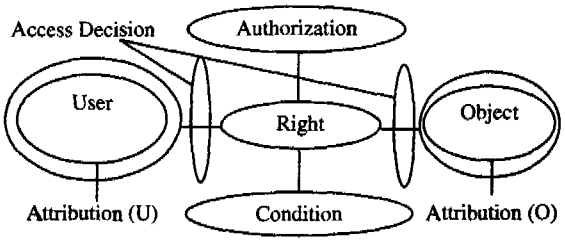

图 3 对用户访问系统的控制模型

用户在获得安全管理员指派的角色之后，就可以提出相应的安全请求。如图 3 所示，系统不但要检查用户和对象、权限的属性是否满足安全策略，而且要检查用户是否满足系统全局的条件(Conditions)的约束。

3.2 AUCON 模型的定义

AUCON 模型由表 1 所示的一些集合和定义组成。

表 1 AUCON 模型中的基本集合

模型中的英文词语	集合名称	简写
Security Officer	安全管理员	S
Administrative Role	管理角色	AR
Grant	为用户授予角色的过程	G
Revoke	撤销用户角色的过程	V
User	用户	U
Role	普通角色	R
Permission	权限许可	P
Domain	安全域	D
Object	操作对象	O

定义 1 函数的定义

$sAR:S\to 2^{AR}$ $actAR:S\to 2^{AR}$ $sRan:S\to 2^{R}$ $gU:G\to U$

$gR:G\to R$ $vU:V\to U$ $vR:V\to R$ $uDom:U\to D$

$uR:U\to 2^{R}$ $actR:U\to 2^{R}$ $pR:P\to 2^{R}$

定义 2 主体属性和客体属性

$Atrr(S)=\{sAR,actAR,sRan\}$ 安全管理员具有相应的管理角色和所管理的角色范围,在一次会话中,安全管理员可能仅仅激活某些管理角色;

$Attr(G)=\{gU,gR\}$ 对于一个具体的授予角色过程,都对应为某个用户指派某个普通角色;

$Attr(V)=\{vU,vR\}$ 对于一个具体的撤销角色过程,都对应撤销某个用户的某个普通角色;

$Attr(U)=\{uDom,actR,uR\}$ 用户属于某个安全域,具有普通的角色集,在一个会话中,用户可能仅仅激活某些角色;

$Attr(O)=\{pR\}$ 权限许可 Permission 是(Object,Right)的序偶,某个权限许可属于多个普通角色。

定义 3 AUCON 模型$=\{SO,AR,G,V,R,U,D,P,O,Authorization,oBligation,Condition\}$

其中 U、R、P、AR、O、SO 是 RBAC 模型中的基本元素,这里不再重复定义;D 是安全域,G 代表用户角色指派过程,V 代表撤销用户角色的过程,以及在进行用户角色指派和撤销角色的过程中必需的授权(Authorization)、义务(oBligation)和条件(Condition)组件由下面进行定义和描述。

定义 4 AUCON 模型中用户角色指派过程中的授权组件

$Allowed(s,e,g)\Rightarrow actAR(s)\neq\phi\wedge actAR(s)\in sAR(s)\wedge gR(g)\in sRan(s)$

进行用户角色指派的主体必须激活某个管理员角色,而且指派过程对应的角色必须是在该安全管理员的管辖角色范围之内。

定义 5 AUCON 模型中用户角色指派过程中的义务组件

$$getPreOBL(s,e,g)=\begin{cases}\{(u,agree,\exists x,x_{R_1}|\to r_{R_0})\} & \text{if } uDom(u)=\text{'R1'}\\ \{(u,agree,x\wedge\neg y)\} & \text{if } uDom(u)=\text{'Local'}\end{cases}$$

其中 $u=gU(g),r=gR(g)$

$allowed(s,e,g)\Rightarrow preFulfilled(getPreOBL(s,e,g))$

在上述义务组件的定义中,义务主体是授予过程 g 对应的用户 u;义务操作是 agree,义务客体是先决条件,即是义务主体 u 必须满足先决条件的约束。根据用户 u 所属的安全域的不同,用户必须履行的义务客体也互不相同。

对于本地的用户,即 uDom(u)='Local',用户必须满足的条件就是 $x\wedge\neg y$。其中 x 和 y 代表本地的角色,$x\wedge\neg y$ 代表的含义就是用户必须是角色 x 的成员,而且用户不是角色 y 的成员。

对于外域的用户,即 uDom(u)='R1',用户必须满足的条件就是 $\exists x,x_{R1}|\to r_{R_0}$。其中 x 代表外域 R1 中的角色,在外域 R1 中,用户 u 必须至少存在一个角色 x,用户是 x 的成员,而且来自于 R1 域的 x 角色能够被映射到本地角色 r。

在一个安全管理员为某个用户实施角色指派之前,该用户 u 必须满足上述义务组件的约束,否则该用户角色指派操作就不能够进行。

定义 6 用户角色指派的结果

$uRA(u)=uRA(u)\cup\{r\}$,其中 $u=gU(g),r=gR(g)$

用户角色指派过程 g 得到正确实施,用户 u 成为角色 r 的新成员。

定义 7 AUCON 模型中撤销角色过程中的授权组件

$Allowed(s,e,v)\Rightarrow actAR(s)\neq\phi\wedge actAR(s)\in sAR(s)\wedge vR(v)\in sRan(s)$

进行撤销角色的主体必须激活某个管理员角色,而且撤销过程对应的角色必须是在该安全管理员的管辖角色范围之内。

定义 8 撤销角色的结果

$uRA(u)=uRA(u)-\{r\}$,其中 $u=vU(v),r=vR(v)$

撤销角色过程 v 得到实施,用户 u 的角色集中减少一个角色 r。

定义 9 对用户访问系统资源的授权组件

$P=\{(o,r)\}$,即权限许可 P 可以看作是(Object,Right)的序偶。

$Role'=\{role|\exists r1\in uRA(u),\exists r2\in pRA((o,r)),r1\geqslant role\geqslant r2\}$

$Role''=\{role|\exists r1\in actR(u),\exists r2\in pRA((o,r)),r1\geqslant role\geqslant r2\}$

$Allowed(u,r,o)\Rightarrow Role'\neq\phi$

用户 u 至少存在一个角色 role,可以支配(o,r)所属的角色集中的某一个角色。

PreUpdate(actR(u)):

$$actR(u)=\begin{cases}actR(u) & \text{if } Role''\neq\phi\\ actR(u)\cup\Gamma(Role') & \text{if } Role''=\phi\end{cases}$$

如果用户 u 的活动角色集中的角色都不能够支配(o,r)所属的角色,则 r(Role')表示根据系统的安全策略,选择一个能够支配(o,r)所属角色添加到用户 u 的活动角色集中。

定义 10 对用户访问系统资源的条件组件

$$Conditions(u,r,o)=\begin{cases}\Phi & \text{if } uDom(u)=\text{'Local'}\\ CN1\cap CN2\cdots\cap CNn & \text{if } uDom(u)=\text{'R1'}\end{cases}$$

$CNi(i=1,2,\cdots,n)$是一系列的规则表达式,$CNi=\langle CT\rangle\langle OP\rangle\langle Value\rangle$,CT 是一些需要实施控制的约束条件;OP 可以是逻辑操作符$\{=,>,<,\geqslant,\leqslant,\neq\}$,也可以是用户自己定义的操作符;VALUE 是管理员为 CT 设定的值。CNi 用来比较 CT 的当前值和设定的 CT 值,返回一个布尔型的值,满足条件返回真,否则为假,计算 CNi 的过程成为评估用户 u 是否满足 Conditions 组件的过程。

假设系统范围内的约束条件{Time, IPAddress, SecurityLevel, SystemLoad}有如下访问规则:域 R1 中的用户在 8:00 和 18:00 之间、系统安全级别比较高、系统负载比较轻的情况下可以访问系统资源,这一规则的 Conditions 表达式如下:$Conditions(u,r,o)=(Time>8:00\cap Time<18:00\cap IPAddress\ in\ R1\cap SecurityLevel\geqslant High\cap SystemLoad<60\%)$。表达式中 in 是用户自定义的操作符。

如果用户 u 是属于外域 R1 中的用户,则必须满足系统设置的 Condition 组件,否则不能够访问本地的系统资源。这样就可以区别外域用户和本地用户,从而对外域用户提供更为严格的约束和控制。

3.3 模型的对比和讨论

1) 解决了 A-IRBAC2000 模型中先决条件的安全漏洞问题。

在 A-IRBAC2000 模型中，如图 1 所示，R1 中 Guest 角色没有被映射到 R0 域中的 QE1 角色，即 Guest 角色满足 can assignT 关系。如果根据先决条件，则 Guest 角色的成员可能被指派到 R0 域中的 PE1 角色，给系统带来了安全隐患。

在 AUCON 模型中，义务组件已经限定了只有在 R1 域中拥有角色 Admin、Manager 的用户才可能被指派到 R0 中的 PE1 角色，Guest 角色的成员根本不可能满足义务组件，所以弥补了系统原有的安全漏洞。

2) 对本地用户和外域用户的用户角色分配进行了统一管理。

在 URA97 模型、A-IRBAC2000 模型中，为了管理本地用户角色指派和外域角色到本地角色的映射，分别引入了两类安全管理员，带来了系统管理的复杂性。AUCON 模型引入了 oBbligation 组件，对本地和外域的用户角色指派过程进行统一管理，减少了管理的复杂性。

3) 引入 Condition 组件，提供了足够灵活性，可以区别外域用户和本地用户。

在实际的系统中，一定会优先考虑为本域的用户服务。当系统负载很高的时候，会首先拒绝为外域的用户服务；而且外域用户服务带来的安全风险显然会比本地的用户风险高，所以只有在系统状态比较安全的情况下才为外域提供服务。原有的多域安全互操作模型都没有提供这样的灵活性，不能对本地用户和外域进行有效的区分。AUCON 模型引入了 Condition 组件，可以很容易地实现这个目标。

4 AUCON 模型在原型系统中的实施框架

AUCON 模型已在多域实验环境中得以实施，图 4 给出该原型系统中 AUCON 模型实施的总体结构。

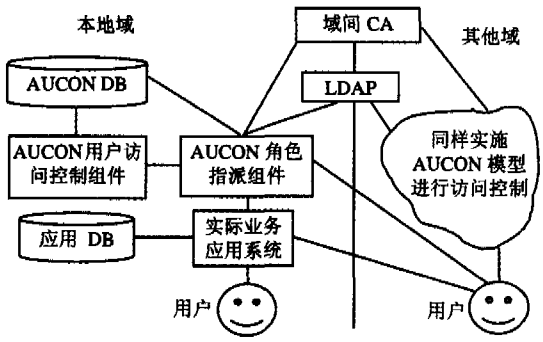

图 4 AUCON 在多域安全互操作应用中的实施框架

域间 CA：为多个域的用户发布 X.509 证书，提供 LDAP 服务，各域的访问控制组件可以通过 LDAP 服务查询有效证书和证书撤销列表；利用证书鉴别机制，可以实现多个域之间的分布式认证，保证来自于外域的用户提供的安全属性、角色信息等是安全可信的。

AUCON 角色指派组件：完成本地用户、角色、权限管理的功能；建立外域角色到本地角色的映射；对本地的和来自于外域的用户角色指派过程实施统一管理；根据系统的安全策略，保证在指派过程实施以前义务主体必须履行义务组件，实施指派过程必须满足授权组件的安全需求。

AUCON 用户访问控制组件：根据系统的安全策略，判定用户的访问请求是否满足授权组件和条件组件的需求，从而判定用户的访问申请是否能够被允许。

实际业务应用系统：是一个模拟的办公业务自动化系统。本系统主要的目标是实现多域之间安全互操作的访问控制研究，该业务应用系统只是一个简单的例子。我们尽力将业务系统和 AUCON 功能组件相互分离，使得 AUCON 模型成为一个通用的访问控制框架，而不仅仅限定于某一个实际的业务系统。

结论 为满足多域安全互操作应用中复杂的访问控制需求，本文提出了可管理的使用控制模型。该模型具有以下优点：①弥补了原有系统的有关先决条件的安全漏洞，对本地和外域用户角色指派过程的系统化的统一管理，减少了管理的复杂性。②该模型引入了 obligation 组件，提供了一种更为丰富的形式化表达约束的方式，更加具备灵活性。③该模型引入了 Condition 组件，能够容易地区分本地用户和外域用户，对外域用户实施更为严格的安全控制；并且 Condition 组件是一组规则表达式，可以根据系统的安全需求，随便添加或者修改规则表达式，很方便地实施扩展。AUCON 模型框架与应用程序分离，obligation 组件和 Condition 组件的修改与访问控制规则无关，不会影响应用程序。

目前，AUCON 模型已经在多域安全互操作应用平台中作为核心的授权与访问控制模块进行实施，取得了良好的应用效果。

参 考 文 献

1 Kapadia A, Al-Muhtadi J, Campbell R, et al. IRBAC2000: Secure Interoperability Using Dynamic Role Translation. In: The 1st International Conference on Internet Computing, June 26th - 29th, 2000, Monte Carlo Resort, Las Vegas, Nevada, USA, 2000

2 Campbell R, Liu Z, Mickunas D, et al. Seraphism: Dynamic interoperable security architecture for active networks. IEEE OPENARCH 2000, Tel-Aviv, March 2000

3 Freudenthal E, et al. dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments [EB/OL]. http://www.cs.nyu.edu/vijayk/papers/drbac-icdcs02.pdf, 2002-06

4 Al-Muhtadi J, Kapadia A, Campbell R H, et al. A-IRBAC 2000 Model: Administrative Interoperable Role-Based Access Control: [Technical Report]. UIUC-DCS-R-2000-2163. http://choices.cs.uiuc.edu/~almuhtad/

5 Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models. IEEE Computer, 1996, 29(2): 38~47

6 Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-Based Administration of Roles. ACM Transactions on Information and System Security, 1999, 2(1): 105~135

7 Park J, Sandhu R. Towards usage control models: beyond traditional access control. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, ACM Press. 57~64

8 Sandhu R, Park J. Usage control: A vision for next generation access control. In: Proceedings of The 2nd International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security. 17~31

9 Park J, Sandhu R. The UCONABC Usage Control Model. ACM Transactions on Information and Systems Security, 2004, 7(1): 128~174

10 Park J, Zhang Xinwen, Sandhu R S. Attribute Mutability in Usage Control. In: Eighteenth Annual Conference on Data and Applications Security, Sitges, Catalonia, Spain, 2004. 15~29