

一种基于角色的使用控制授权模型

谢 辉, 张 斌, 张红旗, 单宝恒

(解放军信息工程大学 电子技术学院, 河南 郑州 450004)

摘 要: 综合基于角色的访问控制 RBAC 模型和使用控制 UCON 模型各自的优势, 提出了一种基于角色的使用控制授权模型. 该模型基于属性分配角色, 通过授权规则、上下文信息约束和属性更新机制来实现动态授权并能有效降低授权管理的规模. 对该模型的基本元素进行了形式化描述, 并用动作时态逻辑 TLA 来分析该模型的动态性和安全性, 最后分析了该模型的特点.

关键词: 使用控制; 角色; 动态授权; 动作时态逻辑

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)06-0137-05

A Role - Based Usage Control Authorization Model

XIE Hui, ZHANG Bin, ZHANG Hong-qi, SHAN Bao-heng

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: Integrating the advantages of RBAC (Role - Based Access Control) and UCON (Usage Control) models, the paper proposes a role - based usage control authorization model. In the model, the role - assignment is based on attributes which can effectively reduce the authorization administration scale. Moreover the model can implement dynamic authorization by updating attributes and context constraints. A formalized description of the model is given and the dynamic authorization process is analyzed t by TLA (Temporal Logic of Actions). Finally the character of the model is analyzed.

Key words: usage control; role; dynamic authorization; temporal logic of actions

1 引言

随着信息化进程的推进, 以及 PKI、PMI 等基础设施的建设, 对授权管理的动态性、实时性提出了新的挑战. 在复杂网络环境中, 用户的权限是受各种因素的制约而动态改变, 仅仅依靠静态授权无法解决权限变化的应用需求. 所谓动态授权是指要求在静态授权的基础上, 在用户访问资源的过程中, 权限能够随着属性的变化 (包括用户、客体及环境属性) 而动态改变、终止或撤销.

很多学者对 RBAC 进行扩展, 如提出基于角色和规则的访问控制模型^[1]、基于角色和上下文的访问控制模型^[2]等, 通过引入上下文环境的约束以达到动态激活角色的目的, 试图解决动态授权问题. 而这些解决办法没有从整体上进行考虑, 适用于某一

具体的应用环境. 文献[3]提出了网格环境下的基于使用控制和上下文的动态访问控制模型, 该模型利用授权组件定义传统的静态授权, 利用条件组件使用有关的动态上下文信息对主体在具体环境中的动态权限进行控制. 然而该模型未考虑到授权规则组件对主体动态权限的控制, 只定义了静态授权规则. UCON 模型从授权规则、条件、控制时机和属性等多个方面对传统的访问控制模型进行扩展^[4], 它的授权连续性和属性可变性能有效支持动态授权. 文中基于 UCON 模型来系统地解决动态授权问题.

2 UCON 模型

UCON 模型是传统的访问控制模型的扩展, 它包括授权规则、条件及义务三大决策组件. 授权规则将根据主体请求的权限, 通过检查主客体的属性来

收稿日期: 2009-05-04; 修回日期: 2009-08-20

基金项目: 国家“八六三”计划项目 (2006AA01Z457)

决定请求是否被允许. 义务是指在访问请求执行以前或过程中必须由义务主体履行的行为, 如用户需要从某个网站下载某项产品手册时, 该网站要求用户必须注册. 条件是指访问请求的执行必须满足某些系统和环境的约束, 如系统负载、访问地点、访问时间限制等, 条件也可以称为上下文信息. 和传统的访问控制模型相比, UCON 模型应用范围更广, 支持动态的授权决策, 能为企业、组织建立系统灵活的访问控制规则.

UCON 模型表达能力强, 应用范围广, 支持动态授权, 但模型在实际应用中授权管理较为复杂. 如何对 UCON 模型进行改进使其既能有效地支持动态授权, 又能方便进行授权管理, 是需要解决的关键问题. 文中通过引入 RBAC 中角色的概念, 基于 UCON 中的授权和条件模型提出了一种基于角色的使用控制 (Role Based Usage Control, RBUCON) 授权模型, 较好地解决了动态授权问题, 也使得模型更实用化.

3 RBUCON 模型

3.1 基本思想

RBUCON 模型的构成是在 UCON 授权和条件模型的基础上, 通过引入 RBAC 模型中的角色元素而提出来的, 模型如图 1 所示. 其基本思想是: 用户通过预先授权获得角色, 角色指派基于授权规则, 而授权规则是基于主客体属性的. 另外角色权限的激活要受到授权规则和条件的约束, 属性的可变性可能会影响到角色的重新分配, 使得授权也是动态变化的. 在该模型中, 授权并不是简单地体现在静态的 (用户 s , 对象 o , 权限 r) 三元组中, 而是有生命周期的, 并伴随着角色激活的执行和属性的更新而改变, 它能使授权、控制资源的使用、收回许可等自动执行, 以保证用户以最小特权执行权限. 角色的引入可以继承基于角色的访问控制模型 RBAC 的优点, 从 UCON 访问控制的思想出发, 角色也属于一种主体属性, 这里将它分离出来同其他主体属性加以区分.

3.2 基本元素

模型的基本元素形式化定义如下:

定义 1 用户集 U (Users)、对象集 OBS (Objects)、角色集 R (Roles)、操作集 OPS (Operations) 及权限集 $PRMS$ (Permissions) 的概念和 RBAC96^[1] 定义的相同, 其中 $U = \{u_1, u_2, \dots, u_m\}$, $OBS = \{obs_1, obs_2, \dots, obs_n\}$, $R = \{r_1, r_2, \dots, r_k\}$, $PRMS = 2^{(OPS \times OBS)} = \{prms_1, prms_2, \dots, prms_i\}, m, n,$

k, i 均为自然数. 这里用户集也称为主体集 (Subjects).

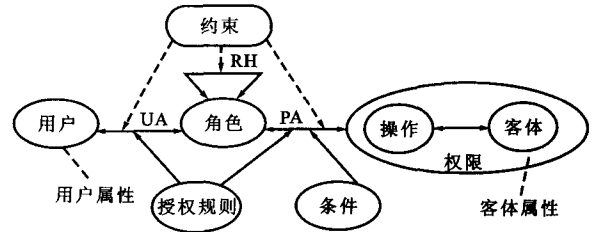


图1 RBUCON 模型

定义 2 模型主要包括以下关系:

(1) $UA \subseteq U \times ROLES$: 用户指派关系, 函数 $assigned_users(r) = \{u \in U \mid (u, r) \in UA\}$ 表示拥有角色 r 的用户集合, 函数 $assigned_roles(u) = \{r \in R \mid (u, r) \in UA\}$ 表示分配给用户 u 的角色集合.

(2) $PA \subseteq PRMS \times ROLES$: 角色指派关系, 函数 $assigned_permissions(r) = \{p \in PRMS \mid (p, r) \in PA\}$ 表示角色 r 具有的权限集合.

(3) $RH \subseteq ROLES \times ROLES$: 角色继承关系, 记作 $\geq$. 若 $r_1 \geq r_2$, 则 r_1 继承 r_2 的所有访问权限, r_2 继承 r_1 的所有用户, 即:

$$r_1 \geq r_2 \Rightarrow authorized_permission(r_2) \subseteq authorized_permission(r_1), authorized_user(r_1) \subseteq authorized_user(r_2).$$

$authorized_user(r : ROLES) \rightarrow 2^{USERS}$ 表示在层次结构上按继承关系委派到角色 r 的一组用户 (包括直接委派的和继承得到的用户), 即:

$$authorized_user(r) = \{u \in USERS \mid \forall r' \geq r, (u, r') \in UA\}.$$

$authorized_permissions(r : ROLES) \rightarrow 2^{PRMS}$ 表示在层次结构上按继承关系授予角色 r 的所有访问权限, 即: $authorized_permissions(r) = \{p \in PRMS \mid \forall r' \geq r, (p, r') \in PA\}$. 继承关系具有自反性等特性.

定义 3 约束集 *Constraints* 主要包括静态角色互斥约束 (SC) 和动态角色互斥约束 (DC). 静态角色互斥约束指满足静态职责分离约束的两个角色不能同时指派给同一个用户. $SC \subseteq (2^{ROLES} \times N)$ 是静态职责分离机制中的对偶 (rs, n) 的集合, 其中 rs 是角色集, n 是自然数且 $n \geq 2$, 则 $\forall (rs, n) \in SC$, 每个用户在 rs 中被分配的角色数必须小于 n . 即: $\forall (rs, n) \in SC, \forall t \subseteq rs : |t| \geq n \Rightarrow \bigcap_{r \in t} assigned_users(r) = \Phi$.

动态角色互斥约束指互斥的角色可以分配给同一个用户,但该用户在一个会话中不能同时激活这些互斥的角色. $DC \subseteq (2^{ROLES} \times N)$ 是动态职责分离机制中的对偶 (rs, n) 的集合,其中 rs 是角色集, n 是自然数且 $n \geq 2$, 则 $\forall (rs, n) \in DC$, 每个用户在 rs 中能够激活的角色数必须小于 n . 即: $\forall rs \in 2^{ROLES}, n \in N, (rs, n) \in DC \Rightarrow n \geq 2 \wedge |rs| \geq n$, 和 $\forall s \in SESSIONS, \forall rs \in 2^{ROLES}, \forall role_subset \in 2^{ROLES}, \forall n \in N, (rs, n) \in DC, role_subset \subseteq rs, role_subset \subseteq session_roles(s) \Rightarrow |role_subset| < n, Constraints = SC \cup DC$.

定义4 属性. 一个属性 att 用属性名 $attname$ 来惟一标识,它有确定的类型来表示属性的定义域,并用关系 $Domain(attname)$ 来表示, att 用二元组 $(attname, Domain(attname))$ 来表示. ATT 是所有属性名的集合,即 $ATT = \{attname_1, attname_2, \dots, attname_n\}$. 所有属性的类型组成的集合称为类型集 $Type = \{type_1, type_2, \dots, type_n\}$, 如整型、时间、日期、URL、布尔型等,也可以是用户根据具体需要自定义的类型. 属性分为用户属性、对象属性和环境属性并且具有可变性.

定义5 用户、对象和环境属性. 为描述方便用 $U.att$ 表示用户属性,用 $O.att$ 表示对象属性,用 $E.att$ 表示环境属性. $U.att = ATT \times TYPE, O.att = ATT \times TYPE, E.att = ATT \times TYPE$. 当前属性的获取用 $att.GetValue()$ 来表示.

定义6 属性表达式. AN 是一系列的规则表达式. $AN = \{AN_1, AN_2, \dots, AN_n\}$, 其中 n 为自然数, $AN_i = \langle attname \rangle \langle OP \rangle \langle Value \rangle$, $attname$ 是属性名, OP 为关系表达式运算符,因属性类型不同,可以是逻辑操作符 $\{=, >, <, \leq, \geq, \neq\}$, 也可以是用户自己定义的操作符, $Value$ 是授权管理员设定的阈值.

定义7 条件 CON , 即环境属性应满足属性表达式用户 u 才具备访问对象 o 的权限 p , 即: $allow(u, o, p) \leftarrow sat(E.att_1.GetValue(), AN_1) \dots \& sat(E.att_n.GetValue(), AN_n)$. 条件是授权的决策因素之一,条件的检测可在访问前 $preCON$, 也可在访问中 $onCON$, 条件不满足可导致访问权限的撤销. 有的文献中也称为上下文信息,如网络带宽、系统负载、系统安全级别、当前的访问时间等.

定义8 授权规则 AR . 它以用户和对象属性为基础,即用户和对象属性需满足一系列属性表达式

用户 u 才能被分配角色 r , 另外角色的激活也要受到授权规则的限制.

为满足最小特权原则,授权应建立在完善的授权规则基础上,结合以上的基本定义制定了如下授权规则:

规则1 预先授权基于用户和对象属性,即:

$allowed(u, o, r) \Rightarrow preA(Authorization(u, r, prms), con)$

规则2 使用中的授权规则: 在用户处于 $accessing$ 状态时,还要检查义务和条件是否满足相应的限制并决定是否继续授权. 即:

$allowed(u, o, r) \Rightarrow onA(Authorization(u, r, prms), con)$

规则3 授权遵循角色继承机制, 即若 $r_1 \geq r_2$, 则 r_1 继承 r_2 的所有访问权限.

规则4 授权受到约束集的限制.

规则5 撤销规则: 当系统检测出当前的环境属性或主、客体属性的变化导致不满足授权规则 AR 时,则撤销激活的角色或为用户指定的角色.

以上,采用了集合论与谓词逻辑对 RBUCON 模型的基本元素进行了形式化定义,集合论和谓词逻辑是访问控制模型形式化的良好工具. 然而 RBUCON 模型具有动态性、并发性和属性更新等特性,集合论和谓词逻辑在描述这些特性时存在不足. 相比较而言,TLA 在描述动态行为上表达能力更强,是一种形式化规格的有效工具. 因此文中将采用 TLA 逻辑对 RBUCON 模型的动态性和安全性进行分析.

4 RBUCON 模型的 TLA 逻辑分析

TLA 是一个表示并发程序及其属性的逻辑,通过将布尔值的动作引入时序逻辑扩展得到,它是规格交互式系统和并发系统及其属性的一个强有力的工具. 交互性、并发性及动态性同时也是开放式网络环境的特性,TLA 对并发性进程和交互式操作描述的有效支持,使得它成为开放式网络环境中的访问控制模型的形式化规格的一种有效工具. TLA 表达形式简洁,易于理解和实现^[5]. 时态操作符语义的详细解释和使用示例参考文献[6],下面用 TLA 逻辑详细分析 RBUCON 模型的动态授权过程.

RBUCON 相关的 TLA 概念定义如下.

(1) 系统状态: 对一组变量的一次赋值,其中变量包括主体属性、客体属性、系统属性这三类变量.

(2) 实体(主体或客体): 表示为一个有限属性

集.

(3) 函数: 一个或多个属性和常量构成的表达式. 在形式上函数是从一组属性值到一个新值的映射.

(4) 使用过程和角色处理过程由 $(s, o, perm)$ 和 (s, r) 来表示, 角色处理过程是使用过程的一部分, 其中 s 表示主体, o 表示对象, $perm$ 表示权限, r 表示角色.

(5) $(s, o, perm)$ 和 (s, r) 的状态被定义为特殊系统变量, 并定义函数 $state(s, o, perm)$ 为从 $\{(s, o, perm)\}$ 到 $\{initial, requesting, accessing, denied, revoked, end\}$ 的映射. 各状态的语义如表 1 所示.

表 1 使用过程状态及语义

状态	语义
initial	$(s, o, perm)$ 尚未产生
requesting	$(s, o, perm)$ 已经产生并正等待系统的使用决策
accessing	根据主体所请求的权限进行相应的角色处理过程, 包括的状态有 $\{request_r, grant_r, enable_r, hond_r, revoke_r\}$
denied	在使用前根据策略系统拒绝了访问请求
revoked	当系统在使用期间撤销了访问, 此 $(s, o, perm)$ 就改变到该状态
end	当主体完成了使用, $(s, o, perm)$ 改变到该状态

函数 $state(s, r)$ 为从 $\{(s, r)\}$ 到 $\{request_r, grant_r, enable_r, hond_r, revoke_r\}$ 的映射. 各状态及语义如表 2 所示.

表 2 角色处理过程状态及语义

状态	语义
request_r	根据请求的权限申请分配相应的角色
grant_r	角色授予状态
enable_r	角色激活状态, 以相应的权限 perm 访问对象
hond_r	角色更新, 处于挂起状态, 暂时不能使用
revoke_r	角色已被撤销不能再使用

(6) 谓词是由变量、函数、常量构成的逻辑表达式. 其语义是从系统状态到布尔值的映射. 若状态中所指派的属性值满足谓词, 则状态满足谓词.

(7) 使用控制动作包括更新属性值的动作、改变使用控制过程状态 $state(s, o, perm)$ 的动作和改变角色状态的 $state(s, r)$ 的动作.

更新属性值的动作包括: preupdate, onupdate, postupdate, 各自在使用前、使用中、使用后执行. 若

系统成功执行了一个更新, 属性值就改变为新值, 动作为 true, 否则为 false.

使用控制动作由改变 (s, o, r) 状态的主体或系统执行. 在一个 (s, o, r) 的生命周期中, $state(s, o, r)$ 存在六种状态值, 从一种状态到另一种状态的转换就是一种使用控制动作. 各动作的執行者及语义如表 3 所示.

表 3 改变使用控制过程状态的动作及语义

动作	执行者	语义
tryaccess($s, o, perm$)	主体 s	产生一个新的访问请求
permitaccess($s, o, perm$)	系统	将对权限 perm 的请求转换为对角色 r 的请求
denyaccess($s, o, perm$)	系统	拒绝访问请求
revokeaccess($s, o, perm$)	系统	撤销一个正在进行的访问
endaccess($s, o, perm$)	主体 s	结束一个访问
preupdate(attribute)	系统	在准予访问前或在拒绝访问后更新主体或客体属性
onupdate(attribute)	系统	在使用期间更新主体或客体属性
postupdate(attribute)	系统	在访问后更新主体或客体属性

改变角色状态的使用控制动作如表 4 所示.

表 4 改变角色状态的使用控制动作及语义

动作	执行者	语义
grant(s, r)	系统	若为 TRUE 则为主体 s 赋予角色 r
enable(s, r)	用户	若为 TRUE 则激活角色, 执行相应的权限
disable(s, r)	系统	中止角色权限
hond(s, r)	系统	若为 TRUE 则表示角色更新, 将原角色挂起
restore(s, r)	系统	恢复原有角色
revoke(s, r)	系统	若为 TRUE 则表示撤销角色, 不能再被使用

使用过程的状态变迁如图 2 所示.

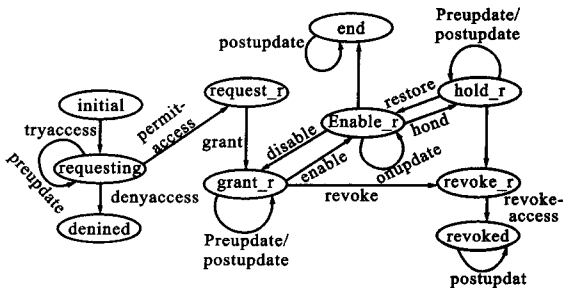


图 2 状态转换图

(8) RBUCON 模型可用四元组 $M = (S, P, E, A)$ 其中 S 表示主体、客体和系统属性的状态序列; P 表示主体和客体属性的谓词的有限集; E 表示上下文信息(环境属性)的谓词的有限集; A 表示动作的有限集.

(9) 逻辑规则是由谓词和动作以及逻辑连接符和时态操作符组成的. RBUCON 中的逻辑规则的BNF 语法定义如下:

$$\phi ::= a \mid p(t_1, t_2, \dots, t_n) \mid (\neg \phi) \mid (\phi \wedge \phi) \mid \forall x : \phi \mid \exists x : \phi \mid \square \phi \mid \diamond \phi \mid \bigcirc \phi \mid \phi \cup \phi \mid \blacksquare \phi \mid \blacklozenge \phi \mid \phi \Theta \mid \phi S \phi$$

其中, a 表示动作, p 表示 n 元谓词, $t_1, t_2, \dots, t_n$ 是谓词的项, x 是变量. $\neg, \wedge, \rightarrow$ 是逻辑连接符, 其语义分别是“非”, “与”, “蕴涵”; $\square, \diamond, \bigcirc, \cup, \blacksquare, \blacklozenge, \Theta, S$ 是时态操作符, 其语义分别是“Always”, “Eventually”, “Next”, “Until”, “Has - always - been”, “Once”, “Previous”, “Since”.

通过以上的 TLA 逻辑分析可知, 在用户访问资源的整个过程中, 使用控制决策要受到授权规则谓词、条件谓词和属性更新动作的限制, 上述因素的变化导致角色状态的变化(撤销、中止、挂起和恢复等), 从而支持了动态授权. 它使资源的使用始终处于合法受控的状态, 相对于静态授权, 能提供更全面的访问控制, 避免静态授权造成权限泄露的产生, 从而提供了更高的安全方式, 在很大程度上满足了实际应用需要和最小特权原则.

5 结束语

文中综合 RBAC 和 UCON 模型的优势提出了一种基于角色的使用控制授权 RBUCON 模型. 在使用定义其基本元素上的基础上, 采用 TLA 逻辑对 RBUCON 动态授权过程进行了分析. 在 RBUCON 模型中, 基于一系列授权规则 AR 来进行角色分配, 角色权限的激活要受到上下文环境的约束, 简化了

授权管理, 更好地支持动态授权, 增强了授权管理的灵活性和安全性. 下一步工作是探讨支持 RBUCON 模型在 PMI 中的应用和动态访问控制策略.

参考文献:

- [1] 芮国荣, 邢桂芬. 基于角色和规则的访问控制[J]. 计算机应用, 2005, 25(4): 864 - 866.
- [2] 姚寒冰, 胡和平, 李瑞轩. 上下文感知的动态访问控制模型[J]. 计算机工程与科学, 2007, 29(5): 1 - 3.
- [3] 崔永泉, 洪帆. 基于使用控制和上下文的动态网络访问控制模型研究[J]. 计算机科学, 2008, 35(2): 37 - 41.
- [4] Ravi Sandhu, Jaehong Park. Usage control: a vision for next generation access control [C]// Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2004: 57 - 64.
- [5] 桂劲松, 陈志刚, 邓晓衡. 一种改进 UCONc 的服务网格授权决策模型[J]. 西安电子科技大学学报, 2008, 35(3): 546 - 553.
- [6] Zhang X, Park J, Parisi - Presicce F, et al. A logical specification for usage control [C]// Proc. of the 9th ACM Symposium on Access Control Models and Technologies. New York, 2004.

作者简介:

谢辉 男, (1983 -), 硕士研究生. 研究方向为授权管理与访问控制.

张斌 男, (1969 -), 博士, 副教授, 硕士生导师. 研究方向为信息安全.

张红旗 男, (1962 -), 教授, 硕士生导师. 研究方向为信息安全.

单宝恒 男, (1983 -), 硕士研究生. 研究方向为授权管理与访问控制.

(上接第 136 页)

参考文献:

- [1] Rind Abdul Razaque, Shahzad Khurram, Qadir M Abdul. Evaluation and comparison of TCP and UDP over wired - cum - wireless LAN [C]// 10th IEEE International Multi-topic Conference 2006, INMIC. Islamabad, Pakistan, 2006: 337 - 342.
- [2] 李建东. 信息网络理论基础 [M]. 西安: 西安电子科技大学出版社, 2002.
- [3] 方乐. 基于无线局域网的 UDP 及 TCP 性能分析 [D]. 上海: 复旦大学, 2000.
- [4] 王毅. 使用 UDP 协议实现数据可靠传输 [D]. 北京: 北京科技大学, 2005.

- [5] Degermark Mikael, Engan Mathias, Nordgren Bjorn, et al. Low - loss TCP/IP header compression for wireless networks [J]. Wireless Networks, 1997, 5(3): 375 - 387.

- [6] Rosenberg J. A framework for conferencing with the STP [EB/OL]. (2006 - 02 - 13) [2009 - 03 - 01]. <http://www.ietf.org/rfc/rfc4353>.

作者简介:

杨云 女, 教授, 硕士生导师. 研究方向为通信网络计算机应用、图形图像处理.

张洁 女, 硕士研究生. 研究方向为 GSM 网络优化的数据分析.