第 31 卷 第 20 期 计 算 机 工 程 2005 年 10 月
Vol.31 № 20 Computer Engineering October 2005
·安全技术· 文章编号：1000—3428(2005)20—0159—03 文献标识码：A 中图分类号：TP309.2

RBAC 策略在 CORBA 分布式对象系统安全中的应用

张志勇，普杰信
（河南科技大学电子信息工程学院，洛阳 471003）

摘 要：基于 RBAC 策略和 CORBASec 框架，引入对象访问的约束机制，给出了一种 CORBA 安全访问控制策略模型——GRBAC for CORBA(General Role-Based Access Control for CORBA)及其访问控制与决策过程。该模型在“基于中间件技术的分布嵌入式系统研究”中得到了实际应用，解决了分布式异构环境下域间访问控制的复杂性问题并且更易于实现企业级自定义安全策略。
关键词：分布式对象系统；CORBA 安全；RBAC；访问控制；访问决策

Application of RBAC Policy in CORBA Distributed Object System Security

ZHANG Zhiyong, PU Jiexin
(School of Electronic and Information Engineering, HAUST, Luoyang 471003)

【Abstract】The constraints of object access is introduced in the basis of RBAC policy and CORBASec frame. An access control model for CORBA, GRBAC for CORBA (General Role-Based Access Control for CORBA), is proposed, including its access control and decision processes. The model is applied in “distributed embedded system based on middleware technology”, and resolves the problem of access control between domains in distributed heterogeneous environment, it can realize self-defined enterprise security policy easily.
【Key words】Distributed object system; CORBA security; RBAC; Access control; Access decision

随着政府、金融等企事业单位信息系统的构建以及电子商务和电子政务的展开，保障信息数据和系统的安全性受到了更多的关注。在基于 Internet 和 Intranet 大规模的分布式对象系统中应当确保信息数据的秘密性、完整性、可用性和可控性，其中分布式异构环境下对象的访问控制问题是分布式对象系统安全性的重点。本文利用具有中性特征的 RBAC 策略和 CORBASec 服务框架，给出一种面向 CORBA 分布式对象系统较为完整的安全访问控制模型 GRBAC for CORBA 及其形式化描述，并对该模型在访问控制与决策中具体过程加以描述。

1 CORBA 安全性与 RBAC 策略

1.1 CORBA 访问控制

CORBA 安全性主要是体现在分布式对象系统的机密性、完整性、可审计和可用性等方面。CORBASec 服务框架主要利用访问控制策略、消息保护策略、审核策略和确认策略，以及备份恢复机制来保障上述 4 个 CORBA 安全特性。

CORBA 访问控制主要是确保主体对客体对象方法的操作是合法的、授权的。在 CORBA 系统中存在大量的主体用户以及对象、方法等客体，因此授权操作将是庞大且复杂的。为简化授权管理和访问控制过程，CORBASec 模型根据主体基元的特权属性把主体划分为不同的用户组，把不同的对象划分到不同的域中，以及把访问权限归结为 4 类操作，从而减少访问规则，降低访问授权与过程的复杂性[4]。

1.2 RBAC 策略与相关模型

RBAC 是一种中性的访问控制策略，主要包括会话、用户、角色、许可和约束等概念。使用 RBAC 策略既可以实现自主访问控制（DAC），也可以实现强制访问控制（MAC）。RBAC 策略的优势体现在利用“角色”这个相对稳定的概念，使得许可分配和角色相联系，而不是直接和用户关联，从而简化了大量繁杂的授权管理；再者，RBAC 策略遵循信息安全中两个规范策略原则“最小特权原则”和“责任分离原则”，以及本身所具有的“数据抽象原则”，更易于实现企业级的信息安全策略与机制。这些 RBAC 特性适合于解决大规模分布式对象系统的访问授权问题。

与 RBAC 策略相关的模型中最具代表性的是 RBAC96 家族和 NIST RBAC。前者是美国 George Mansion 大学 Ravi Sandhu 教授提出的，它是 RBAC 发展历程中的里程碑。随后，在 RBAC96 基础上研究者不断扩展加以完善，使得 RBAC 策略在 Web、WMFS、面向对象系统等诸多领域得到广泛的应用。NIST RBAC 是美国国家标准技术局 RBAC 组织在综合众多 RBAC 相关模型的基础上，提出的一种标准规范化的 RBAC 模型，旨在规范 RBAC 系统工程的创建。在 RBAC 策略基础上定义的面向不同领域的应用模型与实现机制，较好地实现了 RBAC 策略思想，并且体现了它的中性特征。

2 RBAC 在分布式对象访问控制

2.1 GRBAC for CORBA 模型构建与形式化描述

GRBAC for CORBA 是在 CORBASec 框架的基础上，利

基金项目：教育部科学技术重点资助项目；河南省自然科学基金资助项目（0311012600）；河南科技大学青年基金资助项目（2003QN06）
作者简介：张志勇(1975—)，男，讲师、硕士，研究方向：信息安全，智能决策支持系统；普杰信，教授
收稿日期：2004-08-23 **E-mail：**zhangzy@mail.haust.edu.cn

用 RBAC 策略给出的一种面向分布式对象系统安全的访问控制策略模型。它主要由主体、角色、域、对象、方法、许可、约束、会话等部分构成，如图 1 所示。

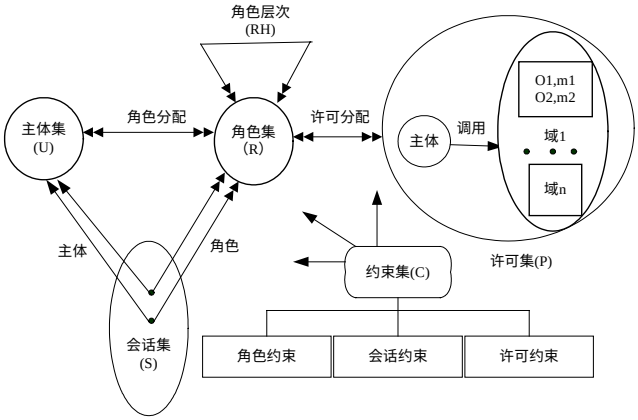

图 1　GRBAC for CORBA 策略模型

用集合论和谓词逻辑形式化描述 GRBAC for CORBA 如下：

定义主体集 U，角色集 R，激活角色集 AR，访问域集 D，对象集 O，方法集 M，许可集 P，约束集 C，会话集 S，策略集 AP。

定义 1（角色指派 Role Assignment） 根据主体凭证中的特权属性为其指派适当的角色，

角色指派关系 RA 是主体与角色之间多对多的关系。

$RA \subseteq U \times R$

$R(u)=\{r|$ 指派给主体 u 的角色，$u \in U\}$

定义 2（许可 Permission） 主体（角色）调用对象方法构成了许可，用三元组表示为：

$P=(U,O,M)$ 或 $P=(R,O,M)$

定义 3（许可指派 Permission Assignment） 根据角色所具有的职能（访问能力）为其指派对于对象方法适当的访问许可。许可指派关系是角色、对象、方法、许可之间多对多的关系，记为 PA=(R,O,M,P)。

$PA \subseteq R \times O \times M \times P$

$PA(r,o,m)=\{p_i|$ 指派给角色 r 关于对象 o 方法中 m 的许可，$r \in R$，$o \in O$，$m \in M\}$

定义 4（访问域与策略 Access Domain and Policy） 访问域是一组相关对象的集合,域间关系是一种偏序关系，满足自反性、反对称性和传递性。每个访问域至多有一个访问控制策略，该策略作用于域中每一个对象成员。访问域是对象组和若干了策略的二元组，记为（O,AP）,AP 表示访问控制策略的集合；域间偏序关系用“ ≥ ”表示。

访问域 $d(d \in D))=((o_1,o_2,\ldots o_n),(ap_1,ap_2,\ldots ap_m)|n>1,m>1)$

域关系性质 1（域层次性 Domain Hierarchy Property） 域间偏序关系使得域本身具有层次性，即在层次域中任意一个低层域中的对象必定也隶属于高层域。

$\forall o,d_i,d_j(o \in O,d_i \in D,d_j \in D)(O \in d_j \wedge d_i \geq d_j \Rightarrow o \in d_i)$

定义 5（角色层次 Role Hierarchy） 角色根据系统上下文的实际环境，具有一定的层次关系。该结构用“ 角色关系图 ”来描述。

$RH \subseteq R \times R$，RH 是角色上的一个偏序关系，称之为角色层次关系或支配关系，一般记为“ ≥ ”。

定义 6（激活角色集 Active Role Set） 主体在一次访问会话开始时所启用的角色集，用 AR(s)表示会话 s 的激活角色集。

$\ni \forall s(s \in S)(AR(s) \subseteq R)$

定义 7 (会话 Session) 主体对客体（对象中的方法）的一次访问过程。一个主体可以启动多个会话，主体与会话的关系是一对多的关系。用 S(u)表示主体 u 一次启用的会话数量。

$\forall u(u \in U)S(u) \geq 1$

会话规则 1（层次角色激活 Cascaded Role Activation） 如果在会话 s 中激活了角色 r_i，那么 r_i 所包含的下层角色 r_j 也同样被会话 s 所激活。

$\forall s,r_i,r_j(s \in S,r_i \in R,r_j \in R)(r_i \in AR(s) \wedge r_i \geq r_j \Rightarrow r_j \in AR(s))$

在 GRBAC for CORBA 策略模型中，约束集中的约束策略规则主要分为两类：(1)该模型必须遵循的规范策略规则；(2)用户在实际分布式对象安全系统构建中可以自定义的策略规则。本文将对规范策略规则加以形式化具体描述，作为 GRBAC for CORBA 系统创建的依据。规范策略主要在角色层、许可层和会话层，分别对角色指派、许可指派和启用会话定义约束规则，并利用访问监控器加以实施。其中角色层的互斥可以进一步细化为静态互斥角色和动态互斥角色。

定义 8（约束集 Constraint Set） 作用在主体对客体访问过程（包括访问授权和会话）中的约束规则构成约束集。它是增强 GRBAC for CORBA 访问控制策略的关键组件。

定义 9（静态互斥角色 Static Mutex Role） 静态互斥角色是指在访问授权时不能同时指派给同一主体的两个或多个角色，所有静态互斥角色构成的集合成为互斥角色集 SMR。

$Sta\_mutex(r_i)=\{ r_j | r_j$ 和 r_i 满足静态互斥,$i \neq j\}$

定义 10（动态互斥角色 Dynamic Mutex Role） 动态互斥角色是指在主体启用会话时不能同时激活的两个或多个角色。所有动态互斥角色构成的集合成为动态互斥角色集 DMR。

$Dyn\_mutex(r_i)=\{ r_j | r_j$ 和 r_i 满足动态互斥,$i \neq j\}$

定义 11（互斥许可 Mutex Permission） 互斥许可是不能同时指派给同一角色的两个或多个许可，所有互斥许可构成的集合成为互斥许可集 MP。

$Perm\_mutex(p_i)=\{p_j|\ p_j$ 和 p_i 满足互斥，$i \neq j\}$

规范约束规则 1（角色约束 Role Constraint） 在 SMR 中的任意两个角色都不能同时指派给任意一个主体。

$\forall u,r_i,r_j(u \in U,r_i \in R,r_j \in R)(u \in R(r_i) \wedge u \in Role\_members(r_j) \Rightarrow r_j \notin Sta\text{-}mutex(r_j))$

规范约束规则 2（会话约束 Session Constraint） 在 DMR 中的任意两个角色都不能在任意一次会话中被启用。

$\forall s,r_i,r_j(s \in S,r_i \in R,r_j \in R)(r_i \in AR(s) \wedge r_j \in AR(s) \Rightarrow r_j \notin Dyn\_mutex(r_j))$

规范约束规则 3（许可约束 Permission Constraint） 在 MP 中的任意两个许可都不能同时指派给任意一个角色。

$\forall r,p_i,p_j(r \in R,p_i \in P,p_j \in P)(p_i \in P(r) \wedge p_j \in P(r) \Rightarrow p_j \notin Perm\_mutex(p_j))$

GRBAC 中的规范约束规则满足了信息安全中责任分离的基本准则，在实际的分布式对象系统中根据需求可以灵活地自定义具体的规范约束规则。

2.2 基于 GRBAC for CORBA 模型的访问决策

在定义 4 中给出了每个域至多存在一个访问控制策略，

但是一个对象可以隶属于多个域，因此它可以有多个访问控制策略。访问决策就是解决域间对象的多个访问控制策略不一致问题。在 CORBASec 模型中使用合并策略对作用于对象的多个策略按照某种规则实施合并综合决策，最后得出一个“允许访问”或“拒绝”的决策结果。然而 CORBASec 模型中并未定义任何合并规则，所以在使用过程中会出现最终访问决策结果不一致的情形[4]。

鉴于域具有层次特性，GRBAC for CORBA 策略模型能够处理层次域和平行域两种类型。当一个对象隶属于层次域时采用“属地规则”实施访问决策，即低层的策略决定访问决策的结果；当对象属于多个平行域时使用“权重规则”进行决策，即决策结果根据每个域的综合权重来决定。

访问决策结果集用 AD 表示，maxweight 函数取得综合权重最大的访问控制策略。

访问决策规则 1（属地规则 Domain Rule） 层次域中的对象在访问决策时，决策结果取决于下层域的访问控制策略。

$$\forall\ o,d_1,d_2,ap_1,ap_2(o\in O,d_1\in D,d_2\in D)d_1\geq d_2 \Rightarrow ap_2\in AD$$

访问决策规则 2（权重规则 Weight Rule） 平行域中的对象在访问决策时，决策结果取决于每个平行域访问控制策略的权重综合值。

$$\forall\ d_1,d_2,ap_1,ap_2(d_1\in D,d_2\in D,ap_1\in P,ap_2\in P)\ \neg(d_1\geq d_2)\wedge\neg(d_2\geq d_1)\Rightarrow maxweight(ap_1,ap2)\in AD$$

2.3 CORBA 的访问控制过程

在 CORBASec 框架中，访问控制的执行是由 accessDecision 对象（ADO）完成的。基于 GRBAC for CORBA 模型的访问控制将在此框架基础上，根据用户自定义约束机制和 2.2 节给出的决策规则实施访问控制与决策。访问控制如图 2 所示，具体过程分 5 个步骤进行。

(1)主体启用自身所具有的角色，发出调用对象方法的消息，从而开始一次会话。

(2)ORB 接受访问请求的消息后，再请求 ADO 对象进行访问决策。

(3)ADO 对象接到 ORB 请求后，从客体对象所在的域取得访问控制策略，从策略中获取主体所具备的许可，通过比较主体访问请求中的活跃角色集与许可和本身所具有的（已授权）许可作出访问决策。如果对象所在多个域，则根据所在域的类型，按照 2.2 节给出的决策规则，进行综合决策。

(4)ORB 收到 ADO 决策结果后执行之，如果决策结果是允许访问，ORB 则调用对象所需的方法，并将结果返回给主体；反之，则拒绝主体调用该方法。

(5)当主体接收到调用执行结果或是“拒绝访问”的错误信息后，本次会话结束。

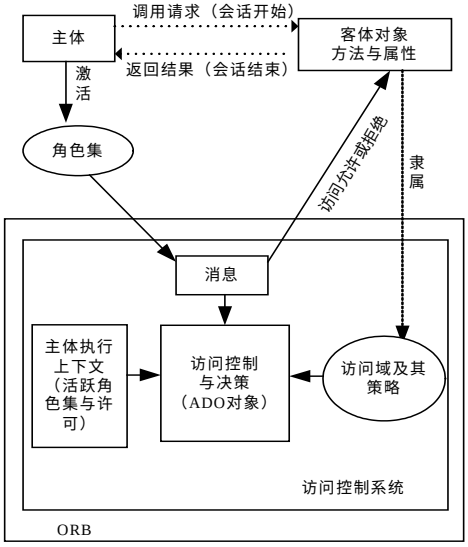

图 2 基于 GRBAC for CORBA 策略模型的访问控制

3 结束语

本文所给出的 GRBAC for CORBA 策略模型弥补了 CORBASec 缺少主体层次关系以及访问约束的不足，使得用户可以自定义分布式对象系统的安全策略，提高了安全表达能力和性能，是一种在分布式对象系统中解决访问控制问题较完备的模型。对于分布式对象系统访问控制中的转授权策略与机制，需做进一步的研究工作以进一步增强分布式对象系统的安全性。

参考文献

1 Obelheiro R R, Fraga J S. Role-based Access Control for CORBA Distributed Object Systems[C]. In:Proceedings of the 7th International Workshop on Object-oriented Real-time Dependable Systems, 2002

2 谭文芳, 胡南军. 基于 CORBA 的分布式访问控制[J].小型微型计算机系统, 2001, 22 (11):1359-1363

3 王传标, 吴　敏. CORBA 安全中的基于角色的访问控制[J].计算机工程, 2002, 28 (12):201-202

4 Blakley B.CORBA 安全性指南[M]. 北京：人民邮电出版社, 2000

(上接第 151 页)

5 总结

本文根据移动设备的应用环境以及可能带来的安全问题提出了一个基于策略的移动设备安全应用框架。该框架采用 XML 描述访问控制策略，结合身份认证、信任连接等机制实现对移动设备自身资源以及设备对网络服务的安全访问。

但是移动设备自身存在的一些弱点，如有限的计算能力、内存、接口和电池寿命等也给在这些设备上使用各种安全措施带来了很多额外的约束。另外它们的轻便和移动性也让它们更有可能处于被盗窃或错误使用的情况下。本文提出的安全应用框架并未能处理上述的这些问题，这也是接下来我们研究的方向。

由于移动设备在普适计算环境中将是主要的计算设备，网络服务也来自于嵌入式设备，而本文提出的框架中网络服务来自于 PC 机。在未来的工作中我们将对该安全应用框架进行扩展，以实现设备对设备的安全访问。

参考文献

1 Jansen W, Karygiannis T, Korolev V, et al. Policy Expression and Enforcement for Handheld Devices. NIST Interagency Report – 6981, 2003-04

2 Bray T. Extensible Markup Language (XML) 1.0. World Wide Web Consortium (W3C), http://www.w3.org/TR/REC-xml, W3C Recommendation, 2000-10-06

3 Windows Development/Driver Development Kit/Network Devices and Protocols. http://msdn.microsoft.com/library

4 Robinson S, Allen K S. 杨　浩, 杨铁男译. C#高级编程. 北京:清华大学出版社, 2003