第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)23—0165—03 文献标识码：A 中图分类号：TP311

一种军用的基于任务-角色的访问控制模型

韩若飞[1]，汪厚祥[1]，杜 辉[1]，王 璐[2]
(1. 海军工程大学电子工程学院，武汉 430033；2. 信息产业部第53所海军代表室，锦州 121000)

摘 要：传统的强制访问控制策略(MAC)可操作性、灵活性差，日益不适应分工明确、分布性广、实时性要求高的军事领域，基于任务-角色的访问控制策略(T_RBAC)结合了基于角色(RBAC)和基于任务(TBAC)访问控制的优点，应用性很广。在分析了强制访问控制思想后，将其引入基于任务-角色的访问控制模型中，构建了一种军用的基于任务-角色的访问控制模型，并对模型的性能作了简要分析。

关键词：强制访问控制；基于任务-角色的访问控制；角色层次；角色组；任务模板

Task_role_based Access Control Model for Military Use

HAN Ruofei[1], WANG Houxiang[1], DU Hui[1], WANG Lu[2]
(1. Electric and Engineering College, Naval University of Engineering, Wuhan 430033;
2. Department of Naval Deputies, The 53rd Graduate School of Dept. of Information Industry, Jinzhou 121000)

【Abstract】The traditional mandatory access control tragedy (MAC), which is weak in maneuverability and flexibility, can not fit well in the military field gradually, which is definitely divided into several posts, geographically widely distributed and high real-timely demanded as well. The task_role_based access control tragedy (T_RBAC) which combines advantages of both RBAC and TBAC has a good practicability. The spirit of MAC is analyzed and then introduced into a task_role_based access control model. At last, a task_role_based access control model for military use is built, and its capability is simply analyzed.

【Key words】MAC; Task_role_based access control(T_RBAC); Role hierarchy; Role group; Task template

访问控制技术是保障信息系统安全性的一项重要技术，在军事领域通常采用强制访问控制策略来保障其安全性。传统的强制访问控制技术在实用性、灵活性方面存在很多缺陷，只能按照已定义好的安全级别实施访问控制，对实际应用造成很多不便。美国 NIST 已采用较为灵活的基于角色的访问控制模型作为其标准，并在军事部门以及其他领域等得到应用。国内也有用 RBAC 改造 MAC 以应用在军事领域的研究。

RBAC 在各个领域中的应用已经很多，暴露出了其在分布式系统、工作流系统以及实时系统中的不足。本文将引入当前研究较多的基于任务-角色的访问控制，并借鉴 MAC 的一些思想，构造一种军用的基于任务-角色的访问控制模型（A_T&RBAC)。

1 强制访问控制策略

强制访问控制的基本思想是对访问的主体和客体都附上一个安全标签，通过比较主体和客体的安全等级来控制主体是否有访问客体的权限。由于加上了不同的安全标签，MAC 依等级严格控制了对访问的授权，正是基于如此，此策略在军事系统中应用较多。

依据强制访问控制策略，有两个应用较广的强制访问控制模型：BLP 模型和 Biba 模型。它们都是基于格的访问控制模型（LBAC)，这种模型通过一种格的偏序关系实现信息流的单向流动，以保证其安全性和机密性。这里的格实际上就是安全标签。其一般规则有

(1)简单安全特性：主体只能读安全级别受其安全级别支配的客体。

(2)星型特性：主体只能写安全级别支配其安全级别的客体。

虽然 MAC 作为一种访问控制策略显得过于简单，灵活性较差，使用不方便。但其用格实现偏序安全等级的思想在对安全性要求高的应用领域仍然很有价值。

2 基于任务-角色的访问控制策略

强制访问控制缺乏灵活性，目前的研究都趋向于用灵活性高的基于角色的访问控制模型来实现 MAC 的思想，由于角色的继承性，很容易实现偏序关系。一般的做法都是通过对一个安全级别分别建立一个读角色和写角色，结合起来实现访问控制。

然而 RBAC 在权限的动态管理方面显得力不从心，仍然无法胜任对分布性、协作性和实时性要求较高的应用领域。解决的方法就是在 RBAC 的框架下再加入任务的概念，结合基于角色和基于任务策略的优点，利用任务来动态管理权限，这就是目前访问控制领域的研究热点：基于任务-角色的访问控制。

目前基于任务-角色的访问控制模型主要有 RTBAC 和 T&RBAC 两种，T&RBAC 的性能相对优良一些。在本人的前期研究中已对 T&RBAC 模型提出了几条改良意见，建立了改良的 T&RBAC 模型，这里只对改良模型作一下简要介绍。

改良模型的基本结构如图 1 所示。

作者简介：韩若飞(1983－)，男，硕士生，主研方向：访问控制，分布式系统；汪厚祥，教授；杜 辉，硕士生；王 璐，硕士、工程师

收稿日期：2006-08-08 **E-mail：**wanghx@public.wh.hb.cn

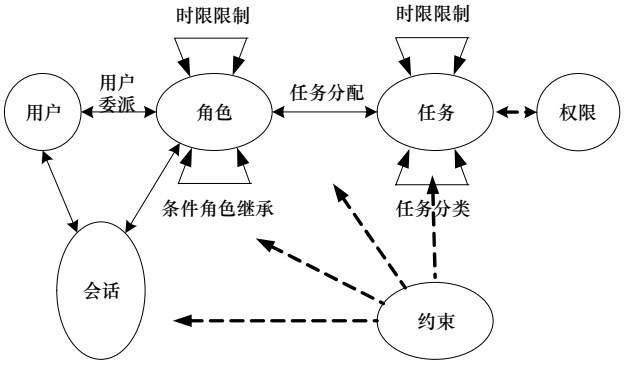

图 1 T&RBAC 改良模型

如前所述，改良模型与原先 RBAC 在结构上的主要区别就是在角色和权限之间加入了任务层，该模型的核心已经不是角色而是任务。模型将权限直接与任务连接起来，角色只有通过执行任务才能获得权限，实际上，角色只是用来限制可执行任务的一个途径。任务本身就是一个动态的概念，动态产生，动态分配权限，真正实现了动态授权和最小权限限制。同时任务之间可以相互协作，并根据上下文环境控制任务的各种状态，再加上执行时间限制，解决了 RBAC 在工作流和实时应用中的不足。

改良模型的几个关键概念如下：

(1)条件角色继承：在实际应用中，很多任务都是其相应角色的专属任务，不能通过角色继承传递给高级角色；即使是可传递的任务，往往也有传递范围控制，因此要给角色任务集中的每个任务加一个传递系数，实现有条件的角色继承。

(2)任务分类：在实际应用中，不是所有任务都直接处理数据对象，有些任务是用来管理或监督其它活动任务的，因此需要对任务作进一步分类。这样更有利于划分任务权限以及任务优先级的配置。

(3)时限控制：这里引用基于时限的访问控制（time-based access control）的思想，对角色的可激活时段做出限制，对应于现实世界的作息时间安排；对活动任务的活跃时间做出限制，超出时间将自动删除任务，防止任务之间竞争资源造成死锁。

条件角色继承实际上打破了传统的角色继承思想。原来的角色继承主要是为了分配权限时的方便，避免权限的重复分配。而现在，权限只与任务关联，角色继承变成了继承任务，又由于专属任务的存在，使得角色继承显得画蛇添足。这里的条件角色继承实际上是通过任务的继承属性实现的，单纯角色之间的继承关系将不复存在，原先 RBAC 的最小角色问题也将消失，因此通过角色继承得到的偏序关系也将不复存在，为了在军事领域中用到偏序关系必须对模型增添内容，这些将在下面构造军用的基于任务-角色模型（A_T&RBAC）时讨论。

此改良模型和 RBAC 一样也是策略中立的，只是一个概念模型，并不面向任何具体的应用领域，因此在将模型应用到实际的应用领域中去的时候需要根据领域的实际情况对模型进行适量的添加或改变。

3 军用的基于任务-角色的访问控制模型

这里将对策略中立的改良模型进行进一步分析、扩展，构造一个军用的基于任务-角色的访问控制模型。

3.1 角色管理

角色实现是对用户和任务的分类。在军事机构中，岗位众多，因此需要的角色也很多，但根据所做工作的类别不同，可以简单分为指挥员、协调员和操控员，所有角色都能化归为这 3 类。

指挥员负责对组内数据、任务的全局管理以及和其他角色组的通信。协调员负责在指挥员授权的条件下分担指挥员的一些职能，并能在指挥员缺席的情况下暂管角色组。操控员负责执行指挥员的命令，对组内数据和设备进行具体的操作。

3.1.1 角色层次

为了在使用条件角色继承的同时继续保持角色间的偏序关系，这里引入角色层次的概念。

角色层次就相当于 MAC 中的安全标签，代表了角色的安全等级，对安全性敏感数据的访问任务引入角色层次限制。例如以递增的顺序定义对访问客体的读任务、拷贝任务、写任务、新建任务、删除任务所需要的角色层次级别，依照 MAC 的两条规则控制，实现数据的单向流动。角色层次的基本思想如图 2 所示。

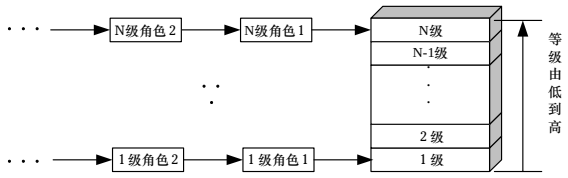

图 2 角色层次的基本思想

3.1.2 角色组

角色组是实施访问控制的基本单元，包含访问控制模型中的各个实体，对应一组用户、一组角色、一组任务、一组数据或设备和一组约束集。在分布式应用中，不同的角色组可能分布在系统的不同组成部分中，是一个相对独立的管理单元。通过角色组来管理，既能对组内应用需求定义特定的角色、任务和访问控制策略，又便于在各组之间提供统一的通信端口，兼顾了分布式应用中的自制性与交互性需求。

组级别对应于军事部门的级别、编制以及一定的角色层次。角色组必须有一个或以上的指挥员角色，指挥员角色的角色层次不能超过该组的组级别，且必须高于直接子组的最高组级别。

角色组类似于 RBAC 中的用户组，但二者是有区别的。用户组仅仅是一组用户的集合，与角色的概念相对独立，用户登录时既要登录用户组又要登录角色，而角色组是访问控制的基本单元，用户只需与角色关联，登录角色就能登录角色组，受一定的访问控制策略约束。角色组的基本结构如图 3 所示。

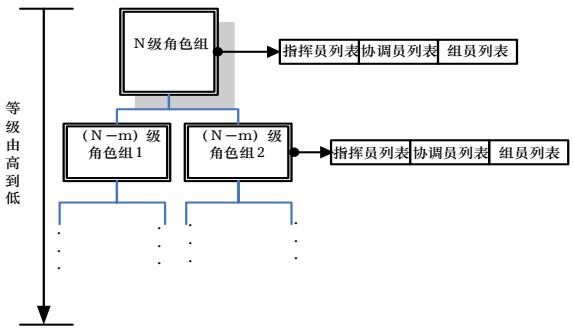

图 3 角色组结构

3.2 任务管理

任务是基于任务-角色模型的核心，用户只有通过角色获

得任务，才能动态地获得权限。任务的思想源于基于任务的访问控制策略，由于任务的动态性和细粒性，对于任务的管理难度较大，目前国内外的研究大都停留在概念模型和算法上，具体的应用模型研究不多。在 A_T&RBAC 模型中，将对具体应用中的一些问题进行研究。

3.2.1 任务分类

为了便于对任务进行管理，在实际应用中需要对任务按主要功能、操作对象等作进一步分类。在军事应用中，有显控、火控、请求与命令、实时任务管理和静态档案管理等众多任务。这里将任务分为以下 6 类。

(1)显示任务：负责向用户显示系统状态、物资状况和战场状况等实时信息。输入数据是组内的显示数据，输出数据是显示信号。角色组内继承，父组继承子组的显示任务。

(2)消息任务：负责在用户或任务之间传送消息，可进一步分为命令消息、请求消息、报告消息和一般消息等。消息类型由消息发出用户和接收用户的角色或任务的状态决定。输入数据是具体的消息内容，输出数据是一定格式的消息结构体。完全角色继承。

(3)数据任务：负责在用户或任务之间传送数据，可有多种数据类型，有数据安全级限制。输入数据是具体的数据内容，输出数据是一定格式的数据结构体。完全角色继承。

(4)操控任务：负责向设备发送控制信号，面向具体的设备，操控员的专属任务。输入数据是指挥员或协调员的命令消息及操控初始数据，输出数据是控制信号和相应的报告消息。不可继承。

(5)任务管理：负责管理角色组内的活动任务，可实时新建工作流任务，取消任务，更改任务权限、优先级等，由指挥员或协调员执行。输入数据是任务操作命令及修改数据，输出数据是操作后的任务信息块或工作流信息块。父组指挥员继承子组指挥员的管理范围。

(6)数据管理：负责管理角色组内的人员、资源和数据，有组级别限制，指挥员任务，有数据安全级限制。输入数据是数据操作命令及修改数据，输出数据是操作后的数据。父组指挥员继承子组指挥员的管理范围。

3.2.2 任务模板

由于任务对应于一定的设备和数据类型，变动相对角色来说会比较频繁，而任务往往又是一个功能模块，因此对任务进行静态管理显得比较麻烦。

这里引入任务模板的概念。任务模板记录了任务的静态信息，如任务的执行角色、操作对象类型、基数限制、时限限制、初始状态约束、输入数据类型、输出数据类型、权限集以及其它一些任务约束等。任务模板由任务资源表管理，表里将记录各个模板的地址。当增加新任务时，需要将该任务的静态信息模块化一个任务模板，并将任务的名称、模板地址等参数注册到任务资源表中，实现统一管理。

任务模板存放在任务的直属角色组中，父组的资源表包含各子组资源表。任务的静态管理如图 4 所示。

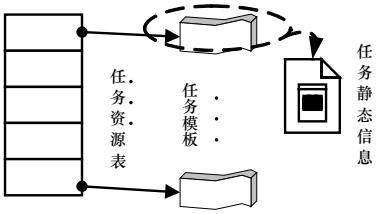

图 4 任务的静态管理

3.2.3 任务调度

在 TBAC 中，任务只是一个逻辑上的概念，实际上是通过控制授权结构体、授权步来实现任务调度的，类似的，这里将引入任务信息块和工作流信息块的概念。

任务信息块是在任务激活时创建，用来管理任务的各种信息的一个结构体。任务信息块包含任务名、任务 ID、任务执行用户 ID、角色名、角色组、任务类型、任务状态、任务权限、任务输入数据类型、输出数据类型、任务地址等任务的基本信息。任务信息块由激活任务的用户创建的会话直接管理。

工作流信息块由指挥员或协调员在新建工作流任务时建立。工作流任务是一组定义了操作顺序及关系的原子任务集合。工作流任务状态与各原子任务任务状态的关系是：当工作流中有一个原子任务处于静止态（活动态或消亡态）时，工作流处于静止态（活动态或消亡态）；当工作流中至少有一个任务处于挂起态，且没有一个处于活动态时，工作流处于挂起态；当所有原子任务都处于终止态时，工作流才处于终止态。工作流信息块中包含了工作流任务中各原子任务的任务信息块，它与任务信息块的关系正如 TBAC 中授权结构体与授权步的关系。工作流信息块包含工作流名、工作流 ID、创建用户 ID、角色名、角色组、工作流状态、工作流初始数据、原子任务信息块列表及执行顺序等信息。工作流信息块由指挥员或协调员的会话管理。任务调度的一般流程如图 5 所示。

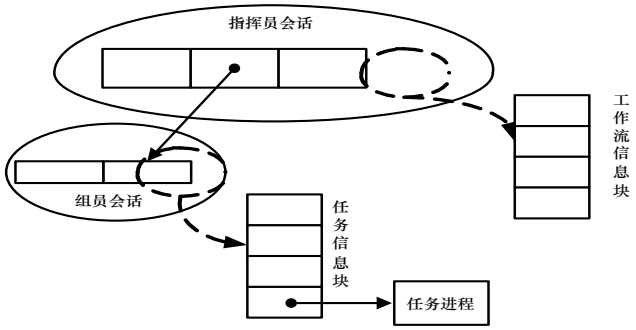

图 5 任务调度

通过以上的研究讨论可得 A_T&RBAC 的结构模型如图 6 所示。

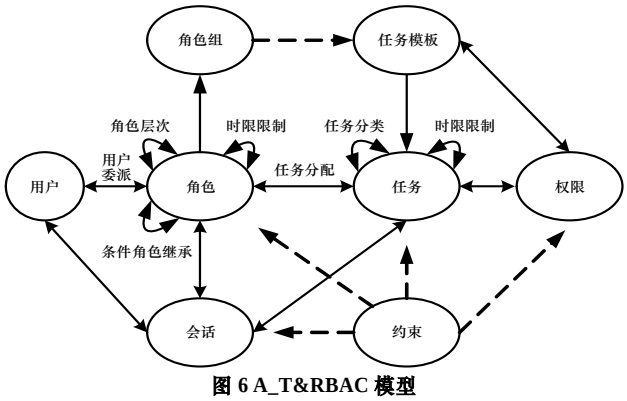

图 6 A_T&RBAC 模型

4 A_T&RBAC 模型安全性分析

首先证明模型能够满足 MAC 的简单安全特性和星型特性：

在 MAC 中，策略通过比较访问主体和客体的安全等级来确定是否授予访问权限，可形式化表示为

（下转第 179 页）

为流密码的第 2 块，如图 2 所示。

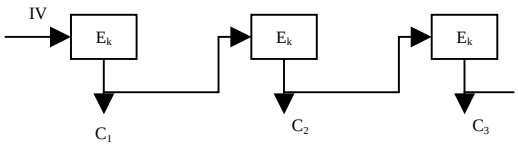

图 2 密钥流生成

由于分组密码体制在设计时已考虑到让算法能够抵抗已知明文攻击，选择明文攻击，因此即使已知 C_1、C_2、C_3 整个序列对于本加密方法而言并不影响密钥安全性，而且在密文中不是 C_1、C_2、C_3，而是它们经过取模运算后的值，可见安全性得到了保障。初始向量可以是保密的，也可以是公开的，关键就是双方的同步问题，必须采用相同的密钥和相同的初始向量。由于分组密码的长度一般在 56bits 以上，扩充项中的选择项数目远远小于 2^{56}，不会存在长度上的问题。

3 外层加密

为了保证安全性，仅仅进行一次上述的加密是不够的，虽然许多信息具有迷惑性，由于语言本身的复杂性、数据库的识别能力和有效性未必很强，一些没有被替换的词直接泄漏了，此外上述加密的处理过程中对于关键词识别的时候存在部分误判，也对于安全性有一定影响。为加强安全性采用一个外层的现代密码学的加密方法，可以运用分组密码加密。

4 解密和伪密钥获取

解密过程是一个相反的过程，首先对于外层的分组密码加密进行相应的解密，其次要对于扩充进行解密。当进行这层解密的时候，先打开文件或者输入外一层解密的内容，读取和识别内容，遇到第 m 个扩充项的起始标记就进行判断和去冗余。解密时没有遇到标记的非扩充项部分直接输出，遇到标记则用上述的方法找出正确选择项，作为输出，最后将所有输出的文档内容保存到相应的文档或者直接输出。

加密解密中有两个密钥，要获取伪密钥，可以将外层分组密码的密钥不变，然后任意选取内层的密钥进行解密，如果没有出现误判问题并且替换有效，这个密钥配合正确的外层分组密码密钥就是一个伪密钥，出现误判等情况可以换一个密钥再来，按照上述方法直到找到合适的伪密钥为止。如果内层采用一次一密进行加密，可以很容易设计出一个误导的伪明文，然后根据算法加以逆推，获取伪密钥来误导密码分析者。

5 结束语

本文针对密码学中的软磨硬泡攻击提出了密钥可信度的概念，并且设计了一种可以用伪密钥误导密码分析者和迷惑密码分析者的算法，本算法已经通过 Delphi 编程实现。关键词数据库可以是通用的，也可以根据实际需要进行设计，这样可以适应实际需要。由于自然语言的复杂性，本设计采用简化的规则，研究还非常初步，有待完善。

参考文献

1 王　勇. 一次一密的安全性与新保密体制[J]. 信息网络安全, 2004, (7): 41-43.

2 Schneier B. Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C[M]. John Wiley & Sons Inc., 1996.

3 Shannon C E. Communication Theory of Secure Systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

4 王　勇. 未来密码学的新思路——更加积极的加密方式[J]. 信息网络安全, 2002, (11).

5 保尔. 吴世忠, 宋晓龙, 李守鹏译. 密码编码和密码分析: 原理与方法[M]. 北京: 机械工业出版社, 2001.

（上接第 167 页）

{Label(S),Label(O)}->Permission

其中，Label(S)、Label(O)分别表示主体和客体的安全等级，Permission 表示对应的权限。而模型定义中已对安全性敏感数据的访问任务限制了访问主体的角色层次，而任务又对应着访问权限，故通过比较主体角色层次和客体的层次需求来决定是否执行任务，授予权限，形式化表示为

{Label(S),Label(O)}->Task->Permission

显然模型可以兼容 MAC 的两项规则。

再证明模型能够满足最小特权原则和职责分离原则：

最小特权原则就是用户只能获得访问客体所必需的最小的权限。传统的 RBAC 是通过角色继承和最小角色来实现，在 A_T&RBAC 中，角色与权限没有直接关系，角色获得任务也不是通过简单的偏序继承，角色只有激活任务才能获得任务的权限，而任务的访问权限更是提前定义好的恰好能实现访问的最小权限，任务完成后权限自动撤消，实现动态授权，显然满足最小特权原则。

职责分离原则包括静态职责分离和动态职责分离，用来确保任何用户不能单独完成任何需要多用户合作完成的任务，避免诈骗行为的产生。职责分离原则主要是通过定义角色互斥来实现的，A_T&RBAC 模型继承了 RBAC 的主体框架，同样可以通过定义互斥角色实现职责分离。

5 结论

A_T&RBAC 模型吸收了大量访问控制领域的控制思想，有 MAC 的偏序安全标记、RBAC 的角色管理思想、TBAC 的动态权限管理思想以及条件角色继承和时限控制的思想，同时加入了任务分类的概念，相对其它访问控制模型有许多良好的特性。其安全性即能满足 MAC 的简单安全特性和星型特性，又能满足动态授权和最小特权原则，通过角色互斥也能满足职责分离原则。模型能够满足分布式、工作流和实时应用，但并不完善，在如何定义工作流任务中各原子任务的执行流程以获得更广泛的适用性方面还需进一步深入研究，初步的设想是可以通过创建一个谓词逻辑系统来实现。

参考文献

1 许　访, 沈昌祥. 基于任务的强制访问控制模型[J]. 计算机应用研究, 2004, 21(11): 70-74.

2 田敬东, 何再朗, 张毓森. 用角色模型实现传统访问控制[J]. 吉林大学学报(信息科学版), 2005, 23(3): 299-305.

3 付松龄, 谭庆平. 基于任务和角色的分布式工作流安全模型[J]. 国防科技大学学报, 2004, 26(3): 57-62.

4 施教芳, 李建华, 薛　质. 一种扩展的 TBAC 访问控制模型研究[J]. 通信技术, 2002, (11): 95-97.