文章编号：1672-2892(2010)04-0463-04

基于网络环境安全的可信访问控制策略

陈虹志[1]，周安民[1]，邓 赟[2]

(1.四川大学 信息安全研究所，四川 成都 610064；2.中国电子科技集团公司 第30研究所，四川 成都 610041)

摘 要：为了抵御网络系统受到非法访问，文章在基于 RBAC 访问控制模型的基础上，结合可信计算的思想和原则，提出了一种基于环境的 ERBAC 访问控制模型。该模型将角色与网络系统环境的安全性相关联，只有当用户的环境条件达到一定的安全阈值时，其对应角色的权限方案才会生效，并能访问相应资源。最后结合实例证明了该模型及其语义实施的正确性。

关键词：基于角色的访问控制；ERBAC 访问控制模型；可信度量；网络安全

中图分类号：TN915.08；TP309.1 **文献标识码：**A

One trusted computing access control strategy based on network environment security

CHEN Hong-zhi[1]，ZHOU An-min[1]，DENG Yun[2]

(1.Institute of Information Security，Sichuan University，Chengdu Sichuan 610064，China；2.The 30th Institute of China Electronics Technology Group Corporation，Chengdu Sichuan 610041，China)

Abstract: To defend network system against the harm done by unauthorized access. basing on theory and conception of trusted computing and Role Based Access Control(RBAC) model，this paper proposes an access control model named Environment Role Based Access Control(ERBAC). This model correlates the role with system environment security. When an user′s environment is secure enough，the permissions corresponding to its roles are valid，and the user is allowed to access resources. An access control application instance is given to prove the effectiveness of the model and semantics.

Key words: Role Based Access Control；ERBAC model；trust measurement；network security

在网络日益发达的今天，如何保护系统，防止其被非法访问，逐渐成为网络安全的研究重点。在文献[1]中提到了基于时态的 RBAC 模型，但是除了时态之外，用户所处环境的可靠性及访问行为本身的实施状况也直接影响到系统的安全，使得用户常常处在一种动态的网络环境当中，这就给现有的 RBAC 模型带来了挑战。

文章在基于 RBAC 访问控制模型[2-5]的基础上，提出了一种基于网络环境安全的角色访问控制 ERBAC 模型，该模型的主要特点是采用将角色与环境属性关联的思想[6-7]，结合可信计算技术[8-9]，在现有的访问控制模型基础上对传统模型进行扩展，扩展后的模型能够有效地确保计算机系统时刻处在用户的控制之下，实现用户对系统的安全访问。

1 ERBAC 策略提出

1.1 ERBAC 策略提出的背景

虽然文献[2]中提出的 RBAC 模型比其他的控制策略更适合于现在的大多数环境，但是由于并没有将系统环境的很多约束机制及实现方法考虑进来，因此其局限性非常明显，使得 RBAC 模型在现有的很多系统访问控制中的问题都没有得到很好的解决。

1.1.1 恶意行为对网络环境的破坏

由于参与网络交互的各个用户形成了访问控制的不同角色，在用户获得了对网络资源的访问权限后，就不可

收稿日期：2009-12-09；修回日期：2010-01-13

避免地会受到具有此权限的用户对资源的修改，因此对整个系统的完整性保护是必要的，一旦某个用户对系统做出不可预知的行为，那么在其他用户访问资源时，就会因资源环境的变化使得当前用户角色和权限之间的变化得到调整。

1.1.2 网络环境的调整问题

网络系统的一个典型特征是动态性，对资源的提供者而言，它可以根据当时的环境情况来决定系统的访问权限，在用户企图实施权限时，其环境必须达到一定的安全性阈值，不同阈值采用不同的动态控制机制实时调整访问控制策略，总之，环境是一系列可能影响安全决策状态信息的集合。

1.1.3 对网络环境的可信度量的问题

根据可信计算的思想和原则，可信度量是指对于任何将要获得控制权的实体，都需要预先通过完整性计算进行度量。因此，在用户访问网络系统之前需要对系统环境资源进行可信度量，只有通过可信度量的实体才有权被访问，这样就为用户访问系统的资源做好了充分的安全准备。

综上所述，文章对原有 RBAC 模型进行了扩展，使其能更好地适用于现有的 ERBAC 策略。

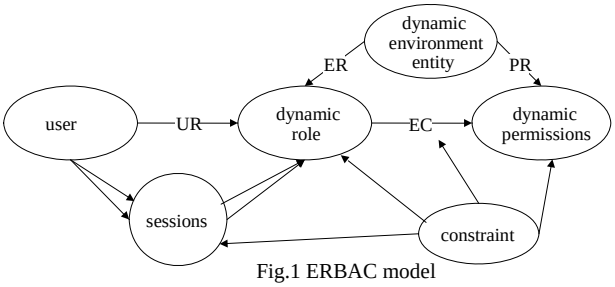

Fig.1 ERBAC model
图 1 ERBAC 模型

2 ERBAC 方案设计及实施

2.1 ERBAC 模型设计

定义(ERBAC 模型)

1) ERBAC 模型(见图 1)继承 RBAC 模型的已有特征。

2) 环境属性实体集合(Environmental Attribute Entity) E：它是可能引发角色及权限变化的要素集合，包括被访资源动态环境变化以及动态产生的敏感信息。

3) UR (用户角色集合)：$UR \subseteq U \times R$，其中 $U = \{u_1, u_2, \cdots, u_i\}$，表示系统中的不同用户集合；$R = \{r_1, r_2, \cdots, r_i\}$ 表示系统中相应用户角色的集合；UR 表示系统不同用户与角色的集合。

4) ER (环境角色集合)：$ER \subseteq E \times R$，其中 $E = \{e_1, e_2, \cdots, e_i\}$ 表示系统中不同环境属性实体集合；$R = \{r_1, r_2, \cdots, r_i\}$ 表示系统中相应用户角色的集合；ER 表示分配给相应环境属性实体的角色集合。

5) EC (环境条件集合)：$EC \subseteq E \times C \times 2^{ER}$，其中 $E = \{e_1, e_2, \cdots, e_i\}$ 表示系统中不同环境属性实体集合，$C = \{c_1, c_2, \cdots, c_i\}$ 表示系统中的不同环境条件的集合；EC 表示当给定的环境角色被激活时，满足相应环境属性实体的环境条件的集合。

6) PR (环境许可集合)：$PR \subseteq P \times R \times 2^{ER}$，其中 $P = \{p_1, p_2, \cdots, p_i\}$ 表示系统不同权限的集合；$R = \{r_1, r_2, \cdots, r_i\}$ 表示系统中不同角色的集合；PR 表示当给定的环境角色被激活时，分配给相应用户的角色权限许可集合。

7) 根据定义 2)~6)环境属性实体对不同角色的访问权限的度量因子为 β，其中 $\beta = f(R, E, EC, PR)$，$\beta \in [0,1]$ 表示赋予角色集合 R 的不同环境实体集合 E，随着环境条件 EC 集合的改变，对应用户权限集合 PR 也会随之改变。

8) 系统对不同的角色与不同的环境条件之间的约束条件设为 RS：其中 $PR \subseteq RS$。

9) 同当前环境实体相关的所有系统资源集合设为 $S = \{s_1, s_2, \cdots, s_i\}$，其中资源集合的可信度由系统提供的可信度量函数 F 来确定。

10) 根据据定义(9)每个同当前环境条件相关的系统资源集合元素 $\{s_i\} \in S$ 在启动之前都必须经过可信度量，根据获得的度量函数的返回值来确定该资源的可信度，得到的可信度量值 $T = F(E, S_i)$，如果 T 大于等于预设阈值 t，则表示当前资源可以访问。

11) 域 $D_i = (U', R')$：其中 $R' \subseteq R$，$U' \subseteq U$，其中 $i \leqslant n$，表示在第 i 个域，将 $i \leqslant n$ 内的用户 U 同角色 R 之间分组映射关系。

12) 权限互斥：对于任意两个访问权限集合 P_1 和 P_2，如果有任何用户都不可能同时拥有它们，则称访问权限集合 P_1 和 P_2 互斥，记为 $Conflict(P_1, P_2) \in PR$。

13) 角色互斥：对任意两个角色集合 R_1 和 R_2，若授予 R_1 的某一访问权限与授予 R_2 的某一访问权限互斥，则称角色 R_1 和 R_2 互斥，记为 $Conflict\left(R_1, R_2\right) \in UR$。

2.2 ERBAC 模型的核心控制

2.2.1 满足环境条件的资源可信度量

根据可信计算的完整性度量定义可知：对于用户即将要获得控制权的实体，都需要预先通过完整性度量机制对其度量。因此由定义 10)知用户访问系统的资源之前需要对其进行可信度量，目的是确保系统各种环境实体(诸如：与进程相关的系统资源)的完整性没有受到破坏，只有通过完整性度量的环境实体才是可以启动的。

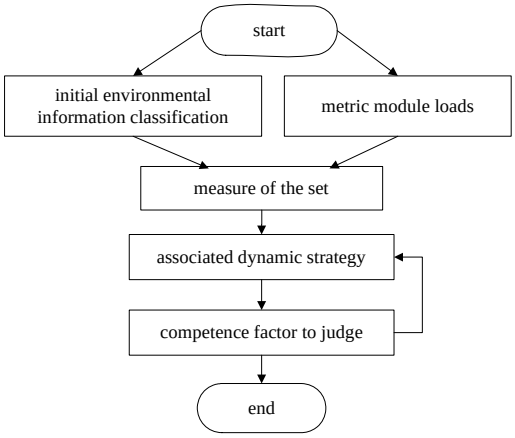

Fig.2 Environment role-based access trust measurement model
图 2 基于环境的可信度量模型

2.2.2 域间动态角色的映射

在 ERBAC 模型中，由定义 5)~6)知道环境实体是作为权限分配给用户角色的，而在角色的分配上根据定义 11),又以域的形式对角色进行管理。因此当用户进入 $D_i\left(i \in \left[0, \cdots, n\right]\right)$ 域时，根据预先设置的条件让不同的用户同不同角色映射。这种以域的形式对用户、角色和权限进行管理的方式减小了系统管理员维护的复杂度。

2.2.3 最小化风险原则

根据定义 7)~9)可知环境实体完全依赖于用户所访问资源的完整性。因此对用户而言，即使系统资源与资源相关的环境条件受到修改，也能将风险限制在一个范围内。

2.2.4 映射的约束

为避免角色与权限相冲突的情况，在进行角色映射时，应该考虑权限互斥与角色互斥的约束问题，建立角色映射时，必须检验定义 12),13)关系式是否成立。

2.2.5 基于可信的度量模型

如图 2 所示，在整个系统中为了对网络环境中的敏感资源进行保护，同时考虑到网络系统环境的变化，需要对网络系统的环境初始信息进行分类和可信度量。对于不同环境实体的度量结果，并结合预先设置访问相应资源的约束条件和策略，通过访问权限度量函数因子来对当前资源的角色–权限进行判断。

3　ERBAC 模型的具体应用和实施流程

如果将该模型的动态环境部分视为应用程序的进程集，则可以实现一个基于通用网络系统的增强安全平台。该平台分为应用层和内核层两部分，其中访问策略定义属于应用层，ERBAC 拦截模块属于内核层，用过滤驱动程序实现。

3.1 应用层

如图 3 所示，在应用层主要实现用户域的管理、用户角色的分配、用户域进程集权限分配。进程集权限分配分为 2 个步骤：一个是用户权限的分配，另一个是进程集权限的分配，其中用户权限的分配采用通用 RBAC 模型分配方案，进程集权限分配采用两级分配方式，一部分由系统管理员设置或采用默认设置，另一部分根据用户访问资源的环境的动态变化来控制，其具体控制方法在内核层实现。

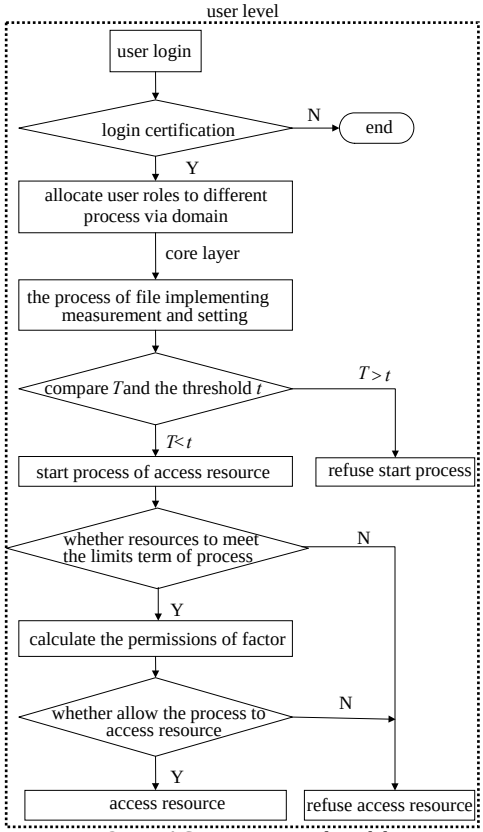

Fig.3 ERBAC process control model
图 3 ERBAC 模型的进程控制流程

3.2 内核层

ERBAC 模型的大部分操作都集中在操作系统内核层，模型通过以下步骤实现对进程集权限的控制：首先由可信度量函数模块实现对进程启动的相关资源可信度量；判断可信度量值是否满足阈值条件，如果用户访问的网络环境遭到恶意修改，则拒绝本次用户操作，并终止进程；然后再对用户访问资源的相应进程权限和约束条件进行判断，并根据度量函数计算权限度量因子；最后根据预置规则判断用户是否具有对特定资源的访问权限。其进程具体控制流程如图 3 所示。

4 结论

本文提出的基于网络环境安全的角色访问控制模型(ERBAC 模型)，将传统 RBAC 模型中的角色与一定的环境安全性策略相关联，将用户访问网络环境的安全性纳入到 ERBAC 权限分配的策略中来，并给出了 ERBAC 模型的实现方案。但是系统的安全性是相对的，因此，对安全模型的研究和建模还有待进一步的深入，而具体方案的技术实现，也有待进一步研究和完善。

参考文献：

[1] 董理君,余胜生,杜敏,等. 一种基于环境安全的角色访问控制模型研究[J]. 计算机科学, 2009,36(1):51-54.
[2] Sandhu R S,Coyne E J,Feinstein H,et a1. Role-based access control models[J]. IEEE Computer, 1996,29(2):38-47.
[3] 宋振. 基于角色和任务的权限管理扩展模型研究及应用[D]. 湖南:长沙理工大学, 2008.
[4] 方钰. 基于角色的系统访问控制模型研究与设计[D]. 安徽:合肥工业大学, 2009.
[5] 刘伟,刘嘉勇. 一种基于扩展角色的访问控制模型和方法[J]. 信息与电子工程, 2009,7(1):76-79.
[6] Covington M J,Long W,Srinivasan S,et al. Securing context-aware applications using environment role[C]// College of Computing Georgia Institute of Technology Atlanta, Georgia USA:[s.n], 2000:10-20.
[7] Miao Liu,He-Qing Guo,Jin-Dian Su. An attribute and role based access control model for Web services[C]// Machine Learning and Cybernetics, Proceedings of 2005 International Conference, Guangzhou:[s.n], 2005:1302-1306.
[8] Sadnghi A Selhorst M Stuble C. TCG TPM Main Specification[Z]. Version 1.2 Revision 94,Part1,Design Principles, 2006.
[9] Sadnghi A Selhorst M Stuble C. TCG TPM Main Specification[Z]. Version 1.2 Revision 94,Part2,TPM Structures, 2006.

作者简介：

陈虹志(1984-)，男，四川巴中人，在读硕士研究生，主要研究方向为网络系统与信息安全.email:chhzh88@sina.com.

周安民(1963-)，男，成都市人，教授，主要研究方向为网络系统与信息安全.

邓 赟(1983-)，男，成都市人，助理工程师，主要研究方向为信息安全.