一种可信度动态调节的 RBAC 策略模型①

胡细玲 王国军 邓月明 (中南大学 计算机科学与技术系 湖南 长沙 410083)

摘 要: 在基于角色的访问控制（RBAC）策略中，用户的身份识别口令可能会因为意外泄露或者他人盗取而使数据信息不安全，因此需对访问过程中的用户行为实施控制。提出了一种可信度动态调节的 RBAC 策略模型。该模型将可信计算技术与访问控制策略有机地结合，采用层次分析法对系统可信度进行评估；通过引入动态调节可信度，将用户的可信度作为系统在进行用户角色指派时的依据。实验将此模型应用于数据库环境中仿真，结果表明，该策略模型通过实施层层可信的访问控制，最终有效地提高了数据库访问的安全性。

关键词: 访问控制; 动态; 可信度; RBAC; 可信计算

RBAC Model on Dynamically Adjustable Trust Degree

HU Xi-Ling, WANG Guo-Jun, DENG Yue-Ming

(Department of Computer Science and Technology, Central South University, Changsha 410083, China)

Abstract: The disclosure of user identification password can endanger information data in a role-based access control (RBAC) policy. In order to achieve access control action for the users, a RBAC policy on dynamically adjustable trust degree is proposed. The policy combines a trusted computing theory with access control policy. Firstly, an analytical hierarchy process is adopted to evaluate the trust degree of the system. Then, a dynamical regulation method of a trust degree is introduced to make the user's trust degree a foundation of the system while assigning user's roles. This model is applied to a virtual database experiment. The result shows that through the implementation of the trusted access control, it is possible to effectively improve the security of database.

Keywords: access control; trust degree; RBAC; trusted computing

1 引言

随着人们对计算机安全信息系统的依赖性不断增强，安全信息系统的可信性研究变得越来越重要。访问控制(Access Control)[1]是安全信息系统重要的安全保障，它是指实施允许被授权的主体对某些客体的访问，同时拒绝向非授权的主体提供服务的策略。简单的说，访问控制就是在操作系统、数据库、网络以及各应用系统层面，确定各类资源(客体)是否允许访问，允许谁来进行访问，允许进行什么类型的访问。

可信计算定义为“系统提供可信赖的计算服务的能力，而这种可信赖性是可以验证的[2]，也就是说，可信计算为我们提供了可靠安全的计算环境。但是要验证系统是可信的，是件很困难的事，因为通常除非有足够的证据证明系统是可信的，否则就可认为系统是不可信的。

由于现有的访问控制策略缺乏足够的安全，本文提出了一种可信度动态调节的 RBAC 策略模型。该策略的基本思想是将可信计算和访问控制策略结合，在实施访问控制策略之前，首先采用层次分析法对系统可信度进行评估，以验证系统是否可信；然后以系统

① 基金项目:国家自然科学基金(90718034,60773013)
收稿时间:2009-12-20;收到修改稿时间:2010-03-14

的可信度作为依据，分配用户的初始可信度，以使得 RBAC 在此初始化可信度基础上进行权限的分配；最后进行可信度的动态调节，以保证了用户应用环境的安全可信。因此在此安全环境上动态调节可信度，使得用户可信度的值每次登陆是都是动态变化的，这样非法用户即使窃取了本次合法登陆用户和可信度值，仍然没有办法执行系统操作，从而有效保证了数据库的安全访问，这也是本文所提出算法的最大目的。

本文第 2 部分首先介绍了访问控制策略的相关工作；第 3 部分给出了采用层次分析法度量数据库系统可信度的方法；第 4 部分在此基础上，提出了一种可信度动态调节的 RBAC 策略模型；第 5 部分对提出的动态调节可信度的 RBAC 策略进行仿真与性能分析；最后对本文进行了总结，并给出了下一步要研究工作。

2　相关工作

关于访问控制策略，文献[3]在标准 RBAC 模型的基础上对其进行增强和扩展，通过将信任管理的思想和方法嵌入基于角色的访问控制理论，使用户的权限获取与用户的可信度关联起来，构造一个基于用户可信度的细粒度访问控制(TBFAC)框架；文献[4-6]提到了基于角色的访问控制策略应用于网络、工作流平台、可信的点对点计算环境；文献[7]提出一种可扩展的 RBAC 模型，主要是针对在拥有多个 RBAC 应用系统的企业中，解决系统管理困难的问题；文献[8]提出扩展 RBAC 模型,该模型细化了客体集、操作集，提出了组别的概念，并对权限进行三维约束，实现了面向应用的 RBAC 体系结构，增强了系统的安全性和易维护性,适用于企业信息化建设。可见，RBAC 模型应用场景广泛，确实是一种值得大家关注并研究的访问控制策略。

3　可信度的评估

在动态调节可信度的 RBAC 策略中，可信度评估方法是基础，它将直接或间接影响访问控制的效果，本文采用层次分析法对系统进行可信度的计算评估。

层次分析法（Analytic Hierarchy Process，简称 AHP）是对一些较为复杂、较为模糊的问题作出决策的简易方法，它特别适用于那些难于完全定量分析的问题。它是美国运筹学家 T.L.Saaty 教授于 70 年代初期提出的一种简便、灵活而又实用的多准则决策方法。

人们在进行社会的、经济的以及科学管理领域问题的系统分析中，面临的常常是一个由相互关联、相互制约的众多因素构成的复杂而往往缺少定量数据的系统。层次分析法为这类问题的决策和排序提供了一种新的、简洁而实用的建模方法，其通常采用下面三个步骤进行：

(i) 建立层次结构模型；

(ii) 构造判断矩阵；

(iii) 一致性检验；

3.1 可信度的层次结构模型

我们主要从平台、系统和安全组件三个方面来分析系统可信度，建立可信度的层次结构模型。下面首先给出相关的定义。

定义 1．可信度就是表示对一个事物为真的相信程度，用 T 表示，取值在 0 到 1 之间。

定义 2．证明向量就是可信报告中每个模块或数据文件的相关信息，通常包括文件名、版本、可信度量值，用 AV 表示。

定义 3．“指纹”数据集 FP 是以规范的格式存储的代码和数据文件的“指纹” 的数据库文件，在数据库中预先为相关的代码和配置文件采用 SHA-1 算法（安全哈希算法）生成其“指纹”。

SHA-1 主要适用于数字签名标准里面定义的数字签名算法。对于长度小于 2^64 位的消息，SHA-1 会产生一个 160 位的消息摘要。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，那么这时候就会产生不同的消息摘要。SHA-1 有如下特性：不可以从消息摘要中复原信息；两个不同的消息不会产生同样的消息摘要。

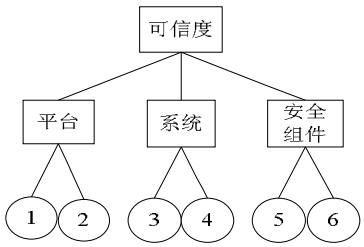

图 1　可信度的层次结构模型图

在可信度的层次结构模型图中，平台是指 TCG 定义的可信平台，它的影响因素有：①BIOS 启动模块②

加载操作系统的引导程序。

系统是指操作系统，它的影响因素有：③操作系统内核④初始进程。

安全组件是指专门增强系统安全的程序，它的影响因素有：⑤检测工具⑥火墙模块。

定义 4. 可信集是从“用户特征”数据集中根据每个模块的更新以及版本信息，选择可以接受的安全漏洞较少的模块“用户特征”组成的集合，用 TS 表示。

定义5. $av \in AV$ ， $fp \in TS$ ， $L=\{0,1\}$ $t: AV \times FP \to L$ 。

$$T(av, fp)=\begin{cases}0 & if \quad Ver(av)<Ver(fp)\\ 1 & if \quad Ver(av)>Ver(fp)\end{cases} \tag{1}$$

称 T 为可信度判定函数，其中函数 Ver()判断模块版本等更新信息。

因此，如果某个待证明系统的可信报告包含 N 个证明向量，其中属于平台、系统和安全组件类型的数量分别为 N_1，N_2，N_3。根据可信度判定函数判断每个类型中的因素与可信集匹配的分别为 M_1，M_2，M_3，则每种类型的可信度分别为 M_1/N_1，M_2/N_2，M_3/N_3。

3.2 构造可信度的判断矩阵

记判断矩阵为 $P=(P_1,P_2,...,P_n)=(b_{ij})$ 。

P：表示某指标（可信度、平台、系统、安全组件）；

b_{ij}：表示指标 P_i 与 P_j 相对重要性的比较结果值，其取值为离散的，通常为 1~9 及其倒数。下表列出了 1~9 标度的含义：

表 1 可信度量表

标度	含义
1	表示两个因素相比，对可信度所带来的影响相同
3	表示两个风险因素相比，一个因素对可信度比另一个因素所带来的影响稍大
5	表示两个风险因素相比，一个因素对可信度比另一个因素所带来的影响大
7	表示两个风险因素相比，一个因素对可信度比另一个因素所带来的影响更大
9	表示两个风险因素相比，一个因素对可信度比另一个因素所带来的影响极大
2，4，6，8	上述两相邻判断的中值
倒数	因素 i 与 j 比较得判断 c_{ij}，则因素 j 与 i 比较的判断 $c_{ji}=1/c_{ij}$

现根据可信度量表，通过平台、系统、安全组件要素来评估可信度而建立可信度的判断矩阵如下：

$$P=\begin{bmatrix}b_{11} & b_{12} & b_{13}\\ b_{21} & b_{22} & b_{23}\\ b_{31} & b_{32} & b_{33}\end{bmatrix}=\begin{bmatrix}1 & 4 & 8\\ 1/4 & 1 & 5\\ 1/8 & 1/5 & 1\end{bmatrix} \tag{2}$$

①计算判断矩阵(3*3)各要素的权重，先计算矩阵各行元素乘积的 3 次根 W_j。

②对 $W_j=(W_1，W_2，W_3)$做归一化处理，即 $W_1=W_1/(\sum W_i)$，则 $W=(W_1，W_2，W_3)$即为所求特征向量。

③计算判断矩阵的最大特征值 λ_{max}；

根据以上步骤计算出判断矩阵的特征向量为：

$$W=(W_1,W_2,W_3)=(0.6986,0.237,0,064)$$

该特征向量即为平台、系统和安全组件这三个方面在系统可信度中所占的比重，即为其权重向量。

3.3 一致性检验

以上特征向量是否就是合理的权重分配，还要对判断矩阵进行一致性检验。一致性检验公式为：

$$CR=CI/RI=(l_{\max}-n)/(n-1)/RI$$

现将 $n=3,\lambda_{max}=3.0940$，RI=0.58 代入，得 CR=0.0810<0.1，表明判断矩阵 P 具有满意的一致性。

接下来，可信度 T 可以由下面公式计算：

$$T(AV)=0.6986*\frac{M_1}{N_1}+0.237*\frac{M_2}{N_2}+0.0643*\frac{M_3}{N_3} \tag{3}$$

如果计算出系统的可信度低于 0.5，将视为不可信系统。系统的可信度值和用户初始可信度值密切相关。

4 可信度动态调节的RBAC策略

由于只有系统可信度值为[0.5,1]，才被认为是可信的，并且为了使初次登陆系统的用户拥有基本的权限并避免一开始就有高权限的出现，我们采用将用层次分析法分析出系统的可信度值的 20%作为用户初始可信度值，也就是使一般用户的初始可信度值在[0.1,0.2]之间。可信度低的用户指派一般角色获取基本权限，只有可信度高的用户才能被指派重要的角色；同时，在访问过程中，根据用户在系统中申请并完成任务的情况对用户可信度动态调节，只有当可信度满足要求时，才能最终获得访问权。

一般的访问控制模型包括主体、客体、策略执行点和策略决策点，其中主体是主动的访问者，客体是一些被动的资源，策略执行点分离主体和客体的直接联系，当主体试图访问客体时，策略执行点将咨询策略决策点，获得访问控制策略，策略决策点则以访问控制策略的形式说明哪些主体以何种方式访问哪些客体。传统的 RBAC 模型[9]从控制主体的角度出发，通过给用户分配合适的角色，一旦用户与访问权限相联系，角色成为访问控制中访问主体和受控对象之间的一座桥梁。而我们关注的是用户和角色的关联，为确保用户可信性，我们在用户和角色之间引入了可信度，并且在 RBAC 模型中考虑角色的动态调整问题。

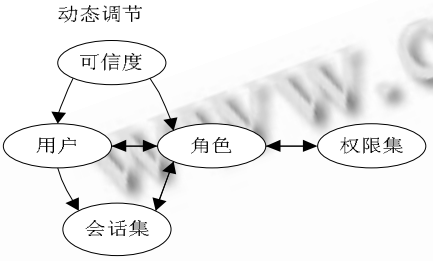

图 2　可信度动态调节的 RBAC 模型

基于传统的 RBAC 模型我们设计出了一种可信度动态调节的 RBAC 模型，具体实现方法如下：

步骤 1.用户输入 ID 和可信度值，策略执行点提交访问请求。

步骤 2.策略执行点向策略决策点提出决策请求。

步骤 3.策略决策点根据可信度向角色服务器发送分配请求。

步骤 4.角色服务器从其数据库中获得角色分配。

步骤 5.角色服务器角色分配给策略决策点。

步骤 6.策略决策点根据可信度和分配的角色向权限分配提出申请，获取角色的使用权限。

步骤 7.策略决策点对比该权限与用户申请的权限是否相同，如果相同则允许此次的访问请求；如果小于用户的请求权限，则拒绝这次的访问请求，把决策结果发送给策略执行点。

步骤 8.策略执行点执行策略决策点的决定，如果允许访问，激活该用户的角色，访问数据库；如果拒绝访问，则向用户返回拒绝信息，退出。

步骤 9.访问之后，审计数据库更新可信度值并将结果通过邮件的方式反馈给用户。

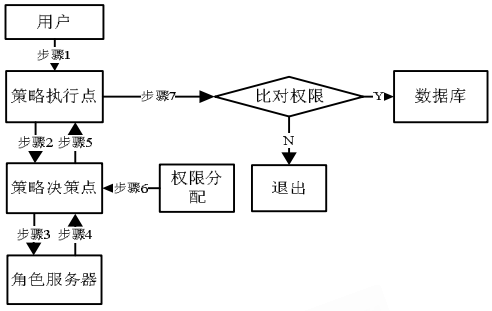

图 3　访问控制策略

根据上述方法，这里基于数据库环境的场景进行实现。首先是用户的认证，用户用 ID 和可信度登录进行认证时，输入的 ID 和可信度并不显示在屏幕上，而只是以某种符号代替，如“*”号，系统根据用户的输入鉴别此用户是否为合法用户。用户先在审计数据库中标识自己，提供相应的口令表。如果与用户输入的相同，则证明此用户为合法用户，并根据该用户拥有的可信度值为用户分配角色，否则，系统认为此用户根本不是合法用户，拒绝进入数据库系统。当用户连续执行认证过程，超过系统管理员指定的次数而认证仍然失败时，系统关闭登录会话。

其次是角色的授权，该方法通过对用户给以不同的可信度分配来确定这些用户的角色，再对用户给以不同的角色配置来确定这些角色的访问权限。本文设计将所有用户角色分为数据库管理员、超级用户、中级用户、初级用户、普通用户。下表 2 为数据库中角色定义授权表。

表 2　角色定义授权表

用户角色	可信度值	数据对象	访问权限
数据库管理员	0.90-1.00	所有数据对象	ALL
超级用户	0.80-0.89	数据库本身、库表、记录、字段和数据元素	READ, WRITE, UPDATE, APPEND, DELETE, CREATE
中级用户	0.60-0.79	库表、记录、字段和数据元素	READ, WRITE, UPDATE, APPEND
初级用户	0.30-0.59	记录、字段和数据元素	READ, WRITE, UPDATE
普通用户	0.10-0.29	数据元素	READ

再次是用户可信度值的更新，为了实现用户可信度值的更新，现假设某用户 U 在申请担任角色 R 并完成了任务 T，则 TF=1，否则 TF= -1。

由于用户的可信度值大于 0.6 后，用户所具有的权限就越高并且能完成任务的能力也越强，所以设置用户可信度值的阈值为 0.6，当用户的可信度超过这个阈值时，用户登录数据库，只用身份 ID 认证，无需输入可信计算值，否则用户必须拥有身份和可信度值进行认证；在会话时要定期使用可信度值认证。

故用户的当前可信度 td(U)可通过以下公式计算得出：

当 TF=-1 时，则

$$td(U)=(td)-t*k/5 \quad 0<(td)<1;$$

当 TF=1 时，则

$$td(U)=\begin{cases}(td)+1/25*t*k & 0.1<(td)<0.6\\(td)+1/10*t*k & 0.6<=(td)<1.0\end{cases}$$

其中，td 为用户的上一次处理任务后的可信度；t 为每次用户登录系统执行的任务次数；k 为实施不同访问权限功能时的可信系数，其取值范围如表 3 所示。

表 3　访问权限可信系数

访问权限	READ	WRITE	UPDATE	APPEND	DELETE	CREATE
k	0.05	0.08	0.11	0.14	0.18	0.2

5　用户可信度值的仿真

本文是对数据库系统进行访问控制的仿真，以验证所提出的一种可信度动态调节的 RBAC 策略模型的有效性和安全性。

不同的可信度初始值对用户申请并完成任务的影响。

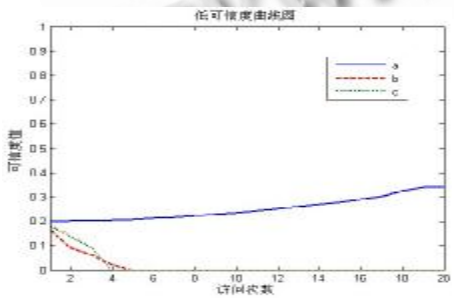

图 4　低可信度曲线图

如图 4 中 a 所示，用户的初始可信度值很低时，在用户权限范围内，每次的权限都能成功申请并完成相应的任务达二十次以上，用户的可信度值增长缓慢；b 和 c 所示一旦权限申请未成功或没有完成任务达三到四次，可信度值将下降为零，直接被系统删除。

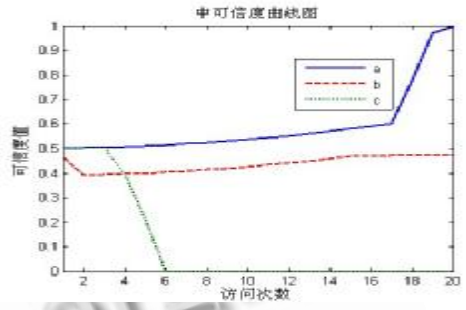

图 5　中可信度曲线图

如图 5 中 a 所示，用户的初始可信度值中等时，在用户权限范围内，申请权限并完成任务十五次以上时，用户能成为高可信度者；b 所示在此过程中允许一两次的失败而成为低可信用户，那么变化过程将如图 5-1；c 所示如果长期申请用户权限外的权限或者未完成任务次数达三到四次，可信度值下降很多，成为低可信用户甚至成为不可信用户。

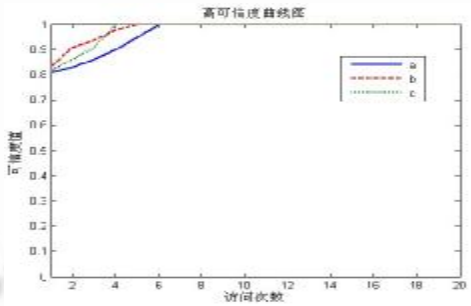

图 6　高可信度曲线图

如图 6 中 a、b、c 所示，用户的初始可信度很高时，无论是要申请高权限或是低权限，用户成功完成任务的概率都是很高的，用户的可信度值的增长也是很快的。

总之，具有高可信度值的用户，完成任务能力更强，获得更高可信度值。否则，反之。同时，在访问过程中，根据用户在系统中以往完成任务的情况对用户可信度动态调节，使用户权限在安全属性范围内动态变化，只有当可信度满足要求时，才能最终获得访问权。用户的可信度具有随机性、动态性，并与用户可信度初始值和完成任务情况密切相关。

因此，一种动态调节可信度的 RBAC 把可信度的动态变化引入了模型中，使得信任评估更符合现实情况，具有更好的适用性。而普通情况下的 RBAC 的可信度计算忽略了信息的动态性，在实际中不能很好的发现并抑制虚假实体或者实体的欺骗行为。由于用户的可信度是动态的，每次访问过后可信度值都是更新的，获得不同的角色，拥有不同的权限，使得该模型对用户的授权具有灵活性。由于该模型的特点使得主体授权者能获取相应的客体信息，未授权者无法获取那些客体信息，从而达到保密性和完整性保护的安全目标。将 RBAC 策略与动态调节相结合，检测并阻止信息的泄露的行为的发生，从而提供了更为完善的保护，有效的提高了数据库的安全性。

6 结语

本文利用可信计算与访问控制策略结合的思想提出了可信计算中的动态调节可信度的 RBAC 策略，该策略有效地实现了用户数据的安全，即使非法用户进入了系统获得管理员身份也不能获得管理员的权限。在整个过程中，根据用户在系统中申请并完成任务的情况对用户进行可信度动态调节，提高了系统安全性。仿真分析说明，此模型实现了有高可信度值的用户授予较高权限，可信度值具有无法预测性，使非法用户无法获得，从而有效地提高了用户数据的安全性。

下一步的工作主要是将可信计算中的动态调节可信度的 RBAC 策略与可信计算平台关联进行更深入的分析，以进一步地从应用层、系统层、数据层分别共同提高数据库的安全。

参考文献

1 Lou H. Viterbi decoder design for the IS-95 CDMA forward link. Proceedings of IEEE 46th Vehicular Technology Conference, 1996,2(1):1346－1350.

2 Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 2004,1(1):11－33.

3 刘宏月,阎军智,马建峰. 基于可信度的细粒度 RBAC 访问控制模型框架.通信学报,2009,30(10A):51－57.

4 Park JS, Sandhu R, Ahn GJ. Role-based access control on the web. ACM Transactions on Information and System Security, 2001,4(1):37－71.

5 Kandala S, Sandhu R. Secure role-based workflow models. Norwell,MA:Kluwer, 2002:45－58.

6 Park JS, An G, Chandra D. Trusted P2P computing environments with role-based access control. Information Security, IET, 2007,1(1):27－35.

7 谭振,杨贯中,曾熠.一种扩展的 RBAC 模型-ERBAC. 计算机系统应用, 2009,18(11):84－87.

8 于小兵,郭顺生,杨明忠. 扩展 RBAC 模型及其在 ERP 系统中的应用. 计算机工程, 2009,35(24):165－167.

9 Ferraiolo D, Sandhu R, Gavrila S, Kuhn D, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 2001,4(3):224－274.