基于 RBAC 和信任管理的访问控制①

石东贤，李迎辉

(浙江经贸职业技术学院，杭州 310023)

摘 要：针对分布式环境下的访问控制问题，本文结合 RBAC 和信任管理的思想，提出了具有 RBAC 的 Keynote 访问控制策略和信任状；然后设计并实现了应用系统的通用访问控制平台；最后通过模拟开发应用系统验证了该平台在访问控制方面的安全性和有效性。

关键词：RBAC；信任管理；Keynote；访问控制平台

Access Control Based on RBAC and Trust Management

SHI Dong-Xian, LI Ying-Hui

(Zhejiang Economic & Trade Polytechnicy, Hangzhou 310023, China)

Abstract：To address the access control problems in the distributed environment, this paper proposes a kind of RBAC Keynote access control strategy and credential based on RBAC and trust management; then we design and implement a general access control platform of application systems. Finally, verifies the platform's securities and effectiveness on access control through simulation and development of application system.

Key words：RBAC; trust management; keynote; access control platform

1 引言

传统的访问控制策略都集中于一个封闭式环境下的信息保护，特别是服务器内部数据对象的访问控制。控制的执行是基于给定的授权规则和对已知用户或进程的身份和属性的鉴别之上。传统的访问控制是认证和授权的结合，接收请求的系统首先要决定签署这个请求的人是谁，然后查询一个本地数据库，根据查询结果来决定请求者是否允许访问请求的资源。这种方法对于当今动态的、分布式网络环境已经不适合[1,2]。

在一个大规模的动态的异构的分布式系统中，系统的授权者无法直接知道用户，因此他必须使用由熟知该用户的第三方所提供的某类信息。这种信任和委托关系使得分布式信任不同于传统的访问控制。M. Blaze 在文献中[6]提出的“信任管理”方法正是为了解决上述问题而提出的一种独立于应用的，更适合在分布式网络中使用的访问控制体系。

本文通过对信任管理机制的分析、研究，特别是由 M. Blaze 等人共同提出来的 Keynote 信任管理访问控制模型，更好地授权用户的操作，认证用户的权限，和匹对用户的动作。本文结合信任管理的思想，利用 Keynote 信任管理引擎和 RBAC 访问控制模型，设计和实现了 RBACKeyNote 访问控制平台，对用户访问控制和资源使用授权进行统一管理，并提供了基于 RBAC 和信任管理的应用系统访问控制软件包，系统具有实用性和通用性，既实现了分布式环境下的授权问题，也实现了安全策略的一致性管理。

2 基于RBAC和信任管理的访问控制策略

2.1 RBAC 概述

RBAC（基于角色的访问控制) 是 20 世纪 90 年代以来最受瞩目的一种访问控制技术[3,4]。它引入角色的概念，通过角色定义分配主体对客体的访问权限, 用户根据其职能和责任被赋予相应的角色。采用 RBAC 最大的好处在于将用户和他具有的权限分离开来，管

① 收稿时间:2011-09-05;收到修改稿时间:2012-02-24

理员可以将用户的授权和权限的划分进行分别处理，将权限授予角色，给用户授予角色来完成授权的操作。图 1 描述了 RBAC0 模型[5]。

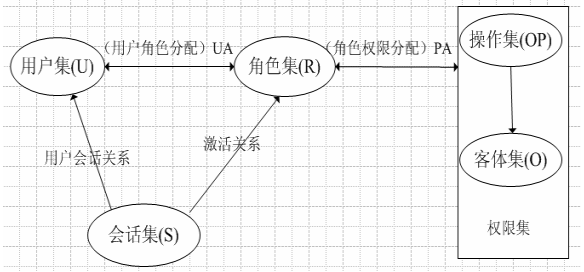


图 1　RBAC0 模型

2.2 信任管理概述

信任管理的概念，最早由 M. Blaze 等人于 1996 年第一次提出[6]，他们将信任管理定义为采用一种统一的方法描述和解释安全策略（Security Policy）、安全凭证（Security Credential），以及用于直接授权关键性安全操作的信任关系（Trust Relationship）[8]。基于该定义，信任管理主要研究的内容包括制定安全策略；获取安全信任状；判断安全信任状是否满足相关的安全策略。信任管理所要回答的问题是："安全信任状集 C 是否能够证明请求 R 满足本地策略集 P"。

根据 M. Blaze 等人对信任管理定义，一个信任管理系统应该包括 5 个基本组成部分：

(1) 一种描述请求行为(action)的语言

(2) 一种识别主体(principals)的机制

(3) 一种定义应用程序策略(policy)的语言

(4) 一种定义信任证书(credentials)的语言

(5) 一个一致性检查器(compliance checker)

为了使信任管理能够独立于特定的应用，M. Blaze 等人提出了一个基于信任管理引擎（Trust Management Engine，TME）的信任管理模型，如图 2 所示。几个典型信任管理系统 Policymaker[7]、Keynote[8]和 Referee[9]均以该模型为基础进行设计并加以实现。

2.3 基于 RBAC 的 Keynote 断言的设计

尽管人们已经对信任管理进行了大量的研究，提出了很多的信任管理模型[10-12]，扩大了信息安全的研究领域，解决了分布式环境下信息安全的一些问题，但是目前大多数的研究成果还是只停留在对信任管理模型的介绍上。M. Blaze 实现的 Keynote 还是目前唯一比较成熟的，并且成功应用于某些场合的信任管理系统。因此本文结合 RBAC 和信任管理的思想，设计了基于 RBAC 和 Keynote 信任管理的断言，断言包括策略和信任状两种类型，以下将分别进行设计。

2.3.1 RBACKeyNote 策略定义

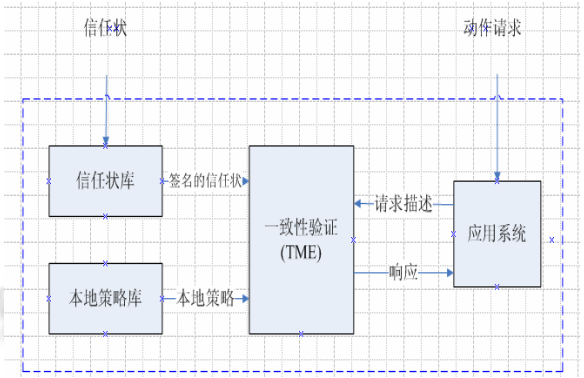


图 2　信任管理模型

结合 Keynote 系统的策略和应用系统的 RBAC 策略，定义图 3 所示结构的 RBACKeyNote 策略。该策略结构的各个字段意义已经在图中表示，其中授权者为 Policy，这个是和信任状不一样的，条件域中包含着角色权限关系，而 Licensees 和 Role 结合起来包含着角色用户关系。

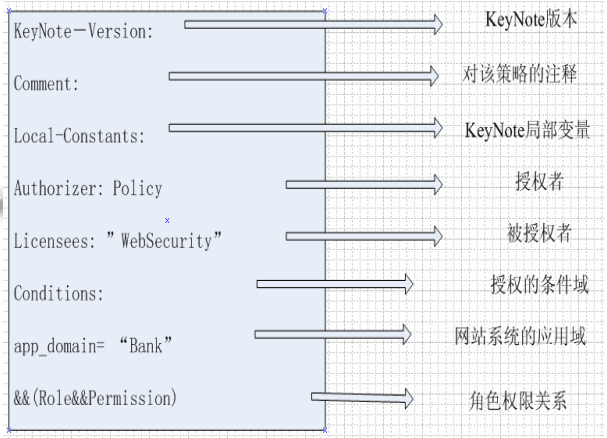


图 3　RBACKeyNote 策略结构定义

2.3.2 RBACKeyNote 信任状定义

结合 Keynote 系统的信任状和应用系统的 RBAC 策略，定义图 4 所示结构的 RBACKeyNote 信任状，该信任状结构的各个字段意义也已经在图中表示，其中授权者 WebSecurity 为 Policy 授权的用户；条件域中包含着角色权限关系；而 Licensees 和 Role 结合起

来包含着角色用户关系；Signature 是授权者的私钥，用来验证该证书的授权者身份。

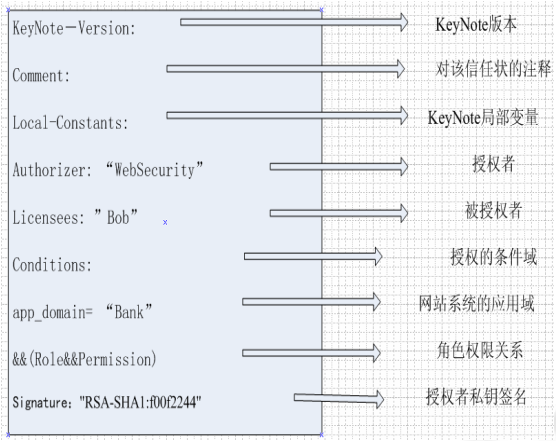


图 4 RBACKeyNote 信任状结构定义

3 RBACKeyNote访问控制平台的设计与实现

RBACKeyNote 是基于上述 RBAC 和信任管理系统设计的访问控制平台，平台采用 BS 结构。服务器包括 RBACKeyNote 访问控制服务平台和应用系统服务器，服务平台主要实现证书管理，应用系统管理（域名管理，权限管理和角色管理），日志管理，并为分布式环境下的用户提供一致性验证服务；应用系统服务器是根据访问控制服务平台提供的接口和设置的应用系统相关参数（应用系统域名，权限和角色）而开发的具体应用系统。客户端是远程用户，通过浏览器来执行应用系统的相应操作。架构图如下图 5 所示：

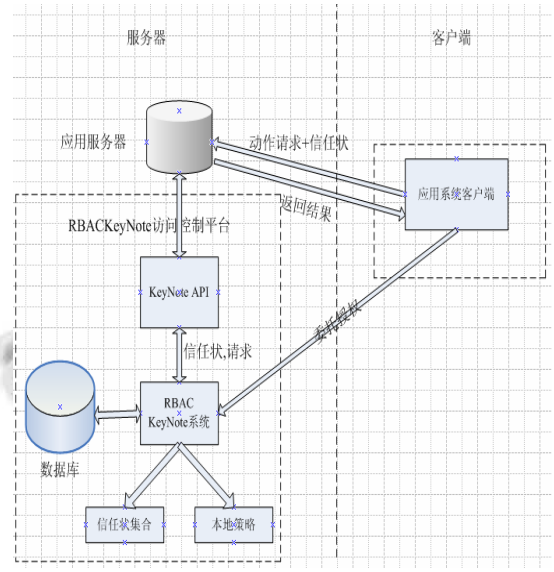


图 5 分布式环境下 RBACKeyNote 平台总体架构

3.1 RBACKeyNote 平台的设计

RBACKeyNote 访问控制服务平台主要是为应用系统的开发者提供访问控制服务，图 6 为该平台的功能结构图：

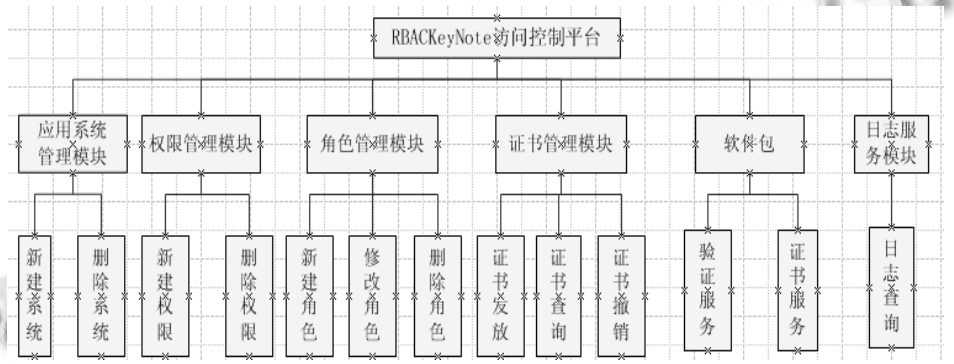


图 6 RBACKeyNote 平台功能结构图

3.1.1 域名管理模块

域名管理模块主要是完成对需要开发的应用系统的域名管理，包括新建域名和删除域名，在定义这些应用系统域名的时候建议域名具有可读性和简练。比如需要开发一个银行系统，可以定义它的域名为 bank，而不要用 web1 等等。

3.1.2 权限管理模块

权限管理模块主要是完成对需要开发的应用系统的权限管理，因此在开发一个应用系统之前必须认真考虑系统所存在的权限集合，这样就不会为后面的权限管理带来混乱，权限管理包括新建权限和删除权限，在定义这些应用系统权限的时候建议权限具有可读性

和简练。比如需要开发一个银行系统，可以定义它的权限为存款(Deposit)，取款(WithDraw)，而不要用存款(Permision1)，取款(Permision2)。

3.1.3 角色管理模块

角色管理模块主要是完成对需要开发的应用系统的角色管理，因此在开发一个应用系统之前必须认真考虑系统所存在的角色集合以及角色层次管理，这样就不会为后面的角色管理带来麻烦，角色管理包括新建角色，修改角色和删除角色，在定义这些应用系统角色的时候建议角色具有可读性和简练。比如需要开发一个银行系统可以定义它的角色为经理(Manager)，工作人员(Staff)，客户（Customer），而不要用经理(role1)，工作人员(role2)，客户（role3）。

3.1.4 证书管理模块

证书管理模块主要是完成对相关证书管理，包括发放证书，查询证书和撤销证书，其中查询证书和撤销证书只有管理员才能进行操作，查询证书指查询该证书的相关信息，包括颁发时间、用户、用户公钥、角色和权限等等，撤销证书指对某类用户的权限禁止，而发放证书可以让分布式环境下的授权用户进行证书的下放，发放证书的时候必须遵守 RBACKeynote 系统的证书结构和内容规范。

3.1.5 访问控制包

RBACKeyNote 平台提供的访问控制包主要提供验证服务、证书服务。验证服务是根据用户提交的证书、证书密码和动作来验证该用户是否有权限执行相关的操作；证书服务是为开发人员确定用户提交证书的相关信息提供查询帮助，以便他们可以根据证书信息来确定显示的内容等等。比如如果用户验证通过后查询到该证书的用户角色是经理，那么让下一页的显示是经理可以操作的页面。

3.1.6 日志管理模块

日志管理模块主要是将哪些用户什么时候在哪个应用系统上执行了哪些操作、验证结果如何等等信息记录下来，既为应用系统作数据统计分析，也为应用层的行为审计提供了数据。

3.2 RBACKeyNote 平台的实现

RBACKeyNote 平台结合 PHP 和 C 语言实现，这里主要介绍访问控制包的实现，访问控制包包括验证服务和证书服务。验证服务名称为 rbackeynote, 具体如下：

1）验证服务命令：rbackeynote，具体命令参数如下：

① certName:上传的证书名称

② certPwd:证书密码

③ action:操作动作

2）证书服务名称为 certkeynote，具体命令参数如下：

① certName:上传的证书名称

② certPwd:证书密码

③ pubKey:证书的公钥

验证关键代码如下：

```
if($upload){//如果上传成功，则利用我们提供的验证服务接口 $verifycom="../certkeynote".$newName."
".$password." role";
        exec($verifycom,$outva1,$retval1);
        $role = $outva1[0];
        $verifycom="../rbackeynote KeyNoteAdmin
".$newName." ".$password." Login";
        exec($verifycom,$outva,$retval);
        if($outva[0]=="true"){//验证成功
          //根据角色进入不同的界面
            if($role=="administrator"){
              $_SESSION['adminpass'] = "true";
                echo '<meta http-equiv="refresh"
content="0; url=admin.php">';
            }
                else{
                  $_SESSION['errmsg'] = "无法登录后台管理系统，请确认你的身份！.";
                  echo '<meta http-equiv="refresh"
content="0; url=../err.php">';
              }
        }else{
                  $_SESSION['errmsg'] = "无法登录后台管理系统，请确认你的证书密码或者有效期！.";
                  echo'<meta http-equiv="refresh"co-
ntent="0; url=../err.php">';
        }
    }
```

3.3 安全性验证

本文以简单的银行系统作为平台的安全性验证，

目标是根据用户的身份进行授权访问。通过上传证书来确认用户的角色，然后确定所拥有的权限。

一般银行系统的各个角色有：经理（manager），员工（staff）和客户（customer）。每个角色有不同的权限，比如经理（manager）可以拥有员工和顾客所拥有的所有权限，除此之外还有更高级的权限，如修改和删除客户。而员工拥有客户的所有权限，和更高级的权限，如添加客户。客户拥有最普通的权限如查询余额。

利用上面提供的访问控制包，银行系统软件开发人员可以将系统的访问控制模块移交给 RBACKeyNote 平台。开发人员只需在银行系统中添加验证服务和证书服务即可，关键代码（php 语言）如下：

```
$verifycom = "rbackeynote bank ".$newName." ".$password." Login";
exec($verifycom,$outva,$retval); //证书验证服务接口
    if($outva[0]=="true"){//验证成功，登录
      //根据角色进入不同的界面
        $verifycom="certkeynote".$newName.""."$password." role";
        exec($verifycom,$outva1,$retval1);
      $role = $outva1[0];
      //判断是否 manager 角色
      if ($role=="manager")
        echo'<meta http-equiv="refresh" content="0; url=roles/manager.php">';
      //判断是否 staff 角色
      else if($role=="staff")
          echo'<meta http-equiv="refresh"content="0; url=roles/staff.php">';
       //判断是否 customer 角色
       else if($role=="customer")
          echo'<meta http-equiv="refresh"content="0; url=roles/customer.php">';
    }else{
    $_SESSION['msg'] = "无法登录银行系统，请确认你的证书和密码！.";
    echo '<meta http-equiv="refresh" content="0; url=message/err.php">';
    }
```

登录成功后可以进行各种功能模块的管理，如图 7 所示：

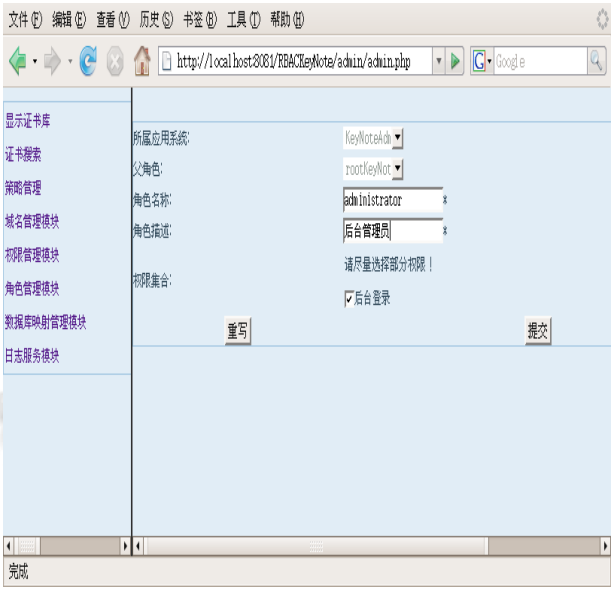


图 7 RBACKeyNote 平台管理界面

实践证明该平台具有较高的安全性，并实现了 RBAC 的访问控制和分布式授权。

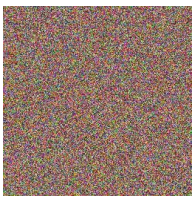
4 结语

本文根据信任管理的原理，提出了一种具有 RBAC 的 Keynote 策略方法，并设计和实现了基于 RBAC 和信任管理的 RBACKeyNote 访问控制平台，解决了分布式环境下的授权管理和策略的一致性管理。同时为应用系统的开发者提供了基于信任管理和 RBAC 的访问控制包，便于开发，减轻了开发者为设计和实现访问控制以及提高应用系统安全性的负担，这也是本文的主要创新点。

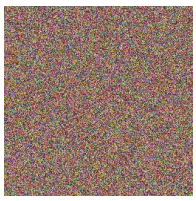
参考文献

1 甘泉.一种企业级分布式访问控制机制改进及实现[硕士学位论文].北京:中国科学院研究生院,2005.
2 郭慧.分布式网络环境中访问控制模型的设计与实现[硕士学位论文].秦皇岛:燕山大学,2006.
3 刘宏月,范九伦,马建蜂.协同环境中基于RBAC模型的访问控制策略.计算机工程,2009,35 (11):140−142.
4 黄超.基于角色的访问控制策略构建方法研究[博士学位论文].杭州:浙江大学,2010.

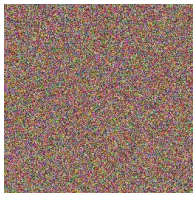
(下转第 125 页)



a. $(x_0, y_0, z_0) = (1.0000000001, 1, 1)$



b. $(x_0, y_0, z_0) = (1, 1.0000000001, 1)$



c $(x_0, y_0, z_0) = (1, 1, 1.0000000001)$

图 5 改变 Lorenz 混沌系统初始值提取的水印信息

由图 5 可见，改变系统初值中的任意一个变量，即使改变只是相差 10^{-10} 时，仍然无法解密出正确的水印图像。由此可以看出，该算法对于密匙具有很强的敏感性。

5 结语

本文提出了基于Arnold变换和Lorenz混沌系统的彩色水印图像加密算法。该算法的特点如下：

（1）水印信息是有意义的彩色水印图像，具有更广的适用范围。

（2）根据灰度水印图像的置乱度定义，提出了彩色图像的置乱度定义，并根据此置乱度定义选择了最优的 Arnold 变换置乱次数对图像进行 Arnold 变换置乱，增加了水印像素的置乱程度。

（3）算法充分利用了 Lorenz 混沌系统产生的三个混沌序列，增加了图像的抗攻击性能。

（4）算法将 Arnold 变换和 Lorenz 混沌系统结合对彩色水印图像进行置乱处理，克服了 Arnold 变换加密水印采用穷举方法就能够被破解，以及 Lorenz 混沌系统置乱度不高的缺点，置乱算法能够使彩色水印信息更具安全性。

（5）算法加密解密过程对于水印信息没有任何损失，是一种新的无损彩色水印加密算法。

参考文献

1 刘方.变换域加密图像数字水印算法研究[硕士学位论文].山东师范大学, 2009.

2 孙新德,路玲.Arnold变换在数字图像水印中的应用研究.信息技术,2006(10):129–132.

3 赵玉霞,康宝生.一种基于混沌序列的数字图像隐藏算法.西北大学学报,2008,(2):194–198.

4 A. TirkeI, GRankin. R. vail, Schyndef, W. Ho, N. Mee, C. Osbome. Elecrtonic watermark. Proc. DICTA 1993. Dec. 1993.666–672.

(上接第 29 页)

5 Sandu RS, Coyne EJ, Feinstein H L. Role based access control models. IEEE Computer, 1996,29 (2):38–47.

6 Ferraiolo DF. Proposed NIST standard for role based access Control. ACM Trans. on Information and Systems Security (TISSEC), 2001,4(3):224–274.

7 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. Dale J, Dinolt G, eds. Proc. of the Symp- osium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 164–173.

8 Blaze M, Feigenbaum J, Ioannidis J, et al. The Role of Trust Management in Distributed Systems Security. Secure Internet Programming Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999.185–210.

9 ChuY–H, Feigenbaum J, et al. REFEREE: trust management for Web Appilications.World Wide Web Journal.

10 易磊,杨长兴.一种改进的基于行为的网格信任模型.计算机系统应用, 2008,17(2):44–47.

11 Ninghui L, Mitchell JC, Winsborough WH. Design of a role–based trust-management framework. Security and Privacy, 2002. Proc. 2002 IEEE Symposium on. 2002,114–130.

12 黎梨苗,陈志刚,邓晓衡,桂劲松.基于模糊理论的主观信任综合评价模型研究.计算机应用研究, 2010,27(5):1860–1862.