第26卷 第10期 计 算 机 工 程 2000年10月
Vol.26 № 10 Computer Engineering October 2000
·博士论文· 文章编号：1000—3428(2000)10—0062—03 文献标识码：A 中图分类号：TP309

用RBAC实现DAC和MAC的一种方法

刘琼波，施 军，尤晋元
（上海交通大学计算机科学与工程系，上海 200030）

摘 要：提出一种用RBAC实现传统的DAC和MAC的方法、给出了形式化描述、并举例说明。只要灵活配置RBAC，就可实现多种安全策略。

关键词：自主访问控制；强制访问控制；访问控制列表；Bell-LaPadula模型；基于角色的访问控制模型

Implementation of DAC and MAC Using RBAC

LIU Qiongbo，SHI Jun，YOU Jinyuan
（Department of Computer Science and Engineering，Shanghai Jiaotong University，Shanghai 200030）

【Abstract】This paper proposes a way to implement traditional DAC and MAC using RBAC，gives the formal expression and some examples. RBAC can be flexibly configured to implement multiple security policies.

【Key words】DAC；MAC；ACL；Bell-LaPadula model；RBAC

美国军方于1985年提出可信计算机系统评估准则TCSEC[1]，描述了两种安全策略：自主访问控制（DAC）和强制访问控制（MAC）。DAC允许用户把他对客体的访问权授予其他用户或从其他用户那里收回他所授予的访问权，它是基于客体-用户的所属关系的访问控制。MAC是一种多级访问控制策略，它依据主体和客体的安全标识来决定主体可否访问客体。其后提出了基于角色的访问控制模型RBAC[2]，它的基本思想是在用户和客体之间插入角色(role)，将对客体的访问权限授予角色，则属于某角色的用户就可获得此角色的访问权限。对角色进行授权，而不是直接对用户进行授权。其优点在于：角色与组织结构相吻合；角色的数目比用户的数目少，适应大规模分布式应用环境；角色比用户稳定，避免了因为人员的调动而引起的授权变化；从而简化了权限的管理。同时复杂的RBAC模型可以实现各种安全策略，如责任分离，事务控制等。

R. S. Sandhu从简单到复杂提出了$RBAC_0$，$RBAC_1$，$RBAC_2$，$RBAC_3$模型[3]。其最简单的$RBAC_0$模型由以下几部分构成：

1）U，R，P和S分别表示用户集合、角色集合、权限集合和主体集合

2）$PA \subseteq P \times R$，权限和角色之间的二元关系

3）$UA \subseteq U \times R$，用户和角色之间的二元关系

4）$user : S \to U$，一个将主体映射到用户的函数

5）$roles : S \to 2^R$，一个在主体和一组角色之间建立联系的函数

$RBAC_1$加入了对角色层次关系的描述，$RBAC_2$引入了约束的概念，$RBAC_3$则是$RBAC_1$和$RBAC_2$的综合。

本文提出了用RBAC实现DAC和MAC的一种方法，只要灵活配置RBAC，就可以实现多种安全策略。

1 RBAC实现DAC

自主访问控制一般采用访问控制矩阵实现，而访问控制列表access control list (ACL）是实现访问控制矩阵的一种通用方法，对应于将访问控制矩阵按列存放，即它可以表示对于每个客体，都有哪些主体对此客体拥有哪些权限。POSIX.6和Windows NT是两个使用ACL的典型实例。在ACL中主体可以是用户或组，这里我们将之简化为ACL_g，认为主体仅指组，对组的数量和组成员的关系没有限制。

在ACL_g中管理员的主要工作是：创建组，管理组员，授予组访问客体的访问权限。而在$RBAC_0$中，管理员的主要工作是：创建角色，建立角色与用户的联系，授予角色访问客体的访问权限。可见在$RBAC_0$和ACL_g之间存在着某种对应关系，可以用$RBAC_0$来实现ACL_g。

存在ACL_g，其定义为；

1）用户的有限集，$U=\{u_i\}$ i=1,2…nu；

2）权限的有限集，$P=\{p_i\}$ i=1,2…np；

3）组的有限集，$G=\{g_i\}$ i=1,2…ng；$g_i \in 2^{U+P}$，即组员是用户或组；

4）f_{per}：$G \to 2^P$，即组的访问权限集。

从ACL_g可以构造一个$RBAC_0$模型。首先对组进行预处理，将嵌套组的用户直接归入上层组，即$(\forall g_i, g_j, u_k)(g_i \subseteq g_j, u_k \in g_i \Rightarrow u_k \in g_j)$，可以将$g_j$改写为$g_j = \{u_i \mid u_i \in g_j \bigcup_{\forall k, g_k \subseteq g_j} u_i \in g_k\}$。这是因为$RBAC_0$没有定义role之间的层次关系，若用$RBAC_1$，可将嵌套的组关系转化为role之间的层次关系。

构造$RBAC_0$主要是要定义二元关系UA和PA，其步骤如下，对任一个u_i：

1）$(\forall g_i) u_j \in g_i \Rightarrow (\exists! r_i)(u_j, r_i) \in UA$；

作者简介：刘琼波(1974～)，女，博士生，主研方向为计算机安全；施 军，博士生；尤晋元，教授，博导

收稿日期：2000-03-06

2) $(\forall g_i) f_{per}(g_i) = \{p_k\} \Rightarrow (\exists! r_i)(p_k, r_i) \in PA$;

2 RBAC实现MAC

实现MAC的访问控制模型包括Bell-LaPadula向下读、向上写的安全模型[4],Biba向下写、向上读的一致性模型[5],以及Clark-Wilson基于一组实际规则的一致性模型[6]。其中最著名的Bell-LaPadula模型实现了一种多级的强制访问控制。这里给出一个适当简化的Bell-LaPadula模型。

定义一个安全标识的偏序关系（L,≤），其中L为安全标识的有限集。如果a的安全标识小于b，则记做Sec(a) ≤ Sec(b)。

规则1：简单安全规则 仅当Sec(o) ≤ Sec(s)，主体可以读客体。

规则2：星规则 仅当Sec(s)≤Sec(o)，主体可以写客体。

用RBAC实现此模型。

1）假设在原MAC模型中的安全标识的有限集L={l_i}i=1,2…n，各安全标识之间为偏序关系。

2）对于任一个l_i，定义相对应的两个role: rl_i,wl_i。这样定义角色的集合为R={rl_i,wl_i}i=1,2…n。角色之间的层次关系分为两个不相交的哈斯图。rl_i之间的关系仍保持和l_i一样的偏序关系，而wl_i之间的关系则恰好与l_i的关系相反。即

$$(\forall l_i, l_j) l_i \le l_j \Rightarrow (\exists! wl_i, wl_j) wl_i \ge wl_j) \cap ((\exists! rl_i, rl_j) rl_i \le rl_j)$$

3）允许的操作集P={(o,re),(o,wr)|o为客体}。

4）建立用户与角色之间的关系。每个用户只可属于两个角色rl_i,wl_i。

5）主体（被激活的用户）与角色关系同4)。

6）定义操作与角色之间的二元关系为 $PA \subseteq P \times R$ ，操作与角色之间的关系应满足下面两个条件:

$$((o, r), rl_i) \in PA \Leftrightarrow ((o, w), wl_i) \in PA$$

$$(\forall rl_i, rj_j)(rl_i \le rl_j) \cap ((o, re), rl_i) \in PA \Rightarrow ((o, re), rl_j) \notin PA)$$

这是因为角色层次之间的权限继承性，使得只需低层次的角色拥有某权限，则高层次的角色自动拥有此权限。

3 例子

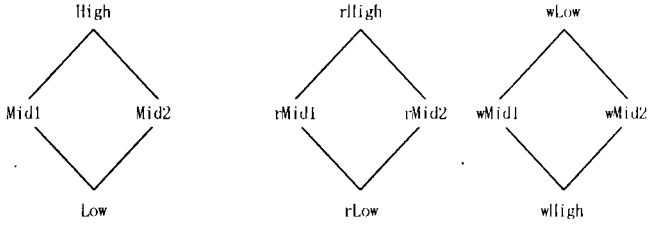
下面用两个例子来说明如何用RBAC实现DAC和MAC。

Windows NT Server 4.0是一个C2级的操作系统。当用户想要访问某个对象时，安全参考监控程序就会根据ACL的内容来决定用户是否可以访问此对象。在安全管理中一般建议用组来管理用户，因为只要设置了组的访问权限，则组中的用户就具有该访问权限；或是在添加用户时，只要将其加入组内，则该用户就具有此组所拥有的访问权限。

下面用一个简单例子说明用RBAC替代ACL。假设有两个组：出货员={张，王，销售员={李，朱，林，权限集合P={(定单,读),(定单,写),(出货单,读),(出货单,写)}，组的权限f_{per}(出货员)=定单，读)，(出货单，写)，(出货单，读)}，f_{per}(销售员)={(定单，写)，(定单，读)，(出货单，读)}。对应这个简单的ACL，构造一个RBAC$_0$。角色的集合R={出货员，销售员，二元关系UA={(张，出货员)，(王，出货员)，(李，销售员)，(朱，销售员)，(林，销售员)，二元关系PA={(定单,读),出货员)，((出货单,读),出货员)，((出货单，写)，出货员)，((定单,读),销售员)，((定单,写),销售员)，((出货单,读),销售员)。

可见在ACL和RBAC之间的对应关系是很简单的。在实践中，RBAC机制常常在一个支持ACL的系统之上实现。

B级和A级的系统实现MAC,包括Amdahl公司的UTS/MLS Version 2.1.5+、HP公司的HP-UX BLS Release 9.0.9+、Trusted Information System有限公司的Trusted XENIX 3.0等。下面用一个抽象的例子来说明如何用RBAC实现Bell-LaPadula模型。



（a）安全标识的偏序关系　　（b）角色的层次关系

图1 偏序关系

有一个系统，其安全标识集合L={High，Mid1，Mid2，Low}，所形成的偏序关系如图1(a)所示。假设系统中的用户集合U={u_1,u_2,u_3,u_4,u_5}，对象集合O={o_1,o_2,o_3,o_4}。其安全标识如表1所示。

表1 用户和对象的安全标识

u_1O_1	High
u_2O_2	Mid1
u_3O_3	Mid2
u4,u5,0_4	Low

从简化了的简单安全规则和星规则，可以得到如表2所示的访问控制列表。

表2 系统的访问控制列表

	o_1	o_2	o_3	o_4
u_1	re,wr	re	re	re
u_2	wr	re,wr		re
u_3	wr		re,wr	re
u_4,u_5	wr	wr	wr	re,wr

根据上面的转化步骤，可以得到角色的层次关系是如图1（b）所示的偏序关系。然后建立角色和用户之间的所属关系UA={(u_1,rHigh),(u_1,wHigh)，(u_2,rMid1)，(u_2,wMid1)，(u_3,rMid2)，(u_3,wMid2)，(u_4,rLow)，(u_4,wLow)，(u_5,rLow)，(u_5,wLow)}得到下面两个基于角色的访问控制列表，如表3所示。

表3 基于角色的访问控制列表

	o_1	o_2	o_3	o_4
rHigh	re	re	re	re
rMid1		re		re
rMid2			re	re
rLow				re
wHigh	wr			
wMid1	wr	wr		
wMid2	wr		wr	
wLow	wr	wr	wr	wr

将表3根据转化步骤中的第6步，即依据角色的权限的继承性，对操作和角色之间的关系进行约束，可以得到如表4所示的简化的基于角色的访问控制列表。

表4 简化的基于角色的访问控制列表

	o_1	o_2	o_3	o_4
rHigh	re			
rMid1		re		
rMid2			re	
rLow				re
wHigh	wr			
wMid1		wr		
wMid2			wr	
wLow				wr

4 结论

目前RBAC得到了相当的关注，它有望取代传统的强制访问和自主访问控制。RBAC很自然地与企业的组织结构相适应，可以简化安全管理，是一种适应于企业的安全策略模型；灵活地配置RBAC，可以实现多种安全策略。

参考文献

1 Department of Defense Computer Security Center.Trusted Computer System Evaluation Criteria. DoD 5200. 28-STD, 1985

2 Ferraiolo D, Cugini J, Kuhn R. Role Based Access Control (RBAC): Features and Motivations.In Proceedings of 11th Annual Computer Security Application Conference, New Orleans, LA,. 1995 -12:241-248

3 Sandhu S, Coyne E J, Feinstein H L, et al. Role-based Access Control Models. IEEE Computer, 1996, 29(2):38-47

4 Bell D, LaPadula L. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, 1973,1

5 Biba K. Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, the MITRE Corporation, Bedford, MA, 1975

6 Clark D, Wilson D. A Comparison of Commercial and Military Computer Security Policies. In IEEE Symposium on Security and Privacy, 1987

※※

（上接第61页）

统后，用户一般不会认为他的第一次联接受到别人的攻击。因而IP劫持具有一定的隐蔽性。

2.3 IP假冒攻击

Unix系统的许多服务（如信任主机）是利用主机的IP地址进行用户身份的识别，即用户的IP满足某种条件，用户不需要输入口令就可进入系统，使用系统的服务。ARP改向攻击就可实现IP的假冒，这样攻击者不需要输入口令就可进入系统。以用户的IP地址来进行用户身份的识别的一次性口令系统也存在着这种安全缺陷。由于交换设备使得牺牲主机不能窃听其它主机的通信，因而在交换式的以太网中，基于ARP改向的IP假冒攻击更具有隐藏性。

2.4 其它网络智能设备的安全缺陷

现在有许多智能网络互连设备，它们同时具有交换机和共享式媒体访问方式的部分特点，如网桥和智能Hub。这些设备同样存在着交换设备的安全缺陷：基于ARP改向的中间人攻击将难于察觉与检测。

2.5 基于域名系统的中间人攻击方式

基于ARP改向的中间人攻击方式的实质是改动了IP地址与MAC地址的映射关系。在Internet中，利用映射关系实现改向的中间人攻击的方式有许多种。一种危害性更大的改向的中间人攻击方法为攻击域名系统的映射关系。它将牺牲主机和域名的IP之间的通信改向到牺牲主机和攻击者的IP地址之间的通信，然后攻击者和域名IP之间进行通信，并将数据反传回牺牲主机。显然，这种攻击方法同ARP改向攻击法非常相象。

3 安全缺陷的改进措施

一种极为简单的方法是取消使用交换式以太网，但交换式以太网具有共享以太网无法比拟的优点，在实际中不可能取消它的使用。因此，更有效的方法是采用其它改进措施。

3.1 静态MAC地址方法

ARP攻击是改动了IP地址与MAC地址的映射关系。若采用静态MAC地址方法，即将IP地址与MAC地址之间的映射关系由人手工一次性输入，以后主机不再对这些映射关系进行改变（即取消MAC地址缓冲区）。显然，这种方法可以使ARP改向攻击失去作用。

但这种方法的缺点也很明显：在一个高度移动或变化的网络环境中，这种手工输入IP地址与MAC地址对应关系的方法不能适用。另外它要求主机所使用的代理程序（如操作系统）必须支持这种配置方式。

另外一种方法是取消使用ARP协议，或采用更加安全的地址解析协议等。

3.2 第3层交换方式

现在，一种基于IP地址交换的第3层交换设备已经商品化，它相当于路由器的功能，不过由于它的"路由"速度已接近于通常的交换机的速度，人们才称它们为第3层交换。在第3层交换技术中MAC地址和ARP协议已不再起作用，因而第3层交换技术可以使ARP改向攻击失去作用。这种方法的缺点是第3层交换机价格昂贵。

4 结论

一般而言，交换式以太网较共享式以太网的安全性高，而ARP改向攻击使得交换式以太网上的主机可以窃听到其它主机之间的通信。并且这种窃听其它主机之间通信的方法在交换式以太网下却极难检测。利用ARP实现改向的窃听方式是一种主动攻击方式，这种方式的实现技术有一定的难度。通过静态MAC地址法和第3层交换技术可使ARP改向攻击失去作用，从而提高交换设备与网络的安全保密性。

参考文献

1 Kaufman C.Network Security.Prentice-Hall,Englewood Cliffs, New Jersey, 1995

2 Robert B.肖文贵译.新版交换式以太网和快速型以太网. 北京：电子工业出版社，1997

3 Plummer D.An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48-bit Ethernet Addresses for Transmission on Ethernet Hardware. RFC826，Symbolics, 1982

4 Maximum Security:A Hacker's Guide to Protecting Your Internet Site and Network.Macmillan Computer Publishing,1997

5 Pittsburgh P A. IP Spoofing Attacks and Hijacked Terminal Connections.CERT,Carnegie Mellon University. CA-95:01 ,1995