文章编号:1673-0291(2010)02-0095-06

一种基于角色的强制访问控制模型

唐为民[1,3],彭双和[1],韩 臻[1],沈昌祥[2]
(1.北京交通大学 计算机与信息技术学院,北京 100044;
2.北京工业大学 计算机学院,北京 100022;3.解放军第96610部队,北京 100085)

摘 要:提出了RBMAC模型,将BLP、BIBA和RBAC融合.RBMAC模型以组织机构的层次化结构描述信息类别和用户角色,以文件处理过程的关键节点描述完整性级别,引入可信主体、任务、角色扮演者和角色聘请的概念,满足重要信息系统的访问控制需求.文中给出了RBMAC模型的形式化描述和安全性定理,提出了模型预定义、任务分配、角色聘请和安全级别匹配4个阶段的操作模式.模型以可信主体调整文件保密级别、完整性级别和信息类别,与重要信息系统的管理运行模式一致,经实际系统试验证明,具有较高的实用性.

关键词:访问控制;BLP模型;BIBA模型;RBAC模型;重要信息系统
中图分类号:TP309.2 **文献标志码**:A

A Role-Based Mandatory Access Control Model

TANG Weimin[1,3], *PENG Shuanghe*[1], *HAN Zhen*[1], *SHEN Changxiang*[2]
(1.School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2.School of Computer Information and Technology, Beijing University of Technology, Beijing, 100022, China;
3.96610'th Unit of Army, Beijing 100085, China)

Abstract: A new Role-based Mandatory Access Control (RBMAC) model which combine BLP, BIBA and RBAC models is proposed. The model describes hierarchical organization structure as information categories and user's roles, define most critical links of file treatment as integral classification and clearance. We also apply some concepts as trusted subject, task, invite role and actor in order to satisfy access control request from important information systems. The formal definition, theorem systems and operation rules of RBMAC model are illustrated in this paper. Trusted subject is responsible for change confidential classification and integral classification and categories in RBMAC model, whose methodology is same as actual works. The experiment shows that RBMAC model is flexible and efficient.

Key words: access control; bell-la padula(BLP) model; BIBA model; role-based access control(RBAC) model; important information system

政府和军队的重要信息系统对信息的保密性和完整性控制有很高的要求,系统中用户变动频繁,用户的知密范围与其业务范围及所执行的任务相关,要求控制粒度更细、限制更严格.重要信息系统的安全保护必须要有严格的访问控制机制和访问控制模型作支撑.

访问控制是一种保护信息资源免受非授权访问的有效安全机制[1].20世纪70年代初, Anderson

收稿日期:2009-05-20
基金项目:国家"863"计划项目资助(2007AA01Z410,2007AA01Z177);国家"973"计划项目资助(2007CB307101);北京交通大学科技基金项目资助(2008RC021);长江学者与创新团队发展计划项目资助(IRT0707)
作者简介:唐为民(1968—),男,河北唐山人,博士生.**email**:twm68@sohu.com.
沈昌祥(1940—),男,浙江宁波人,院士,博士生导师.

提出访问监控器的概念[2],为访问控制成为安全关键技术奠定了理论基础.30多年来,国内外学者研究提出大量访问控制模型,主要分为自主访问控制模型(DAC)、强制访问控制模型(MAC)和基于角色的访问控制模型(RBAC)[3].强制访问控制模型的代表是BLP模型[4]和BIBA模型[5].BLP模型主要解决保密性控制问题,以"下读上写"规则防止信息由高保密级流向低保密级;BIBA模型主要解决完整性控制问题,以"上读下写"规则防止信息由低完整级流向高完整级.当系统对保密性和完整性均有严格控制要求时,需要将BLP与BIBA模型结合,两个模型结合重点要解决信息完整性级别定义和BLP与BIBA模型的对偶性带来的反向信息流动困难问题,BLP与BIBA的结合模型及实用性研究一直是安全模型研究的热点.

Sandhu试图运用格的方法将BLP和BIBA模型结合,但严格的读写控制条件严重阻碍了信息的流动.郑志蓉和李益发针对反向信息流动问题,在其模型中引入可信代理(可信主体)充当保密性和完整性检查员[6-7].当违反安全策略的操作发生时,由可信主体对操作是否会破坏系统安全性作出判断,协助主体完成反向信息访问操作.但在实际系统中,可信主体难以实时、准确地完成安全性检查,另外可信主体权限过大会影响系统安全性,这成为其实用化的障碍.针对模型信息完整性级别定义困难的问题,蔡谊等引入可信度的概念,提出了二维标识安全模型[8].该模型仍采用对客体安全级检查的思想,用于调节信息双向流动,显然其实用性仍存在问题.文献[9-11]研究了支持动态安全标识及控制可信主体最小特权的安全模型,保证在违反BLP安全策略时安全地实现反向信息流.动态安全标识思想在模型实用化方面进了一步.

按照最小特权和按需获知的原则实施访问控制,主、客安全标识要能够更细化地区分主体或客体之间的差异,安全标识是否方便管理成为模型实用化的前提.BLP和BIBA模型的安全标识固化了主体访问客体的权限,在用户变动频繁时,系统对主体安全标识的管理相当繁琐,难以根据任务需要变换主体的安全标识.RBAC模型恰恰在此方面具有优势:一是主体与权限通过角色作为中介相关联,主体或权限变动,只需修改主体与角色或角色与权限的映射关系,降低管理复杂度;二是将权限与应用的具体工作相关联,可细化访问控制的粒度,从而实现最小特权和按需获知.Osborn指出RBAC可根据需要配置为DAC或MAC模型[12],梁彬研究了一种基于RBAC实现BLP模型的方法[13].RBAC模型一般用于应用层工作流控制,在操作系统层面上应用时,需要准确定义由谁代理角色完成访问操作,许峰提出的角色扮演者概念[14]值得借鉴.

上述安全模型研究取得了很大进展,但在保密性和完整性双重控制以及实用性方面还不能满足重要信息系统的访问控制要求,本文作者提出了基于角色的强制访问控制(Role-Based Mandatory Access Control, RBMAC)模型.它与传统的MAC及RBAC模型相比有以下特点:①将BLP和BIBA模型相结合,实现保密性与完整性一体的强制访问控制;②以信息生成、处理的关键环节描述完整性级别,使信息完整性控制与实际工作相对应;③引入可信主体概念,由可信主体更改客体的安全等级标识;④以安全等级动态范围描述主体安全等级标识,增强访问控制过程中主体对客体访问的适应性;⑤将安全等级标识中的类别作为角色定义的依据,类别以单位的组织结构树描述,将RBAC模型与强制控制模型融合;⑥引入角色扮演者和聘请角色扮演者的概念,针对具体任务选取角色扮演者,进一步将用户、角色和权限的关联关系动态化,角色扮演者与应用程序进程合理对应,体现计算环境的安全级别,加强对用户行使角色权限的控制能力.

1 基于角色的强制访问控制模型

1.1 有关概念和记号

政府和军队组织严密,按照所担负的任务形成树形的组织结构,此结构也代表了组织内部的业务关系.层次化的业务关系也就成了岗位职能的自然表述.图1给出了一个单位机关组织结构的示例.

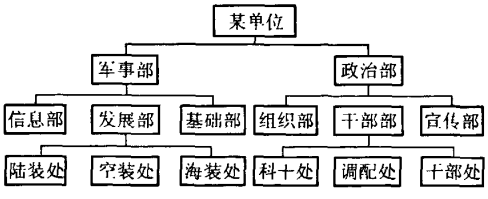

图1 单位组织机构示例

Fig.1 Organizational structure of a unit

定义1 岗位.在单位内部,组织机构的岗位有3种描述方式:①单位领导岗 $P_1 = D_1, D_2, \cdots, D_n. J_{0m}$或$J_{1m}$;②个人岗位 $P_2 = D_1, D_2, \cdots, D_n. J_{2i}$;③部门岗位 $P_3 = D_1, D_2, \cdots, D_n. J_{0m}$.

对于岗位 P_1 和 P_2,$D_1 \sim D_n$ 表示单位中各级部门,J_{0m}表示单位主官,J_{1m}表示单位副职,J_{2i}表示单位内部普通人员,其中 m 和 i 作为序号可描述多

个人员;对于岗位 P_3,以最后一级部门作为岗位,用于描述群组用户,该岗位内任一用户均可处理该岗位业务.单位内部上下级之间构成业务包含关系,单位主官对内部其他岗位有业务包含关系,如图1中 $D_1.\mathrm{Mlt.Dvp} \supseteq D_1.\mathrm{Mlt.Dvp.Air}$, $D_1.\mathrm{Mlt.Dvp.Air}.J_{01} \supseteq D_1.\mathrm{Mlt.Dvp.Air}.J_{11} \supseteq D_1.\mathrm{Mlt.Dvp.Air}.J_{21}$,同级单位之间业务隔离 $D_1.\mathrm{Mlt.Dvp.Air} \cup D_1.\mathrm{Mlt.Dvp.Sea}$.上述描述方式,可清晰地定义单位的业务关系,用于定义信息类别或角色时,可明确体现信息的类别属性或主体的信息处理范围.该描述方式可用X.500目录结构实现,易于存储和检索.

定义2　安全等级标识.主体和客体的安全等级标识记为三元组 $SC=(L,I,C)$,其中 L 是线性全序保密级别;I 是线性全序完整性级别;C 是信息类别.若 (L,I,C) 支配 (L',I',C'),则 $L \geqslant L' \wedge I \leqslant I' \wedge C \supseteq C'$. $f_{sc}()=(L,I,C)$ 为安全等级获取函数,$f_{sc}(S)$ 和 $f_{sc}(O)$ 分别用于获取主体和客体的安全等级标识,其中 $f_{sc}{}^{L}()=L$, $f_{sc}{}^{I}()=I$, $f_{sc}{}^{C}()=C$.

保密级别包含非密、敏感、秘密、机密、绝密5级,记为 $L=\{\mathrm{NS},\mathrm{ND},\mathrm{CD},\mathrm{SS},\mathrm{TS}\}$,级别依次升高,NS < ND < CD < SS < TS.

完整性级别包含未检测、草稿、校稿、定稿和签批5级,记为 $I=\{\mathrm{NC},\mathrm{DF},\mathrm{CF},\mathrm{FF},\mathrm{SF}\}$,级别依次升高,NC < DF < CF < FF < SF.外部非可信文件定为NC级,单位内部生成的文件,依据处理过程定为DF以上的级别.主体的完整性级别则代表主体处理信息的能力,如单位主官能够签批文件则为SF级.

主体的安全等级标识中,L 和 I 为二维标识,L_{RH} 表示最高读保密级,L_{WL} 为最低写保密级;I_{WH} 表示主体所具备的最高写完整性级别,I_{RL} 为读最低级别,一般设为NC.

客体分为静态标识客体和动态标识客体.静态标识客体为系统中作为输入端口和输出端口的客体,在其生命周期中安全级别不变,如打印机.动态标识客体采用二维标识,在其生命同期内可变,如文件.

定义3　角色.角色是组织机构中业务职能与责任的抽象描述.角色表示为三元组 (L,I,P),其中 L 为保密级别,I 为完整性级别,P 为岗位(见定义1).

可见,以业务关系描述信息类别和岗位时,角色与安全等级标识的表示方法一致,从而建立起RBAC与MAC融合的基础.在强制访问控制模型中,安全等级标识赋予主体和客体,而RBMAC模型中安全等级标识赋予角色和客体.

定义4　会话.请求访问的用户在发出访问请求时建立会话,选取用户所属的一组角色.

会话将请求访问的用户与为其指派的角色相关联.由于任务的需要,一个用户一次可同时建立多个会话,在会话有效期内,用户与角色的映射不变.

定义5　角色扮演者.角色扮演者是任务实例运行过程中,响应会话产生的一个动态对象,是用户以某角色执行任务实例的代理.角色扮演者记为actor, actor = < user, tasking, role, lifetime >,其中,user是actor所代理的用户,tasking是任务实例,role是任务实例所需要的角色,lifetime为actor的生存周期.

actor是一个动态对象.在任务实例执行过程中,用户发出访问申请,根据用户角色指派关系为每个角色建立会话,系统服务根据角色与任务指派关系选取角色,此时若会话的角色与任务实例所需的角色一致时,相应地激活一个actor,这个过程称为聘请角色扮演者.actor在用户、角色、任务实例之间建立联系,角色的权限相应地传递给actor,代理用户以特定角色完成任务中规定的操作.这种关系随着任务实例结束而结束.系统可通过actor的行为和状态,对用户及角色的行为实施安全监控.在实际系统中,actor可与应用进程相对应.

定义6　可信主体.可信主体满足以下条件:①静态程序经权威部门测评认证,程序行为不会对系统的安全造成影响,称为可信程序;②在启动运行时,可信程序经过完整性验证,证实未被修改,所形成的进程称为可信进程;③使用可信进程对客体操作的用户为系统授权的可信用户,其行为违反安全策略也不对系统安全性造成影响.

模型中客体的安全等级标识只能由可信主体修改,主体集合记为 S,可信主体集合记为 S^{T},普通主体集合记为 $S^{\mathrm{U}}=S-S^{\mathrm{T}}$.可信主体相当于实际系统中的保密员,文件的级别由保密员确定、修改.

模型中将客体的生成和处理分为不同的操作,包括添加(a)、只读(r)、读写(w)、执行(e)和属性修改(m)等5种.

1.2　RBMAC的形式化描述

定义7　RBMAC模型.RBMAC模型具有如下元素:

1) 客体集OBJS,用户集USERS,角色集ROLES,角色扮演者集ACTS,操作集OPS,任务集TASKS,任务实例集TSKINS,会话集SESSION,时间集TIME.

2) role = (L,I,P),定义角色.

3) $\mathrm{UA} \subseteq \mathrm{USERS} \times \mathrm{ROLES}$,用户角色指派.

4) assigned.users: $\mathrm{ROLES} \rightarrow 2^{\mathrm{USERS}}$,将角色role

映射到用户集合,形式化为 assigned.users (role) = {user|(user,role)∈UA}.

5) TASKS⊆OPTS × OBJS,任务定义.定义一项任务对客体进行的操作.

6) TA⊆ROLES × TASKS,角色任务指派.

7) assigned.roles: TASKS→2^{ROLES},将任务映射到角色集合,形式化为 assigned.roles(task) = {task|(task,role)∈TA}.

8) SESSION⊆USERS × 2^{ROLES},建立会话.用户发出访问请求时,选取为其指派的角色,建立会话.

9) user: SESSION→2^{USERS},会话到用户映射. assigned.users(session) = {(session, role)|(user, role)∈UA}.

10) role: SESSION→2^{ROLES},将会话映射到角色. session.role(session) = {∃role|(user, role)∈UA}.

11) TSKINS⊆TIME × TASKS,生成任务实例. tskins: TASKS $\xrightarrow{time}$ 2^{TSKINS},某个任务在特定时间执行时形成任务实例.

12) ACTS⊆TSKINS × SESSION,任务实例角色扮演,任务实例按约定聘请角色扮演者执行任务. invite.act(tskins) = {(user, tskins)| ∃ (user, role)∈TA}.

13) session: TSKINS→$2^{SESSION}$, 将任务实例映射到一组会话.

14) f_{sc}(actor) = f_{sc}(role)⊕ $f_{sc}(ev^{user})$,计算角色扮演者的安全等级. ev^{user}是用户 user 所使用的计算环境, $f_{sc}(ev^{user})$获取计算环境的安全等级. ⊕为安全等级的二元运算, $(L', I', C') = (L_1, I_1, C_1) \oplus (L_2, I_2, C_2)$,其中 $L' = \min\{L_1, L_2\}$, $I' = I_1$, $C' = C_1$.

15) actor 在任务实例中对客体进行操作,符合自主安全规则、安全读规则、安全写规则、动态标识客体安全等级确定规则和客体安全等级调整规则.

由 RBMAC 模型构造安全的系统,重要的是给出系统安全状态和状态安全转换函数(规则),本文沿用 BLP 模型对系统、状态和安全的定义.

规则 1 自主安全规则.一个系统状态 $v = (b \times M \times F)$ 满足自主安全规则,当且仅当 $\forall b = (actor, obj, op) \in B$, $op \in M_{s,obj}$, 其中 actor 是主体 s 的运行代理.

其中, v 表示一个系统状态; b 表示在 v 状态下角色扮演者 actor 对客体 obj 请求进行操作 op; M 为访问控制矩阵; F 表示所有角色和客体所具有的安全等级集合.

规则 2 安全读规则.一个系统状态 $v = (b \times M \times F)$ 满足安全读规则,当且仅当 $\forall b = (actor, obj, op) \in B \Rightarrow$ ① $actor \in S^U$, $(op = e \vee op = r) \wedge (f_{sc}^L(actor)_{WH} \geqslant f_{sc}^L(obj)) \wedge (f_{sc}^I(actor)_{RL} \leqslant f_{sc}^I(obj)) \wedge (f_{sc}^C(actor) \supseteq f_{sc}^C(obj))$; ② $actor \in S^T$, $op = e \vee op = r$, $(f_{sc}^L(actor)_{RH} \geqslant f_{sc}^L(obj)) \vee (f_{sc}^I(actor)_{RL} \leqslant f_{sc}^I(obj)) \vee (f_{sc}^C(actor) \supseteq f_{sc}^C(obj))$.

规则 2 表明,角色扮演者只读或读写客体,那么角色扮演者的安全等级必须支配客体的安全等级.

规则 3 安全写规则.一个系统状态 $v = (b \times M \times F)$ 满足安全写规则,仅当 $\forall b = (actor, obj, op) \in B \Rightarrow$ ① $actor \in S^U$, $(op = a \vee op = w) \wedge (f_{sc}^L(actor)_{WL} \leqslant f_{sc}^L(obj)) \wedge (f_{sc}^I(actor)_{RL} \geqslant f_{sc}^I(obj)) \wedge (f_{sc}^C(actor) \subseteq f_{sc}^C(obj))$; ② $actor \in S^T$, $op = a \vee op = w$, $(f_{sc}^L(actor)_{WL} \leqslant f_{sc}^L(obj)) \vee (f_{sc}^I(actor)_{WH} \geqslant f_{sc}^I(obj)) \vee (f_{sc}^C(actor) \subseteq f_{sc}^C(obj))$.

规则 3 表明,角色扮演者只写或读写访问客体,那么客体的安全等级必须支配角色扮演者的安全等级.

规则 2 和规则 3 体现了现实的安全策略:可信主体可读单位内部任意密级的客体,只能修改内部 CF 以下级别的客体.

规则 4 动态标识客体安全等级确定规则.若 actor 有安全等级标识($f_{sc}^L(actor)$, $f_{sc}^I(actor)$, $f_{sc}^C(actor)$),客体 obj 为动态标识客体,具有标识 ($f_{sc}^L(obj)$, $f_{sc}^I(obj)$, $f_{sc}^C(obj)$),若 actor 可写 obj,写操作后,obj 的安全标识变为 ($f_{sc}^{L'}(obj)$, $f_{sc}^{I'}(obj)$, $f_{sc}^{C'}(obj)$). 其中, $f_{sc}^{L'}(obj) = \max\{f_{sc}^L(actor)_{WL}, f_{sc}^L(obj)\}$, $f_{sc}^{I'}(obj) = f_{sc}^I(obj)$, $f_{sc}^{C'}(obj) = f_{sc}^C(actor) \cup f_{sc}^C(obj)$.

写客体时,动态标识客体的安全等级变化范围比较小,且仅变化密级,完整性级别变化及保密级别的大范围变化由可信主体通过规则 5 实现.

规则 5 客体安全等级调整规则. $\forall b = (actor, obj, m) \in B$, $actor \in S^T$, $\exists P(obj, sc)$, $sc \in SC$: ① $f_{sc}^L(obj) < f_{sc}^L(sc) \Rightarrow f_{sc}^{L'}(obj) = f_{sc}^L(sc)$; ② $(f_{sc}^L(obj) > f_{sc}^L(sc)) \wedge$ (obj 中的高涉密信息已清除或过保密期) $\Rightarrow f_{sc}^{L'}(obj) = \max\{f_{sc}^L(sc), ND\}$; ③ $(f_{sc}^I(obj) < f_{sc}^I(sc)) \wedge$ (obj 经检测不含低完整级信息) $\Rightarrow f_{sc}^{I'}(obj) = f_{sc}^I(sc)$; ④ $(f_{sc}^I(obj) > f_{sc}^I(sc)) \wedge (f_{sc}^I(obj) \neq SF) \Rightarrow f_{sc}^{I'}(obj) = f_{sc}^I(sc)$; ⑤ $f_{sc}^C(obj) \subset f_{sc}^C(sc) \Rightarrow f_{sc}^{C'}(obj)$

$= f_{sc}^{C}(sc)$; ⑥ $(f_{sc}^{C}(\text{obj}) \supset f_{sc}^{C}(sc)) \wedge (f_{sc}^{C}(\text{sc}) \neq \phi) \Rightarrow f_{sc}^{C}(\text{obj}) = f_{sc}^{C}(sc)$.

该规则限制了修改客体安全级的操作只能由可信主体完成,限定的修改操作与实际工作中的保密员职责相当.

1.3 RBMAC的状态安全性

按照上述 RBMAC 的定义,采取 BLP 模型的证明方法,可证明以下定理.

定理 1 若 $v = (b \times M \times F)$ 是一个满足 BLP 模型的安全状态,则在规则 3 和规则 4 下,系统仍然进入安全状态.

定理 2 若 $v = (b \times M \times F)$ 是一个满足 BLP 模型的安全状态,则在规则 5 下,系统仍然进入安全状态.

定理 3 若 $v = (b \times M \times F)$ 是一个满足 BIBA 模型的安全状态,则在规则 3 和规则 4 下,系统仍然进入安全状态.

定理 4 若 $v = (b \times M \times F)$ 是一个满足 BIBA 模型的安全状态,则在规则 5 下,系统仍然进入安全状态.

2 RBMAC的运行机制

RBMAC是一个随时间、进程和应用语境发生变化的动态的访问控制模型.访问控制的实施过程分为预定义、权限分配、角色聘请、安全等级匹配 4 个阶段,如图 2 所示.

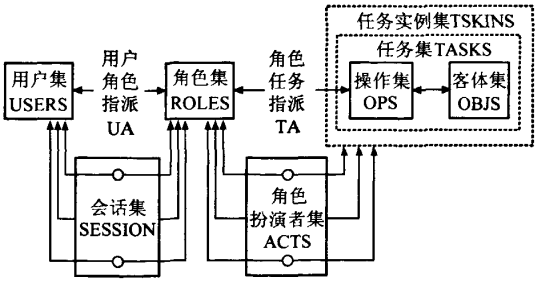

图 2 RBMAC模型运行机制

Fig.2 Working mode of RBMAC model

2.1 预定义

预定义阶段包括用户、角色和任务预定义 3 个过程:①系统管理员收集、管理单位中的所有用户信息,形成用户集 USERS,为用户生成用户身份介质(包括用户数据证书);②系统管理员根据单位的组织机构和应用系统需求,按照单位的树形业务结构预定义角色,形成角色集 ROLES;③应用管理员根据系统信息访问操作预定义客体集 OBJS 和操作集 OPS,并依据应用系统对客体的操作需求定义任务集 TASKS.

2.2 权限分配

权限分配阶段包括 2 个过程:①系统安全管理员为用户分配角色,即用户角色指派 UA;②应用安全管理员定义承担各项任务的角色,即角色任务指派 TA.

2.3 角色聘请

角色聘请包括 3 个过程:①用户申请访问信息,系统根据用户所指派的角色,为每个可能的角色建立一个会话,所有会话形成会话集 SESSION;②应用系统运行任务集中的任务,形成任务实例,所有实例形成任务实例集 TSKINS;③在符合要求的会话中选取一个会话,并为之生成进程,成为角色扮演者 actor,这个过程即是聘请角色扮演者,所有角色扮演者构成角色扮演者集 ACTS.在 RBAC96 模型和后续改进模型中,用户通过会话直接获得角色的权限.而在 RBMAC 模型中,用户通过会话激活角色,但是角色并不具备权限,应用系统根据任务需要选择角色,在已建会话中聘请角色,并生成与之对应的 actor,actor 真正获得访问客体的操作权限,从而建立用户、角色、任务、权限的对应关系.但这种权限是暂时的,当会话中断(用户退出)或任务实例结束时,操作权限立即失效.

2.4 安全等级匹配

安全等级匹配阶段包括 3 个过程:①角色扮演者通过协议获得用户计算环境安全等级,通过角色与用户计算环境安全等级的二元运算,得到角色扮演者的安全等级;②任务实例执行操作前,由访问监控器按照规则 1 ~ 5,对角色扮演者和客体的安全等级进行匹配,符合规则要求时则允许访问;③访问完成后,由访问监控器按照规则 1 ~ 5,对客体安全等级进行调整.由于一项任务可指派多个角色完成,当角色扮演者作为真实用户的代理访问客体时,首先要与用户计算环境 TCB 联络,获得计算环境的安全等级,将角色与用户计算环境的安全等级融合,actor 代表角色和用户工作环境访问客体,满足安全规则时才真正实施对客体的操作.写动态标识客体,客体的密级会发生变化,可保证生成应用要求最低保护等级的文件.

在实际工作中,文件的安全等级随办理过程发生变化.模型中客体的安全等级,尤其是完整性级别和类别发生变化时,由可信主体通过属性修改操作对客体的安全等级进行调整,该操作需要可信授权主体(部门领导)授权.这种方式与实际工作中单位

文件定级及定稿控制过程一致.

3 结束语

RBMAC模型针对重要信息系统访问控制的需求,将BLP、BIBA和RBAC模型有机结合,实现了"最小特权"、"职责分离"和"按需获知",在实用性方面得到很大提高:①以政府、军队等重要部门具有层次化组织结构的岗位描述角色,并作为业务关系描述主客体的信息类别,与重要部门的用户及业务管理模式一致;②通过引入敏感(涉密未定级)作为保密等级、以文件处理关键过程描述客体完整性级别,从而将保密和完整性控制与实际工作结合起来,贴近重要部门信息安全保密要求;③引入任务、角色扮演者和角色邀请的概念,对RBAC模型进行了深入改造,使模型具备了良好的访问权限控制粒度和动态性,不仅满足系统层访问控制需求,而且能够满足应用层工作流控制需求,更好地与应用系统融合,使系统层与应用层安全策略保持一致.以RBMAC模型为核心的访问控制机制在某重要信息系统中应用,取得良好的安全控制效果.

参考文献:

[1] Stoneburger G. Information System Security Engineering Principles-Initial Draft Outline[Z]. 2000.

[2] Anderson J P. Computer Security Technology Planning Study[R]. Bedford, MA: Air Force Electronic Systems Division, Hanscom AFB, 1972.

[3] Sandhu R, Coync E J, Feinstein H L. Role Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

[4] Lapadula L J, Bell D E. Secure Computer System: A Mathematical Model[R]. MTR-2547, 1973.

[5] Biba K. Integrity Considerations for Secure Computer Systems[R]. U.S. Air Force Electronic Systems Division, 1977.

[6] 郑志蓉,蔡谊,沈昌祥.操作系统安全结构框架中应用类通信安全模型的研究[J].计算机研究与发展,2005, 42(2): 328-332.
ZHENG Zhirong, CAI Yi, SHEN Changxiang. Research on an Application Class Communication Security Model on Operating System Security Framework [J]. Journal of Computer Research and Development, 2005, 42(2): 328-332. (in Chinese)

[7] 李益发, 沈昌祥. 一种新的操作系统安全模型[J]. 中国科学:E辑, 2004, 36(4): 347-356.
LI Yifa, SHEN Changxiang. A New Model of Operating Systems[J]. Science in China: Series E, 2006, 36(4): 347-356. (in Chinese)

[8] 蔡谊, 郑志蓉, 沈昌祥. 基于多级安全策略的二维标识模型[J]. 计算机学报, 2004, 27(5): 619-624.
CAI Yi, ZHENG Zhirong, SHEN Changxiang. A Planar Attributes Model Based on Multi-Level Security Policy[J]. Chinese Journal of Computers, 2004, 27(5): 619-624. (in Chinese)

[9] 谢钧, 许峰, 黄皓. 基于可信级别的多级安全策略及其状态机模型[J]. 软件学报, 2004, 15(11): 1700-1708.
XIE Jun, XU Feng, HUANG Hao. Trust Degree Based Multilevel Security Policy and Its Model of State Machine [J]. Journal of Software, 2004, 15(11): 1700-1708. (in Chinese)

[10] 武延军,梁洪亮,赵琛.一个支持可信主体特权最小化的多级安全模型[J].软件学报,2007,18(3):730-738.
WU Yanjun, LIANG Hongliang, ZHAO Chen. A Multi-Level Security Model with Least Privilege Support for Trusted Subject[J]. Journal of Software, 2007, 18(3): 730-738. (in Chinese)

[11] 石文昌, 孙玉芳. 多级安全政策的历史敏感性[J]. 软件学报, 2003, 14(1): 91-96.
SHI Wenchang, SUN Yufang. History Sensitivity of the Multilevel Security Policies [J]. Journal of Software, 2003, 14(1): 91-96. (in Chinese)

[12] Osborn S, Sandhu R, Munawer Q. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies[J]. ACM Transactions on Information and System Security, 2000, 2: 85-106.

[13] 梁彬,孙玉芳,石文昌,等. 一种改进的以基于角色的访问控制实施BLP模型及其变种的方法[J].计算机学报,2004,27(5):636-644.
LIANG Bin, SUN Yufang, SHI Wenchang, et al. An Improved Method to Enforce BLP Model and Its Variations in Role-Based Access Control[J]. Chinese Journal of Computers, 2004, 27(5): 636-644. (in Chinese)

[14] 许峰,赖海光,黄皓,等.面向服务的角色访问控制技术研究[J].计算机学报,2005,28(4):686-693.
XU Feng, LAI Haiguang, HUANG Hao, et al. Service-Oriented Role-Based Access Control[J]. Chinese Journal of Computers, 2005, 28(4): 683-693. (in Chinese)

一种基于角色的强制访问控制模型

作者： 唐为民， 彭双和， 韩臻， 沈昌祥， TANG Weimin， PENG Shuanghe， HAN Zhen， SHEN Changxiang

作者单位： 唐为民,TANG Weimin(北京交通大学,计算机与信息技术学院,北京,100044;解放军第96610部队,北京,100085)， 彭双和,韩臻,PENG Shuanghe,HAN Zhen(北京交通大学,计算机与信息技术学院,北京,100044)， 沈昌祥,SHEN Changxiang(北京工业大学,计算机学院,北京,100022)

刊名： 北京交通大学学报 ISTIC PKU

英文刊名： JOURNAL OF BEIJING JIAOTONG UNIVERSITY

年，卷(期)： 2010,34(2)

被引用次数： 3次

参考文献(14条)

1. Stoneburger G Information System Security Engineering Principles-Initial Draft Outline 2000

2. Anderson J P Computer Security Technology Planning Study 1972

3. Sandhu R;Coync E J;Feinstein H L Role Based Access Control Models 1996(02)

4. Lapadula L J;Bell D E Secure Computer System:A Mathematical Model v 1973

5. Biba K Integrity Considerations for Secure Computer Systems 1977

6. 郑志蓉;蔡谊;沈昌祥 操作系统安全结构框架中应用类通信安全模型的研究[期刊论文]-计算机研究与发展 2005(02)

7. 李益发;沈昌祥 一种新的操作系统安全模型[期刊论文]-中国科学E辑 2004(04)

8. 蔡谊;郑志蓉;沈昌祥 基于多级安全策略的二维标识模型[期刊论文]-计算机学报 2004(05)

9. 谢钧;许峰;黄皓 基于可信级别的多级安全策略及其状态机模型[期刊论文]-软件学报 2004(11)

10. 武延军;梁洪亮;赵琛 一个支持可信主体特权最小化的多级安全模型[期刊论文]-软件学报 2007(03)

11. 石文昌;孙玉芳 多级安全政策的历史敏感性[期刊论文]-软件学报 2003(01)

12. Osborn S;Sandhu R;Munawer Q Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies 2000

13. 梁彬;孙玉芳;石文昌 一种改进的以基于角色的访问控制实施BLP模型及其变种的方法[期刊论文]-计算机学报 2004(05)

14. 许峰;赖海光;黄皓 面向服务的角色访问控制技术研究[期刊论文]-计算机学报 2005(04)

本文读者也读过(9条)

1. 许俊伯.周洪昊.蒋明.柏文阳.徐洁磐 基于角色的强制访问控制模型的研究与应用[期刊论文]-计算机工程与应用2003,39(17)

2. 于昇.祝璐.沈昌祥.YU Sheng.ZHU Lu.SHENG Chang-xiang 多级安全模型[期刊论文]-计算机工程与设计 2010,31(13)

3. 崔艳莉.沈昌祥.CUI Yan-li.SHEN Chang-xiang 属性远程证明中完整性测量的可信性证明[期刊论文]-计算机工程2010,36(21)

4. 郭瑞明.刘益和.戴宗坤.GUO Rui-ming.LIU Yi-he.DAI Zong-kun 基于应用区域边界体系结构的多主体访问控制安全模型[期刊论文]-四川大学学报（工程科学版）2008,40(4)

5. 魏永合.岳明凯.WEI Yong-he.YUE Ming-kai 基于角色的强制访问控制模型[期刊论文]-探测与控制学报 2009,31(4)

6. 黄刚.王汝传.田凯.HUANG Gang.WANG Ru-chuan.TIAN Kai 基于RBAC策略的可信网格访问控制模型[期刊论文]-

计算机应用研究2010,27(4)

7. 张兴.陈幼雷.沈昌祥.ZHANG Xing.CHEN You-lei.SHEN Chang-xiang 基于进程的无干扰可信模型[期刊论文]-通信学报2009,30(3)

8. 李勇.王飞.胡俊.沈昌祥.LI Yong.WANG Fei.HU Jun.SHEN Chang-xiang TCB可信扩展模型研究[期刊论文]-计算机工程与应用2010,46(13)

9. 刘威鹏.张兴.LIU Wei-peng.ZHANG Xing 基于非传递无干扰理论的二元多级安全模型研究[期刊论文]-通信学报2009,30(2)

引证文献(3条)

1. 甘宏.潘丹 基于面向服务的多租户访问控制模型研究[期刊论文]-数字通信 2013(5)

2. 李振阳.曹慧.马金刚.宋晓瑞 RBAC模型在中医药信息资源管理平台中的应用研究[期刊论文]-山东科学 2011(6)

3. 熊雄.王福喜.左海洋 面向多级多域信息系统的访问控制方法研究[期刊论文]-计算机工程与设计 2011(11)

引用本文格式：唐为民.彭双和.韩臻.沈昌祥.TANG Weimin.PENG Shuanghe.HAN Zhen.SHEN Changxiang 一种基于角色的强制访问控制模型[期刊论文]-北京交通大学学报 2010(2)