第一次作业 习题一

1. RBAC96模型族由哪几个模型组成？各个模型的主要区别是什么？

RBAC96模型族由四个概念模型组成，分别是RBAC0，RBAC1，RBAC2，RBAC3。

它们的主要区别是：

RBAC0反应了RBAC的基本需求；

RBAC1在RBAC0的基础上加角色层次，反应多级安全需求；

RBAC2在RBAC0的基础上加上约束集合，体现了职责分离；

RBAC3是RBAC1和RBAC2的功能的集合。

1. RBAC1主要体现为角色层次，并基于角色层次实现权限继承与用户继承。怎样用RBAC2的约束条件实现RBAC1?

RBAC2是在RBAC0的基础上加上约束集合，RBAC1在RBAC0的基础上加角色层次，如果需要用RBAC2的约束条件实现RBAC1，则是需要用约束集合实现角色层次，对于RBAC1来说，针对用户，角色与权限的关系，应该可以这样约束：

如果对于任意用户指派了某一角色，则应该指派比该角色低的所有角色该用户；如果对于任意角色赋予了某种权限，则应该赋予比该角色高的所有角色该权限，用数字语言表示如下：

对于任意ui，如果(ui,ri)加入UA，则对于任意r’<=ri，(ui, r’)也应加入UA。

对于任意pi，如果(pi,ri)加入PA，则对于任意r’>=ri，(pi, r’)也应加入PA。

1. 如何通过RBAC来实现自主访问控制和强制访问控制？

自主访问控制指对某个客体具有拥有权（或控制权）的主体能够将对该客体的一种访问权或多种访问权自主地授予其它主体，并在随后的任何时刻将这些权限回收。在这种访问控制方式下，用户和权限是直接联系在一起的。

任意oi属于O，置一个角色Roj，具有权限(r,w,a,d,e,own,c)。只有Roj有own权限。若主体si对客体oj具有拥有权，在RBAC中，将(Si,Roj)加入UA，同时将(r,Roj),(w,Roj),(a,Roj),(d,Roj),(e,Roj),(own,Roj),(c,Roj)也加入PA。

客体oj的拥有者si可用：

assign(Roj,y,{ojr,ojw,oja,ojd,oje,ojc})(其中ojr，ojw，oja，ojd，oje，ojc为常规角色，分别具有对oj的r，w，a，d，e，c权限)

将r，w，a，d，e，c权限授给某些用户。

当需要收回相应的权限时使用：

revoke (oja,y,{ojr,ojw,oja,ojd,oje,ojrc,ojwc,ojac,ojdc,ojec})

若主体si对客体oj无拥有权，则在RBAC中si就不是Roj的成员，当然对oj无own权，其余的权限也不会被分配。

综上，这样具体配置以后，就得到了传统的自主访问控制机制。

第二次作业 习题二

1. 试设计一个算法，检测建立一个从外域角色到本域角色映射是否会发生角色冲突，若发生了冲突，给出该映射与那些映射是冲突的。

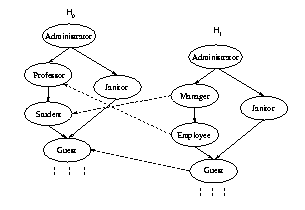


图1 存在冲突的映射

首先先看图1，图1是存在冲突的域间映射，H1为外域，H0为内域Employee这个角色的权限本应该比Manager角色的权限低，但是在映射中，由于Employee角色映射到Teacher，Manager角色映射到Student，又由于Teacher比Student权限高，所以Employee间接获得了Student的权限，而这个权限本来是Manager角色才能够获得的，所以发生了冲突。角色冲突也是如此，所以要检查冲突，算法可以这样表示：

在角色关联集R1，R2中，对于R2任意不同角色ri和rj，在R1中也存在两个角色ri’和rj’，如果有这样两个关联，ri->ri’，rj->rj’，但是ri<rj且ri’>rj’或是ri>rj且ri’<rj’，则存在冲突。

该算法中，需要找到每一个r角色的所有父节点和子节点，在满足映射的条件下，如果ri是rj的子节点且ri’是rj’的父节点，或者ri是rj的父节点且ri’是rj’的子节点，则存在冲突。

1. 从角色映射、角色授权、角色信息披露等方面对比IRBAC2000、SVE和结合PKI的RBAC实现，分析各自采用的跨域的访问控制技术，说明各自优点和缺点。

IRBAC2000：在角色映射上，是通过在本域和外域角色层次之间建立一系列关联来实现两个或多个域之间的安全互操作，在角色授权上，这个关联构成一个组合的角色层次，并且该角色层次仍然是偏序的，通过这个组合偏序关系可以获得期望的灵活性级别，外域角色被转换成本域实体所理解的本地角色，也获得本地角色相应的权限，在角色信息上，可由角色管理器管理信息和各种关联。

优点：1、具有灵活性，它没有强制安全员为外域角色层次中每一个角色都提供一个映射。2、具有动态性，若在本地域或外域角色层次中增加新的角色，该模型自动适应这种变化，不需要安全员作任何改动。

缺点：1、角色层次的冲突，即安全员可能会授予外域角色比原本想要给予的访问权限更高的权限，如上面的第四题。2、域穿梭，当一个域的主体试图和另一个域的某个目标进行互操作（或访问）时，它必须穿过域边界，然而，多域穿梭能隐蔽提升主体在角色层次的级别，可能存在一些风险。

SVE：使用分布式应用技术支持跨域共享操作的软件体系结构。既有安全共享，同时支持本地资源的自治管理。对应用透明，不用修改商业用途的OS和开放的网络协议。SVE完整的Policy包括四个部分：主体domain，客体type、访问矩阵、constrains。SPEX Controller产生一个聚合器，负责将外域节点的rules和本地域的domain规则进行聚合，然后统一交付给本地的访问控制决策机构。访问控制决策机构负责检查是否允许一个访问请求得以执行，首先区分是外域domain，还是localdomain；本地安全管理员不是将外域domain转换到本地，而是单独设计新的访问控制矩阵，然后执行不同的访问矩阵的检查; 执行访问控制矩阵以后,还要看是否满足constrains条件的约束。主体的domain信息被披露。SVE policy使用Java Object模拟policy，由管理员调用Policy GUI 进行初始化，然后由SPEX controller进行域之间的分发，最后存储在Access Calculation中; 安全策略（主体domain，客体type，访问矩阵，constrains）都被压缩成元数据，然后提供和Access Calculation的查询接口。Access Calculation提交查询请求，安全策略元数据对象进行决策，给出一个判定结果。

优点：对应用透明，不用修改商业用途的OS和开放的网络协议。基于分布式应用的中间件技术，从软件体系结构的模式出发，设计和实现了一个跨域的安全互操作体系框架，能够对共享的安全对象实施细粒度的访问控制，并且支持节点对本域安全对象的自治管理。

缺点：从跨越多域的角色转换和委托模型方面来看，创造性不是很充分。并且本地要对外域角色授权，而不是对其进行映射。

结合PKI的RBAC实现：针对大规模的分布式系统环境下如何识别用户的身份问题，现阶段主要采用PKI的技术。每一个组织内部建立PKI机制，为每一个用户发布X.509证书来证实身份。不同的组织之间借助交叉认证技术来相互识别和信任。对整个系统而言，把提供在线服务的用户称为服务器域，提出访问请求的用户称为客户域。针对服务器域和客户域，系统需要进行不同的访问控制设置。服务器提供的资源信息需要受到安全策略的保护，系统必须针对角色进行相应的授权设置。服务器采用访问控制表(ACL)的形式将权限和角色联系起来。服务器域相信客户域为每一个提出访问请求的用户，分配相应的角色。客户机必须给服务器提供如下证据：通过明确的指派表明用户是客户域的一个成员；在客户域中，用户拥有相应的角色。使用用户角色证书表明用户是某个客户域的成员，证书中不仅包含有该用户的公钥信息，而且为用户指派一个非常明确具体的角色，其中公钥信息主要是为了验证用户的身份。因为在用户角色证书设计时，主要强调其角色信息，所有省略了其公钥信息。如果在客户域内角色集是具有层次关系的，就必须保证用户的角色能够完整的体现它在角色层次中的位置。当客户域内的角色层次发生变化时，系统必须对相应的用户角色证书和角色层次证书进行撤销，而撤销行为当然也会影响到服务器端ACL列表中的相关设置。用户角色和角色层次关系均可以被撤销。

优点：安全性高，主要与PKI技术相关，从安全的角度分析，服务器需要针对客户域内的角色进行单独的授权，与SVE技术不同的是，客户域无需把每一个用户的主体识别规则都发送给服务器域，因为客户域的用户成员众多，而且经常发生变化。服务器域不用保存客户域的主体识别规则，只需要验证提出访问请求的用户是否具有相应的角色即可。从这个方面来看，结合PKI的跨域的基于角色访问控制技术比SVE技术更加灵活和简单。

缺点：RBAC的关键文件如角色信息、用户授权信息、用户名表等必须采用其他方式保证其完整性。

1. 对比分析RT0模型与DRBAC的异同点，分析各自的优势与不足。

RT0是RT的基础，它主要用来定义实体、角色名字和角色。一个实体对应一个用户，一般使用公钥来唯一标识一个主体。实体可以发送信任状和提出访问请求。RT0要求每个实体可以单独的被验证，而且可以判断哪个实体发布一个特殊的信任状或者访问请求。RT0是基于信任管理的访问控制技术。

DRBAC综合了传统的基于角色的访问控制和信任管理系统的优点。DRBAC的三个特征：

1）第三方委托(third-party delegations)：一个实体如果被授予了指派委托(delegation of assignment)后，就可以委托它的名字空间以外的角色，从而提高表现力；

2）值属性(valued attributes)：通过分配和处理与角色有关的数值的机制来调整传递的访问权限；

3）证书预定(credential subscription)：用pub/sub基础设施来跟踪可被回收证书的状态，从而实现对建立的信任关系进行持续监控。

相同处：RT0模型与DRBAC都使用公钥来唯一标识一个主体，实体和角色的表示形式类似。

不同处：DRBAC的委托相较于RT0模型中的信任状，功能更加丰富、表现力更强，除了对象委托外，还可以进行指派委托和第三方委托，这是信任状不能实现的。

RT0模型的优势与不足。

优势：分散管理；可扩展；可鉴别不安全网络中的个体。

不足：不提供反映组织自然结构的委托语言；因证书状态的变化而需对信任关系进行持续监控的问题没有陈述。

DRBAC的优势与不足。

优势：DRBAC采用公私钥对代表一个实体；DRBAC通过委托链将角色在不同的实体之间传递。

不足：DRBAC缺乏对强制安全访问控制策略的支持；DRBAC缺乏对委托链的传递控制。