Web信息系统中基于RBAC模型的访问控制模块的设计与实现

王宇
wangy@mail.neu.edu.cn
东北大学网络中心
2005年11月

主要内容

- Web信息系统中访问控制的必要性
- 主要的访问控制模型
- RBAC访问控制模型
- Web信息系统中RBAC模型的应用
- 具体应用实例
- 结束语

Web信息系统中访问控制的必要性

- 功能越来越复杂
- 涉及的资源种类越来越多，层次越来越低
- 相关人员的类别越来越多
- 验证的方式越来越多
- 潜在攻击者越来越多

综上，对Web信息系统进行严格的访问控制很有必要。

主要的访问控制模型

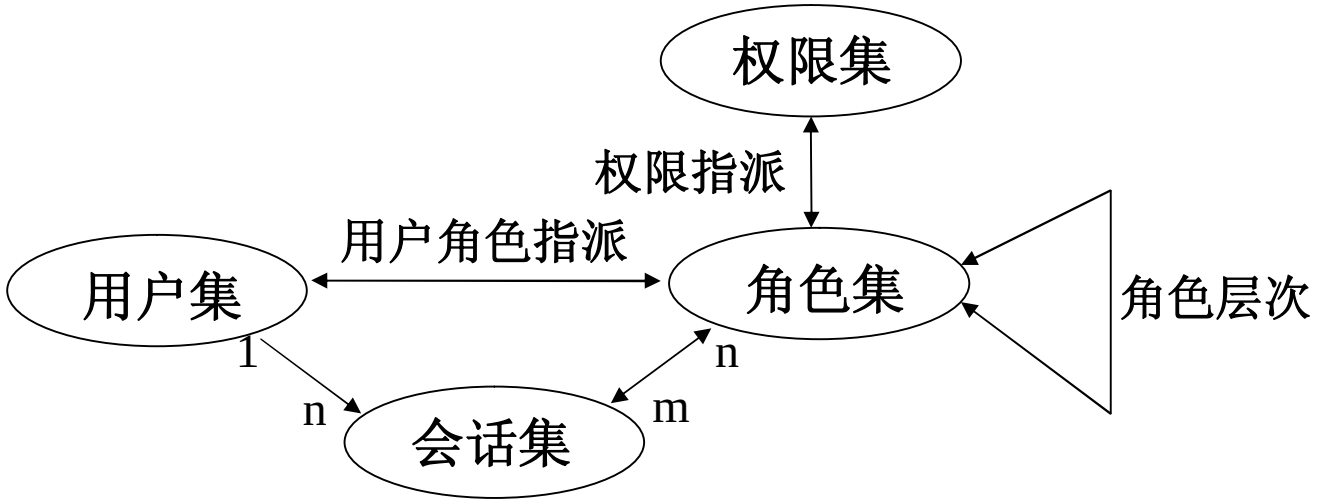
- 自主访问控制模型(Discretionary Access Controls, DAC)
- 强制访问控制模型(Mandatory Access Controls, MAC)
- 基于角色的访问控制模型(Role-Based Access Control)
- 基于任务的访问控制模型(Task-Based Access Control)

主要的访问控制模型(续)

- 基于对象的访问控制模型(Object-based Access Control Model, OBAC)
- 信息流模型

RBAC访问控制模型

- RBAC的基本模型及概念结构对应关系包含了四类实体：用户（User）、角色（Role）、权限（Permission）、会话（Session）



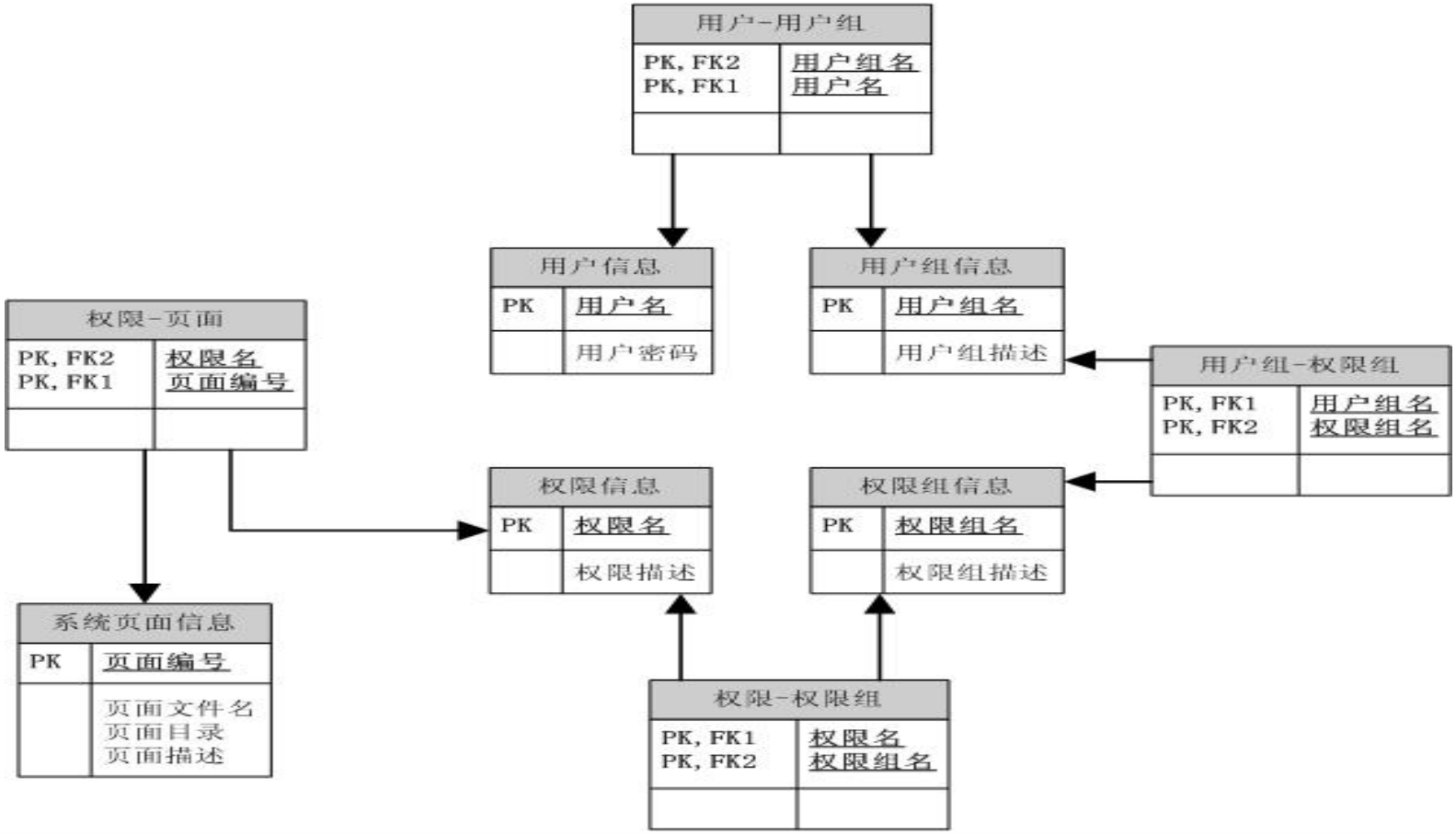
Web信息系统中RBAC模型的应用

- Web信息系统大多是用户通过客户端浏览器，访问网络上的Web服务器上的页面集合。
- 访问控制大多是针对Web服务器上的资源和数据库中的数据资源，并在Web服务器上具体实现。
- 由于通常的Web信息系统是由一组与功能相关的服务器端脚本文件和系统文件组成，我们可以将文件看作和权限相关联的资源实体，通过控制角色对文件的访问来实现Web信息系统资源的访问控制。

Web信息系统中RBAC模型的应用(续)

- 包含的数据实体有用户、用户组、权限组（角色）、权限和系统页面组；数据实体间的关联包含用户-用户组关联、权限-权限组（角色）关联、权限-页面关联和用户组-权限组（角色）关联。如图：

Web信息系统中RBAC模型的应用(续)



Web信息系统中RBAC模型的应用(续)

- 1) 权限管理部分

  用于维护信息系统中与访问控制相关的信息，包括数据实体（用户、用户组、权限组（角色）、权限和系统页面组）信息的添加、修改和删除，和数据实体间关联信息的添加与删除。在维护访问控制信息的时候，需要遵循RBAC访问控制模型的角色约束规则。此模型实例因降低模型复杂度，简化了角色层次结构。
- 2) 权限验证部分

  根据系统信息对用户访问进行验证，通过用户名和所访问的页面信息对资源访问进行验证。

具体应用实例

- 东北大学校庆接待管理系统
- 东北大学校友总会网站
- 东北大学网络中心信息管理系统(开发中)

结束语

RBAC访问控制模型实现了用户与访问权限的逻辑分离，减少了授权管理的复杂性，降低了管理开销，而且与日常信息系统管理的架构类似，降低了管理复杂度。但在实际的信息系统的设计与开发中，仍需要根据实际需求采用最适当的权限管理模型，以达到系统复杂度和效率的平衡。

Thanks a lot!