网络安全 - 访问控制技术（授权与认证）

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

什么是“访问”

常规领域

- Visit

安全领域

- Access

美国国防部

…要讨论安全，…陈述安全。

…安全的系统会利用一些…安全特性来控制对信息的访问，…被授权的人…可以读、写、创建和删除这些信息。

访问控制技术

要保证计算机系统实体的安全，必须对计算机系统的访问进行控制

访问控制的基本任务

- **防止非法用户即未授权用户进入系统**
- **合法用户即授权用户对系统资源的非法使用**

访问控制技术

访问控制技术是从计算机系统的处理能力方面对信息提供保护。

按事先确定的规则决定主体对客体的访问是否合理。

网络的访问采用基于争用和定时两种方法。

- 争用意味着网上所有站点按先后顺序争用带宽

谁是“被授权的人”？

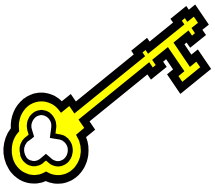
授权予谁?

来者何人?

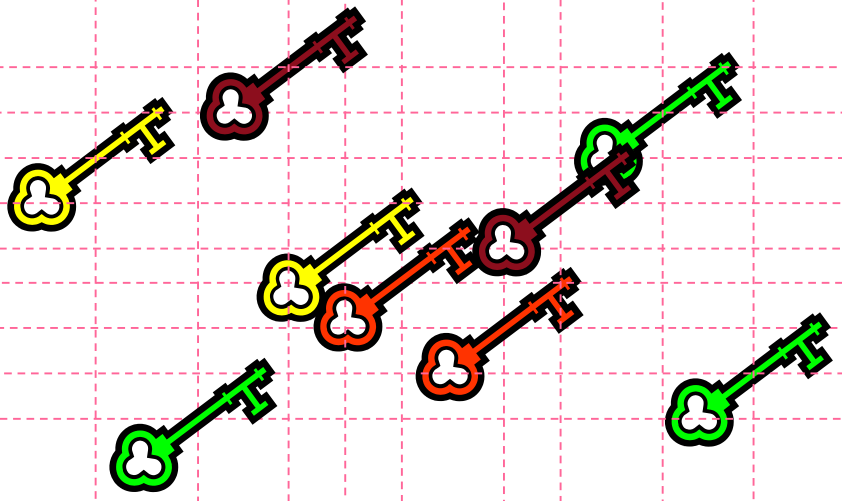
授权予谁

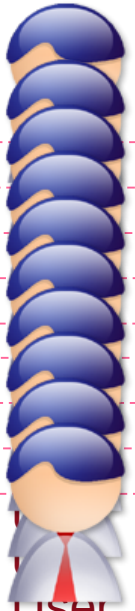
授权者

被授权者 (User)



授权予谁





User
User

基本概念

主体：信息系统中用户或进程，系统所有的用户与进程形成主体集合

客体：系统中被处理、被控制或被访问对象（如文件、程序、存储器等）

访问控制关系：根据制定的系统安全策略，形成主体与客体、主体与主体、客体与客体相互间的关系。

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

自主访问控制方法 – 章节分解

基于访问者 (行)

- **基于访问对象 (列)**

访问控制矩阵

	内容 1	内容 2	…	…	…	…
被授权者 1	A\B	A\B\C				
被授权者 2		A\B\C				
…						
…		…				
…					…	
…		…				

自主访问控制方法 - 1

基于访问者 (行)

- **权力表 (Capabilities List)**
- **前缀表 (Profiles)**
- **口令 (Password)**

基于访问对象 (列)

- **保护位 (Protection Bits)**
- **访问控制表 (Access Control List, ACL)**

自主访问控制方法 - 2

基于访问者 (行)

- **权力表 (Capabilities List)**
- **前缀表 (Profiles)**
- **口令 (Password)**

基于访问对象 (列)

- **保护位 (Protection Bits)**
- **访问控制表 (Access Control List, ACL)**

基于行 – 权利表

访问客体的钥匙

权利表决定用户是否可以对客体进行访问，以及以何种模式的访问（读，写，执行）。

可以动态的发放和回收、删除或增加权利。

由于不能确定有权访问客体的所有主体，所以利用权利表不能实现完整的自主访问控制。

访问控制矩阵 - 权利表

	内容 1	内容 2	…	…	…	…
被授权者 1	A\B	A\B\C				
被授权者 2		A\B\C				
…						
…		…				
…					…	
…		…				

基于行 – 前缀表

前缀表中存放着主体可访问的客体名和访问权限。

当主体要访问某个客体时，系统将检查该主体的前缀中是否具有它所请求的访问权。

基于行－前缀表存在的问题

主体的前缀表可能很大，增加了系统管理的困难。

只能由系统管理员进行修改，销毁与删除困难。

要系统回答“谁对某一客体具有访问权”这样的问题比较困难，但这个问题在安全系统中却是很重要的。

基于行－口令

每个客体相应地有一个口令，当主体请求访问一个客体时，必须向系统提供该客体的口令。

为了安全性起见，一个客体至少要有两个口令，一个用于控制读，一个用于控制写。

利用口令机制对客体实施的访问控制是比较麻烦的和脆弱的。

基于行－口令机制的缺陷

系统不知谁访问了客体

- **对客体访问的口令是手工分发的，不需要系统参与**

安全性脆弱

- **需要把该客体的口令写在程序中，这样很容易造成口令的泄露。**

使用不方便

- **每个用户需要记忆许多需要访问的客体的口令**

管理麻烦

- **撤消某用户对某客体的访问权，只能改变该客体的口令，且通知新口令给其他用户。**

自主访问控制方法 - 3

基于访问者 (行)

- 权力表 (Capabilities List)
- 前缀表 (Profiles)
- 口令 (Password)

基于访问对象 (列)

- 保护位 (Protection Bits)
- 访问控制表 (Access Control List, ACL)

基于列 – 保护位 1

保护位对所有主体、主体组以及该客体的拥有者指定了一个访问权限的集合，UNIX中利用了这种机制。

在保护位中包含主体组名字和拥有者名字。

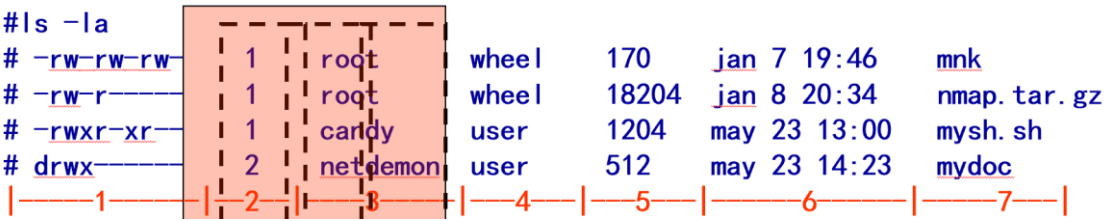
保护位机制中不包含可访问该客体的各个主体的名字。

由于保护位的长度有限，用这种机制完全表示访问矩阵实际上不可能。

基于列 – 保护位 2

用户组是具有相似特点的用户集合。生成客体的主体称为该客体的拥有者。它对客体的所有权仅能通过超级用户特权来改变。

拥有者（超级用户除外）是唯一能够改变客体保护位的主体。一个用户可能不只属于一个用户组，但是在某个时刻，一个用户只能属于一个活动的用户组。用户组及拥有者名都体现在保护位中。



基于列 – 访问控制表

在这种机制中，每个客体附带了访问矩阵中可访问它自己的所有主体的访问权限信息表（即ACL表）。

该表中的每一项包括主体的身份和对该客体的访问权。

如果利用组或通配符的概念，可以使ACL表缩短。

ACL方式是实现DAC策略的最好方法。

客体	ID_1. 读	ID_2. 写	ID_3. 读 ……	ID_n. 执行	

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

自主访问控制的类型 – 章节分解

- 等级型
- 属主型
- 自由型

等级型

层次型的（Hierarchical）文件的控制关系一般都呈树型的层次结构。

系统管理员可修改所有文件的ACL表，文件主体可以修改自己文件的ACL表。

优点

- 可以通过选择可信的人担任各级权限管理员

缺点

- 一个客体可能会有多个主体对它具有控制权，发生问题后存在一个责任问题

属主型

该类型的访问权控制方式是为每一个客体设置拥有者，一般情况下客体的创建者就是该客体的拥有者。

拥有者拥有对自己客体的全部控制权，但无权将该控制权转授给其他主体。

拥有者是唯一可以修改自己客体的ACL表的主体，也可以对其他主体授予或撤消对自己客体的访问操作权。

如果主体（用户）被调离他处或死亡，系统需要利用某种特权机制来删除该主体拥有的客体。

自由型

客体的拥有者（创建者）可以把对自己客体的许可权转授给其他主体。

也可以使其他主体拥有这种转授权，而且这种转授能力不受创建者自己的控制。

由于这种许可权（修改权）可能会被转授给不可信的主体，因此这种对访问权修改的控制方式很不安全。

授权于谁

访问控制表

- **基于访问者**
- **基于访问对象**

基于角色的访问控制技术

- **RBAC (Role-Based Access Control)**

基于任务的访问控制技术

- **TBAC (Task-Based Access Control)**

基于组机制的访问控制技术 (基于偏序关系)

…

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

自主访问控制优缺点

优点

- **方便、实用**
- **可自由定制**
- **可扩展性强**

缺点

- **不能控制主体对客体的间接访问**
- **允许用户自主地转授访问权，带来不安全隐患**
- **系统无法区分是用户合法修改还是木马程序非法修改**
- **无法解决因用户无意（如程序错误、某些误操作等）或不负责任的操作，造成的敏感信息的泄漏问题**

来者何人

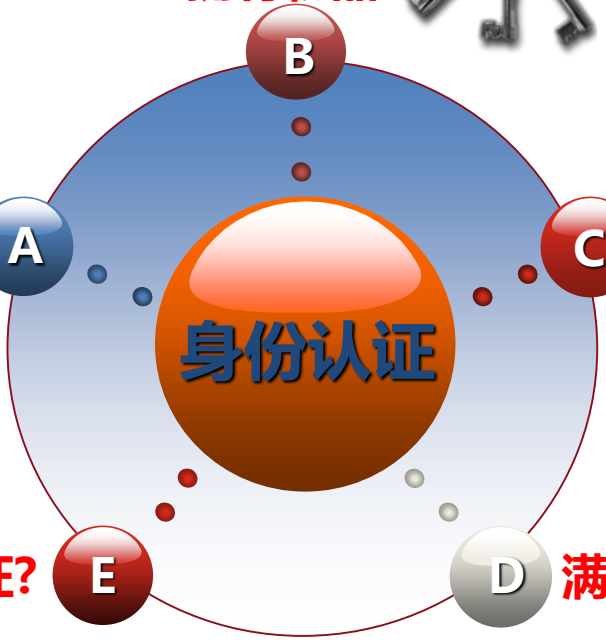
知道秘密?

拥有物品?

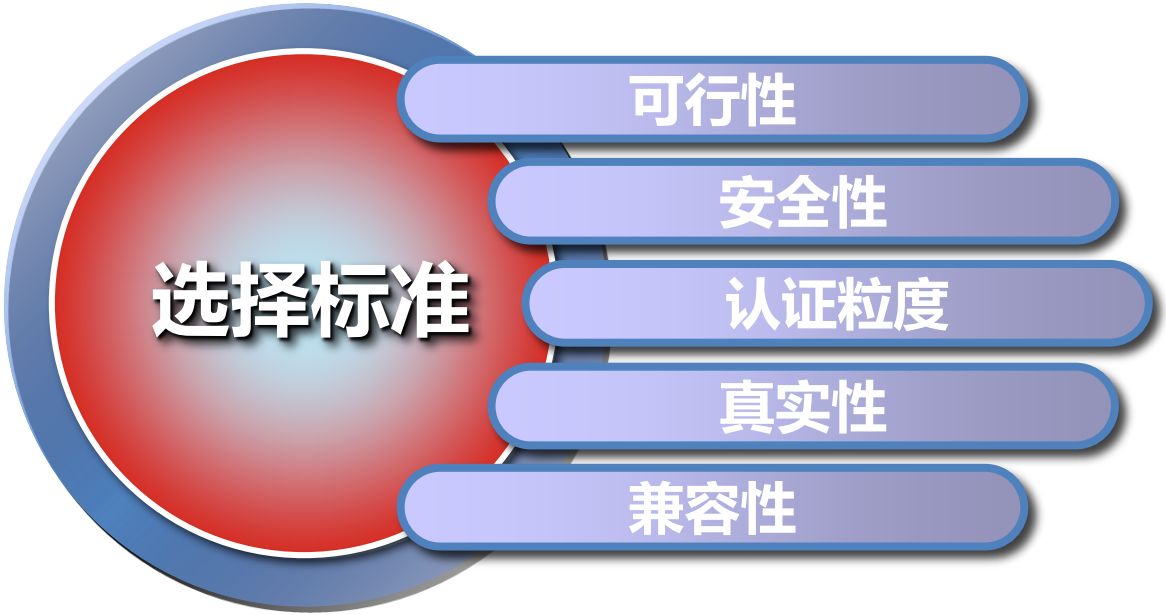
具备生物特征?

有权威认证?

满足时空条件?



身份认证



思考题

1. 如何确保身份认证数据的真实性?

2. 什么是自主访问控制？方法有哪些?

3. 为什么自主访问控制无法抵御特洛伊木马攻击?

谢谢!