计算机网络访问控制技术研究

1 访问控制的安全意义

近年来，随着全球网络化热潮的迅速涌起，计算机网络正在日益广泛而深入地渗透到社会的各个领域，并深刻地改变着整个社会的行为和面貌。与此同时，网络安全问题也迅速地突现出来， 成为困扰和阻碍网络技术进一步普及和应用的绊脚石。 尤其在商业、金融和国防等领域的网络应用中， 能否保证网络具有足够的安全性是首先要考虑的问题。 安全问题若不能有效地得到解决，必然会严重到影响整个网络事业的发展。

2 访问控制的概念

为此，国际化标准组织 ISO 在网络安全体系的设计标准 (ISO7498-2) 中，提出了层次型的安全体系结构，并定义了五大安全服务功能：身份认证服务、访问控制服务、 数据保密服务、 数据完整性服务和不可否认服务。 作为五大服务之一的访问控制服务，在网络安全体系结构中具有不可替代的作用。 它可以合理限制不同用户对关键资源的访问， 防止非法用户的侵入和因合法用户的不慎操作所造成的破坏， 是网络环境中最为基础和最为关键的安全服务之一。

在访问控制系统中一般包括 3 个要素：

（1）主体：发出访问操作的主动方，通常指用户或用户的某个进程。

（2）客体：被访问的对象，包括：网络中的一些活跃元素（例如：程序、进程等)、数据、信息、各种网络服务和功能、网络设备设施。

（3）授权策略：一套规则，用以确定某个主体是否对某个客体拥有访问能力。

从数学的角度来看， 授权策略实际上就是一个矩阵，行 (或列) 表示客体，

列(或行)表示主体,行和列的交叉点表示某个主体对某个客体的访问权限(读、写、执行、修改、删除等),如表 1 所示。

表 1 授权策略的数学表示

	主体 1	主体 2	主体 3	…
资源 A	r, w	r	r, w, x	…
资源 B	r, w	r, x	r	…
资源 C	r, x	r, w, x	r, w	…
…	…	…	…	…

注:上表中,r 表示读权限;w 表示写权限;x 表示执行权限

访问控制在狭义上是指:系统在确认主体的身份后,根据访问策略控制主体对客体的访问过程。可见,主体的身份认证是实施狭义访问控制的先决条件,而且在实际应用中,身份认证与狭义上的访问控制往往相互作用,联系十分密切,所以访问控制还有一个广义上的含义,它包括了身份认证和授权控制两大部分,这里的授权控制在含义上与狭义上的访问控制大抵一致。 在广义的访问控制概念中, 身份认证就是确定主体的真实身份的过程; 授权控制就是控制主体对客体的访问的过程。 身份认证是广义访问控制的前提,授权控制则是广义访问控制的核心。 本文中主要讨论广义上的访问控制。

3 访问控制技术的研究

根据授权策略的不同,目前在理论上主要有 4 种不同类型的访问控制技术:自主访问控制(DAC)、强制访问控制(MAC)、基于角色的访问控制(RBAC)和基于任务的访问控制(TBAC)。

3.1 自主访问控制和强制访问控

①自主访问控制(Discretionary Access Control,DAC)

DAC 的主要特征体现在主体可以自主地把自己所拥有的对客体的访问权限

授予其他主体或者从其他主体收回所授予的权限，访问控制的粒度是单个用户。DAC 是在确认主体身份及所属的组的基础上，对访问进行限定的一种控制策略，访问控制策略保存在一个矩阵中，行为主体，列为客体。 为了提高效率，系统不保存整个矩阵， 在具体实现时是基于矩阵的行或列来实现访问控制策略的。目前以基于列客体的访问控制列表（Access Control List，ACL）采用的最多。ACL 的优点在于表述直观、易于理解，而且比较容易查出对一特定资源拥有访问权限的所有用户。

但 ACL 也存在着一些问题，ACL 直接将用户与权限关联使 ACL 变得复杂、庞大，大量的用户/权限关联意味者需要管理大量的用户/权限关联对。 尤其在 ACL 应用到网络规模较大、需求复杂的企业的内部网络时，需要在环境中设定大量的表项，当用户的职位、职责发生变化时，为反映这些变化，管理员需要修改用户对所有资源的访问权限， 使得访问控制的授权管理需要花费很大的人力，不但容易出错，也无法实现复杂的安全策略。

而且，根据自主访问控制授权策略，用户可以自主地把自己所拥有的客体的访问权限授予其他用户。 但是在很多商业部门中，终端用户并不“拥有”他们所能访问的信息，这些信息的真正“拥有者”是企业（公司）。这种情况下，访问控制应该基于职员的职务，即访问控制是由各个用户在部门中所担任的角色来确定的，这样就造成概念上的不一致。

最后，DAC 将赋予或取消访问权限的一部分权力留给用户个人， 这使得安全管理员难以确定哪些用户对哪些资源有访问权限， 不利于实现统一的全局性访问控制。

②强制访问控制（Mandatory Access Control，MAC）

MAC 是指系统强制主体服从事先制订的访问控制策略。 在 MAC 安全系统中，所有信息都有一个密级，例如：绝密级、机密级、秘密级、无密级；每个用户也都相应地有一签证。 例如要决定是否允许某用户读一个文件， 那么就比较该用户的签证是否与该文件的密级相符。 安全策略要求，为了合法地得到某一信息，用户的安全级必须大于或等于该信息的安全级， 并且该信息属于用户的信息访问类别。 可见，MAC 通过梯度安全标签实现单向信息流通模式。

MAC 安全体系中通过授权进行访问控制的技术，可以直接应用于数据库中的信息管理和网络及操作系统中的信息管理， 但它更主要的是用于多层次安全级别的军事应用系统中。 MAC 缺点在于主体访问级别和客体安全级别的划分与现实要求无法完全一致， 在同级别间缺乏控制机制。

3.2 基于角色的访问控制（Role-Based Access Control，RBAC）

RBAC 主要研究将用户划分成与其在组织结构体系相一致的角色，以减少授权管理的复杂性，降低管理开销和为管理员提供一个比较好的实现复杂安全策略的环境。

在应用级信息系统的设计中， 采用 RBAC 具有以下优势：

（1）降低了管理的复杂度。 管理授权数据通常是系统管理员的一项繁重工作， 而在 RBAC 中根据用户的能力与责任把用户与角色关联，一方面定义角色、添加与删除角色中的用户,易于操作；另一方面由于用户与权限不直接关联，可以通过改变角色的权限来改变该角色中所有用户的权限。 例如某个工作岗位有 U 个用户，需要完成 P 种操作，采用 ACL 需管理 U×P 个用户/权限关联对。 使用 RBAC 只需定义一个角色，然后把该角色授权给 U 个用户，从而减少了管理的授权数据（为 U+P 个关联）；当该工作岗位的职能发生变化时，系

统管理员只需要改变角色的权限而不必像 ACL 那样改变所有的用户/权限关联对。

(2) 能够方便地描述复杂的安全策略。 安全的整个领域既复杂又广泛， 安全策略实质上表明系统在进行一般操作时，在安全范围内什么是允许的，什么是不允许的。 策略通常不作具体规定，即它只是提出什么是最重要的，而不确切地说明如何达到所希望的这些结果。策略建立起安全技术规范的最高一级，不像 ACL 只支持低级的用户/权限关系。 RBAC 支持角色/权限、角色/角色的关系，由于 RBAC 的访问控制是在更高的抽象级别上进行的，系统管理员可以通过定义角色、角色分层、 角色约束来实现企业的安全策略， 管理用户的行为。 在 RBAC 中对角色的安全管理与企业特有的安全策略是相符的， 角色权限的不同反映出角色在企业组织结构中所担任的不同职责（例如上、下级关系）。

(3) 降低了管理中的错误。 系统管理员一旦完成了角色与角色间关系的定义， 由于角色的职能具有一定的稳定性，而用户的职能变动频繁，所以系统管理员的主要工作就是添加与删除角色中的用户，与 ACL 相比较，操作简单方便，减少了出错的风险。

3.3 基于任务的访问控制 (Task-Based Access Control，TBAC)

TBAC 是一种新型的访问控制和授权管理模式 ，它非常适合多点访问控制的分布式计算和信息处理活动以及决策制定系统。 TBAC 采取面向任务，而不是传统的面向主体对象访问控制方法。 如果实现 TBAC 思想，权限体系的生成就会更及时，而且这些权限是执行操作时所需的， 这一点在包含事务和工作流的应用环境中尤其适用。TBAC 方法还将使自我管理的访问控制模型提升到更高程度，从而降低总体费用。

TBAC 模型现在还处于一种高度抽象的概念层次,还没有具体化，离实用阶段还有一段距离。 但它有很广的潜在应用性， 从对客户—服务器交互这样精细活动实施访问控制， 到对跨部门和组织边界的分布式应 用和工作流这样的粗单元实施访问控制都适用。TBAC 访问控制涉及到与一定应用逻辑一致的任务完成过程中不同点的授权， 这一点在其他的主体对象访问控制方法中不能得到满足。 相比之下，在传统访问控制中，访问控制决策制定太简单了，本质上与高层应用程序语义和要求脱节。

TBAC 从基于任务的角度来实现访问控制， 能有效解决提前授权问题，是一种主动访问控制模型。 它给出了动态授权的概念。 所谓动态授权，就是将授权不仅同用户、角色联系，还同任务相关。 当任务即将执行时，才对用户授权；当任务执行完就撤销用户的权限。 这样就可以保证权限只有在用户需要时才得到， 满足最小特权原则。

TBAC 在完成任务的过程中，要监视权限的状态， 按照进行中的任务状态确定权限是活动状态或非活动状态，因此它是积极参与访问控制管理的。

TBAC 是一种新兴的访问控制技术，预计未来一段时期内将在办公自动化、电子商务自动化处理等领域得到广泛的应用。