基于授权管理基础设施的授权及访问控制机制①

王毅彦 （武汉大学信息管理学院 430072）

摘要：与传统的权限管理机制相比，基于授权管理基础设施实现的集中式访问控制机制，能够有效地实现权限的统一管理和权限信息的相对独立，使系统具有更高的安全性和灵活性。文章介绍了基于授权管理基础设施的集中式授权及访问控制机制，并重点探讨其不同的实现方式。

关键词：信息安全 授权 集中式访问控制 授权管理基础设施

授权及访问控制机制是网络安全的重要内容之一，也是统一的安全管理中要解决的主要问题。传统的权限管理机制主要有：基于用户名和口令的权限管理和基于公钥证书的权限管理。基于用户名和口令的权限管理方式将网络用户及系统权限存储在用户权限数据库中，通过查找用户权限表来验证用户的权限；基于公钥证书的权限管理方式利用了公钥证书扩展项功能，将用户权限信息存储在公钥证书的扩展项中，在身份认证的同时完成权限认证。

传统的权限管理方式产生了许多问题：权限管理混乱，同一单位或部门内不同的系统采用的是不同的权限管理策略；系统管理员的负担过重，容易造成管理方面的漏洞，可能会带来系统的不安全的因素；权限管理模型没有统一，增加了系统的费用。虽然基于公钥证书的权限管理方式通过将用户的身份标识与权限相绑定来实现权限的集中管理，但它缺乏必要的灵活性。

相对于传统的权限管理机制的不足，基于授权管理基础设施实现的集中式访问控制机制，有效地实现了权限的统一管理和权限信息的相对独立，使系统具有更高的安全性和灵活性。

1 授权管理基础设施

PMI 是 X.509v4 中提出的授权模型，它建立在 PKI 提供的可信身份认证服务的基础上，其具体的实现方式有多种。X.509v4 中建议基于属性证书 AC（Attribute Certificate）实现其授权管理。PMI 向用户发放属性证书，提供授权管理服务；PMI 将对资源的访问控制权统一交由授权机构进行管理；PMI 可将访问控制机制从具体应用系统的开发和管理中分离出来，使访问控制机制与应用系统之间能灵活而方便的结合和使用，从而可以提供与实际处理模式相应的、与具体应用系统开发和管理无关的授权和访问控制机制。

1.1 PMI 与 PKI

在信息安全技术领域里，公开密钥加密技术近年来发展很快，在这项技术的基础上形成和发展起来的公开密钥基础设施（PKI），很好地适应了互联网的特点。它通过方便灵活的密钥和证书管理方式，提供了在线身份认证的有效手段，为电子政务、电子商务、电子社区、远程教育、远程医疗等各种网络应用及类似的网络服务奠定了坚实的安全基础。然而，随着网络应用的扩展和深入，仅仅能确定“某人是谁”已经不能满足需要，安全系统要求提供一种手段能够进一步确定“某人能做什么”，即某人是否拥有使用某种服务的特权。为了解决这个问题，特权管理基础设施（Privilege Management Infrastructure，PMI）应运而生。

授权管理基础设施需要公钥基础设施为其提供身份认证服务。同公钥基础设施相比，两者的主要区别在于：PKI 证明用户是谁，并且由各类应用共同信任的有关机构提供统一管理；而 PMI 证明这个用户有什么权限，能干什么，为各类应用提供相对独立的授权管理，并且各类应用相互之间的权限资源独立。

① 本文系教育部博士点研究项目（基于网络的信息资源整合与共享）研究成果之一。
项目批准号：03JB870005

1.2 属性证书与公钥证书

在 X.509v3(1997 年)证书规范中引入了属性证书的概念,X.509v4(2000 年)进一步描述了属性证书与公钥证书的关系以及属性证书的使用模式。属性证书是由 PMI 的属性权威机构 AA(Attribute Authority)签发的包含某持有者的属性集(如角色、访问权限及组成员等)和一些与持有者相关信息的数据结构。由于这些属性集能够用于定义系统中用户的权限,因此作为一种授权机制的属性证书可看作是权限信息的载体。属性权威 AA 的数字签名保证了实体与其权力属性相绑定的有效性和合法性。由于属性证书是一个由属性权威签名的文档,因此其中应包括这些属性:

① 名字。特权验证者 PV(Privilege Verifier)必须能够验证持有者与属性证书中的名称的确是相符的。宣称具有该属性的实体应该提交一个公钥证书,并证明自己是相应的公钥拥有者。

② 一个由签发者与序列号共同确定的、特定的用于数字签名的公钥证书。属性验证者必须能够确保该宣称者与证书中公钥的真正持有者是同一个人。

作为权限管理体系 PMI 的授权实现机制,属性证书及其属性授权机构 AA 考虑的是基于属性的访问控制,而不像公钥证书考虑的是基于用户或 ID 的身份鉴别。公钥证书 PKC 如同网络环境下的一种身份证,它通过将某一主体(如人、服务器等)的身份与其公钥相绑定,并由可信的第三方,即证书权威机构 CA 进行签名,以向公钥的使用者证明公钥的合法性和权威性;而属性证书 AC 则仅将持有者身份与其权力属性相绑定,并由部门级别的属性权威从进行数字签名,再加上由于它不包含持有者的公钥,所以这一切都决定了它不能单独使用,必须建立在基于公钥证书的身份认证基础之上。由此可见,尽管一个人可以拥有好几个属性证书,但每一个都需与该用户的每个公钥证书相关联,与公钥证书结合使用。

1.3 PMI 体系结构与特权委托模型

PMI 特权管理体系结构一般由三部分组成:对象(Object)、特权声称者(Privilege Asserter)和特权验证者(Privilege verifier)。其中对象指的是受保护的资源。例如在访问控制应用中,对象就是指被访问的资源。这种类型的对象常具有一定的援引方法。如当对象是某文件系统中的文件时,则该文件具有"读"、"写"和"执行"等对象方法。特权声称者即指拥有一定特权并针对某一特定服务声称具有其权限的实体。特权验证者指的是根据用户声称的特权对其是否享有某一服务作出判断的实体。

特权验证者在获得用户的属性证书后,将依据以下四点判断是否允许该用户访问某一资源:

(1) 特权声称者的权限(Privilege of the Privilege Asserter)。封装在特权声称者属性证书(或公钥证书中的 SubjectDiretoryAttributes 主体目录属性扩展字段)中的属性。特权持有者的权限反映了证书发放机构对其的信任程度。

(2) 权限策略(Privilege Policy)。规定访问某一特定对象所需权限的最小集合或门限。它精确地定义了特权验证者为了允许特权持有者访问某一请求对象、资源或应用服务应包含的特权集。权限策略因其完整性和真实性应受到严密的保护。

(3) 当前环境变量(Current Environment Variables)。特权验证者在进行访问控制判断时依据权限策略规定需要使用的一些参数,如访问时间,请求者的源地址。需要注意的是,环境变量的提交完全是一种局部事件。

(4) 对象方法的敏感度(Sensitivity of the Object Method)。它反映了将要处理的文档或请求的属性,文件内容的机密等级等。对象方法的敏感度既可以显式地加密于联合安全标签中或由对象方法支持的属性证书内,也可以隐式地封装于数据对象的数据结构中。当然,它也可以用其他方法进行加密。在一些应用环境中,对象方法的敏感度是不需要的。

将特权验证者与任意属性权威 AA 进行任意绑定是没有必要的。正如特权持有者可以拥有许多不同从颁发给他的属性证书,特权验证者也可以验证由许多从发布的证书。

PMI 特权委托模型可以分为三级(参见图 1),分别是信任源点(SOA),属性权威机构(AA)和授权服务代理(ARA)。SOA 是授权给特权持有者的最初签发人。它是整个 PMI 授权系统的最终信任源和最高管理机构,对授权策略的制定、属性权威 AA 的设立及授权均负有主要责任,相当于 PKI 系统中的根 CA。通常由 SOA 委托的特权持有者充当的是 AA 的角色,AA 相当于 PKI 系统中的 CA。进一步授权给其他实体由 AA 执

行，但授予的权力属性只能是该 AA 拥有权限的子集，这也是 PMI 特权委托模型中的一条通用法则。作为权威中心的 SOA 完全可以对其实施的特权委托加以限制。例如特权委托的路径深度，对证书路径中较靠后的证书的数量和主体名字空间的限制等。每一个由上一级 AA 授权的实体同样可以再次充当 AA 的角色。充当特权委托者的 AA 同样可以对其下属 AA 的权力加以限制。AA 由具有设立 AA 中心业务需求的各应用单位负责建设，并与 SOA 中心通过业务协议达成相互信任的关系。AA 中心的主要职责包括：应用授权受理、属性证书的签发和管理，下属 AA 的设立以及 ARA 的设立审核和管理等。ARA 中心是 PMI 特权委托模型中的用户代理节点，直接与属性证书的用户发生业务交互，相当于 PKI 系统中的 RA 。ARA 中心的主要职责包括授权服务代理和授权审核代理等。

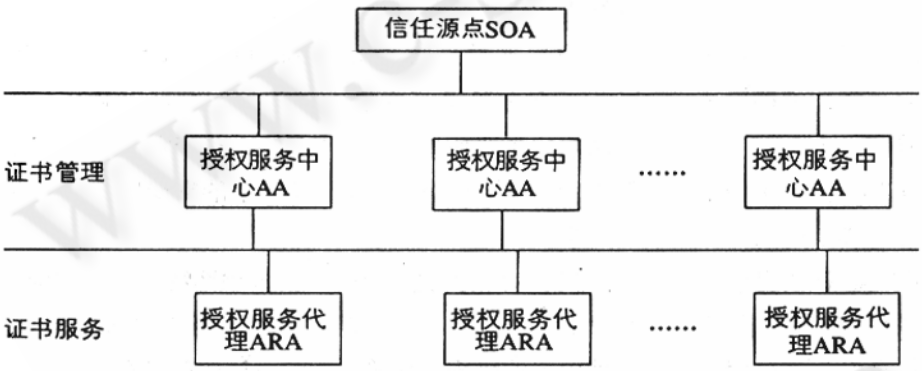

图 1　PMI 特权委托模型

2　基于授权管理基础设施的访问控制的实现

基于授权管理基础设施的集中式授权访问模型主要可分为如下三种：一是以数据资源为中心；二是以用户资源为中心；三是前两种方式的综合，也称为混合模式。这三种不同的实现模式是根据应用的不同情况和用户的要求来决定的。

2.1　以数据资源为中心的模式

这主要是为了支持完全基于 Web 的应用系统，而且需要进行权限控制的系统对权限控制的粒度较粗，是在文件一级的控制。这种方式的权限组织如图 2 所示。

以数据资源为中心的权限组织是通过基于角色的两次授权实现的：一是属性权威机构 AA 向用户发放属性证书，属性证书通过用户公钥证书的 ID 号将特定的用户角色绑定到对应的用户上，实现对用户的授权；二是由资源的所有者或管理者将一定的角色赋予资

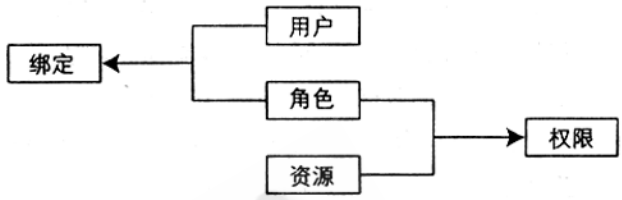

图 2　以数据资源为中心的权限组织

源，即通过表明哪些角色对特定的资源具有访问权限来实现对资源的授权。利用角色信息将两次授权的结果相关联就得到访问控制列表（ACL），从而实现用户到资源的访问控制。

这种方式的优点在于：所有的权限验证都是在应用系统之外进行的，不需要对应用系统内部做任何权限处理的工作。对于一些老的应用系统来说，如果此应用系统是完全基于 Web 的应用，或者原有的系统没有权限控制，需要增加权限控制，并且只要求将权限控制到文件一级，这种方式是最佳选择，因为不需要对原有的应用系统做任何改动，只需要在原有的系统之外增加此权限集中控制系统就可以达到权限集中控制的目的。

但是，这种方式也存在一个较大的缺点：权限控制粒度较粗，只能控制到文件一级。因此，如果原有的系统是建立在数据库基础上的，并且要求对权限的控制达到文件内容或数据字段，此方式就达不到要求。

另外，在这种方式下，用户的角色对所有的应用系统而言是固定的，也就是说，一旦用户的角色分配以后，除非重新分配，否则此用户的角色就是固定不变的。

2.2　以用户资源为中心的模式

这种方式主要是为了适应那些要求细粒度权限控制的需求而定制的，只对用户进行角色的分配，而权限的控制和验证是在应用系统内部完成的。这种方式的

权限组织如图 3 所示。

除了可以固定地对用户分配角色外，在应用系统内部还可以需要根据系统的流程动态分配当前用户的角色。

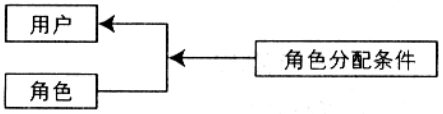

图 3 以用户资源为中心的权限组织

这种方式的优点有两个：一是能进行细粒度权限控制、二是能动态确定用户的角色。如果应用系统原来是通过用户名和口令的访问控制列表来实现权限控制的，可以通过对应用系统的修改来实现基于角色的集中统一管理，这样就能保证细粒度的权限控制。

但这种方式有一个最大的缺点是：需要在应用系统内部实现对权限的验证。如果系统是老的应用系统，则需要对原来的应用系统的结构或源代码进行修改。如果是新系统，则需要新系统通过权限集中管理系统提供的接口来实现权限的验证，并且需要按权限管理系统中的角色划分方式进行权限控制的验证。从上面的分析可以看出，这两种方式有着各自的优缺点，选择什么样的方式是由用户根据需求，并根据应用的具体情况来决定的。

2.3 混合模式

以数据资源为中心的权限管理和以用户资源为中心的权限管理方式各有优缺点。在实际应用中可以将以上两种方式综合运用，发挥二者的优点。

在权限管理系统中，可以对资源进行粗粒度的权限控制，然后在应用系统内部可以增加细粒度的权限控制，而且在应用系统内部是否进行细粒度控制是用户可以根据需求选择的。这种方式下的权限组织与以数据资源为中心的权限组织方式相同。只是数据资源可能是更粗粒度的，如系统、模块或目录，也可以是文件名等。

这种管理方式的优点是：可以灵活地控制用户对数据资源的访问权力。并且用户可以根据具体的情况分步骤实现系统，即可以首先进行粗粒度的权限控制，然后在此基础上通过对应用系统增加插件或修改系统实现更细粒度的权限控制。

同时这种实现方式也存在与以用户资源为中心的管理方式一致的缺点：当用户需要对数据资源进行细粒度权限控制时，必须对应用系统进行相应的修改。

参考文献

1 马爱国等，开放式属性证书及其权限认证策略，计算机工程，2004(10)。
2 许长枫、刘爱江、何大可，基于属性证书的 pmi 及其在电子政务安全建设中的应用，计算机应用研究，2004(1)。
3 姜楠、王健，电子政务中基于 PKI 的角色授权管理策略，通信技术，2003(9)。
4 国家信息安全工程技术研究中心，电子政务总体设计与技术实现，北京 电子工业出版社，2003(7)。
5 刘远航、崔维利，电子政务信息安全和 PKI/PMI 体系，网络安全技术与应用，2002(7)。