第5章 身份认证与访问控制技术

【本章学习目标】

- 理解身份认证的概念
- 了解常用身份认证方式
- 理解访问控制的概念
- 掌握自主访问控制、强制访问控制及基于角色的访问控制模式
- 了解数字签名的概念
- 掌握数字签名原理
- 掌握原文加密的数字签名实现方法

在当前开放式的网络环境中，任何在网络上的通信都可能遭到黑客的攻击，窃听机密消息，伪造、复制、删除和修改消息等攻击越来越多。所有的攻击都可能对正常通信造成破坏性的影响，给在线电子交易和网银的安全性带来极大的挑战。各种层出不穷的计算机犯罪案件引发了人们对网络身份的信任危机，证明访问用户身份及防止身份被冒名顶替变得极为重要。身份认证技术和访问控制技术是网络安全的最基本要素，是用户登录网络时保证其使用和交易“门户”安全的首要条件。

5.1 身份认证技术

5.1.1 身份认证概述

1. 身份认证概念

认证(Authentication)是指通过对网络系统使用过程中的主客体双方互相鉴别确认身份后，对其赋予恰当的标志、标签和证书等的过程。认证可以解决主体本身的信用问题和客体对主体访问的信任问题。认证可以为下一步的授权奠定基础，是对用户身份和认证信息的生存、存储、同步、验证和维护的全生命周期的管理。

身份认证(Identity and Authentication Management)是网络用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的过程。

2. 身份认证作用

在网络系统中，身体认证是网络安全中的第一道防线，极为重要，是其他安全机制的基石。如图5-1所示，用户在访问系统前，先要经过身份认证系统进行身份识别，可以通过访问监控设备(系统)，根据用户的身份和授权数据库，确定所访问系统资源的权限。授权数据

库由安全管理员按照需要配置。审计系统根据设置记载用户的请求和行为。访问控制和审计系统都依赖于身份认证系统提供的“认证信息”鉴别和审计。

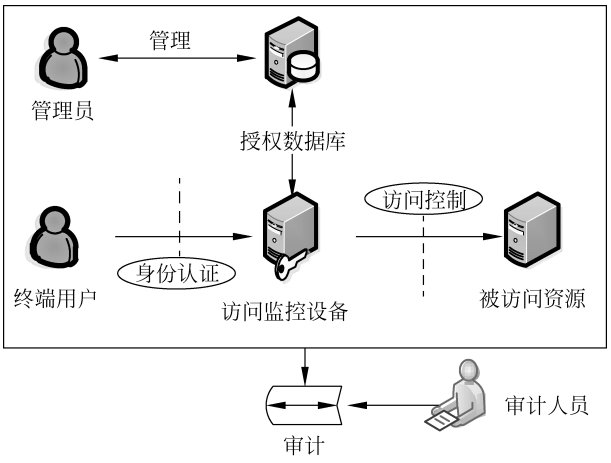


图 5-1　身份认证和访问控制过程

5.1.2　身份认证方式

网络系统中常用的身份认证方式主要有静态密码认证、动态口令认证、USB Key 认证、生物识别认证和 CA 认证等。

1. 静态密码认证

静态密码方式是指以用户名及密码认证的方式，是最简单、应用最广泛的身份认证方法。所有用户的密码由用户自己设定，只有用户本人知道。只要能够正确输入密码，信息系统就认为操作者是合法用户，其安全性在很大程度上依赖于密码强度。实际上，很多用户为了方便起见，经常使用生日、电话号码等具有用户自身特征的字符串作为密码，为系统安全留下隐患。同时，由于密码是静态数据，在验证过程中需要在网络介质中传输，很容易被木马程序或监听设备截获。因此，用户名及密码方式是安全性比较低的身份认证方式。

2. 动态口令认证

动态口令是应用较广的一种身份认证方法，采用哈希算法产生。基于动态口令的认证方式主要有动态短信密码和动态口令牌两种方式。口令一次一密，每次登录都用不同的密码，可以避免口令丢失的逻辑漏洞。前者是将系统发给用户注册手机的动态短信密码进行身份认证，后者则以发给用户动态口令牌进行认证，如图 5-2 所示。动态口令认证方式不需要用户定期修改密码，无须担心密码泄露，该认证方式广泛应用在 VPN、网上银行及电子商务等领域。

3. USB Key 认证

USB Key(U 盾)认证方式近几年得到了广泛应用。它主要采用软硬件相结合、一次一密的强双因素认证模式，很好地解决了安全性与易用性之间的矛盾。该方式以一种 USB 接口的硬件设备，内置单片机或智能卡芯片，可存储用户的密钥或数字证书，利用其内置的密码算法实现对用户身份的认证。其身份认证系统主要有两种认证模式：基于冲击/响应模式和基于 PKI 体系的认证模式。常用的网银 USB Key 如图 5-3 所示。

图 5-2　动态口令牌

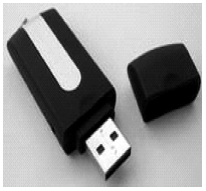


图 5-3　网银 USB Key

4. 生物识别认证

生物识别认证是指通过可测量的生物信息和行为等特征进行身份认证的一种技术。认证系统测量的生物特征一般是用户唯一生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括指纹、掌形、视网膜和 DNA 等；行为特征包括签名、语音和行走步态等。

5. CA 认证

CA(Certification Authority)是国际认证机构的通称，是对申请用户进行发放、管理、校验或取消数字证书的机构。CA 认证用于审查证书持有者身份的合法性，并签发管理证书，以防止证书被伪造或篡改。如表 5-1 所示，其发放、管理和认证是一个复杂的过程，即 CA 认证过程。

表 5-1　证书的类型与作用

证书名称	证书类型	主要功能描述
个人证书	个人证书	个人网上交易、网上支付、电子邮件等
单位证书	单位身份证书	用于企事业单位网上交易、网上支付等
	E-mail 证书	用于企事业单位内安全电子邮件通信
	部门证书	用于企事业单位内某个部门的身份认证
服务器证书	企业证书	用于服务器、安全站点认证等
代码签名证书	个人证书	用于个人软件开发者对其软件的签名
	企业证书	用于软件开发企业对其软件的签名

CA 作为网络安全可信认证及证书管理机构，其主要职能是管理和维护所签发的证书，并提供各种证书服务，包括证书的签发、更新、回收和归档等。CA 系统的主要功能是管理其辖域内的用户证书，因此，CA 系统功能及 CA 证书的应用将围绕证书进行具体的管理。

5.1.3　身份认证系统

身份认证系统的组成一般包括三个部分：认证服务器、认证系统客户端和认证设备。认证系统主要通过身份认证协议和认证系统软硬件来实现。其中，身份认证协议又分为单向认证协议和双向认证协议。若通信双方只需一方鉴别另一方的身份，则称为单项认证协议；如果双方都需要验证身份，则称为双向认证协议。

AAA(Authentication，Authorization，Accounting)认证系统现阶段应用最为广泛。其中，认证(Authentication)是验证用户身份与可使用网络服务的过程，授权(Authorization)是依据认证结果开放网络服务给用户的过程，审计(Accounting)是记录用户对各种网络操作及服务的用量并进行计费的过程。

5.1.4 身份认证方法

在网络系统中，各用户以数字认证方式确定身份。网络中的各种资源通过认证机制来实现安全保护。认证机制与授权机制经常结合在一起，通过认证的用户才可获得使用权限。互联网最常用的认证方法有固定口令、一次性口令、双因素安全令牌和单点登录等。

1. 固定口令

固定口令认证是网络中最常用的认证系统，是一种以检验用户设定的固定字符串来进行系统认证的方式。当通过网络访问系统资源时，系统要求输入用户名和密码。在账户和密码被确认后，用户便可访问授权的资源。这种认证方式简单，但由于其相对固定，很容易受到多种攻击。而且很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，很容易分辨出某种特定系统的认证数据，并提取出用户名和密码。

2. 一次性口令

为了提高固定口令的安全性，出现了一次性口令(One Time Password，OTP)认证体制，即在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，从而提高系统安全性。一次性口令认证系统的组成如下。

(1) 生成不确定因子。常用的生成不确定因子的方式有三种：口令序列方式、挑战/回答方式和时间同步方式。

(2) 生成一次性口令。利用不确定因子生成一次性口令的方式有以下两种。

① 硬件卡。在具有计算功能的硬件卡上输入不确定因子，卡中集成的计算逻辑对输入数据进行处理，并将结果反馈给用户作为一次性口令。基于硬件卡的一次性口令大多属于挑战/回答方式，一般配备有数字按键，便于不确定因子的输入。

② 软件。与硬件卡基本原理类似，以软件代替其计算逻辑。软件口令生成方式及灵活性较高，某些软件还可限定用户登录的地点。

3. 双因素安全令牌

双因素身份认证系统由身份认证服务器、安全令牌、认证代理、认证应用开发包等几部分组成。身份认证服务器提供数据存储、AAA 服务、管理等功能，是整个系统的核心部分。安全令牌是重要的双因素认证方式，系统提供多种形式的安全令牌，供不同用户选用。

双因素安全令牌用于生成用户当前登录的动态口令，采用加密算法及可靠设计，可防止读取密码信息。该令牌每 60s 得到一个新动态口令显示在液晶屏上，动态口令具有极高的抗攻击性。

4. 单点登录

单点登录(Single Sign On，SSO)也称单次登录，是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统，安全凭证可以在不同的应用系统中共享，是目前比较流行的企业业务整合的解决方案之一。其中，对网络服务器认证由专门的认证服务器负责，并且统一对登录用户授权。

单点登录与传统的登录相比较，优势主要体现在以下 5 个方面。

(1) 管理简单。现有的操作系统实现中，SSO 的相关任务可以作为日常维护工作的一部分，使用与其他任务管理相同的工具来执行。

(2) 管理控制便捷。Windows 中所有的网络管理信息，包括 SSO 的特定信息，都存放

在一个用 Active Directory 组织的存储库中。对每个用户的权限与特权，仅有一个授权列表，使管理员在更改或维护用户特权后，可将结果传送到整个网络系统。

(3) 用户使用简便。用户不用多次登录，也无须在访问网络资源时记住很多密码。

(4) 安全性更高。SSO 可用的方法都提供用户身份验证，并为用户与网络资源的会话加密奠定了基础。它不仅取消了多次访问密码，还降低了用户习惯写或多次输入密码而被盗用密码的危险。此外，由于将网络管理信息并入存储库，管理员还可确认所禁用的用户账号，从而使网络系统的安全性更高。

(5) 合并异构网络。通过连接各种网络，相关的网络管理工作也可以进行合并，从而优化了管理，实现整个系统安全策略统一实施。

5.2 访问控制技术

如果说身份证认证技术解决了用户是“谁”的问题，那么用户“能够做什么”则是由访问控制决定的。访问控制技术作为国际标准化组织定义的 5 项标准安全服务之一，是实现信息系统安全的一项重要机制。美国国防部的可信计算机系统评估标准把访问控制作为评价系统安全的主要指标之一，因此，访问控制对提高系统安全的重要性是不言而喻的。

5.2.1 访问控制概述

1. 访问控制概念

访问控制(Access Control)指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源的能力，通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。访问控制包括以下三个要素。

(1) 主体 S(Subject)。指一个提出请求或要求的实体，是动作的发起者，但不一定是动作的执行者。主体可以是某个用户，也可以是用户启动的进程、服务和设备。

(2) 客体 O(Object)。是授受其他实体访问的被动实体。客体的概念也很广泛，凡是可以被操作的信息、资源、对象都可以认为是客体。在信息社会中，客体可以是信息、文件、记录等的集合体，也可以是网络的硬件设施，无线通信中的终端，甚至一个客体可以包含另一个客体。

(3) 控制策略 A(Attribution)。是主体对客体的访问规则集，即属性集合。访问策略实际上体现了一种授权行为，也就是客户对主体的权限允许。

2. 访问控制作用

访问控制的主要作用是，保证合法用户访问受权保护的网络资源，防止非法的主体进入受保护的网络资源，并防止合法用户对受保护的网络资源进行非授权的访问。

访问控制组件包括了 4 个部分：发起者(initiator)、访问控制执行功能(Access Control Enforcement Function，AEF)、访问控制决策功能(Access Control Decision，ADF)以及目标(target)。如图 5-4 所示，发起者是指信息系统中系统资源的使用者，是访问控制系统中的主体。目标是指被发起者访问或试图访问的基于计算机或通信的实体，是访问控制系统中的客体。AEF 的功能是负责建立起发起者与目标之间的通信桥梁，它必须按照 ADF 的授权

查询指示来实施上述动作。即当发起者对目标提出执行操作要求时，AEF 会将这个请求信息通知 ADF，并由 ADF 作出是否允许访问的判断。在信息系统中，ADF 是访问控制的核心。当 ADF 对发起者提出的访问请求进行判断时，所依据的是一套访问控制策略和上下文信息。

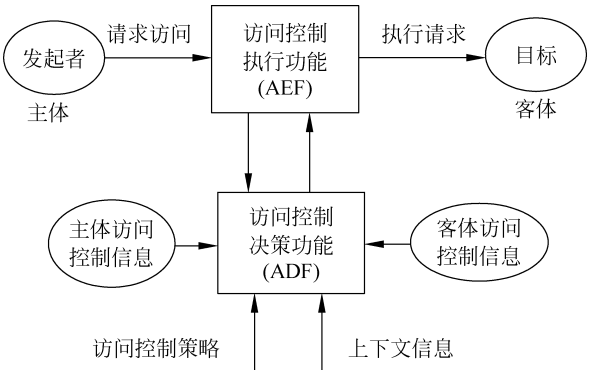


图 5-4　访问控制作用

3. 访问控制模式

主要的访问控制模式有三种，即自主访问控制、强制访问控制和基于角色的访问控制。

(1) 自主访问控制(Discretionary Access Control，DAC)。指资源的所有者决定是否允许特定的人访问资源，类似于目前大多数企业系统管理采取的做法。这种访问控制模式的有效性依赖于资源的所有者对企业安全政策的正确理解和有效落实。

(2) 强制访问控制(Mandatory Access Control，MAC)。指定义几个特定的信息安全级别，将资源归属于这些安全级别中。主体的权限取决于其访问许可等级。

(3) 基于角色的访问控制(Role-Based Access Control，RBAC)。指主体基于特定的角色访问客体，操作权限定义在角色当中。

5.2.2　自主访问控制

自主访问控制最早出现在 20 世纪 70 年代初期的分时系统中，它是多用户环境下最常用的一种访问控制技术，也是目前计算机系统中实现最多的访问控制机制。在自主访问控制的机制下，客体的拥有者全权管理有关该客体的访问授权，有权泄露、修改该客体的有关信息。也就是说，允许某个主体显式地指定其他主体对该主体所拥有的信息资源是否可以访问以及可执行的访问类型。因此自主访问控制又被称为基于拥有者的访问控制。

自主访问控制一般采用访问控制矩阵、访问控制列表和访问控制能力列表三种机制来存放不同主体的访问控制权限，从而完成对主体访问权限的限制。

实现自主访问控制最直接的方法是利用访问控制矩阵。访问控制矩阵的每一行表示一个主体，每一列表示一个受保护的客体，矩阵中的元素表示主体可对客体进行的访问模式(例如读、写、执行、修改、删除等)。

表 5-2 是一个自主访问控制矩阵的示例，表中的 John、Alice、Bob 是三个主体，客体有 4 个文件和两个账户。需要指出的是，Own 的确切含义可能因不同的系统而异，通常一个文件的 Own 权限可以授予或者撤销其他用户对该文件的访问控制权限。例如 John 拥有文件 1 的 Own 权限，他就可以授予 Alice 读或者 Bob 读、写的权限，也可以撤销赋给他们的权限。

表 5-2　访问控制矩阵示例

	文件 1	文件 2	文件 3	文件 4	账户 1	账户 2
John	Own R W		Own R W		Inquiry Credit	
Alice	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
Bob	R W	R		Own R W		Inquiry Debit

访问控制矩阵虽然直观，但是我们可以发现并不是每个主体和客体之间都存在着权限关系。相反，实际的系统中虽然可能有很多的主体和客体，但主体和客体之间的权限关系可能并不多，这样就存在着很多的空白项。因此在实现自主访问控制时，因为将矩阵整体地保存起来效率会很低，所以通常不这么做。实际的方法是基于矩阵的行（主体）或列（客体）来表示访问控制信息。

1. 基于行的自主访问控制

基于行的自主访问控制是在每个主体上都附加一个该主体可访问的客体的列表。根据列表的内容不同，又有不同的实现方式。主要利用能力表（capability list）、前缀表（profiles list）和口令（password）来实现。其中最常用的方法是利用能力表实现。能力决定用户是否可以对客体进行访问以及进行何种模式的访问，拥有相应能力的主体可以以给定的模式访问客体。

如图 5-5 所示，在访问控制能力表中，由于它着眼于某一主体的访问权限，以主体为出

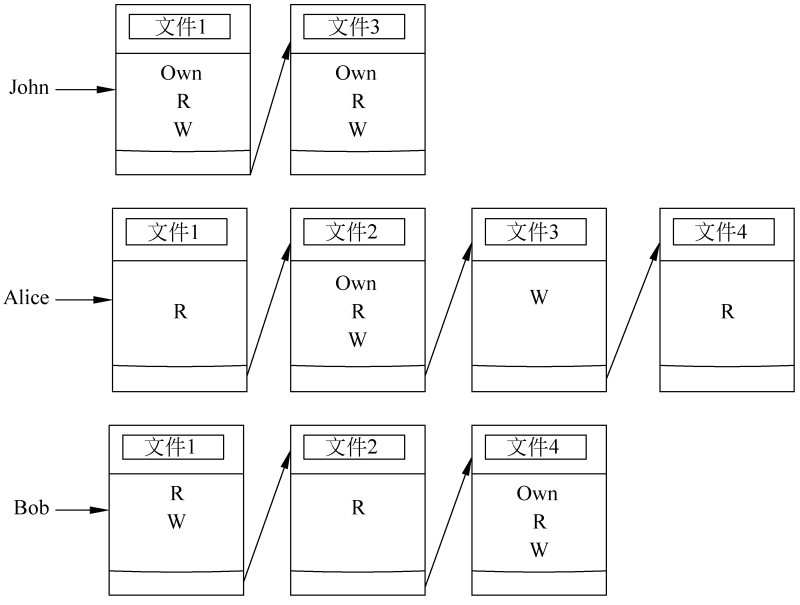


图 5-5　访问控制能力表示意图

发点描述控制信息，因此很容易获得一个被主体授权可以访问的客体及其权限，但是如果要求获得对于某一特定权限的所有主体会比较困难。而且当一个客体被删除之后，系统必须在每个客户的表上清除该客体相应的条目。

2. 基于列的自主访问控制

在基于列的自主访问控制中，每个客体都附加一个可访问它的主体明细表。基于列的自主访问控制最常用的实现方式是访问控制列表。

访问控制列表(Access Control List，ACL)是实现基于列的自主访问控制采用最多的一种方式。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。图 5-6 所示为访问控制列表的示例。

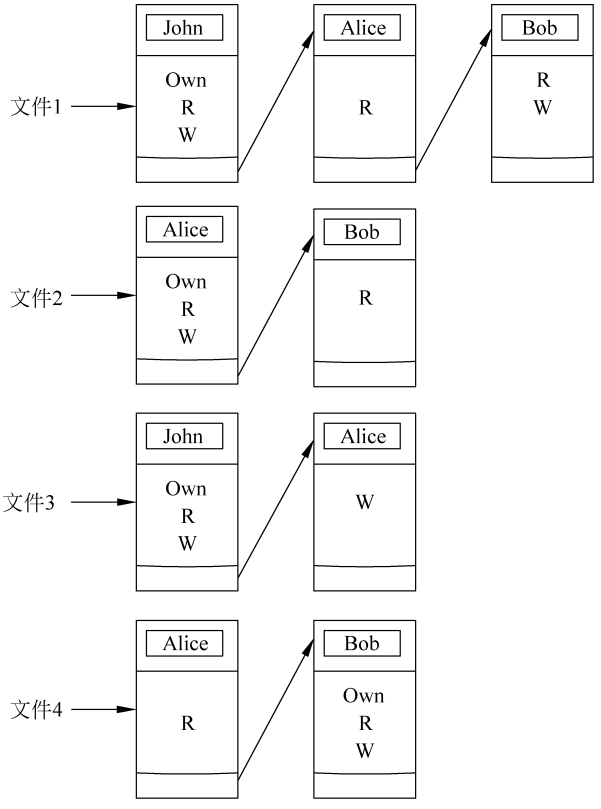


图 5-6　访问控制列表示意图

ACL 的优点在于表述直观，易于理解，而且比较容易查出对某一特定资源拥有访问权限的所有用户，可以有效地实施授权管理。在一些实际应用中，还对 ACL 做了扩展，从而进一步控制用户的合法访问时间，决定是否需要审计等。

尽管 ACL 灵活方便，但将它应用到网络规模较大、需求复杂的企业内部网络时，ACL 需对每个资源指定可以访问的用户或组以及相应的权限。当网络中资源很多时，需要在 ACL 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。另外，在许多组织中，服务器一般是彼此独立的，各自设置自己的 ACL。为了实现整个组织范围内的一致的控制策略，需要各管理部门的密切合作。所有这些使得访问控制的授权管理变得费力而烦琐，且容易出错。

上述两种自主访问控制方法都存在一些局限性，主要体现在：资源管理比较分散；用户间的关系不能在系统中体现出来，不易管理；信息容易泄露，无法抵御特洛伊木马的攻击。在自主访问控制下，一旦带有特洛伊木马的应用程序被激活，特洛伊木马可以任意泄露和破坏接触到的信息，甚至改变这些信息的访问控制模式。

在自主访问控制系统中，一个拥有一定访问权限的主体可以直接或间接地将权限传给其他主体。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访问控制。另外，在许多组织中，用户对自己所能访问的资源并不具有所有权，组织本身才是系统中资源的真正所有者。各组织一般希望访问控制与授权机制的实现结果能与组织内部的规章制度相一致，并且由管理部门统一实施访问控制，不允许用户自主地处理，显然，自主访问控制已不能适应这些需求。

5.2.3 强制访问控制

顾名思义，强制访问控制是“强加”给访问主体的，即系统强制主体服从访问控制策略。

强制访问控制的基本思想是：每个主体都有既定的安全属性，每个客体也都有既定安全属性，主体对客体是否能执行特定的操作，取决于二者安全属性之间的关系。这些安全属性是不能改变的，它是由管理部门（如安全管理员）自动地按照严格的规则来设置，不像访问控制列表那样可以由用户直接或间接地修改。当主体对客体进行访问时，根据主体的安全属性和访问方式，比较主体的安全属性和客体的安全属性，从而决定是否允许主体的访问请求。主体不能改变自身的或任何客体的安全属性，包括不能改变属于用户的客体的安全属性，而且主体也不能将自己拥有的访问权限授予其他主体。

强制访问控制和自主访问控制是两种不同类型的访问控制机制，它们常结合起来使用。仅当主体能够同时通过自主访问控制和强制访问控制检查时，它才能访问一个客体。利用自主访问控制，用户可以有效地保护自己的资源，防止其他用户的非法获取；而利用强制访问控制可提供更强有力的安全保护，使用户不能通过意外事件和有意识的误操作逃避安全控制。强制访问控制特别适用于多层次安全级别的军事应用，也适用于政府部门、金融部门等。

安全级由以下两方面的内容构成。

（1）保密级别：又叫敏感级别，可以分为绝密级、机密级、秘密级、无密级等。

（2）范畴集：指在组织系统中，根据人员的不同职能所划分的不同领域。如人事处、财务处等。

安全级包括一个保密级别和任意多个范畴。安全级通常写成保密级别后跟随一个范畴集的形式，如{机密：人事处，财务处}；范畴集可以为空。

在安全级中保密级别是线性排列的，例如，无密＜秘密＜机密＜绝密；范畴集则是互相独立和无序的，两个范畴集之间的关系是包含、被包含或无关。

强制访问控制最主要的优势在于它有阻止特洛伊木马的能力。特洛伊木马是在执行某些合法功能的程序中隐藏的代码，它利用运行此程序的主体的权限违反安全策略，通过伪装成有用的程序在进程中泄露信息。

阻止特洛伊木马的策略是基于非循环信息流，所以在一个级别上读信息的主体一定不能在另一个违反非循环规则的安全级别上写信息。所谓上读，指的是低级别的用户能够读高敏感度区域，下读指低级别用户只能读更低级别的敏感信息，不能读高级别敏感信息。所

谓上写，指的是不允许高敏感的信息写入低敏感区域，下写则允许高敏感度的信息写入低敏感区域。一般用上读/下写来保证数据完整性及利用下读/上写来保证数据的机密性，同样，在一个安全级别上写信息的主体也一定不能在另一个违反非循环规则的安全级别上读信息。由于强制访问控制策略是通过梯度安全标签实现信息的单向流通，所以它可以很好地阻止特洛伊木马的泄密。

强制访问控制的主要缺陷在于实现工作量太大，不够灵活。而且强制访问控制过于偏重保密性，对其他方面如系统连续工作能力、授权的可管理性等考虑不足。

5.2.4 基于角色的访问控制

随着网络技术的发展，网络应用系统所面临的一个难题就是如何对日益复杂的数据资源进行安全管理。传统的访问控制技术都是由主体和访问权限直接发生关系，在实际应用中，当主体和客体的数目都非常大时，传统访问控制技术已远远不能胜任复杂的授权管理的要求。

目前，大部分信息资源服务器对信息没有进行统一管理，特别是没有根据信息的安全要求来进行管理。有些资源服务器虽然采取了一些诸如身份认证、访问控制等安全策略，但由于管理的力度太弱，无法做到对资源的全面控制。还有些资源服务器根据信息的秘密程度分为未知、普通、秘密、机密、绝密 5 级，然后给用户赋予访问权限，这种方式在一定程度上能解决信息的非授权访问问题，但这种方式往往会出现为用户分配的权限比它实际应该具有的权限要大的情况，即没有实现最小特权机制。这些问题都给信息资源的安全留下了重大隐患。

近年来，为了满足新的安全需求，各国学者对访问控制技术进行了大量研究。一方面，对传统访问控制技术的不足进行改进；另一方面，研究新的访问控制技术以适应当前计算机信息系统的安全需求，从而产生了一些更为灵活的访问控制技术。其中，基于角色的访问控制的应用最为广泛。RBAC 的概念早在 20 世纪 90 年代就已经提出，但在相当长的一段时间内没有得到人们的重视。进入 20 世纪 90 年代，安全需求的发展使得 RBAC 又引起人们极大的关注。目前美国的很多学者和研究机构都在从事这方面的研究，NIST(National Institute of Standard Technology)的研究人员认为 RBAC 将成为 DAC 和 MAC 的替代者。

RBAC 的核心思想是将访问权限与角色相联系，通过给用户分配合适的角色，让用户与访问权限相关联。角色是根据企业内为完成各种不同的任务需要而设置的，根据用户在企业中的职权和责任来设定他们的角色。用户可以在角色间进行转换，系统可以添加、删除角色，还可以对角色的权限进行添加、删除。通过应用 RBAC，可以将安全性放在一个接近组织结构的自然层面上进行管理。因此，在 RBAC 中，可以根据组织结构中不同的职能岗位划分角色，资源访问权限被封装在角色中，用户通过赋予的角色间接地访问系统资源，并可对系统资源进行许可范围内的操作。

如图 5-7 所示，RBAC 包含三个实体：用户(user)、角色(role)和权限(privilege)。

用户是对数据对象进行操作的主体，可以是人或计算机等。权限表示对系统中客体进行特定模式访问的操作许可，即对某一数据对象的可操作权利。对数据库系统而言，数据对象可以是表、视图、字段、记录，相应的操作有读、插入、删除和修改等。一项许可就是可以对某一个数据对象进行某一种特定操作的权利。

在 RBAC 中，角色对应于组织中某一特定的职能岗位，具有处理某些事物的许可。这与实际生活中的角色很相似，以学校为例，角色可以是校长、处长、科长、教师、学生等，不过

在 RBAC 中的角色与实际的角色概念有所不同。在一个 RBAC 模型中，一个用户可以被赋予多个角色，一个角色也可以对应多个用户，这些角色是根据系统的具体实现来定义的。同样的一个角色可以拥有多个权限，一个权限也可以被多个用户所拥有。这样在权限管理中，角色作为中间桥梁把用户和权限联系起来，一个角色与若干个权限关联可以看作是该角色拥有的一组权限集合，与用户关联也可以看作是若干具有相同身份的用户集合。

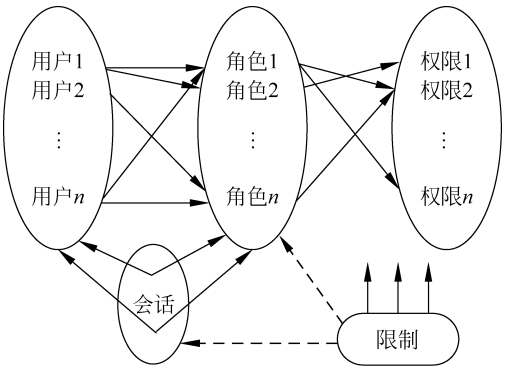


图 5-7　用户、角色和权限的关系图

会话是一个动态的概念，一次会话是用户的一个活跃进程，代表用户与系统进行的一次交互。用户与会话是一对多关系，一个用户可同时打开多个会话。在 RBAC 中，在用户和访问权限之间引入角色的概念。用户与特定的一个或多个角色相联系，角色与一个或多个权限相联系，角色可以根据实际的工作需要生成或取消，而且登录到系统中的用户可根据自己的需要动态激活自己拥有的角色，从而避免用户无意中危害系统安全。除此之外，角色之间、权限之间、角色和权限之间定义了一些关系，如角色间的层次性关系，而且也可以按需要定义各种约束，如定义出纳和会计这两个角色为互斥角色（即这两个不能分配给一个用户）。

从图 5-7 中，我们不难理解角色之间有重叠，如果将重叠部分设置为一个角色 R，其他角色既包含该角色 R 也包含自己的私有部分，这样就产生了角色层次。例如，处长的权限包括了他所主管的各科长的权限，科长的权限包括了其属下各科员的权限。

约束是施加于单个角色之上或多个角色之间的，用来表达权限的执行是有条件的。最常见的约束有基数约束即可被赋予某特定角色的用户数目的约束；或者是用户分配阶段有些权限不能同时被同一个用户获得的静态责任互斥。

用户所执行的操作与其所扮演的角色的职能相匹配，这正是 RBAC 的根本特征。即依据 RABC 策略，系统定义了各种角色，每种角色可以完成一定的职能。不同的用户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体之间无直接联系，他只有通过角色才能享有该角色所对应的权限，从而访问相应的客体，因此用户不能自主地将访问权限授予别的用户，这是 RBAC 与 DAC 的根本区别所在。RBAC 与 MAC 的区别在于，MAC 是基于多级安全需求的，而 RBAC 不是，因为军用系统中主要关心的是防止信息从高安全级流向低安全级，重点考虑的是信息的机密性，而基于角色控制的系统中主要关心的是保护信息的完整性。

综上所述，RBAC具有以下特点。

(1) 以角色作为访问控制的主体。用户以什么样的角色对资源进行访问，决定了用户拥有的权限以及可执行何种操作。RBAC的基本思想是：授权给用户的访问权限通常由用户在一个组织中担当的角色来确定。传统的访问控制是将主体和受控客体直接相联系，而RBAC在主体与客体之间加入了角色，通过角色沟通主体与客体。这样分层的优点是当主体发生变化时，只需修改主体与角色之间的关联，而不必修改角色与客体的关联。

(2) 角色继承。RBAC中利用角色之间的层次关系提高授权效率，避免相同权限的重复设置。RBAC采用了“角色继承”的概念，角色继承是指角色不仅具有直接为其分配的权限，还可以继承其他角色的权限。角色继承把角色组织起来，能够很自然地反映组织内部人员之间的职权、责任关系。

角色继承可以用父子关系来表示。如图5-8所示，角色2是角色1的“父亲”，它包含角色1的属性与权限。在角色继承关系图中，处于最上面的角色拥有最大的访问权限，越下端的角色拥有的权限越小。

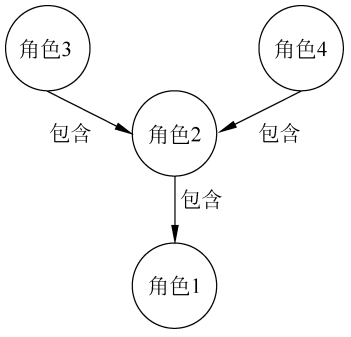


图5-8　角色的继承关系示意图

(3) 最小特权原则。所谓最小特权原则(least privilege policy)是：用户所拥有的权力不能超过他执行工作时所需的权限。实现最小特权原则，需分清用户的工作内容，确定执行该项工作的最小权限，然后将用户限制在这些权限范围之内。在RBAC中，可以根据组织内的规章制度、职员的分工等设计拥有不同权限的角色，只有角色需要执行的操作才授予给角色。当一个主体准备访问资源时，如果该操作不在主体当前活跃角色的授权操作之内，该访问将被拒绝，由此体现了最小特权原则。

5.3　数字签名技术

5.3.1　数字签名概述

在实际网络通信中，用户可能受到来自多方面的攻击。在现实环境中，可以通过当面交易的方式或者通过手写签名盖章的方式来解决通信双方的欺骗和抵赖行为。但在网络环境中，每个人都是虚拟的，如何能够实现同现实中手写签名类似的功能？这就是数字签名要解决的问题，在了解数字签名概念之前，先看下面的例子。

用户A与B相互之间要进行通信，双方拥有共享的会话密钥K，在通信过程中可能会遇到以下问题：

A伪造一条信息，并称该消息来自于B。A只需要产生一条伪造的消息，用A和B的共享密钥通过哈希算法产生认证码，并将认证码附于消息之后。由于哈希算法的单向性和密钥K是共享的，因此无法证明该消息是A伪造的。

B可以否认曾经发送过某条消息。因为任何人都有办法伪造消息，所以无法证明B是否发送过该消息。

上述例子说明使用哈希算法可以进行报文鉴别，但无法阻止通信用户的欺骗和抵赖行

为。因此，当通信双方不能相互信任的情况下，需要用除了报文鉴别以外的技术来防止类似的抵赖和欺骗行为。

1. 数字签名概念

数字签名(Digital Signature)指用户用私钥对原始数据加密所得的特殊数字串，用于保证信息来源的真实性、数据传输的完整性和防抵赖性。数字签名在电子银行、证券和电子商务等方面应用非常广泛，如汇款、转账、订货、票据、股票成交等。用户以电子邮件等方式，使用个人私有密钥加密数据或选项后，发送给接收者。接收者用发送者的公钥解开数据后，就可确定数据源。数字签名同时也是对发送者发送信息真实性的证明，发送者对所发送的信息不可抵赖。

2. 数字签名功能

(1) 签名是可信的。文件的接收者相信签名者是慎重地在文件上签名的。

(2) 签名是不可抵赖的。发送者事后不能抵赖对报文的签名，可以核实。

(3) 签名不可伪造。可以证明是签字者而不是其他人在文件上签字。

(4) 签名不可重用。签名是文件的一部分，不可将签名移动到其他的文件。

(5) 签名不可变更。签名和文件不能改变，也不可分离。

(6) 数字签名有一定的处理速度，能够满足所有的应用需求。

3. 数字签名种类

1) 手写签名或印章的识别

将手写签名或印章作为图像，用光扫描经光电转换后在数据库中加以存储。当验证手写签名或印章时，也用光扫描输入，并将原数据库中的对应图像调出，用模式识别的数学计算方法对两者进行比对，以确认该签名或印章的真伪。这种方法曾经在银行会计柜台使用过，但由于需要大容量的数据库存储，而且每次手写签名和印章存在差异，实用性不强，也不适合在互联网上传输。

2) 生物识别

生物识别技术是利用人体生物特征进行身份认证的一种技术。生物特征是一个人与他人不同的唯一表征，可以测量、自动识别和验证。生物识别系统对生物特征进行取样，提取其唯一的特征进行数字化处理，转换成数字代码，并进一步将这些代码组成特征模板存储在数据库中。人们同识别系统交互进行身份认证时，识别系统获取其特征并与数据库中的特征模板进行比对，以确定是否匹配，从而决定确认或否认此人。生物识别技术主要包括指纹、声音、人像、掌形、视网膜、虹膜、脸型、DNA 和多种方法综合等识别技术。

3) 密码、密码代号或个人识别码

密码、密码代号或个人识别码主要是指用一种传统的对称密钥加/解密的身份识别和签名方法。甲方需要乙方签名一份电子文件，甲方可产生一个随机码传送给乙方，乙方用事先双方约定好的对称密钥加密该随机码和电子文件后回送给甲方，甲方用同样的对称密钥解密后得到电文并核对随机码，如随机码核对正确，甲方即可认为该电文来自乙方。

4) 基于量子力学的计算机

基于量子力学的计算机被称为量子计算机，是以量子力学原理直接进行计算的计算机，比传统的图灵计算机具有更强大的功能，其计算速度比现代的计算机快几亿倍。量子计算机对目前采用的密码技术提出了挑战，它采用一种新的量子密码方式，即利用光子的相位特性编码。传统密码在被窃听者破解时不留下痕迹，但这种密码不同，由于量子力学的随机性

非常特殊，无论多么聪明的窃听者，在破译这种密码时都会留下痕迹，甚至在密码被窃听的同时会自动改变。这将是世界上最安全的密码认证和签名方法，然而，这种量子计算机或光子计算机还只处于研究阶段，没有被广泛应用。

5）基于 PKI 的电子签名

基于 PKI 的电子签名就是数字签名。由于电子签名虽然获得了技术中立性，但使用却不方便，法律上又对电子签名做了进一步规定，如联合国国际贸易法委员会的《电子签名示范法》和欧盟的《电子签名共同框架指令》中就规定了“可靠电子签名”和“高级电子签名”，实际上就是规定了数字签名的功能，这种规定使数字签名获得了更好的应用安全性和操作性。目前，具有实际意义的电子签名只有公钥密码理论，所以目前国内外普遍使用的还是基于 PKI 的数字签名。作为公钥基础设施，PKI 可提供多种网上安全服务，如认证、数据保密性、数据完整性和不可否认性，这些都采用了数据签名技术。

5.3.2 数字签名过程及实现

对一个电子文件进行数字签名并在网上传输，通常需要的技术实现过程包括上网身份认证、进行签名和对签名的认证。

1. 身份认证的实现

PKI 提供的服务首先是认证，即身份识别与鉴别，就是确认实体（用户或所用主机的操作设备或邮箱）即为自己所声明的实体。认证的前提是双方都具有第三方 CA 所签发的证书，认证分为单向认证和双向认证。

1）单向认证

双方在网上通信时，甲只需要认证乙的身份。这时甲需要获取乙的证书。获取证书的方式有两种，一种是在通信时乙直接将证书传给甲，另一种是甲向 CA 的目录服务器查询索取。甲获得乙的证书后，先用 CA 的根证书公钥验证该证书的签名，验证通过说明该证书是第三方 CA 签发的有效证书，然后检查证书的有效期、时效性（LRC 检查）及黑名单。

2）双向认证

双方在网上通信时，双方互相认定身份。其认证过程的各方都与上述单向认证过程相同。双方采用轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）在网上查询对方证书的有效性及黑名单。

2. 数字签名原理

在互相认证身份后，网上通信的双方即可发送签名的数据电文。数字签名过程分为两部分：签名过程和验证过程，如图 5-9 所示。发送方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密求得数字签名，然后将原文与数字签名一起发送给接收方。接收方验证签名，即用发送方公钥解密数字签名，得出数字摘要。接收方将原文采用同样的哈希算法又得一个新的数字摘要，将两个数字摘要进行比较，如果两者匹配，说明经数字签名的电子文件传输成功。

3. 数字签名的签名过程

数字签名的签名过程如图 5-10 所示，需要有发送方的签名证书的私钥及其验证公钥。数字签名具体的实际操作过程为：生成被签名的电子文件后，对电子文件用哈希算法做数字摘要，再对数字摘要用签名私钥做非对称加密，即做数字签名；将以上的签名、电子文件原文及签名证书的公钥一起封装，形成签名结果发送给接收方验证。

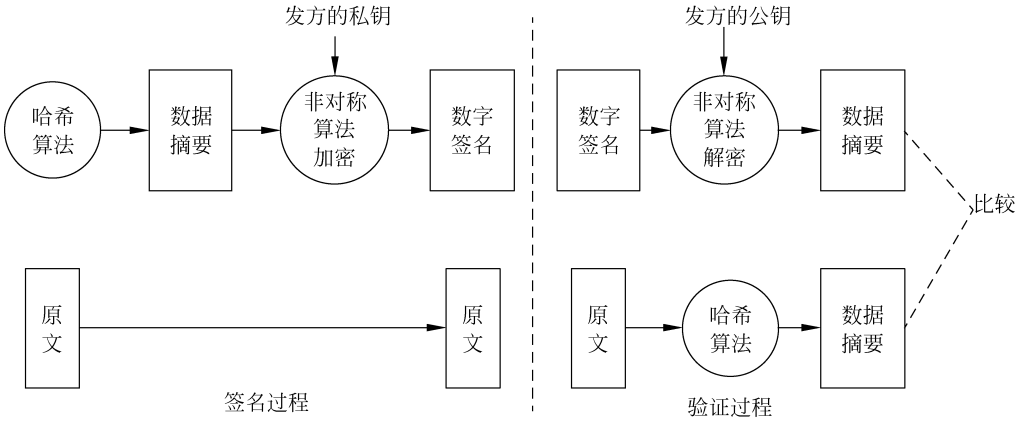


图 5-9　数字签名原理

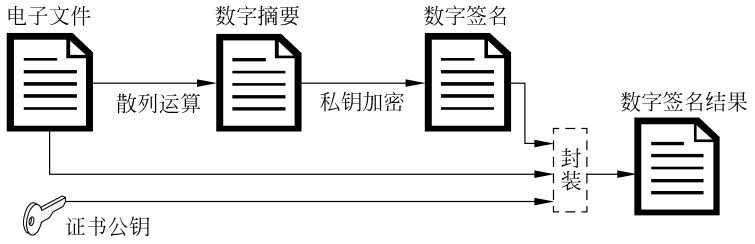


图 5-10　签名过程

4. 数字签名的验证过程

接收方收到发送方的签名后进行签名验证，其具体操作过程如图 5-11 所示，接收方收到数字签名的结果，即待验证的数据，包括数字签名、电子原文和发方公钥。然后，接收方用发送方公钥解密数字签名，导出数字摘要，并对电子文件原文做同样的哈希算法得到一个新的数字摘要，将两个摘要的散列值进行比较，若结果相同则说明签名得到验证，否则签名无效。

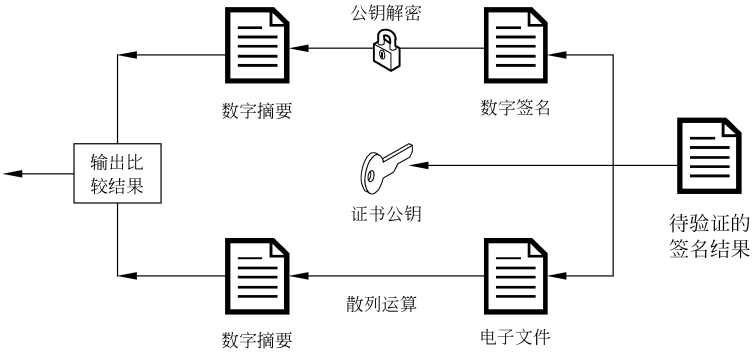


图 5-11　验证过程

如果接收方对发送方的数字签名验证成功，就可以说明三个实质性的问题。

(1) 该电子文件确实是由签名者的发送方所发出的，电子文件来源于该发送者，因为签署时电子签名数据由电子签名人所控制。

(2) 被签名的电子文件确实是经发送方签名后发送的,说明发送方用了自己的私钥做的签名,并得到验证,达到不可否认的目的。

(3) 接收方收到电子文件在传输中没有被篡改,保持了数据的完整性,因为签署后对电子签名的任何改动都能够被发现。

5. 原文加密的数字签名

原文加密的数字签名的过程要求对数字签名方法的实现涉及"数字信封"的问题,此处理过程稍微复杂一些,但数字签名的基本原理仍相同,其签名过程如图 5-12 所示。

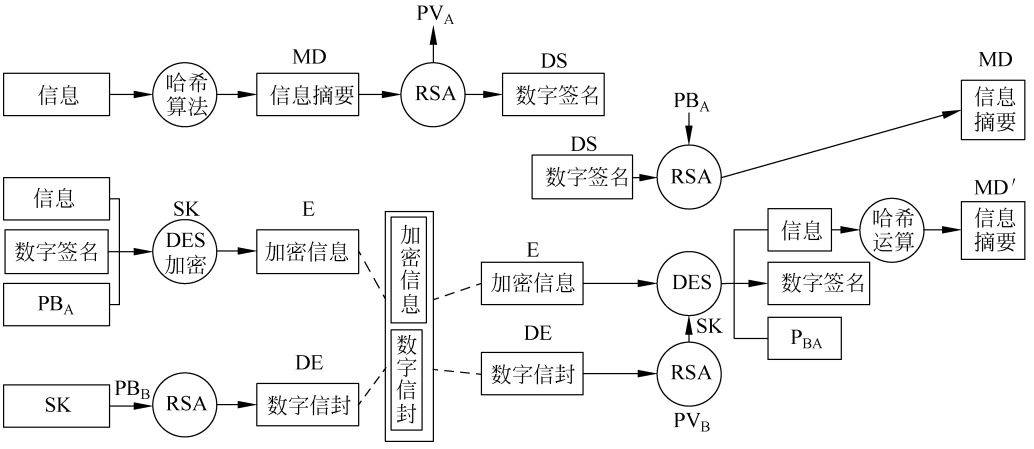


图 5-12 原文加密的数字签名实现方法

这是一个典型的"数字信封"处理过程。其基本原理是将原文用对称密钥加密传输,而将对称密钥用接收公钥加密发送给对方。如同将对称密钥放在同一个数字信封,接收方收到数字信封,用自己的私钥解密信封,取出对称密钥解密原文。

原文加密的数字签名的过程如下。

(1) 发送方 A 将原文信息进行哈希算法,得到一哈希值,即数字摘要 MD。

(2) 发送方 A 用自己的私钥 PV_A,采用非对称 RSA 算法对数字摘要 MD 加密,即得数字签名 DS。

(3) A 用对称密钥 SK 对原文、数字签名 DS 及 A 证书的公钥 PB_A 加密,得加密信息 E。

(4) 发送方用接收方 B 的公钥 PB_B,采用 RSA 算法对对称密钥 SK 加密,形成数字信封 DE,就好像将对称密钥 SK 装到了一个用接收方公钥加密的信封里。

(5) 发送方 A 将加密信息 E 和数字信封 DE 一起发送给接收方 B。

(6) 接收方 B 接收到数字信封 DE 后,首先用自己的私钥 PV_B 解密数字信封,取出对称密钥 SK。

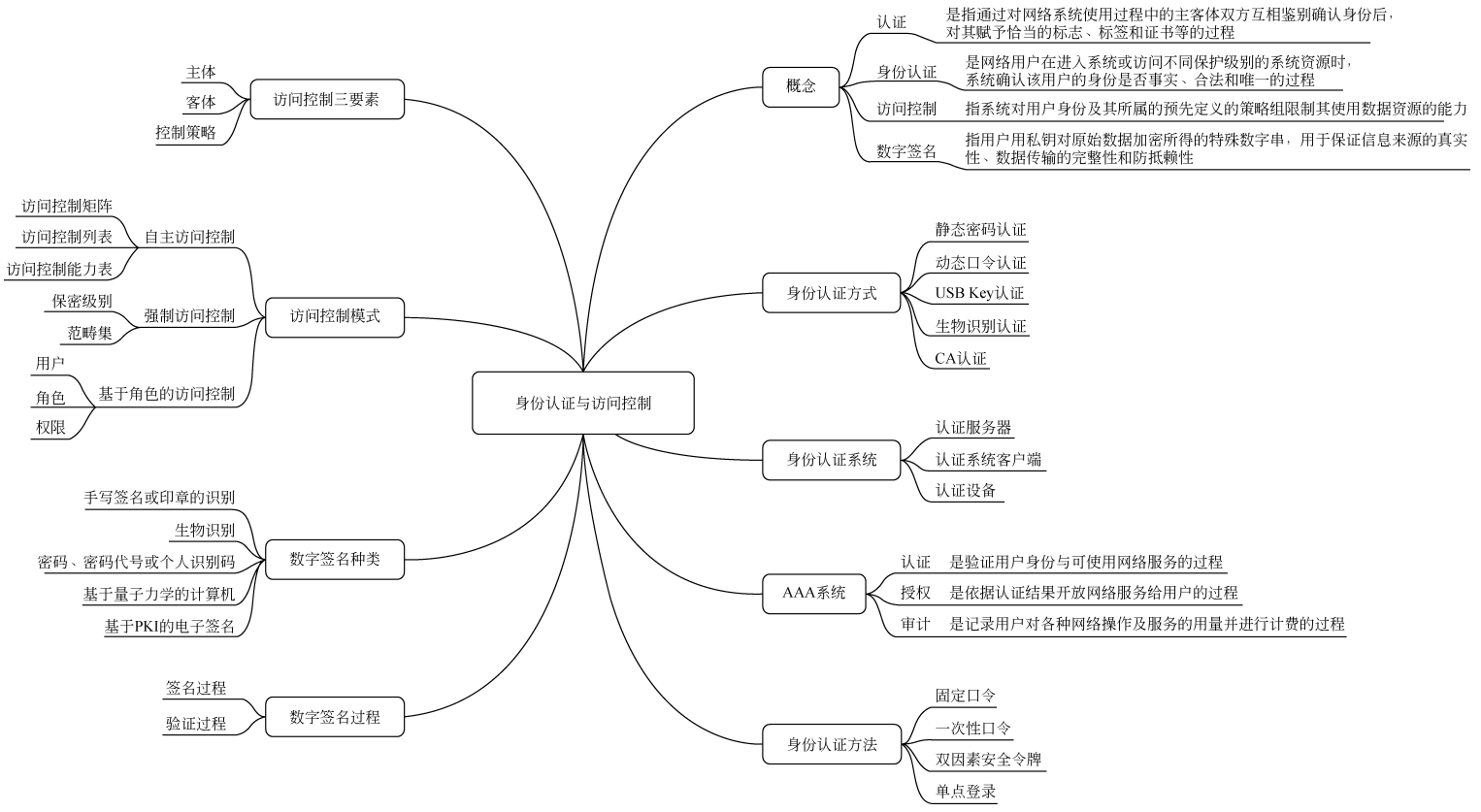
(7) B 用对称密钥 SK 以 DES 算法解密 E 还原出原文、数字签名 DS 及发送方 A 证书的公钥 PB_A。

(8) 接收方 B 验证数字签名,先用发送方 A 的公钥解密数字签名得数字摘要 MD。

(9) 接收方 B 同时将原文信息用同样的哈希算法,求得一个新的 MD'。

(10) 将两个数字摘要 MD 和 MD'进行比较,若相等则说明数据没被篡改,签名真实,否则拒绝该签名。此过程实现了机密信息在数字签名的传输中不被篡改的保密目的。

5.4 本章小结


身份认证与访问控制
概念
认证
是指通过对网络系统使用过程中的主客体双方互相鉴别确认身份后，对其赋予恰当的标志、标签和证书等的过程
身份认证
是网络用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否事实、合法和唯一的过程
访问控制
指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源的能力
数字签名
指用户用私钥对原始数据加密所得的特殊数字串，用于保证信息来源的真实性、数据传输的完整性和防抵赖性
身份认证方式
静态密码认证
动态口令认证
USB Key认证
生物识别认证
CA认证
身份认证系统
认证服务器
认证系统客户端
认证设备
AAA系统
认证 是验证用户身份与可使用网络服务的过程
授权 是依据认证结果开放网络服务给用户的过程
审计 是记录用户对各种网络操作及服务的用量并进行计费的过程
身份认证方法
固定口令
一次性口令
双因素安全令牌
单点登录
访问控制三要素
主体
客体
控制策略
访问控制模式
自主访问控制
访问控制矩阵
访问控制列表
访问控制能力表
强制访问控制
保密级别
范畴集
基于角色的访问控制
用户
角色
权限
数字签名种类
手写签名或印章的识别
生物识别
密码、密码代号或个人识别码
基于量子力学的计算机
基于PKI的电子签名
数字签名过程
签名过程
验证过程

5.5 习　　题

一、填空题

1.（　　）认证方式是最简单、应用最广泛的身份认证方法。

2.（　　）是国际认证机构的通称，是对数字证书的申请用户进行发放、管理、校验或取消的机构。

3. AAA 认证系统中（　　）是依据认证结果开放网络服务给用户的过程。

4.（　　）模式是指定义几个特定的信息安全级别，将资源归属于这些安全级别中。

5. 自主访问控制一般采用（　　）、访问控制列表和访问控制能力列表三种机制来存放不同主体的访问控制权限。

二、选择题

1. 数字签名的（　　）功能是指签名可以证明是签名者而不是其他人在文件上签字。

A. 签名不可伪造　　B. 签名不可变更

C. 签名不可抵赖　　D. 签名是可信的

2.（　　）不属于 AAA 系统提供的服务类型。

A. 认证　　B. 授权　　C. 访问　　D. 审计

3. PKI 解决信息系统中的（　　）问题。

A. 身份信任　　B. 权限管理　　C. 安全审计　　D. 安全传输

4. 以下关于 CA 认证中心说法正确的是（　　）。

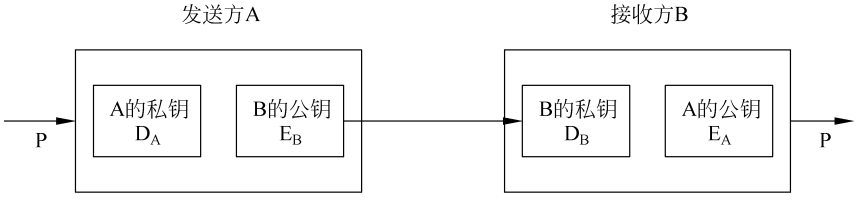
A. CA 认证是使用对称密钥机制的认证方法

B. CA 认证中心只负责签名，不负责证书的产生

C. CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份

D. CA 认证中心不用保持中立，可以任意找一个用户来作为 CA 认证中心

5. 下图为一种数字签名方案，防止 A 抵赖的证据是（　　）。



A. P　　B. $D_A(P)$　　C. $E_B(D_A(P))$　　D. D_A

三、判断题

1. 基于行的自主访问控制一般采用访问控制能力列表来实现。

2. RBAC 的核心思想就是将访问权限与角色相联系，通过给用户分配合适的角色，让用户与访问权限相关联。

3. 身份认证技术解决了用户是“谁”的问题，访问控制决定了用户“能够做什么”。

4. 访问控制策略是主体对客体的访问规则集，即属性集合。

5. 访问控制列表是实现基于列的自主访问控制采用最多的一种方式。

四、简答题

1. 访问控制包括哪三个要素？

2. AAA 系统提供哪些服务？

3. 在实际应用中，数字信封常用来解决什么问题？如何解决？

4. 什么是身份认证？

5. 访问控制模式有哪三种模式？

6. 什么是数字签名？

五、综合题

下图为数字签名工作原理示意图，发送方为 A，接收方为 B。图中①～⑥省略密钥名称。如果对称密钥为 K，发送方私钥为 SA，发送方公钥为 PA，接收方私钥为 SB，接收方公钥为 PB。

（1）请写出图中①～⑥省略的密钥名称。

（2）给出接收方比较 MD 和 MD′的目的。