第五章 身份认证

第五章 身份认证

教学目标

- 熟悉常见的身份认证技术
- 了解什么是身份认证技术
- 了解身份认证技术的作用
- 了解基于X.509的数字证书的认证

5.1身份认证技术概述

- 5.1.1身份认证技术的基本概念
- 5.1.2基于信息秘密的身份认证
- 5.1.3基于信任物体的身份认证
- 5.1.4基于生物特征的身份认证

5.1.1身份认证技术的基本概念

1.身份认证的概念

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、标签和证书等过程。认证可以解决主体本身的信用问题和客体对主体的访问的信任问题，认证可以为下一步的授权奠定基础，是对用户身份的认证信息的生成、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）是网络系统的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。数据完整性可以通过消息认证进行保证，是网络系统安全保障的重要措施之一。

5.1.1身份认证技术的基本概念

2.身份认证的作用

在网络系统中，身份认证是网络安全中的第一道防线，对网络系统的安全有着重要的意义。用户在访问系统前，先要经过身份认证系统进行有效身份识别，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，来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录用户的请求和行为，同时入侵检测系统检测异常行为。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”进行鉴别和审计，如图5.1所示。

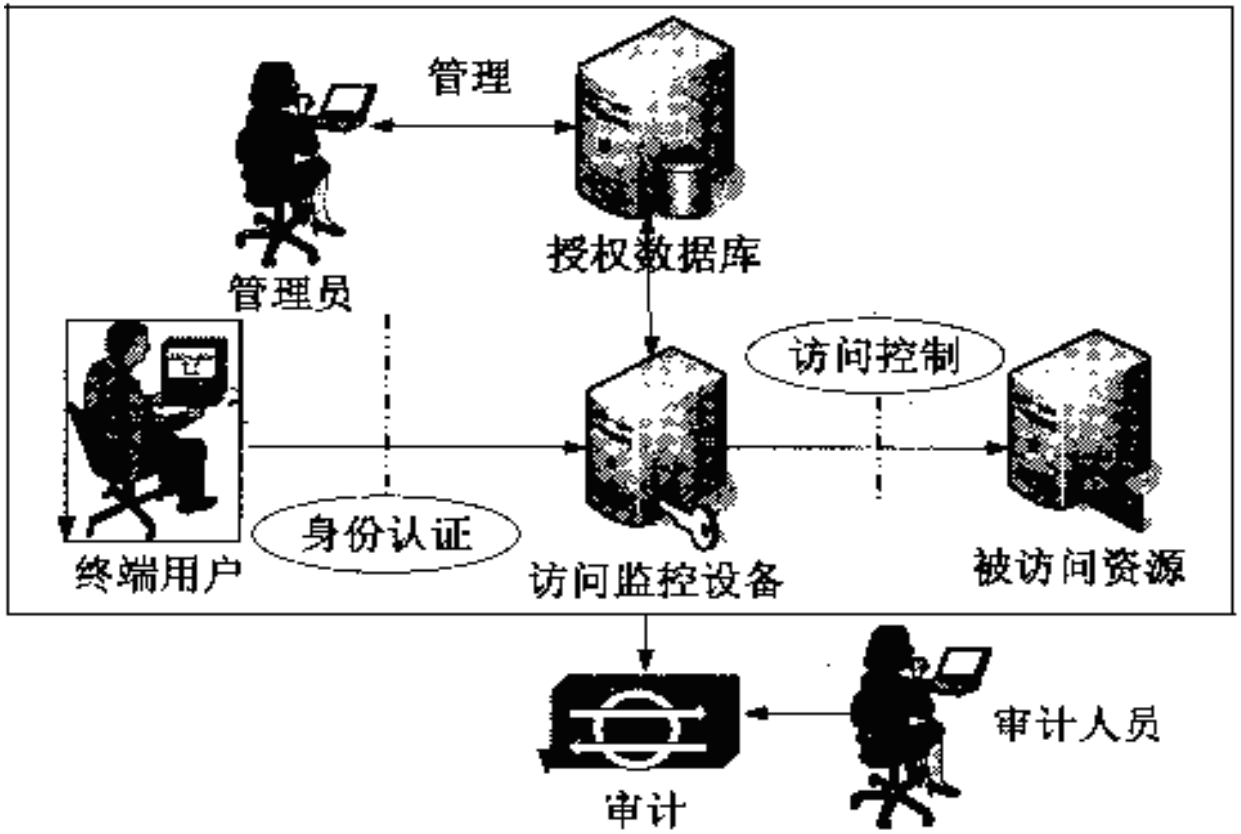


图5.1 身份认证的过程

5.1.1身份认证技术的基本概念

3. 认证技术的类型

认证技术是用户身份鉴别确认的重要手段，也是网络系统安全中的一项重要内容。从鉴别对象上可以分为两种：消息认证和用户身份认证。

消息认证：用于保证信息的完整性和不可否认性。通常用来检测主机收到的信息是否完整，以及检测信息在传递过程中是否被修改或伪造。

身份认证：鉴别用户身份。包括识别和验证两部分内容。其中，识别是鉴别访问者的身份，验证是对访问者身份的合法性进行确认。

5.1.1身份认证技术的基本概念

4.常见的身份认证技术

在现实世界中，对用户的身份认证基本方法可以分为三种：

（1）基于信息秘密的身份认证：就是根据你所知道的信息来证明你的身份（what you know你知道什么）；

（2）基于信任物体的身份认证：就是根据你所拥有的东西来证明你的身份（what you have，你有什么）；

（3）基于生物特征的身份认证：就是直接根据独一无二的身体特征来证明你的身份（who you are，你是谁），比如指纹、面貌等。

在网络世界中手段与真实世界中是一致的，为了达到更高的身份认证安全性，某些场景会将上面3种情况挑选出其中的两种进行混合，即所谓的双因素认证。

5.1.2基于信息秘密的身份认证

基于信息秘密的身份认证是根据双方共同所知道的秘密信息来证明用户的身份（what you know），并通过对秘密信息进行鉴别来验证身份。例如，基于口令、密钥、IP地址、MAC地址等身份因素的身份认证。主要包括：

1.网络身份证

网络身份证即虚拟身份电子标识VIEID（Virtual identity electronic identification）技术。就是在网络上可以证明一个人身份及存在的虚拟证件。VIEID是网络身份证的工具或服务协议，也是未来互联网络基础设施的基本构成之一。

5.1.2基于信息秘密的身份认证

（1）将用户现实中的身份资料包括文字资料、语音、指纹等信息采集到权威服务机构，然后生成一个账户。账户内包含VIEID的账户ID、公钥和私钥等信息；

（2）当用户在相应客户端识别系统中输入VIEID的账户ID和公钥，识别系统会在VIEID库中搜索公钥解密还原出该VIEID持有人的资料从而识别其身份或某种资格。

另外，网络身份证应具有公开性（IP）、一致性（统一性）和保密性、区域性等特点。

5.1.2基于信息秘密的身份认证

2.静态口令

这是现在普遍采用的一种方法，用户的密码是由用户自己设定的。在网络登录时输入正确的密码，计算机就认为操作者就是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。如果密码是静态的数据，在验证过程中需要在计算机内存中和传输过程可能会被木马程序或网络中截获。因此，静态密码机制无论是使用还是部署都非常简单，但从安全性上讲，用户名/密码的方式是一种不安全的身份认证方式。 它利用what you know方法。

5.1.2基于信息秘密的身份认证

3.一次性口令

一次性口令认证也称为动态口令认证，是目前应用最广的一种身份识别方式。基于动态口令认证的方式主要有动态短信密码和动态口令牌（卡）两种方式，口令一次一密。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（机构）用户动态口令牌进行认证，如图所示。很多世界500强企业都运用其来保护系统登入的安全，被广泛应用在VPN、网上银行和电子商务等领域。

5.1.2基于信息秘密的身份认证

动态口令认证的主要优点：

无须像保护静态口令那样定期修改口令，方便管理；

一次一口令，有效防止黑客一次性口令窃取就获得永久访问权；

由于口令使用后即被废弃，可以有效防止身份认证中的重放攻击。

动态口令认证的主要缺点：

客户端和服务器的时间或事件若不能保持良好的同步，可能发生合法用户无法登录的问题；

口令是一长串较长的数字组合，一旦输错就得重新操作。

5.1.3基于信任物体的身份认证

基于信任物体的身份认证是根据双你所拥有的东西来证明用户的身份（what you have）。例如，通过信用卡、智能卡、USB Key等方式进行身份认证。主要包括：

1.智能卡（IC卡）

智能卡一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。

智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。它利用what you have方法。

5.1.3基于信任物体的身份认证

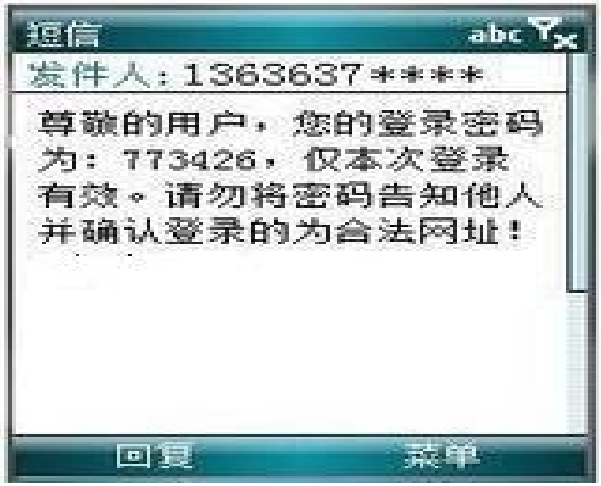
智能卡自身就是功能齐备的计算机，它有自己的内存和微处理器，该微处理器具备读取和写入能力，允许对智能卡上的数据进行访问和更改。智能卡被包含在一个信用卡大小或者更小的物体里（比如手机中的SIM就是一种智能卡）。智能卡技术能够提供安全的验证机制来保护持卡人的信息，并且智能卡的复制很难。从安全的角度来看，智能卡提供了在卡片里存储身份认证信息的能力，该信息能够被智能卡读卡器所读取。智能卡读卡器能够连到PC上来验证VPN连接或验证访问另一个网络系统的用户。

这个验证方式的成本比较高，现在有的国内银行的网上银行采用这个验证办法。

5.1.3基于信任物体的身份认证

2.短信密码

短信密码以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。如图所示。



5.1.3基于信任物体的身份认证

具体优点表现如下：

（1）安全性

（2）普及性

（3）易收费

（4）易维护

由于短信网关技术非常成熟，大大降低短信密码系统上马的复杂度和风险，短信密码业务后期客服成本低，稳定的系统在提升安全同时也营造良好的口碑效应，这也是银行也大量采纳这项技术很重要的原因。

5.1.3基于信任物体的身份认证

3. USB Key认证

USB Key（U盾）认证方式是近几年才得到广泛应用的。它主要采用软硬件相结合、一次一密的强双因素（两种认证方法）进行认证，很好地解决了安全性与易用性之间的矛盾。以一种USB接口的硬件设备，内置单片机或者智能芯片卡，可存储用户的秘钥或数字证书，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。常见的网银USB Key如图所示。

5.1.4基于生物特征的身份认证

认证系统测量的生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。使用传感器或者扫描仪来读取生物的特征信息，将读取的信息和用户在数据库中的特征信息比对，如果一致则通过认证。

生物特征分为身体特征和行为特征两类。目前我们接触最多的是指纹识别技术，应用的领域有门禁系统、微型支付等。我们日常使用的部分手机和笔记本电脑已具有指纹识别功能，在使用这些设备前，无需输入密码，只要将手指在扫描器上轻轻一按就能进入设备的操作界面，非常方便，而且别人很难复制。例如，通过指纹、声纹、视网膜、虹膜等方式进行身份认证。主要包括：

5.1.4基于生物特征的身份认证

1.指纹识别技术

指纹识别技术是最传统、最成熟的生物鉴定方式。它就是通过分析指纹的全局特征和指纹的局部特征来确定身份，从指纹中抽取的特征值应尽可能地详尽，足以可靠地通过指纹来确认一个人的身份。主要优势如下：

（1）稳定性：从胎儿6个月时指纹完全形成到人死亡后，指纹的纹线类型、结构等始终不会有明显变化；

（2）独特性：至今未找到两个指纹完全相同的人。根据指纹学理论，两枚指纹完全匹配上12个特征的几率为10^{-50}；

（3）便利性：提取指纹作为永久记录存档比较简单易行。

5.1.4基于生物特征的身份认证

2.声纹识别技术

声纹识别技术是指根据语音波形中反映说话人生理和行为特征的语音参数，自动识别说话人身份。每个人说话的声音都会有自己的特点，人对语音的识别能力是特别强的。在商业和军事等安全性要求较高的系统中，常常靠人的声纹来实现个人身份的验证。

声纹识别与传统语音识别的区别：

（1）声纹识别利用语音信号中的说话人信息，而无须考虑语音中的字词意思，它强调的是说话人的个性。

（2）语音识别的目的是识别出语音信号中的言语内容，并不考虑说话人是谁，它强调共性。

5.1.4基于生物特征的身份认证

3.视网膜识别技术

人的视网膜血管的图样具有良好的个人特征，基于视网膜开发的识别系统在身份验证上有着独特的优势。视网膜识别的基本方法是用光学和电子仪器将视网膜血管图样记录下来，一个视网膜血管的图样可压缩为小于35字节的数字信息，可根据对图样的节点和分支的检测结果进行分类识别。

视网膜识别的验证效果相当好，但成本较高，运行的难度大（要求被识别人的合作并允许进行视网膜特征的采样），因此，只在军事或银行系统中被采用。

5.1.4基于生物特征的身份认证

4.虹膜图样识别技术

从理论上讲，虹膜认证是基于生物特征的认证中最好的一种认证方式。虹膜（眼睛中的彩色部分）是眼球中包围瞳孔的部分，上面布满极其复杂的锯齿网络状花纹，而每个人虹膜的花纹都是不同的。虹膜识别技术就是应用计算机对虹膜花纹特征进行量化数据分析，用以确认被识别者的真实身份。虹膜识别可以在35-40厘米的距离采样，比采集视网膜图样要方便，易为人所接受。基于虹膜的识别系统可用于安全入口、接入控制、信用卡、POS、ATM等应用系统中，有效进行身份识别。

一个虹膜识别系统一般由4部分组成：虹膜图像的采集、预处理、特征提取及模式匹配，如图所示。

5.1.4基于生物特征的身份认证