第4章 身份认证技术

《计算机网络安全技术》

4.1 身份认证概述

4.1.1 身份认证的概念

- 身份认证（Authentication）是系统审查用户身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限。身份认证通过标识和鉴别用户的身份，提供一种判别和确认用户身份的机制。
- 计算机网络中的身份认证是通过将一个证据与实体身份绑定来实现的。实体可能是用户、主机、应用程序甚至是进程。
- 身份认证技术在信息安全中处于非常重要的地位，是其他安全机制的基础。只有实现了有效的身份认证，才能保证访问控制、安全审计、入侵防范等安全机制的有效实施。

- 在真实世界中，验证一个用户的身份主要通过以下三种方式：
- ·所知道的。根据用户所知道的信息（what you know）来证明用户的身份。
- ·所拥有的。根据用户所拥有的东西（what you have）来证明用户的身份。
- ·本身的特征。直接根据用户独一无二的体态特征（who you are）来证明用户的身份，例如人的指纹、笔迹、DNA、视网膜及身体的特殊标志等。

《计算机网络安全技术》

4.1.2 认证、授权与审计

- 在计算机网络安全领域，将认证、授权与审计统称为AAA或3A，即英文Authentication（认证）、Authorization（授权）和Accounting（审计）。
- 1. 认证
- 认证是一个解决确定某一个用户或其他实体是否被允许访问特定的系统或资源的问题。
- 2. 授权
- 授权是指当用户或实体的身份被确定

3. 审计

审计也称为记帐（Accounting）或审核，出于安全考虑，所有用户的行为都要留下记录，以便进行核查。所采集的数据应该包括登录和注销的用户名、主机名及时间。用户对资源的访问过程如图4-1所示。

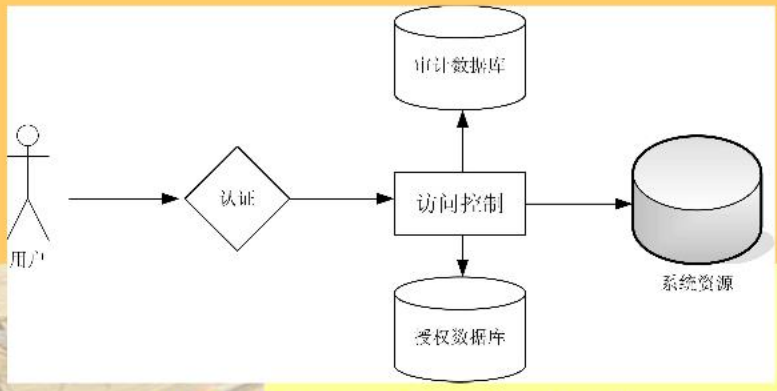


图4-1 用户访问系统资源的过程

4.2 基于密码的身份认证

- 4.2.1 密码认证的特点
- 密码是用户与计算机之间以及计算机与计算机之间共享的一个秘密，在通信过程中其中一方向另一方提交密码，表示自己知道该秘密，从而通过另一方的认证。密码通常由一组字符串来组成，为便于用户记忆，一般用户使用的密码都有长度的限制。但出于安全考虑，在使用密码时需要注意以下几点：
- （1）不使用默认密码、（2）设置足够长的密码、（3）不要使用结构简单的词或数字组合、（4）增加密码的组合复杂度、（5）使用加密、（6）避免共享密码 、（7）定期更换密码

- 就密码的安全使用来说，计算机系统应该具备下列安全性：
- （1）入侵者即使取得储存在系统中的密码也无法达到登录的目的。这需要在密码认证的基础上再增加其他的认证方式，如地址认证。
- （2）通过监听网络上传送的信息而获得的密码是不能用的。最有效的方式是数据加密。
- （3）计算机系统必须能够发现并防止各类密码尝试攻击。可使用密码安全策略。

4.2.2 密码认证的安全性

- 早在1974年，Purdy就提到为了保护密码的安全，绝对不能以明文的方式储存密码，提出将密码以单向函数y=f(x)转换后，以加密的方式将密码与账户资料存放在一个验证表中，单向函数应具有下列特性：
- ·知道x可以很容易计算出y。
- ·知道y要算出x，在计算上是不可行的。

- 使用一次性密码（即“一次一密”）技术可以防止重放攻击的发生，这相当于用户随身携带一个密码本，按照与目标主机约定好的次序使用这些密码，并且每一个密钥只使用一次，当密码全部用完后再向系统管理员申请新的密码本。S/Key认证系统就是基于这种思想的一次性密码认证系统。
- 在S/Key认证系统中，用户每一次登录系统所用的密码都是不一样的，攻击者通过窃听得到的密码无法用于下一次认证，这样S/Key认证系统很好地防止了密码重放攻击。相对于可重放的密码认证系统，S/Key认证系统具有很好的安全性，而且符合安全领域的发展趋势。

《计算机网络安全技术》

Lamport算法是另一种防止重放攻击的有效方法。Lamport算法使用安全单向[illegible]（x）的动态密码认证方法，使用者每一次登录的密码都不同。即用安全单向函数 y=F（x）对用户的密码明文经过多次迭代运算，产生一系列一次性口令，即：

$$PW_i = F^{N+1-i}(password) \qquad i = 1,2,3,\ldots\ldots,N$$

根据以上函数关系，可以计算出第一个一次性密码为 PW_1，这时用户的密码明文经过了 N 次迭代运算；第二个一次性密码为 PW_2，这时用户的密码明文经过 N-1 次迭代运算；依此类推，得到所有的一次性密码列表。

把第一个一次性密码 PW_1 和迭代次数 N 存放到服务器上。当用户通过网络对服务器进行访问时，服务器把迭代次数 m（m<N）发送给用户端，用户端根据迭代次数 m 计算出下一个一次性密码 PW_{m+1}，并通过网络发送到服务器。服务器经过一次单向 Hash 函数运算，把结果和保留在服务器上的用户密码进行比较，如果两者相等，通过认证，允许访问；否则拒绝访问。如果成功进行了访问，则用刚传过来的一次性密码 PW_{m+1} 来替换掉服务器端存储的用户密码 PW_m，并把迭代次数 m 减 1。

这样攻击者既使从网络上窃取了用户密码，也无法计算出下一个正确的用户密码，因为单向函数是不可逆的，知道函数输出值，无法计算得到函数的输入值。这个方法必须依赖 F（x）是一个安全的函数，也就是 F（x）函数不可被破解，而且在系统运行中不能更换 F（x）函数。

一次性口令有其安全的地方，但在实际应用中很不方便。如密码更改问题，初始化问题等。本次密码列表中的密码被全部使用后，用户必须向系统管理员重新申请新的密码和迭代函数。

4.2.3 密码认证中的其他问题

- 1. 社会工程学
- 社会工程学（Social Engineering）是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行的诸如欺骗、伤害等危害手段，取得自身利益的手法，近年来已成迅速上升甚至滥用的趋势。
- 2. 按键记录软件
- 按键记录软件是一种间谍软件，它以木马方式值入到用户的计算机后，可以偷偷地记录下用户的每次按键动作，并按预定的计划把收集到的信息通过电子邮件等方式发送出去。

《计算机网络安全技术》

- 3. 搭线窃听
- 攻击者通过窃听网络数据，如果密码使用明文传输，可被非法获取。目前，在IP网络中Telnet、FTP、HTTP等大量的通信协议来用明文来传输密码，这意味着在客户端和服务器端之间传输的所有信息（其中包括明文密码和用户数据）都有可能被窃取。
- 4. 字典攻击
- 攻击者可以把所有用户可能选取的密码列举出来生成一个文件，这样的文件被称为“字典”。当攻击者得到了一些与密码有关的可验证信息后，就可以结合字典进行一系列的运算，来猜测用户可能的密码，并利用得到的信息来验证猜测的正确性。

《计算机网络安全技术》

5. 暴力破解

暴力破解也称为“蛮力破解”或“穷举攻击”，是一种特殊的字典攻击。在暴力破解中所使用的字典是字符串的全集，对可能存在的所有组合进行猜测，直到得到正确的信息为止。

6. 窥探

窥探是攻击者利用与被攻击系统接近的机会，安装监视设备或亲自窥探合法用户输入的账户和密码。窥探还包括攻击者在用户计算机中植入的木马。

7. 垃圾搜索

垃圾搜索是攻击者通过搜索被攻击者的废弃物（如硬盘、U盘、光盘等），得到与攻击系统有关的信息。

4.3 基于地址的身份认证

- 4.3.1 地址与身份认证
- 基于IP地址的身份认证：不可靠，也不可取
- 基于物理地址（如MAC地址）的身份认证较为可靠，目前在计算机网络中的应用较为广泛。
- 4.3.2 智能卡认证
- 智能卡（Smart Card）也称IC卡，是由一个或多个集成电路芯片（包括固化在芯片中的软件）组成的设备，可以安全地存储密钥、证书和用户数据等敏感信息，防止硬件级别的窜改。智能卡芯片在很多应用中可以独立完成加密、解密、身份认证、数字签名等对安全较为敏感的计算任务，从而能够提高应用系统抗病毒攻击以及防止敏感信息的泄漏。

《计算机网络安全技术》

- 智能卡具有硬件加密功能，所以安全性性较高。
- 智能卡认证是基于“what you have”的手段，通过智能卡硬件不可复制来保证用户身份不会被仿冒。
- 双因素身份认证，简单地讲是指在身份认证过程中至少提供两个认证因素，如“密码+PIN”等。双因素认证与利用ATM（自动柜员机）取款很相似：用户必须利用持银行卡（认证设备），再输入密码，才能提取其账户中的款项。双因素认证提供了身份认证的可靠性。

4.4 生物特征身份认证

4.4.1 生物特征认证的概念

生物特征认证又称为“生物特征识别”，是指通过计算机利用人体固有的物理特征或行为特征鉴别个人身份。在信息安全领域，推动基于生物特征认证的主要动力来自于基于密码认证的不安全性，即利用生物特征认证来替代密码认证。人的生理特征与生俱来，一般是先天性的。

- 满足以下条件的生物特征才可以用来作为进行身份认证的依据：
- 普遍性。即每一个人都应该具有这一特征。
- 唯一性。即每一个人在这一特征上有不同的表现。
- 稳定性。即这一特征不会随着年龄的增长和生活环境的改变而改变。
- 易采集性。即这一特征应该便于采集和保存。
- 可接受性。即人们是否能够接受这种生物识别方式。

4.4.2 指纹认证

- 利用人的生物特征可以实现“以人识人”，其中指纹是人的生物特征的一种重要的表现形式，具有“人人不同”和“终身不变”的特征，以及附属于人的身体的便利性和不可伪造的安全性。
- 指纹认证的特点如下：
- ·独特性。
- ·稳定性
- ·方便性

图4-2 不同的指纹形状 《计算机网络安全技术》

- 如图4-3所示，指纹识别的过程包括2个子过程：指纹注册过程和指纹比对过程。其中：
- ① 指纹采集。
- ② 图像增强。
- ③ 提取特征值。是指对指纹图案上的特征信息进行选择（如图4-4所示）、编码和形成二进制数据的过程。
- ④ 特征值模板入库。
- ⑤ 比对匹配。

图4-4 指纹图案信息的选择

4.4.3 虹膜认证

- 从理论上讲，虹膜认证是基于生物特征的认证方式中最好的一种认证方式。虹膜[illegible]瞳孔的[illegible]及其复杂[illegible]的花纹[illegible]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。

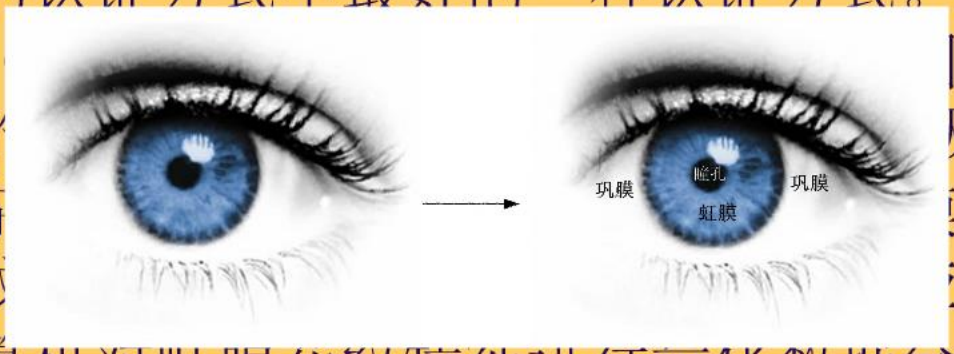


图4-5 虹膜在眼球中的位置

- 如图4-6所示，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。

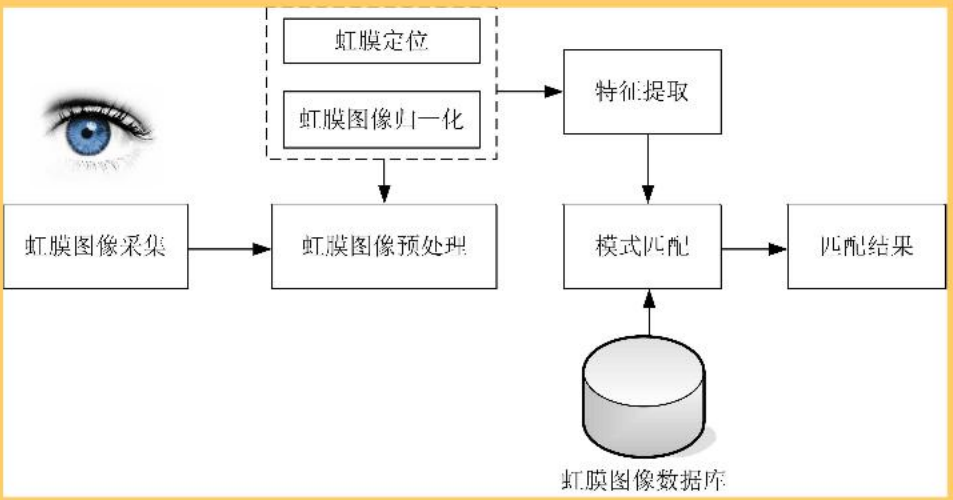


图4-6 虹膜识别系统的组成

- 其中：
- ① 虹膜图像采集。虹膜图像采集是虹膜识别系统一个重要的且困难的步骤。
- ② 虹膜图像的预处理。这一操作分为虹膜定位和虹膜图像的归一化两个步骤。
- ③ 虹膜纹理的特征提取。采用转换算法将虹膜的可视特征转换成为固定字节长度的虹膜代码。
- ④ 模式匹配。识别系统将生成的代码与代码数据库中的虹膜代码进行逐一比较，当相似率超过某一个预设置值时，系统判定检测者的身份与某一个样本相符。

4.5 零知识证明身份认证

4.5.1 零知识证明身份认证的概念

零知识证明（zero-knowledge proof）是由在20世纪80年代初出现的一种身份认证技术。零知识证明是指证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。

零知识证明实质上是一种涉及两方或多方的协议，即两方或多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使验证者相信自己知道某一消息或拥有某一物品，但证明过程不需要（也不能够）向验证者泄漏。零知识证明分为交互式零知识证明和非交互式零知识证明两种类型。

《计算机网络安全技术》

4.5.2 交互式零知识证明

- 零知识证明协议可定义为证明者（Prover，简称P）和验证者（Verifier，简称V）。交互式零知识证明是由这样一组协议确定的：在零知识证明过程结束后，P只告诉V关于某一个断言成立的信息，而V不能从交互式证明协议中获得其他任何信息。即使在协议中使用欺骗手段，V也不可能揭露其信息。这一概念其实就是零知识证明的定义。
- 如果一个交互式证明协议满足以下3点，就称此协议为一个零知识交互式证明协议：
- ·完备性。如果P的声称是真的，则V

- 简单地讲，交互式零知识证明就是为了证明P知道一些事实，希望验证者V相信他知道的这些事实而进行的交互。为了安全起见，交互式零知识证明是由规定轮数组成的一个“挑战/应答”协议。通常每一轮由V挑战和P应答组成。在规定的协议结束时，V根据P是否成功地回答了所有挑战来决定是否接受P的证明。

4.5.3 非交互式零知识证明

- 在非交互式零知识证明中，证明者P公布一些不包括他本人任何信息的秘密消息，却能够让任何人相信这个秘密消息。在这一过程（其实是一组协议）中，起关键作用的因素是一个单向Hash函数。如果P要进行欺骗，他必须能够知道这个Hash函数的输出值。但事实上由于他不知道这个单向Hash函数的具体算法，所以他无法实施欺骗。也就是说，这个单向Hash函数在协议中是V的代替者。

《计算机网络安全技术》

4.6 身份认证协议

- 4.6.1 Kerberos协议
- 1. Kerberos协议简介
- Kerberos是为基于TCP/IP的Internet和Intranet设计的安全认证协议，它工作在Client/Server模式下，以可信赖的第三方KDC（密钥分配中心）实现用户身份认证。在认证过程中，Kerberos使用对称密钥加密算法，提供了计算机网络中通信双方之间的身份认证。
- Kerberos设计的目的是解决在分布网络环境中用户访问网络资源时的安全问题。

- 由于Kerberos是基于对称加密来实现认证的，这就涉及到加密密钥对的产生和管理问题。在Kerberos中会对每一个用户分配一个密钥对，如果网络中存在N个用户，则Kerberos系统会保存和维护N个密钥对。同时，在Kerberos系统中只要求使用对称密码，而没有对具体算法和标准作限定，这样便于Kerberos协议的推广和应用。
- Kerberos已广泛应用于Internet和Intranet服务的安全访问，具有高度的安全性、可靠性、透明性和可伸缩性等优点。
- 目前广泛使用的Kerberos的版本是第4版（v4）和第5版（v5），其中Kerberos v5弥补了v4中存在的一些安全漏洞。

《计算机网络安全技术》

2. Kerberos系统的组成

一个完整的Kerberos系统主要由以下几个部分组成：

- （1）用户端（Client）。
- （2）服务器端（Server）。
- （3）密钥分配中心（Key Distribution Center，KDC）。
- （4）认证服务器（Authentication Server，AS）。
- （5）票据分配服务器（Ticket Granting Server，TGS）。
- （6）票据。
- （7）时间戳。

❑3. Kerberos的基本认证过程

❑ Kerberos的基本认证过程如图4-7所示。

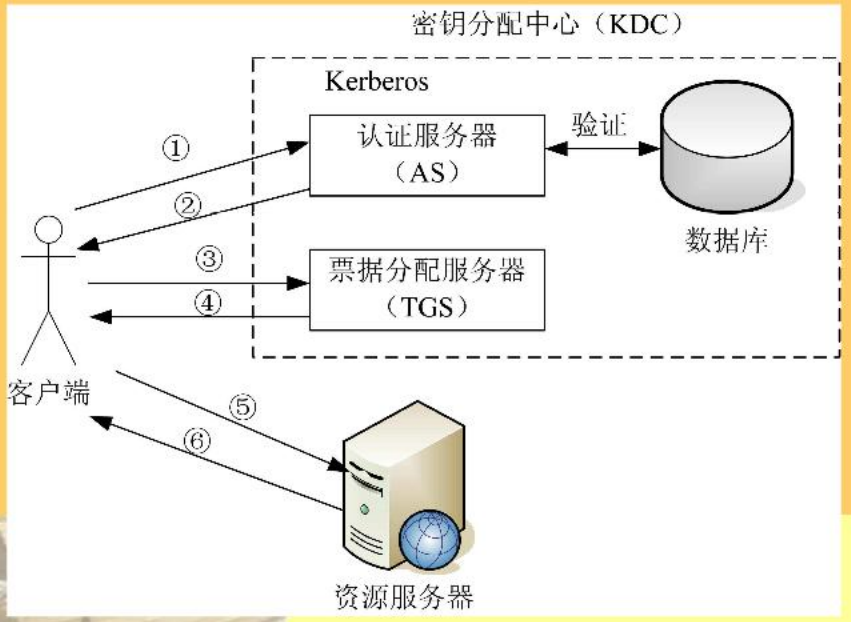


图4-7 Kerberos系统认证过程示意图

4.6.2 SSL协议

- 1、SSL协议概述
- SSL是一种点对点之间构造的安全通道中传输数据的协议，它运行在传输层之上、应用层之下，是一种综合利用对称密钥和公开密钥技术进行安全通信的工业标准。在通信过程中，允许一个支持SSL协议的服务器在支持SSL协议的客户端使协议本身获得信任，使客户端得到服务器的信任，从而在两台机器间建立一个可靠的传输连接。SSL协议主要提供了3个方面的安全服务。
- 认证。利用数字证书技术和可信任的第三

- 如图4-8所示，SSL协议分为上下两部分：上层为SSL握手协议，下层为SSL记录协议。其中SSL握手协议主要用来建立客户机与服务器之间的连接，并协商密钥；而SSL记录协议则定义了数据的传输格式。

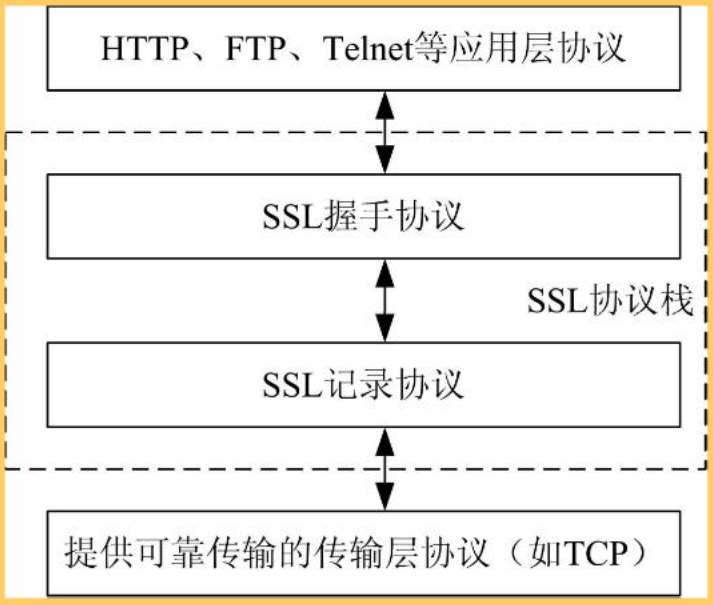


图4-8 SSL协议栈的组成

- 2. SSL握手协议
- SSL握手协议提供了客户机与服务器之间的相互认证，协商加密算法，用于保护在SSL记录中发送的加密密钥。握手协议在任何应用程序的数据传输之前进行。如图4-9描述了SSL握手协议一次握手的操作过程。

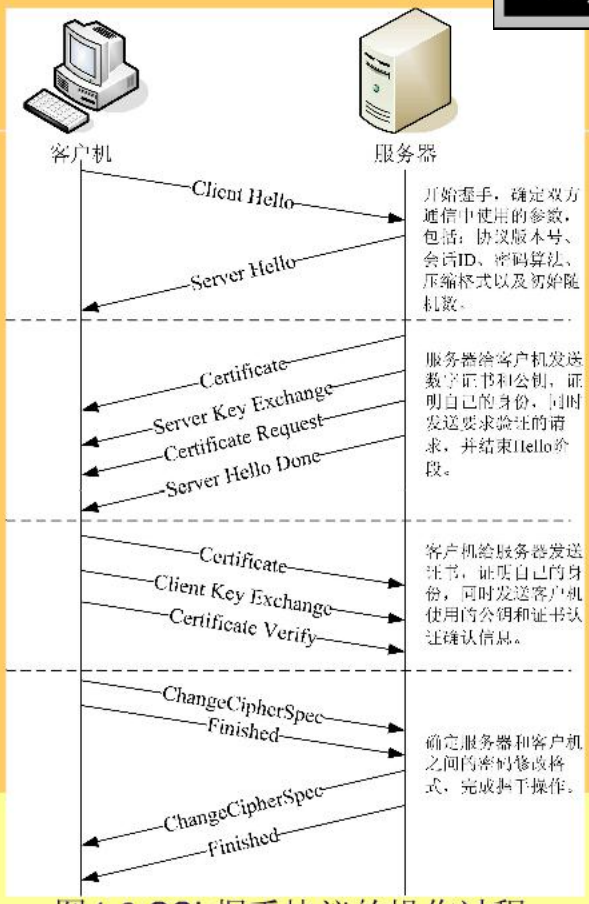


图4-9 SSL握手协议的操作过程

《计算机网络安全技术》

3. SSL记录协议

SSL记录协议建立在可靠的传输层协议（如TCP）之上，为高层协议（如HTTP、FTP等）提供数据封装、压缩、加密等基本功能的支持。如图4-10所示描述了SSL记录协议的操作过程。

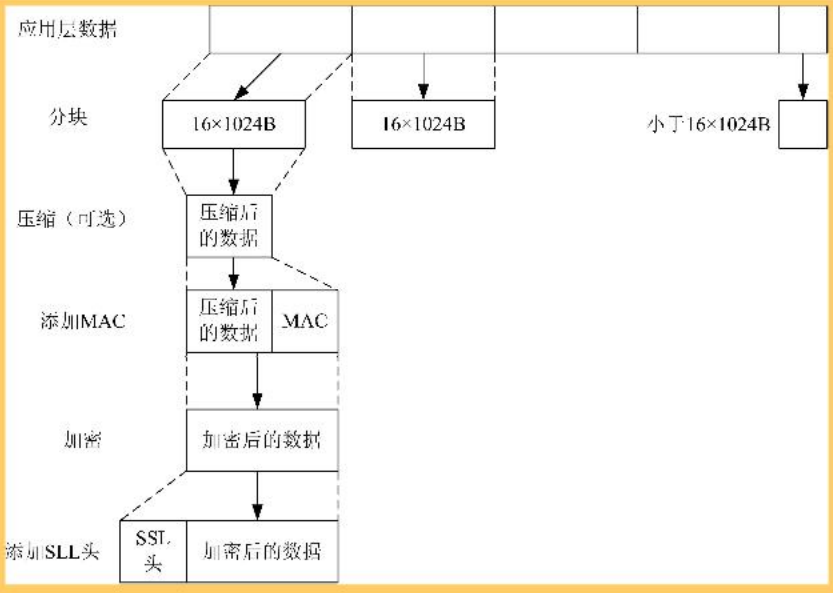


图4-10 SSL记录协议的操作过程

- 其中，对SSL记录头内容所示的几

8bit	8bit	8bit	16bit
内容类型	主版本号	次版本号	压缩长度
明文数据（压缩可选）			
MAC（0，16，20B）			

图4-11 SSL记录协议字段

4. SSL协议的特点

- SSL是一个通信协议。为了实现安全性，SSL的协议描述比较复杂，具有较完备的握手过程。这也决定了SSL不是一个轻量级的网络协议。另外，SSL还涉及到大量的计算密集型算法：非对称加密算法，对称加密算法和数据摘要算法。
- IETF将SSL进行了标准化，即RFC 2246，并将其称为TLS（Transport Layer Security）。从技术上讲，TLSv1.0与SSLv3.0的差别非常小。

4.7 实验操作—基于IEEE 802.1x协议的RADIUS服务器的配置和应用

❑4.7.1 实验设计

❑ 本实验是一个具有较大应用价值的综合实验：一是本实验立足目前的网络应用实际，可以直接在安全要求不太高的网络环境中使用；二是本实验的实现原理与目前市面上流行的记费认证系统基本相同，通过本实验可以帮助读者了解一些商业软件的功能特点；三是通过实践将会加深对本章前面介绍的理论知识的认识。

- 为便于实验的进行，设计了如图4-12所示的实验拓扑。其中，用于身份认证、授权和审计的RADIUS服务器由一台安装了“Internet验证服务”组件的Windows Server 2003的计算机扮演，其IP地址为172.16.2.10（读者也可以自定）。实验中使用的交换机必须是一台支持IEEE 802.1x协议的可网管交换机，在实验中需要启用交换机上的IEEE 802.1x协议。

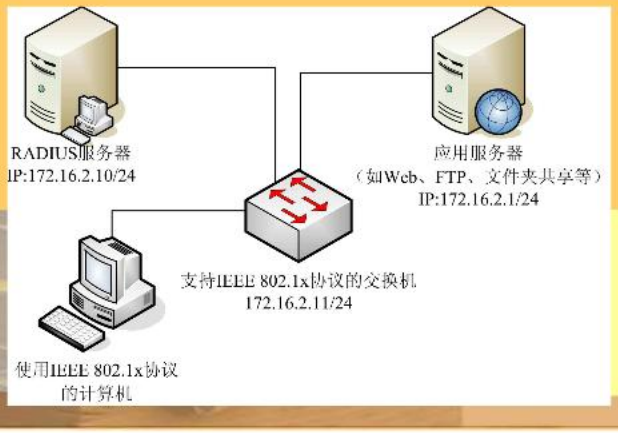


图4-12 实验拓扑

4.7.2 IEEE 802.1x和RADIUD服务器的概念

- 基于IEEE 802.1x和RADIUS服务器的身份认证系统目前已被用户广泛使用，为便于读者后面的操作，本小节首先介绍相关的概念。
- 1. IEEE 802.1x
- IEEE 802.1x是一个基于端口的网络访问控制协议，该协议的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而实现认证与业务的分离，保证了网络传输的效率。
- IEEE 802. 1x协议采用现有的可扩展认证协议（Extensible Authentication Protocol，EAP），它是IETF提出的PPP协议的扩展，最早是为解决基于IEEE 802.11标准的无线局域网的认证而开发的。

- 2. RADIUS服务器
- RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证服务）服务器提供了三种基本的功能：认证（Authentication）、授权（Authorization）和审计（Accounting），即提供了3A功能。其中审计也称为“记账”或“计费”。
- 在如图4-13所示的网络中，RADIUS服务器对RADIUS客户端（图4-13中直接标为“客户端”）进行用户验证、资源访问授权、记账等操作

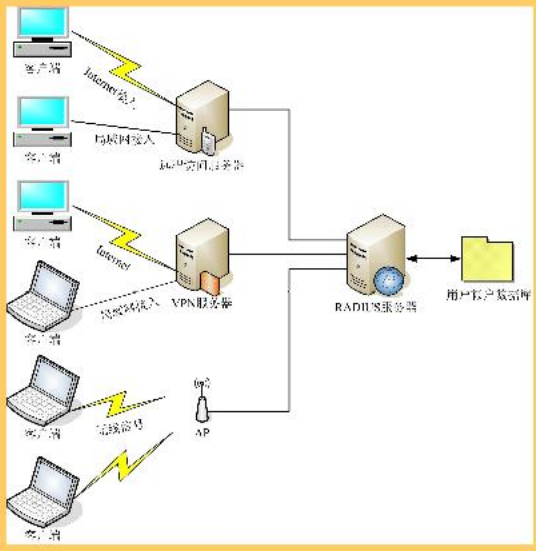


图4-13 RADIUS系统的组成

4.7.3 安装RADIUS服务器

- 在一台运行Windows Server 2003操作系统的计算机上通过安装“Internet验证服务”组件，将其配置为一台RADIUD服务器。如果这台计算机是一台Windows Server 2003的独立服务器（未升级成为域控制器，也未加入域），则可以利用SAM来管理用户账户信息；如果是一台Windows Server 2003域控制器，则利用活动目录数据库来管理用户账户信息。
- 具体安装过程见教材。

4.7.4 创建RADIUS客户端

- 本节要创建的RADIUS客户端，是指类似于图4-12中的交换机设备，在实际应用中也可以是VPN服务器、无线AP等，而不是用户端的计算机。
- RADIUS服务器只会接受由RADIUS客户端设备发过来的请求，为此需要在RADIUS服务器上来指定RADIUS客户端。
- 具体操作步骤见教材。

4.7.5 创建用户账户

- 在基于RADIUS和IEEE802.1X的系统中，需要为所有通过认证才能够访问网络的用户在RADIUS服务器中创建账户。这样，当用户的计算机连接到启用了端口认证功能的交换机上的端口上时，启用了IEEE 802.1x认证功能的客户端计算机需要用户输入正确的账户和密码后，才能够访问网络中的资源。
- 具体操作过程见教材。

4.7.6 设置远程访问策略

- 在RADIUS服务器的“Internet验证服务”窗口中，需要为交换机及通过该交换机进行认证的用户设置远程访问策略。
- 具体内容见教材。

4.7.7 交换机（RADIUS客户端）的配置

- 对支持IEEE 802.1x认证协议的交换机进行配置，使它能够接授用户端的认证请求，并将请求转发给RADIUS服务器进行认证，最后将认证结果返回给用户端。
- 具体内容见教材。

4.7.8 用户端连接测试

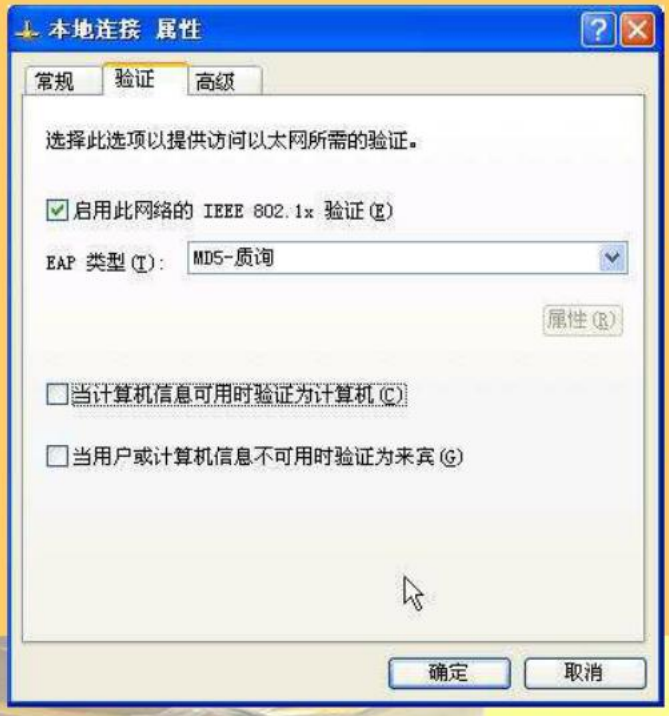


图4-33 启用客户端IEEE 802.1x验证

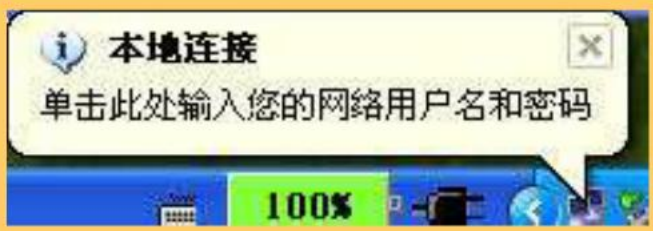
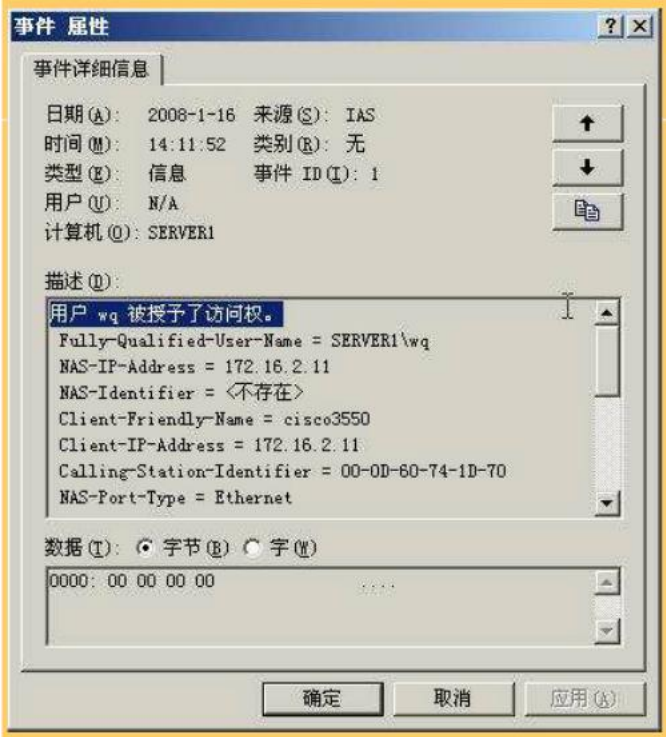


图4-34 系统要求输入用户名和密码

图4-35 输入用户名和密码对话框

在RADIUS服务器上打开“事件查看器”，在“系统”事件中将会显示用户的认证情况，如图4-36所示。当用户端提示“身份验证失败”时，在RADIUS服务器的“系统”事件中，将会显示如图4-37所示的事件说明，对用户wangqun的认证未通过。



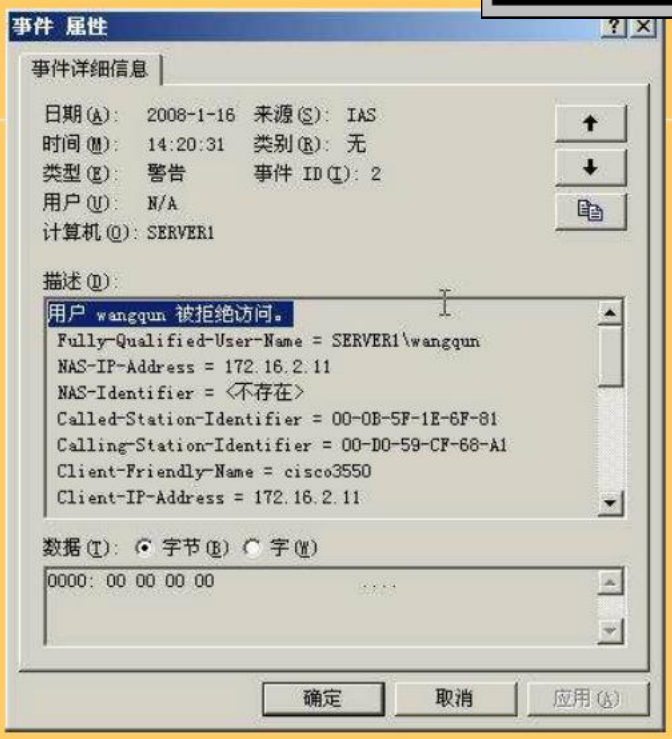


图4-36 通过认证的用户事件记录

图4-37 未通过认证的用户事件记录