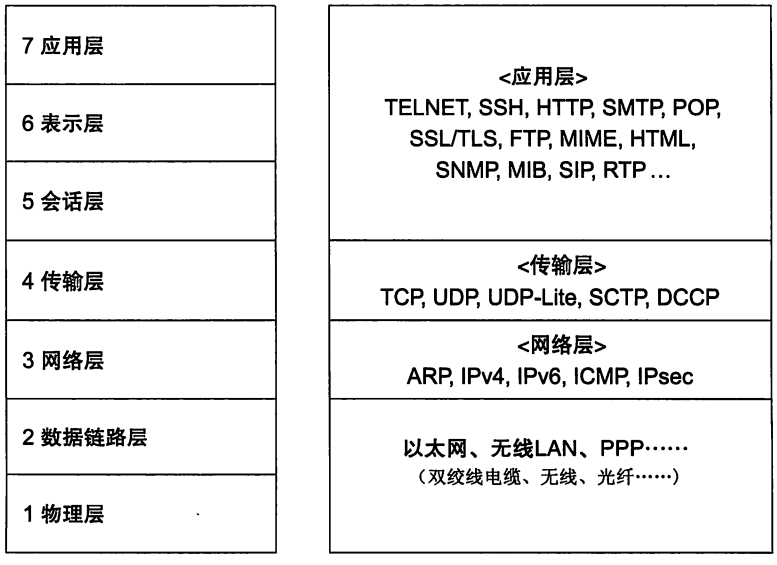
第9章

网络安全

本章旨在介绍互联网中网络安全的重要性及其相关的实现技术。



9.1 TCP/IP 与网络安全

起初，TCP/IP 只用于一个相对封闭▼的环境，之后才发展为并无太多限制、可以从远程访问更多资源的形式。因此，“安全”这个概念并没有引起人们太多的关注。然而，随着互联网的日益普及，发生了很多非法访问、恶意攻击等问题，着实影响了企业和个人的利益。由此，网络安全逐渐成为人们不可忽视一个重要内容。

▼并非不固定数目，而是在一个特定的用户群范围内。

互联网向人们提供了很多便利的服务。为了让人们能够更好、更安全的利用互联网，只有牺牲一些便利性来确保网络的安全。因此，“便利性”和“安全性”作为两个对立的特性兼容并存，产生了很多新的技术。随着恶意使用网络的技术不断翻新，网络安全的技术也在不断进步。今后，除了基本的网络技术外，通过正确理解安全相关的技术、制定合理的安全策略▼、按照制定的策略进行网络管理及运维成为一个重要的课题。

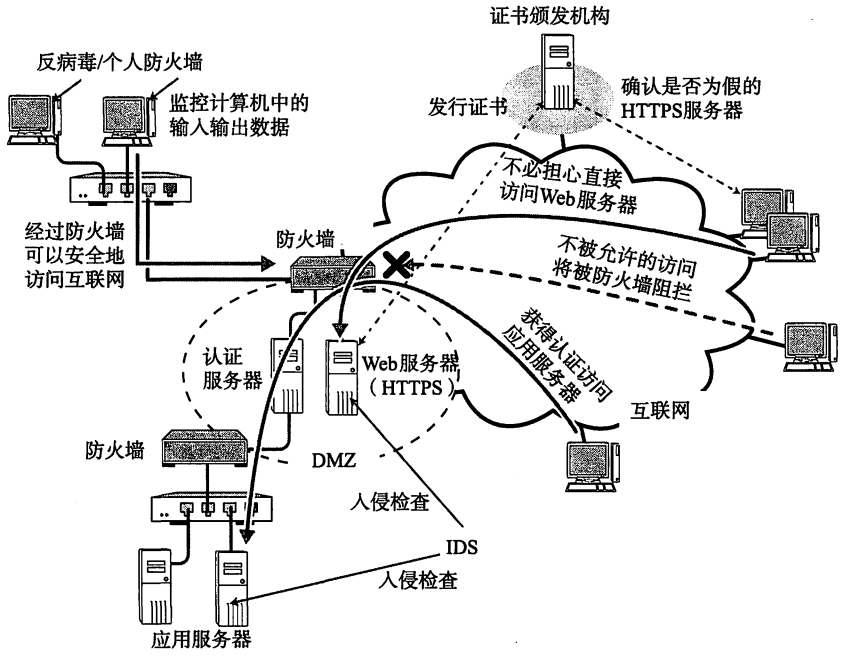
▼安全策略是指在如公司等组织内部，针对信息处理明文规定的统一标准和方法。

9.2 网络安全构成要素

随着互联网的发展，对网络的依赖程度越高就越应该重视网络安全。尤其是现在，对系统的攻击手段愈加多样化，某种特定程度的技术远不足以确保一个系统的安全。网络安全最基本的要领是要有预备方案。即不是在遇到问题的时候才去处理，而是通过对可能发生的问题进行预测，在可行的最大范围内为系统制定安保对策，进行日常运维，这才是重中之重。

TCP/IP 相关的安全要素如图 9.1 所示。在此，我们针对每一个要素进行介绍。

图 9.1 构造安全系统的要素



9.2.1 防火墙

组织机构（域）内部的网络与互联网相连时，为了避免域内受到非法访问的威胁，往往会设置防火墙▼。

▼使用 NAT（NAPT）的情况下，由于限定了可以从外部访问的地址，因此也能起到防火墙的作用。

防火墙的种类和形态有很多种。例如，专门过滤（不过滤）特定数据包的包过滤防火墙、数据到达应用以后由应用处理并拒绝非法访问的应用网关。这些防火墙都有基本相同的设计思路，那就是“暴露给危险的主机和路由器的个数要有限”。

如果网络中有 1000 台主机，若为每一台主机都设置非法访问的对策，那将是非常繁琐的工作。而如果设置防火墙的话，可以限制从互联网访问的主机个数▼。将安全的主机和可以暴露给危险的主机加以区分，只针对后者集中实施安全防护。

▼具体请参考 9.2.2 节后面的 DMZ。

如图 9.2 所示，这是一个设置防火墙的例子。图中，对路由器设置了只向其发送特定地址和端口号的包。即设置了一个包过滤防火墙。

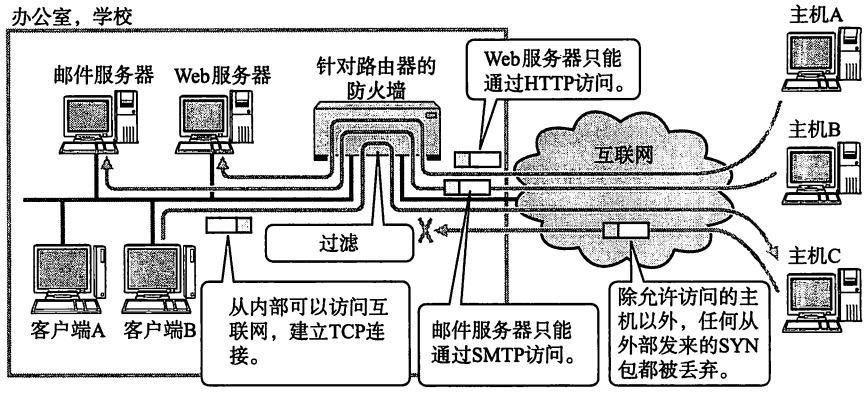
当从外部过来 TCP 通信请求时，只允许对 Web 服务器的 TCP 80 端口和邮件服务器的 TCP 25 端口的访问。其他所有类型的包全部丢弃▼。

▼实际上还有一些 DNS 等其他不得不让通过的包。

此外，建立 TCP 连接的请求只允许从内网发起。关于这一点，防火墙可以通

过监控 TCP 包首部中的 SYN 和 ACK 标志位来实现。具体为，当 SYN=1，ACK=0 时属于互联网发过来的包，应当废弃。有了这样的设置以后，只能从内网向外建立连接，而不能从外网直接连接内网。

图 9.2
防火墙举例



9.2.2　IDS（入侵检测系统）

数据包符合安全策略，防火墙才会让其通过。即只要与策略相符，就无法判断当前访问是否为非法访问，所以全部允许通过。

而 IDS 正是检查这种已经侵入内部网络进行非法访问的情况，并及时通知给网络管理员的系统。

IDS 根据不同的用途可以提供各种不同的功能。从设置形式上看，一般在防火墙或 DMZ 等边界设备上进行设置。有了这样监控、检测边界的功能，就可以设置在网络内部、全网或个别特殊的服务器上进行监控。

从功能上看，IDS 有定期采集日志、长期监控、通知异常等功能。它可以监控网络上流动的所有数据包。为了确保各种不同系统的安全，IDS 可以与防火墙相辅相成，实现更为安全的网络环境。

DMZ 定义

在连接互联网的网络中，可以设置一个服务器并在这台服务器上建立一个允许从互联网直接进行通信的专用子网。这种将外网与内网隔开的专用子网就叫做 DMZ（DeMilitarized Zone，非军事化区）。

在 DMZ 中设置的这个服务器对外公开，从而可以排除外部过来的非法访问。万一这台对外公开的服务器遇到侵袭，也不会波及内部网络。

作为 DMZ 的主机必须充分实施安全策略才能得以应付外来入侵。

9.2.3　反病毒/个人防火墙

反病毒和个人防火墙是继 IDS 和防火墙之后的另外两种安全对策，它们往往是用户使用的计算机或服务器上运行的软件。既可以监控计算机中进出的所有包、数据和文件，也可以防止对计算机的异常操作和病毒入侵。

一个企业，通常会保护自己网内所有的客户端 PC。这样可以防范病毒穿过防火墙之后的攻击。

近年来，网络上的攻击形式日趋复杂，其方法的不断演化真可谓“用心良苦”。有些黑客发送带有病毒或蠕虫的邮件感染系统，还有些可能会直接攻击操作系统本身的弱点。这些黑客甚至通过时间差或复杂的传染路径等方式隐藏攻击源，行为及其恶劣，严重影响了人们正常的工作生活。

反病毒/个人防火墙正是为了防范上述威胁、保护客户端 PC 的一种方法。这种方法不仅可以达到防范病毒的目的，一旦某一台机器发生病毒感染时，它可以通过消除病毒，使其尽量避免因病毒的扩散而产生更严重后果的影响。

此外，一般的反病毒/个人防火墙的产品也开始提供诸如防止垃圾邮件的接收、阻止广告弹出以及阻止访问受禁止网站的 URL 过滤等功能。有了这些功能可以防止一些潜在的威胁以及避免降低生产力。

PKI（公钥基础结构）

PKI（Public Key Infrastructure，公钥基础结构）是一种通过可信赖的第三方检查通信对方是否真实而进行验证的机制。这里所提到的可信赖的第三方在 PKI 中称作认证机构（CA：Certificate Authority）。用户可以利用 CA 颁发的“数字证书”验证通信对方的真实性。

该数字证书包含用户身份信息、用户公钥信息▼以及证书签发机构对该证书的数字签名信息。其中证书签发机构的数字签名可以确保用户身份信息和公钥信息的真实合法性。而公钥信息可以用于加密数据或验证对应私钥的签名。使用公钥信息加密后的数据，只能由持有数字证书的一方读取，这在使用信用卡等对于安全要求较高的场合极为重要。

PKI 还用于加密邮件和 Web 服务器的 HTTPS▼通信中。

▼公钥信息用于加密数据。持有数字证书的一方若想使用公钥加密的数据，只能由自己持有的私钥进行解密后方可使用。关于公钥、私钥的更多细节请参考 9.5 节。

▼关于 HTTPS 的更多细节请参考 9.4.2 节。

9.3 加密技术基础

一般情况下，网页访问、电子邮件等互联网上流动的数据不会被加密。另外，互联网中这些数据经由哪些路径传输也不是使用者可以预知的内容。因此，通常无法避免这些信息会泄露给第三方。

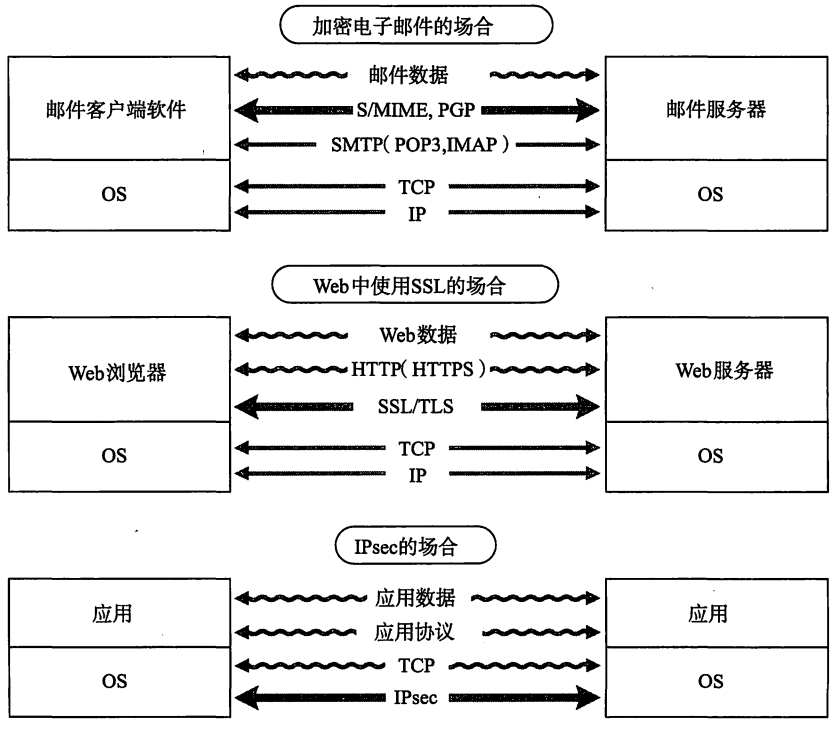
为了防止这种信息的泄露、实现机密数据的传输，出现了各种各样的加密技术。加密技术分布与 OSI 参考模型的各个阶层一样，相互协同保证通信。

表 9.1
加密技术的逐层分类

分　层	加密技术
应用层	SSH、SSL-Telnet、PET▼ 等远程登录、PGP、S/MIME 等加密邮件
表示层、传输层	SSL/TLS、SOCKS V5 加密
网络层	IPsec
数据链路层	Ethernet、WAN 加密装置、PPTP（PPP）

▼ Privacy Enhanced Telnet

图 9.3
各层加密应用举例

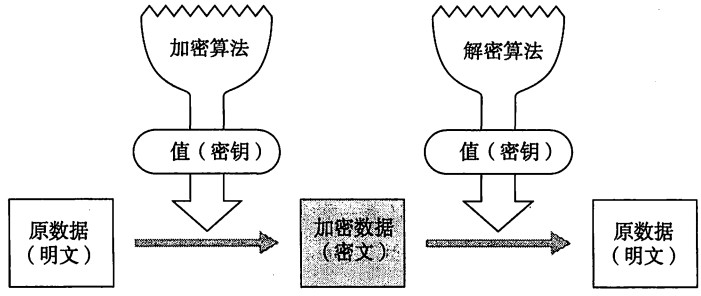


*大箭头表示进行加密的阶层。
从而可以保护在该层以上的数据不被窃听。

9.3.1 对称密码体制与公钥密码体制

加密是指利用某个值（密钥）对明文的数据通过一定的算法变换成加密（密文）数据的过程。它的逆反过程叫做解密。

图 9.4
加密过程



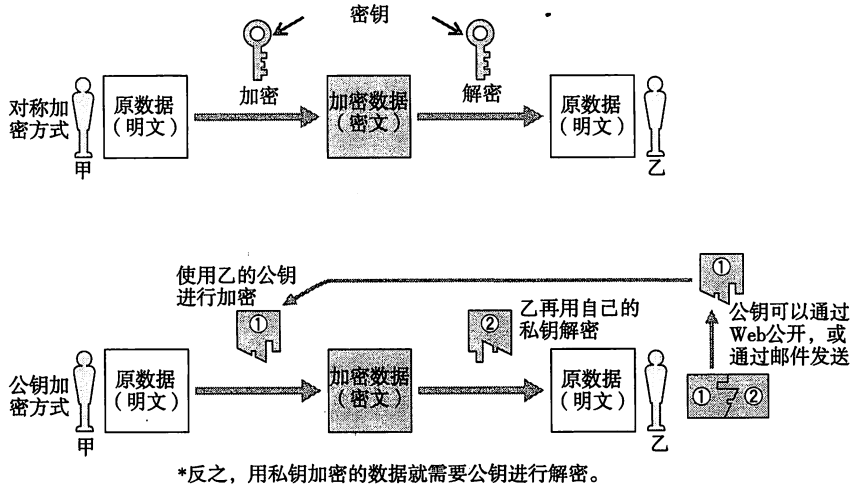
加密和解密使用相同的密钥叫做对称加密方式。反之，如果在加密和解密过程中分别使用不同的密钥（公钥和私钥）则叫做公钥加密方式。在对称加密方式中，最大的挑战就是如何传递安全的密钥。而公钥加密方式中，仅有一方的密钥是无法完成解密的，还必须严格管理私钥。通过邮件发送公钥、通过 Web 公开发布公钥、或通过 PKI▼ 分配等方式，才得以在网络上安全地传输密钥。不过，相比对称加密方式，后者在加密和解密上需要花费的时间较长，在对较长的消息进行加密时往往采用两者结合的方式▼。

▼关于 PKI 请参考 9.2.3 节的最后部分。

▼参考 9.2.4 节。

对称加密方式包括 AES（Advanced Encryption Standard）、DES（Data Encryption Standard）等加密标准，而公钥加密方法中包括 RSA、DH（Diffie-Hellman）、椭圆曲线等加密算法。

图 9.5
对称加密方式与公钥加密方式



*反之，用私钥加密的数据就需要公钥进行解密。

9.3.2 身份认证技术

在实施安全对策时，有必要验证使用者的正确性和真实性。如果不是正当的使用者要拒绝其访问。为此，需要数据加密的同时还要有认证技术。

认证可以分为如下几类。

- 根据所知道的信息进行认证

  指使用密码或私有代码（私有识别码）的方式。为了不让密码丢失或不被轻易推测出来，用户自己需要多加防范。使用公钥加密方式进行的数字认证，就需要验证是否持有私钥。

- 根据所拥有的信息进行认证

  指利用 ID 卡、密钥、电子证书、电话号码等信息的方式。在移动手机互联网中就是利用手机号码或终端信息进行权限认证。

- 根据独一无二的体态特征进行认证

  指根据指纹、视网膜等个人特有的生物特征进行认证的方式。

从认证级别和成本效益的角度考虑，一般会综合上述 3 种方式的情况更为普遍。另外，还有一种集合各种终端、服务器和应用的认证于一起进行综合管理的技术叫做 IDM（IDentity Management）。

9.4 安全协议

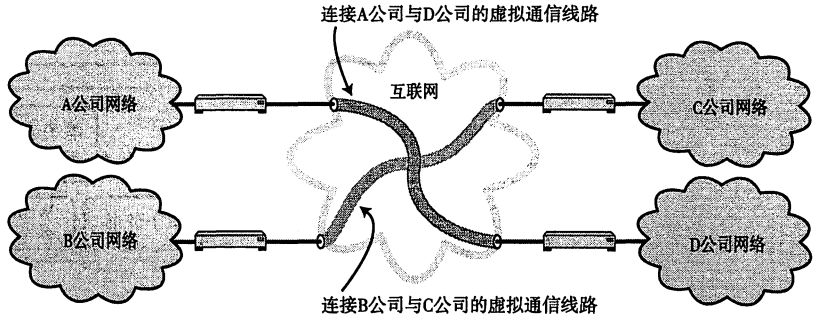
9.4.1 IPsec 与 VPN

以前，为了防止信息泄露，对机密数据的传输一般不使用互联网等公共网络（Public Network），而是使用由专线连接的私有网络（Private Network）。从而在物理上杜绝了窃听和篡改数据的可能。然而，专线的造价太高是一个不可回避的问题。

为了解决此类问题，人们想出了在互联网上构造一个虚拟的私有网络。即VPN（Virtual Private Network，虚拟专用网）▼。互联网中采用加密和认证技术可以达到“即使读取到数据也无法读懂”、“检查是否被篡改”等功效。VPN正是一种利用这两种技术打造的网络。

▼关于VPN请参考3.7.7节。

图9.6 互联网上的VPN



在构建VPN时，最常被使用的是IPsec。它是指在IP首部的后面追加“封装安全有效载荷”▼和“认证首部”▼，从而对此后的数据进行加密，不被盗取者轻易解读。

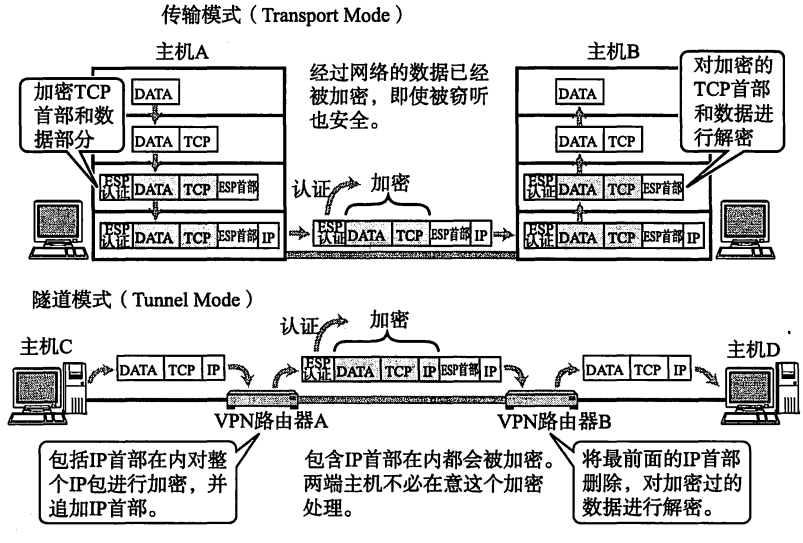
▼ESP，Encapsulating Security Payload。

▼AH，Authentication Header。

在发包的时候附加上述两个首部，可以在收包时根据首部对数据进行解密，恢复成原始数据。由此，加密后的数据不再被轻易破解，即使在途中被篡改，也能够被及时检测。

基于这些功能，VPN的使用者就可以不必设防地使用一个安全的网络环境。

图9.7 通过IPsec加密IP包



9.4.2　TLS/SSL 与 HTTPS

现在有很多互联网应用已经逐渐进入人们的生活。例如网上购物、网上订车票、订飞机票或预订演出票等。在这些系统的支付过程中经常会涉及信用卡网上支付，而网上银行系统还需要用户直接在网上输入账号和密码。

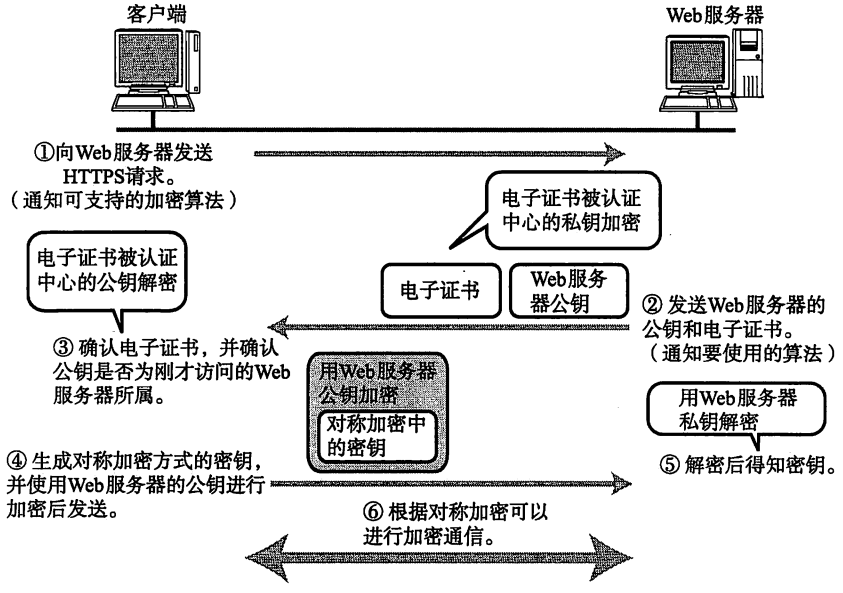
而信用卡卡号、银行账号、密码都属于个人的机密信息。因此，在网络上传输这些信息时有必要对它们进行加密处理。

Web 中可以通过 TLS/SSL▼ 对 HTTP 通信进行加密。使用 TLS/SSL 的 HTTP 通信叫做 HTTPS 通信。HTTPS 中采用对称加密方式。而在发送其公共密钥时采用的则是公钥加密方式▼。

▼ Transport Layer Security/Secure Sockets Layer。由网景公司最早提出的名称叫 SSL，标准化以后被称作 TLS。有时两者统称为 SSL。

▼对称加密虽然速度快，但是密钥管理是巨大的挑战。公钥加密密钥管理相对简单，但是处理速度非常慢。TLS/SSL 将两者进行取长补短令加密过程达到了极好的效果。由于谁都可以发送公钥，使得密钥管理更为简单。

图 9.8
HTTPS



▼ Certificate Authority

确认公钥是否正确主要使用认证中心（CA▼）签发的证书，而主要的认证中心的信息已经嵌入到浏览器的出厂设置中。如果 Web 浏览器中尚未加入某个认证中心，那么会在页面上提示一个警告信息。此时，判断认证中心合法与否就要由用户自己决定了。

9.4.3　IEEE802.1X

IEEE802.1X 是为了能够接入 LAN 交换机和无线 LAN 接入点而对用户进行认证的技术。并且它只允许被认可的设备才能访问网络。虽然它是一个提供数据链路层控制的规范，但是与 TCP/IP 关系紧密。一般，由客户端终端、AP（无线基站）或 2 层交换机以及认证服务器组成。

IEEE802.1X 中当有一个尚未经过认证的终端连接 AP（如图 9.9 中的①）时，起初会无条件地让其连接到 VLAN，获取临时的 IP 地址。然而此时终端只能连接认证服务器（如图 9.9 中的②）。

连到认证服务器后，用户被要求输入用户名和密码（如图 9.9 中的③）。认证服务器收到该信息以后，将该用户所能访问的网络信息通知给 AP 和终端（如

图 9.9 中的④)。

随后 AP 会进行 VLAN 号码（该终端连接网络必要的信息）的切换（如图 9.9 中的⑤)。终端则由于 VLAN 的切换进行 IP 地址重置（如图 9.9 中的⑥)，最后才得以连接网络（如图 9.9 中的⑦)。

公共无线局域网中，一般也会进行用户名和密码的加密和认证。不过也可以通过 IC 卡或证书、MAC 地址确认等第三方信息进行更为严格的认证。

IEEE802.1X 中使用 EAP▼。EAP 由 RFC3748 以及 RFC5247 定义。

▼ Extensible Authentication Protocol，可扩展身份认证协议。

图 9.9
IEEE802.1X