第 4 章　电子商务安全

本章学习目标

本章主要介绍电子商务安全的基础知识，以及电子商务安全的策略与技巧。通过本章的学习，读者应掌握以下内容:

- 计算机病毒防治
- 防火墙技术
- 安全检测措施
- 识别和认证技术
- 电子加密技术
- 安全电子交易技术
- 保证电子商务的安全性、合法性和确认网络上交易双方的身份

案例：网银大盗

2004 年 9 月 9 日台湾警方侦破首宗两岸黑客联手入侵台湾网络银行的重大金融犯罪，在花莲市逮捕台湾黑客陈崇顺，查扣邮件账号资料 4500 万笔。嫌犯在 3 个月内盗领 5 家网络银行数百万元新台币，被害客户中甚至有存款金额高达 2 亿元新台币的“大户”。警方于 8 日持搜捕证赴花莲直捣黄龙，当场破获该黑客盗领集团的台湾地区犯罪工作室与布满密密麻麻网络线路的计算机机房，现场查出作案用的网络服务器主机 4 部、调制解调器 4 台、网络交换机一台、台湾各家网络银行客户账号密码及知名网络公司拍卖账号密码数万笔、邮件账号名单 4500 万笔，并将涉案盗领转账的台湾主要犯罪嫌疑人陈崇顺抓获。

陈崇顺与大陆黑客勾结，先取得最新型木马程序，再利用工作室中的 4 台服务器主机，将木马程序伪装成微软公司或是色情、拍卖网站等广告信件大量寄发电子邮件，自 2004 年 2 月中旬开始发送电子邮件，一直持续到 3 月中旬，总计散发了 1800 多万份的有效电子邮件，好奇的群众被广告信件吸引开启邮件，在不知不觉中下载木马程序常驻计算机中，陈崇顺再伺机撷取被害人在网络上使用的网络银行网址及账号、密码等机密资料，自动回传给位于大陆的伺服主机，待陈崇顺登入该主机收取账号、密码等资料后，再通过台湾主机层层转接遥控位于世界各地的跳板主机，侵入岛内网络银行客户账户中盗转存款至台湾人头账户，最后由他人在大陆的 ATM 提款机提领现金，借此，避免警方发现逃避警方追查。

据陈崇顺估计，自 2004 年 2 月至案发时至少已得手约数十万笔民众账户密码，但警方查到的只有数万笔而已，陈崇顺对此供称其中约 10 万笔网络银行账户密码已转交给大陆黑客使用，伺机盗领存款，自己未留备份，所以不在他的数据库中。

“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖也并不

“刻意”感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种者电脑的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种者的电脑。

近日被我国反病毒专家截获的“网银大盗”就属于木马病毒的一种，而且很快就出现变种，当该病毒检测到用户在网上银行网页上进行支付或转账等操作时，就会记录当前的键盘输入，然后发送到病毒作者的服务器上，从而达到窃取用户账号和密码的目的。

有关数据显示，网上银行的用户已有近千万，每年通过网上银行流通的资金超过千亿。可见，当前制约电子商务发展的关键因素，已不仅仅是产品技术方面的问题，更多的是出自对安全性的考虑。

【资料来源】：新浪科技讯　时间：2004-08-04

4.1　网络安全与防范

随着网络的发展，一系列侵犯网络安全和信息安全的恶性事件不断地给人们敲响警钟。根据国际标准化组织 ISO 对网络安全的定义，它是指为数据处理系统建立和采取的科技和管理的安全保护，以保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和显露。

4.1.1　计算机病毒防治

4.1.1.1　网络病毒的威胁

病毒本身已是令人头痛的问题。但随着 Internet 开拓性的发展，病毒可能为网络带来灾难性后果。Internet 带来了两种不同的安全威胁，一种威胁来自文件下载，这些被浏览的或是通过 FTP 下载的文件中可能存在病毒。而共享软件（Public Shareware）和各种可执行文件，如格式化的介绍性文件（Formatted Presentation）已经成为病毒传播的重要途径。并且 Internet 上还出现了 Java 和 ActiveX 形式的恶意小程序。另一种威胁来自于电子邮件。大多数的 Internet 邮件系统提供了在网络间传送附带格式化文档邮件的功能。只要简单地敲敲键盘，邮件就可以发给一个或一组收信人。因此，受病毒感染的文档或文件就可能通过网关和邮件服务器涌入企业网络。

另一种网络化趋势也加重了病毒的威胁。这种趋势是向群件应用程序发展的，如 Lotus Notes、Microsoft Exchange、Novell Groupwise 和 Netscape Colabra。由于群件的核心是在网络内共享文档，那么就为病毒的发展提供了丰富的基础。而群件不仅仅是共享文档的储藏室，它还提供合作功能，能够在相关工作组之间同步传输文档。这大大提高了病毒传播的机会。因此群件系统的安全保护显得格外重要。

1. 计算机网络病毒的类型

计算机网络病毒包括下面几种类型：

（1）蠕虫。

（2）逻辑炸弹。

（3）特洛伊木马。

（4）陷阱入口。

（5）核心大战。

2. 计算机网络病毒的危害

（1）对网络的危害。病毒程序通过“自我复制”传染正在运行的其他程序，并与正常运

行的程序争夺计算机资源；病毒程序可冲毁存储器中的大量数据，致使计算机其他用户的数据蒙受损失；病毒不仅侵害所使用的计算机系统，而且侵害与该系统联网的其他计算机系统；病毒程序可导致以计算机为核心的网络失灵。

（2）病毒对计算机系统的危害。破坏磁盘文件分配表，使用户在磁盘上的信息丢失；将非法数据置入操作系统（如 DOS 的内存参数区），引起系统崩溃；删除硬盘或软盘上特定的可执行文件或数据文件；修改或破坏文件的数据；影响内存常驻程序的正常执行；在磁盘上产生虚假坏分区，从而破坏有关的程序或数据文件；更改或重新写入磁盘的卷标号；不断反复传染拷贝，造成存储空间减少，并影响系统运行效率；对整个磁盘或磁盘上的特定磁道进行格式化；系统挂起，造成显示屏幕或键盘的封锁状态。

4.1.1.2 企业范围的病毒防治

首先应该考虑在何处安装病毒防治软件。在企业中，重要的数据往往保存在位于整个网络中心结点的文件服务器上，这也是病毒攻击的首要目标。为保护这些数据，网络管理员必须在网络的多个层次上设置全面保护措施。

有效的多层保护措施必须具备 4 个特性：

（1）集成性：所有的保护措施必须在逻辑上是统一的和相互配合的。

（2）单点管理：作为一个集成的解决方案，最基本的是必须有一个安全管理的聚焦点。

（3）自动化：系统需要有能自动更新病毒特征码数据库和其他相关信息的功能。

（4）多层分布：这个解决方案应该是多层次的，适当的防毒部件在适当的位置分发出去，最大限度地发挥作用，而又不会影响网络负担。防毒软件应该安装在服务器工作站和邮件系统上。

工作站是病毒进入网络的主要途径，所以应该在工作站上安装防病毒软件。这种做法是比较合理的。因为病毒扫描的任务是由网络上所有工作站共同承担的，这使得每台工作站承担的任务都很轻松，如果每台工作站都安装最新防毒软件，这样就可以在工作站的日常工作中加入病毒扫描的任务，性能可能会有少许下降，但无需增添新的设备。

邮件服务器是防病毒软件的第二个着眼点，邮件是重要的病毒来源。邮件在发往其目的地前，首先进入邮件服务器并被存放在邮箱内，所以在这里安装防病毒软件是十分有效的。假设工作站与邮件服务器的数量比是 100:1，那么这种做法显而易见节省费用。

备份服务器是用来保存重要数据的。如果备份服务器崩溃了，那么整个系统也就彻底瘫痪了。备份服务器中受破坏的文件将不能被重新恢复使用，甚至会反过来感染系统。避免备份服务器被病毒感染是保护网络安全的重要组成部分，因此好的防病毒软件必须能够解决这个冲突，它能与备份系统相配合，提供无病毒的实时备份和恢复。

网络中任何存放文件和数据库的地方都可能出问题，因此需要保护好这些地方。文件服务器中存放企业重要的数据。在 Internet 服务器上安装防病毒软件是头等重要的，上载和下载的文件不带有病毒对你和客户的网络都是非常重要的。

4.1.1.3 布署和管理防病毒软件

布署防病毒软件的实际操作一般包括以下步骤：

（1）制定计划。了解所管理的网络上存放的是什么类型的数据和信息。

（2）调查。选择能满足要求并且具备尽量多功能的防病毒软件。

（3）测试。在小范围内安装和测试所选择的防病毒软件，确保其工作正常并且与现有的网络系统和应用软件相兼容。

（4）维护。管理和更新系统确保其能发挥预计的功能，并且可以利用现有的设备和人员进行管理；下载病毒特征码数据库更新文件，在测试范围内进行升级，彻底理解这种防病毒系统的重要方面。

（5）系统安装。在测试得到满意结果后，就可以将此种防病毒软件安装在整个网络范围内。

4.1.2　防火墙技术

1. 防火墙原理

作为近年来新兴的保护计算机网络安全技术性措施，防火墙（FireWall）是一种隔离控制技术，在某个机构网络和不安全网络（如 Internet）之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止专利信息从企业的网络上被非法输出。防火墙是一种被动防卫技术，由于它假设了网络的边界和服务，因此对内部的非法访问难以有效地控制。因此，防火墙最适合于相对独立的与外部网络互连途径有限、网络服务种类相对集中的单一网络。

作为 Internet 网的安全性保护软件，FireWall 已经得到广泛的应用。通常企业为了维护内部的信息系统安全，在企业网和 Internet 间设立 FireWall 软件。企业信息系统对于来自 Internet 的访问，采取有选择的接收方式。它可以允许或禁止一类具体的 IP 地址访问，也可以接收或拒绝 TCP/IP 上的某一类具体的应用。如果在某台 IP 主机上有需要禁止的信息或危险的用户，则可以通过设置使用 FireWall 过滤掉从该主机发出的包。如果企业只是使用 Internet 的电子邮件和 WWW 服务器向外部提供信息，那么就可以在 FireWall 上设置使得只有这两类应用的数据包可以通过。这对于路由器来说，就不仅要分析 IP 层的信息，而且还要进一步了解 TCP 传输层甚至应用层的信息以进行取舍。FireWall 一般安装在路由器上以保护子网，也可以安装在主机上，保护主机不受侵犯。

2. 防火墙的种类

真正意义下的防火墙有两类：一类被称为标准防火墙；一类叫双家网关。标准防火墙系统包括一个 Unix 工作站，该工作站的两端各安一个路由器进行缓冲。其中一个路由器的接口是外部世界，即公用网；而另一个则连接内部网。标准防火墙使用专门的软件，并要求较高的管理水平，而且在信息传输上有一定的延迟。而双家网关则是对标准防火墙的扩充，双家网关又称堡垒主机或应用层网关，它是单个系统，但却能同时完成标准防火墙的所有功能，其优点是能运行更复杂的应用，同时防止在互联网和内部系统之间建立的任何直接的连接，可以确保数据包不能直接从外部网络到达内部网络，反之亦然。

随着防火墙技术的进步，在双家网关的基础上又演化出两种防火墙配置：一种是隐蔽主机网关；另一种是隐蔽智能网关（隐蔽子网）。隐蔽主机网关是一种常见的防火墙配置。顾名思义，这种配置一方面将路由器进行隐蔽，另一方面在互联网和内部网之间安装堡垒主机。堡垒主机装在内部网上，通过路由器的配置，使该堡垒主机成为内部网与互联网进行通信的惟一系统。目前技术最为复杂而且安全级别最高的防火墙当属隐蔽智能网关。所谓隐蔽智能网关是将网关隐藏在公共系统之后，它是互联网用户惟一能见到的系统。所有互联网功能则是经过这个隐藏在公共系统之上的保护软件来进行的。一般来说，这种防火墙是最不容易被破坏的。

从实现原理上分，防火墙技术包括四大类：网络级防火墙（也叫包过滤型防火墙）、应用级网关、电路级网关和规则检查防火墙。它们之间各有所长，具体使用哪种或是否混合使用，要看具体需要。

（1）网络级防火墙。网络级防火墙一般是基于源地址和目的地址、应用或协议以及每个IP 包的端口来做出通过与否的判断。路由器便是“传统”的网络级防火墙，大多数的路由器都能通过检查信息来决定是否将所收到的包转发，但它不能判断出 IP 包来自何方、去向何处。

防火墙检查每条规则直至发现包中的信息与某规则相符。如果没有规则能符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。

（2）应用级网关。应用级网关能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册和稽核。它针对特别的网络应用服务协议即数据过滤协议，并且能够对数据包分析并形成相关报告。应用网关对某些易于登录和控制所有输出输入的通信环境给予严格控制，以防有价值的程序和数据被窃取。在实际工作中，应用网关一般由专用工作站系统来完成。但每一种协议需要相应的代理软件，使用时工作量大，效率不如网络级防火墙。

应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏“透明度”。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟并且必须多次登录（Login）才能访问 Internet 或 Intranet。

（3）电路级网关。电路级网关用来监控受信任的客户或服务器与不受信任主机间的 TCP 握手信息，这样来决定会话（Session）是否合法，电路级网关是在 OSI 模型中的会话层上来过滤数据包，这样比包过滤防火墙要高两层。

电路级网关还提供一个重要的安全功能：代理服务器（Proxy Server）。代理服务器是设置在 Internet 防火墙网关的专用应用级代码。这种代理服务准许网管员允许或拒绝特定的应用程序或应用的特定功能。包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许特定的数据包通过，一旦判断条件满足，防火墙内部网络结构和运行状态便“暴露”在外来用户面前，这就引入了代理服务的概念，即防火墙内外计算机系统应用层的“链接”由两个终止于代理服务的“链接”来实现，这就成功地实现了防火墙内外计算机系统的隔离。同时代理服务还可用于实施较强的数据流监控、过滤、记录和报告等功能。代理服务技术主要通过专用计算机硬件（如工作站）来承担。

（4）规则检查防火墙。规则检查防火墙结合了包过滤防火墙、电路级网关和应用级网关的特点。它像包过滤防火墙一样，规则检查防火墙能够在 OSI 网络层上通过 IP 地址和端口号，过滤进出的数据包。它也像电路级网关一样，能够检查 SYN 和 ACK 标记和序列数字是否逻辑有序。当然它也像应用级网关一样，可以在 OSI 应用层上检查数据包的内容，查看这些内容是否符合企业网络的安全规则。

规则检查防火墙虽然集成前三者的特点，但是不同于应用级网关的是，它并不打破客户机/服务器模式来分析应用层的数据，允许受信任的客户机和不受信任的主机建立直接连接。规则检查防火墙不依靠与应用层有关的代理，而是依靠某种算法来识别进出的应用层数据，这些算法通过已知合法数据包的模式来比较进出数据包，这样从理论上就比应用级代理在过滤数据包上更有效。

3. 使用防火墙

防火墙是企业网安全问题的流行方案，即把公共数据和服务置于防火墙外，使其对防火

墙内部资源的访问受到限制。一般来说，防火墙是不能防病毒的，尽管有不少的防火墙产品声称其具有这个功能。防火墙技术的另一个弱点在于数据在防火墙之间的更新是一个难题，如果延迟太大将无法支持实时服务请求。此外，防火墙采用滤波技术，滤波通常使网络的性能降低50%以上，如果为了改善网络性能而购置高速路由器，又会大大提高经济预算。

作为一种网络安全技术，防火墙具有简单实用的特点，并且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求。但是如果防火墙系统被攻破，则被保护的网络处于无保护状态。如果企业希望在 Internet 上开展商业活动，与众多的客户进行通信，则防火墙不能满足要求。

4. 防火墙的安全体系

（1）双重宿主主机体系。防火墙内部的网络系统能与双重宿主主机通信，同时防火墙外部的网络系统（在互联网上）也能与双重宿主主机通信。

双重宿主主机需要仔细检查所通过数据包的内容，并将其改头换面重新包装。如果数据包中有违禁的东西，则根据内部网络的安全策略进行处理。例如图 4-1 中外部网络的 A 数据包通过防火墙后则变成了 A’数据包，内部网络的 B 数据包通过防火墙后就变成了 B’数据包。在双重宿主主机上，有内外数据的缓冲区，当通信繁忙时也可以起缓冲的作用。

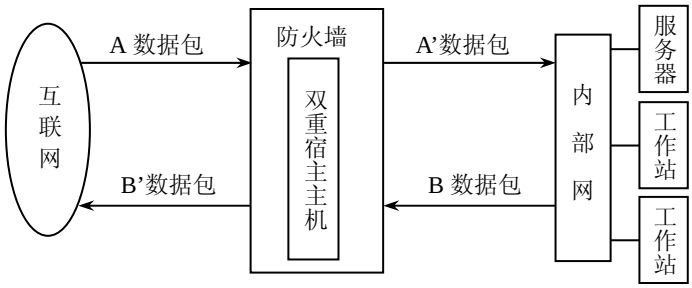

图 4-1　双重宿主主机体系结构示意图

（2）屏蔽主机体系。屏蔽主机体系是使用单独的路由器提供来自与内部网络相连的主机服务。这种体系的防火墙是由路由器和堡垒主机组成。如图 4-2 所示就是路由器充当防火墙的体系。从图中可以看出，堡垒主机位于内部网络上，在屏蔽的路由器上的数据包过滤是按这种方式设置的：即堡垒主机是互联网连接到内部网络系统的桥梁，任何外部系统试图访问内部系统或服务，都必须连接到这台堡垒服务器上。因此堡垒主机需要拥有高等级的安全。

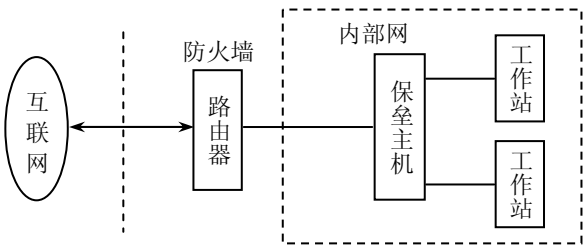

图 4-2　屏蔽主机体系结构示意图

（3）屏蔽子网体系。屏蔽子网体系增加额外的安全层到被屏蔽主机体系中，即通过添加

虚拟的内部网络更进一步地把内部网络与互联网隔开（如图 4-3 所示）。

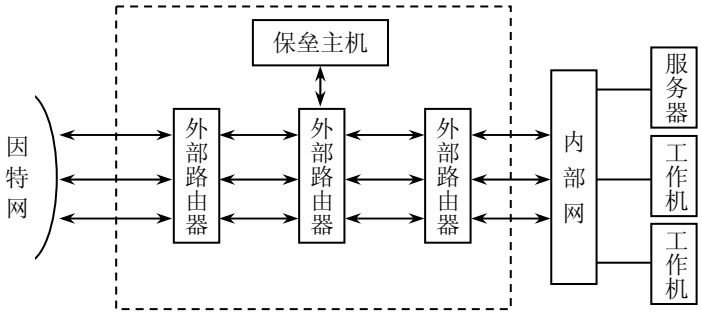

图 4-3　屏蔽子网体系结构示意图

即使侵袭者通过了第一道防火墙，他所看到的是虚拟的内部网络和堡垒主机，在这个虚拟的环境中，他看到的只是一个假象，并没有什么实质的东西供他利用；相反，如果他稍有“不慎”，可能就会露出“马脚”。

屏蔽子网体系的最简单形式是防火墙为两个屏蔽路由器，每一个都连接到虚拟的内部网即周边网上。一个位于周边网与内部网之间，另一个位于周边网与外部网之间（通常为互联网）。

4.1.3　安全检测措施

1. 网络安全检测思路与技巧

对于主机的安全检测，通常直接采用 nmap 或者类似软件进行扫描，然后针对主机操作系统及其开放端口判断主机的安全程度，但这种方法往往失之粗糙，仔细考虑了一下觉得按下面的流程进行判别是比较完整的。

（1）通过 DNS 查询得到目标网络拓扑基本情况，比如有几台主机，各自起到的服务等。这是必要的步骤因为检测应该针对网络而不是单一主机。

（2）用 nmap 进行端口扫描，判断操作系统，结合自己的经验，必要的时候抓 banner，判断出目标主机的操作系统类型。

（3）用 nessus 进行普通漏洞的扫描，得到大致的报告。对报告进行分析，nessus 的报告有些地方并不准确而且有漏扫或误报的情况。比如严重的 unicode 漏洞机器明明有，它却扫不到，对这种情况必须有人工的判断。

（4）cgi 漏洞也必须有专门的扫描器进行，可以结合 whisker 或者 twwwscan 或者 xscan，自己判断需要增加哪些危险 cgi 的检测。

上面只是最简单的初学电脑的人都能够较好完成的工作流程，但是如果在上面的各种扫描方式得到的信息无法分析出目标操作系统的情况甚至系统类型时，应该怎么办呢？这种事情现在经常遇到，因为大多数防火墙或者入侵检测系统现在都具备了动态地将 TCP/IP 协议栈如 TTL、TOS、DF、滑动窗口大小等修改或者屏蔽，使扫描工具无法得出正确结果。互联网上也有许多免费工具可以达到这一效果。因此下面要谈到其他检查方式：

（1）在有防火墙的情况下：建议使用如 hping、firewall 之类的工具，更加灵活地探测目标主机的情况，根据数据包的返回做更进一步的判断。这需要操作者掌握 TCP/IP 基本知识，并能灵活运用判断。

（2）对主页程序的检测，虽然只能在外面做些基本的输入验证检测，但按照现在常见的 web 错误，可以从下面几个方面着手分析：

1）特殊字符的过滤: &;`‘\"　*?~<>^（）[]{}$\n\r 这些字符由于在不同的系统或运行环境中具有特殊意义，如变量定义、赋值、取值、非显示字符、运行外部程序等，而被列为危险字符。但在许多编程语言、开发软件工具、数据库甚至操作系统中遗漏其中某些特殊字符的情况时常出现，从而导致出现带有普遍性的安全问题。当需要 Web 用户输入时，根据不同的数据库系统、编程语言提交带不同参数变量的 url，很可能造成服务器端资料泄露甚至可执行系统命令。

2）Web 服务器的错误编码或解码可能导致服务器信息的泄露、可执行命令、源代码泄露等错误。比较典型的是 unicode 漏洞以及各种 IIS 服务器、Apache 服务器的源代码泄露漏洞。

3）利用程序错误的边界判断而造成的缓冲区溢出进行攻击。最近的典型案例应该是 eeye.com 发现的.printer 溢出漏洞。这是 Web Server 本身的问题；但网站应用程序的编写者也可能犯下同样的错误，就是对用户输入不加验证。但这方面的错误比较不容易试出来。当在进行远程扫描时，在没有本地账号或者权限的情况下，能够搜集到尽量多的信息了。当然，主机面临的并非是远程风险，还需要具体分析。

2. 网络安全检测工具种类

（1）扫描器。扫描器是自动检测远程或本地主机安全性弱点的软件，通过使用扫描器可不留痕迹地发现远程服务器各种 TCP 端口的分配及提供的服务，以及相关的软件版本。这就能间接或直观地了解到远程主机所存在的安全问题。扫描器通过选用远程 TCP/IP 不同端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用信息（比如，是否能用匿名登录、是否有可写的 FTP 目录、是否能用 TELNET，HTTPD、是用 ROOT 还是 nobody）。

（2）嗅探器（Sniffer）。嗅探器具有软件探测功能，能够捕获网络报文的设备。嗅探器的正当用处在于分析网络的流量，以便找出所关心网络中潜在的问题。例如，假设网络的某一段运行得不是很好，报文的发送比较慢，而又不知道问题出在什么地方，此时就可以用嗅探器来做出精确的问题判断。嗅探器在功能和设计方面有很多不同。有些只能分析一种协议，而另一些能够分析几百种协议。不同的场合有不同的用处。

（3）Sniffit。Sniffit 是指网络端口探测器，配置在后台运行可以检测端口（如 TCP/IP 端口上用户的输入/输出信息。常被攻击者用来检测主机端口 23（telnet）和 110（pop3）端口）上的数据传送情况，以便轻松得到登录口令和 E-mail 账号密码。Sniffit 是破坏者所利用的工具。为了增强自身站点的安全性，必须知道攻击者所使用的各种工具。

（4）Tripwire。Tripwire 是用来检验文件完整性的非常有用的工具，通常文件检测运行的模式是：数据库生成模式、数据库更新模式、文件完整性检查、互动式数据库更新。当初始化数据库生成的时候，它生成对现有文件的各种信息的数据库文件，如果系统文件或者各种配置文件被意外地改变、替换、删除，它将每天基于原始的数据库与现有文件进行比较，发现哪些文件被更改，这样就能根据 E-mail 的结果判断是否有系统入侵等意外事件发生。

（5）Logcheck。Logcheck 是用来自动检查系统安全入侵事件和非正常活动记录的工具，它分析各种 Lintlx log 文件，像/var/log/messages、/var/log/secure、/var/log/maillog 等，然后生成一个可能有安全问题的检查报告自动发送 E-mail 给管理员。只要设置它基于每小时或者每

天用 crond 来自动运行即可。

（6）Nmap。Nmap 是用来对比较大的网络进行端口扫描的工具，它能检测该服务器有哪些 TCP/IP 端口正处于打开状态。运行它可以确保已经禁止掉不该打开的不安全的端口号。

（7）状态监视技术。状态监视技术是第三代网络安全技术。状态监视服务的监视模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各个层次实行监测，并作为安全决策的依据。监视模块支持多种网络协议和应用协议，可以方便地实现应用和服务的扩充。状态监视服务可以监视 RPC（远程过程调用）和 UDP（用户数据报）端口信息，而包过滤和代理服务则无法做到。

（8）PAM（Plug gable Authentication Modules）。PAM 是一套共享库，为系统管理员进行用户确认提供广泛地控制，它提供前端函数库用来确认用户的应用程序。PAM 库可以用单独的文件来配置，也可以通过一组配置文件来配置。PAM 可以配置成提供单一的或完整的登录过程，使用户输入口令就能访问多种服务。例如，ftp 程序传统上依靠口令机制来确认希望开始进行 ftp 会议的用户。配置了 PAM 的系统把 ftp 确认请求发送给 PAM API（应用程序接口），后者根据 pam.conf 或相关文件中的设置规则来回复。系统管理员可以设置 PAM 使一个或多个认证机制能“插入”到 PAM API 中。PAM 的优点在于其灵活性，系统管理员可以精心调整整个认证方案而不用担心破坏应用程序和计算机病毒攻击。

（9）智能卡技术。智能卡就是密钥的一种媒体，它本身含有微处理器，就像信用卡一样由授权用户所持有并由该用户赋予它口令或密码字。该密码与内部网络服务器上注册的密码一致。当口令与身份特征共同使用时，智能卡的保密性能还是相当有效的。

3. 无线入侵检测系统

现在随着黑客技术的提高，无线局域网（WLANs）受到越来越多的威胁。配置无线基站（WAPs）的失误导致会话劫持以及拒绝服务攻击（DoS）都像瘟疫一般影响着无线局域网的安全。无线网络不但因为基于传统有线网络 TCP/IP 架构而受到攻击，还有可能受到基于电气和电子工程师协会 （IEEE） 发行 802.11 标准本身的安全问题而受到威胁。为了更好的检测和防御这些潜在的威胁，无线局域网也使用了一种入侵检测系统（IDS）来解决这个问题。

（1）来自无线局域网的安全。无线局域网容易受到各种各样的威胁。像 802.11 标准的加密方法和有线对等保密（Wired Equivalent Privacy）都很脆弱。在“Weaknesses in the Key Scheduling Algorithm of RC-4”文档里就说明了 WEP key 能在传输中通过暴力破解攻击。

黑客通过欺骗（Rogue）WAP 得到关键数据。无线局域网用户在不知情的情况下，以为通过很好的信号连入无线局域网，却不知已遭到黑客的监听了。低成本和易于配置造成了无线局域网的流行，许多用户也可以在传统局域网架设无线基站（WAPs），随之而来的一些用户在网络上安装的后门程序，也造成了对黑客开放的不利环境。这正是没有配置入侵检测系统的组织机构开始考虑配置 IDS 解决方案的原因。或许架设无线基站的传统局域网用户也同样面临着遭到黑客监听的威胁。

基于 802.11 标准的网络还有可能遭到拒绝服务攻击（DoS）的威胁，从而使得无线局域网难于工作。无线通讯由于受到物理上的威胁会造成信号衰减，这些威胁包括：树木、建筑物、雷雨和山峰等破坏无线通讯的物体。像微波炉、无线电话也可能威胁基于 802.11 标准的无线网络。黑客通过无线基站发起恶意的拒绝服务攻击（DoS）会造成系统重启。另外，黑客还能通过欺骗 WAP 发送非法请求来干扰正常用户使用无线局域网。

另外一种威胁无线局域网的是 ever-increasing pace。这种威胁确实存在，并可能导致大范围地破坏，这也正是让 802.11 标准越来越流行的原因。对于这种攻击，现在暂时还没有好的防御方法，但会在将来提出更好的解决方案。

（2）入侵检测。入侵检测系统（IDS）通过分析网络中传输的数据来判断破坏系统和入侵事件。传统的入侵检测系统仅能检测和对破坏系统作出反应。如今入侵检测系统已用于无线局域网来监视分析用户的活动，判断入侵事件的类型，检测非法的网络行为，对异常的网络流量进行报警。

无线入侵检测系统同传统的入侵检测系统类似。但无线入侵检测系统加入了无线局域网的检测和对破坏系统反应的特性。

无线入侵检测系统可以通过提供商来购买，为了发挥无线入侵检测系统的优良性能，他们同时还提供无线入侵检测系统的解决方案。如今在市面上流行的无线入侵检测系统是 Airdefense RogueWatch 和 Airdefense Guard。一些无线入侵检测系统也得到了 Linux 系统的支持。例如，自由软件开放源代码组织的 Snort-Wireless 和 WIDZ 。

（3）架构。无线入侵检测系统用于集中式和分散式两种。集中式无线入侵检测系统通常用于连接单独的 sensors，搜集数据并转发到存储和处理数据的中央系统中。分散式无线入侵检测系统通过多种设备来完成 IDS 的处理和报告功能。分散式无线入侵检测系统适合较小规模的无线局域网，因为它价格便宜和易于管理。当过多的 sensors 需要时有着数据处理 sensors 花费将被禁用。所以多线程的处理和报告的 sensors 管理比集中式无线入侵检测系统花费更多的时间。

无线局域网通常被配置在相对大的场所。像这种情况，为了更好的接收信号需要配置多个无线基站（WAPs），在无线基站的位置上部署 sensors 会提高信号的覆盖范围。由于这种物理架构，大多数的黑客行为将被检测到。另外就是加强了同无线基站（WAPs）的距离能更好地定位黑客的详细地理位置。

（4）物理回应。物理定位是无线入侵检测系统的重要部分。针对 802.11 的攻击经常很快地执行，因此对攻击的回应就是必然的了，像一些入侵检测系统封锁非法的 IP。就需要部署找出入侵者的 IP 而且一定要及时。不同于传统的局域网，黑客可以攻击远程网络，无线局域网的入侵者就在本地。通过无线入侵检测系统就可以估算出入侵者的物理地址。通过 802.11 的 sensors 数据分析找出受害者，就可以更容易定位入侵者的地址。一旦确定攻击者的目标缩小，特别反映小组就拿出 Kismet 或 Airopeek 根据入侵检测系统提供的线索迅速找出入侵者。

（5）策略执行。无线入侵检测系统不但能找出入侵者还能加强策略。通过使用强有力的策略，会使无线局域网更安全。

（6）威胁检测。无线入侵检测系统不但能检测出攻击者的行为，还能检测到 rogue WAPs，识别出未加密的 802.11 标准的数据流量。

为了更好的发现潜在的 WAP 目标，黑客通常使用扫描软件如 Netstumbler 和 Kismet，使用全球卫星定位系统（Global Positioning System）来记录他们的地理位置。这些工具正因为许多网站对 WAP 的地理支持而变得流行起来。

比探测扫描更严重的是无线入侵检测系统检测到的 DoS 攻击，DoS 攻击在网络上非常普遍。DoS 攻击是因为建筑物阻挡造成信号衰减而发生的。黑客也喜欢对无线局域网进行 DoS 攻击。无线入侵检测系统能检测黑客的这种行为。

除了上文介绍的还有无线入侵检测系统能检测到 MAC 地址欺骗，它是通过顺序分析，找出那些伪装 WAP 的无线上网用户。

（7）无线入侵检测系统的缺陷。无线入侵检测系统有很多优点，但缺陷也同时存在。无线入侵检测系统毕竟是一门新技术，新技术在刚应用时都有一些 bug，无线入侵检测系统或许也存在这样的问题。随着无线入侵检测系统的飞速发展，问题也会慢慢解决。

无线入侵检测系统未来将成为无线局域网中的重要部分。虽然无线入侵检测系统存在着缺陷，但总体上优势大于劣势。无线入侵检测系统能检测到扫描，DoS 攻击和其他 802.11 的攻击，再加上强有力的安全策略，基本满足无线局域网的安全问题。随着无线局域网的快速发展，对无线局域网的攻击也越来越多，这样的系统也是非常必要的。

4.2 信息安全技术

4.2.1 识别和认证技术

按照全面的安全保护要求，认证和识别确保参与加密对话的是其本人。厂家依靠许多机制来实现认证，从安全卡到身份鉴别。前一个安全保护能确保只有经过授权的用户才能通过个人计算机进行 Internet 网上的交互式交易；后者则提供一种方法，用它生成某种形式的口令或数字签名，交易的另一方据此来认证交易伙伴。用户管理的口令通常是前一种安全措施；硬件/软件解决方案则不仅正逐步成为数字身份认证的手段，同时它也可以被可信第三方用来完成用户数字身份（ID）的相关确认。

4.2.1.1 认证和识别的基本原理

认证就是指用户必须提供他是谁的证明，如某个雇员、某个组织的代理、某个软件过程（如股票交易系统或 Web 订货系统的软件过程）。认证的标准方法就是弄清楚他是谁，他具有什么特征，他知道什么可用于识别他的东西。比如说系统中存储了他的指纹，接入网络时就必须在连接到网络的电子指纹机上提供他的指纹（这就防止他以假的指纹或其他电子信息欺骗系统），只有指纹相符才允许他访问系统。更普通的是通过视网膜血管分布图来识别，原理与指纹识别相同，声波纹识别也是商业系统采用的识别方式。网络通过用户拥有什么东西来识别的方法，一般用智能卡或其他特殊形式的标志，这类标志可以从连接到计算机上的读卡器读出来。至于说“他知道什么”，最普通的就是口令，口令具有共享秘密的属性。例如，使服务器操作系统识别入网的用户，那么用户必须把用户名和口令送到服务器。服务器将它与数据库里的用户名和口令进行比较，如果相符，就通过了认证，可以上网访问。这个口令由服务器和用户共享。更保密的认证可以是几种方法组合而成，例如用 ATM 卡和 PIN 卡。在安全方面最薄弱的一环是规程分析仪的窃听，如果口令以明码（未加密）传输，接入到网上的规程分析仪就会在用户输入账户和口令时将它记录下来，任何人只要获得这些信息就可以上网工作。

智能卡技术将成为用户接入和用户身份认证等安全要求的首选技术。用户将从持有认证执照的可信发行者手里取得智能卡安全设备，也可从其他公共密钥密码安全方案发行者那里获得。这样智能卡的读取器必将成为用户接入和认证安全解决方案的关键部分。越来越多的业内人士在积极提供智能卡安全性的解决方案。尽管这一领域的情形还不明朗，但没有理由排除这样一种可能，在数字 ID 和相关执照的可信发行者方面，某些经济组织或由某些银行拥有的信

用卡公司将成为这一领域的领导者。

电子商务的关键是安全，网上安全交易的基础是数字证书。要建立安全的电子商务系统，必须首先建立稳固、健全的 CA。否则一切网上交易都没有安全保障。

所谓系统就是大的网络环境。系统从功能上基本可以划分为 CA、RA 和 WP。核心系统和 CA 放在单独的封闭空间中，为了保证运行的绝对安全，其人员及制度都应有严格的规定，并且系统设计为离线网络。CA 的功能是在收到来自 RA 的证书请求时颁发证书。一般的个人证书发放过程都是自动进行无须人工干预。

证书的登记机构 Register Authority，简称 RA，分散在各个网上银行的地区中心。RA 与网银中心有机结合，接受客户申请并审批，把证书正式请求通过银行内部网发送给 CA 中心。RA 与 CA 双方的通信报文也通过 RSA 进行加密，确保安全。系统的分布式结构适于新业务网点的开设，具有较好的扩充性。

证书的公布系统 Web Publisher 简称 WP，置于 Internet 网上，是普通用户和 CA 直接交流的界面。对用户来讲它相当于在线的证书数据库。用户的证书颁发之后，CA 用 E-mail 通知用户，然后用户用浏览器下载证书。

4.2.1.2　认证的主要方法

为了解决安全问题，一些公司和机构正千方百计地解决用户身份认证问题，主要有以下几种认证方法。

（1）双重认证。如波斯顿的 Beth Isreal Hospital 公司和意大利一家居领导地位的电信公司采用“双重认证”办法来保证用户的身份证明。也就是说他们不是采用一种方法，而是采用有两种形式的证明方法，这些证明方法包括令牌、智能卡和仿生装置，如视网膜或指纹扫描器。

（2）数字证书。这是一种检验用户身份的电子文件，也是企业可以使用的一种工具。这种证书可以授权购买，提供更强的访问控制，并具有很高的安全性和可靠性。随着电信行业坚持放松管制，GTE 已经使用数字证书与竞争对手（包括 Sprint 公司和 AT＆T 公司）共享用户信息。

（3）智能卡。这种解决办法可以持续较长的时间，更加灵活，存储信息更多，并具有可供选择的管理方式。

（4）安全电子交易（SET）协议。这是迄今为止最完整、最权威的电子商务安全保障协议。

4.2.1.3　CA 认证系统

公共网络系统的安全性依靠用户、商家的认证，数据的加密及交易请求的合法性验证等多方面措施来保证。

电子交易过程中必须确认用户、商家及所进行的交易本身是否合法可靠。一般要求建立专门的电子认证中心（CA）以核实用户和商家的真实身份以及交易请求的合法性。认证中心将给用户、商家、银行等进行网络商务活动的个人或集团发电子证书。

CA 是电子商务中网上银行建立的关键，只有建立一个较好的 CA 体系才能较好地发展网上银行，才能实现网上支付，电子购物才真正实现。CA 的机构如多方并进，各建各的，以后会出现各 CA 之间的矛盾，客户的多重认证等。应有一家公认的机构如银行、邮电或安全部来建立权威性认证机构（CA）。

1. SET 的认证（CA）

在用户身份认证方面，SET 引入了证书（Certificates）和证书管理机构（Certificates

Authorities）机制。

（1）证书。证书就是一份文档，它记录了用户的公共密钥和其他身份信息。在 SET 中，最主要的证书是持卡人证书和商家证书。

持卡人实际上是支付卡的一种电子化表示，它是由金融机构以数字签名形式签发的，不能随意改变。持卡人证书并不包括账号和终止日期信息，取而代之的是用单向哈希算法根据账号、截止日期生成的一个编码，如果知道账号、截止日期、密码值即可导出这个码值，反之则不行。

商家证书表示可接受何种卡来进行商业结算，它是由金融机构签发的，不能被第三方改变。在 SET 环境中，商家至少应有一对证书。商家也可以有多对证书，表示它与多个银行有合作关系，可以接受多种付款方法。

除了持卡人证书和商家证书以外，还有支付网关证书、银行证书、发卡机构证书。

（2）证书管理机构。是受一个或多个用户信任提供用户身份验证的第三方机构。证书一般包含拥有者的标识名称和公钥，并且由 CA 进行数字签名。

CA 的功能主要有：接收注册请求，处理、批准/拒绝请求，颁发证书。用户向 CA 提交自己的公共密钥和代表自己身份的信息（如身份证号码或 E-mail 地址），CA 验证了用户的有效身份之后，向用户颁发经过 CA 私有密钥签名的证书。

（3）证书的树形验证结构。在两方通信时，通过出示由某个 CA 签发的证书来证明自己的身份，如果对签发证书的 CA 本身不信任，则可验证 CA 的身份。依次类推，一直到公认的权威 CA 处，就可确信证书的有效性。SET 证书正是通过信任层次来逐级验证的。通过 SET 的认证机制，用户不再需要验证并信任每一个想要交换信息的用户的公共密钥，而只需要验证并信任颁发证书的 CA 的公共密钥就可以了。CA 树形验证体系示意图如图 4-4 所示。

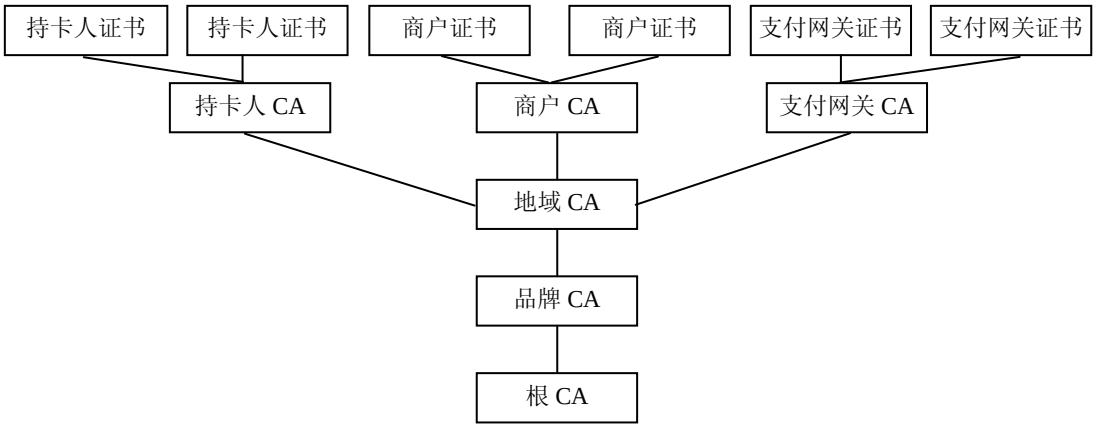

图 4-4　CA 树形验证体系示意图

2. 招商银行 CA 方案

我国的电子商务正在发展，各种规范要求还没有形成。目前招商银行、中国银行、中国建设银行、中国工商银行都准备开发网上银行业务。这里以招商银行为例介绍其 CA 方案。

招商银行 CA 系统用于 Web 服务器的 SSL 公开密钥证书，也可以为浏览器客户发证，在 SSL 协议的私有密钥交换过程中加密密钥参数。今后会开发其他的密码服务，并在国家有关部

门规定下开展公开密钥认证服务。

CA 系统处于非联机状态，运行 CA 的系统在私有网上，用户不能通过 Internet 访问。CA 会在 Web 服务器上提供查询和客户证书申请接口，用户可以查询证书状态，提交证书请求。Web 服务器运行 CA 数据库的独立副本，与 CA 没有网络连接。

本方案采用层次认证结构，层次设置采用 PEM 规定的认证层次，设置以下目标类型：

IPRA（Internet Policy Registration Authority）：IPRA 负责管理认证策略，认证 PCA，检查 PCA 运行与其策略的一致性。

PCA（Policy Certification Authority）：PCA 负责根据业务需求指定认证策略，交 IPRA 审批，根据认证策略认证下一级 CA，保证 CA 运行与策略的一致性。

CA（Certification Authority）：CA 根据需要，选择相应的认证策略，提供用户公开密钥认证。

用户：用户就是 X.509 中的最终实体。

RA（Registration Authority）：当用户与 CA 通信有困难时，CA 就不可能对用户进行身份鉴别，由 RA 代替 CA 根据 CA 的业务要求进行用户身份鉴别。

CA 管理提供 CA 密钥管理，认证策略管理和配置，以及服务级别的管理。CA 管理的重要职能是 CA 密钥和策略管理。包括生成新的密钥对、安装证书、撤消证书、备份 CA 的私有密钥、安装备份的 CA 私有密钥等。这些功能需要两个安全管理员同时注册才能完成。

目前，CA 支持以下公开密钥算法：RSA/DH/DSA，并可提供上述密钥的证书，计划将增加对椭圆曲线加密算法的支持。此外，为了提高 CA 密钥的安全性，必须对 CA 密钥加密后保存，今后 CA 所有与密钥有关部门的工作将在 IC 卡中完成。

世界上较早的数字证书认证中心是美国的 Verisign 公司（www.verisign.com）。中国比较知名的认证中心有：

- 中国数字认证网（www.ca365.com）。
- 中国金融认证中心（www.cfca.com.cn）。
- 中国电子邮政安全证书管理中心（www.chinapost.com.cn/CA/index.htm）。
- 北京数字证书认证中心（www.bjca.org.cn）。
- 广东省电子商务认证中心（www.cnca.net）。
- 上海市电子商务安全证书管理中心有限公司（www.sheca.com）。
- 海南省电子商务认证中心（hn.cnca.net）。
- 天津 CA 认证中心（www.ectj.net/ca/ca-1/ca.htm）。
- 山东省 CA 认证中心（www.ca.gov.cn）。

4.2.2　电子加密技术

1. 加密

数据加密技术从技术上的实现分为软件和硬件两方面。按作用不同数据加密技术主要分为数据传输、数据存储、数据完整性的鉴别以及密钥管理技术四种。

在网络应用中一般采取两种加密形式：对称密钥和公开密钥，采用何种加密算法要结合具体应用环境和系统，而不能简单地根据加密强度来作出判断。因为除了加密算法本身之外，密钥合理分配、加密效率与现有系统的结合性，以及投入产出分析都应在实际环境中具体考虑。

对于对称密钥加密，其常见加密标准为 DES 等，当使用 DES 时，用户和接受方采用 64

位密钥对报文加密和解密，当对安全性有特殊要求时，则要采取 IDEA 和三重 DES 等。作为传统企业网络广泛应用的加密技术，私有密钥效率高，它采用 KDC 来集中管理和分发密钥并以此为基础验证身份，但是并不适合 Internet 环境。

在 Internet 中使用更多的是公钥系统，即公开密钥加密，它的加密密钥和解密密钥是不同的。一般对于每个用户生成一对密钥后，将其中一个作为公钥公开，另外一个则作为私钥由属主保存。常用的公钥加密算法是 RSA 算法，加密强度很高。具体作法是将数字签名和数据加密结合起来。发送方在发送数据时必须加上数据签名，做法是用自己的私钥加密一段与发送数据相关的数据作为数字签名，然后与发送数据一起用接收方密钥加密。当这些密文被接收方收到后，接收方用自己的私钥将密文解密得到发送的数据和发送方的数字签名，然后用发布方公布的公钥对数字签名进行解密，如果成功，则确定是由发送方发出的。数字签名每次还与被传送的数据和时间等因素有关。由于加密强度高，而且并不要求通信双方事先建立某种信任关系或共享某种秘密，因此十分适合 Internet 网上使用。

下面介绍几种最常见的加密体制的技术实现。

（1）常规密钥密码体制。所谓常规密钥密码体制，即加密密钥与解密密钥是相同的。在早期的常规密钥密码体制中，典型的有代替密码，其原理可以用一个例子来说明。

将字母 a，b，c，d，…，w，x，y，z 的自然顺序保持不变，但使之与 D，E，F，G，…，Z，A，B，C 分别对应（即相差 3 个字符）。若明文为 student 则对应的密文为 VWXGHQW（此时密钥为 3）。由于英文字母中各字母出现的频度早已有人进行过统计，所以根据字母频度表可以很容易对这种代替密码进行破译。

（2）数据加密标准 DES。DES 算法原是 IBM 公司为保护产品的机密于 1971 年至 1972 年研制成功的，后被美国国家标准局和国家安全局选为数据加密标准，并于 1977 年颁布使用。ISO 也已将 DES 作为数据加密标准。

DES 对 64 位二进制数据加密，产生 64 位密文数据。使用的密钥为 64 位，实际密钥长度为 56 位（有 8 位用于奇偶校验）。解密过程和加密相似，但密钥的顺序正好相反。DES 的保密性仅取决于对密钥的保密，而算法是公开的。DES 内部的复杂结构是至今没有找到捷径破译方法的根本原因。现在 DES 可由软件和硬件实现。美国 AT＆T 首先用 LSI 芯片实现了 DES 的全部工作模式，该产品称为数据加密处理机 DEP。请参考图 4-5。

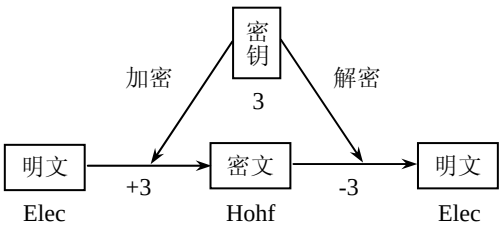

图 4-5　对称密钥加密体系示意图

（3）公开密钥密码体制。公开密钥（Public Key）密码体制出现于 1976 年，它最主要的特点就是加密和解密使用不同的密钥，每个用户保存着一对密钥，即公开密钥 PK 和私有密钥 SK。因此，这种体制又称为双钥或非对称密钥密码体制。在这种体制中，PK 是公开信息，用作加密密钥，而 SK 需要由用户自己保存，用作解密密钥。加密算法 E 和解密算法 D 也都是

公开的。虽然 SK 与 PK 成对出现，但却不能根据 PK 计算出 SK。公开密钥算法的特点如下：

1）用加密密钥 PK 对明文 X 加密后，再用解密密钥 IK 解密，即可恢复出明文，或写为：IK（PK（X））=X。

2）加密密钥不能用来解密，即 PK（PK（X））≠X。

3）在计算机上可以容易地产生成对的 PK 和 IK。

4）从已知的 PK 实际上不可能推导出 IK。

5）加密和解密的运算可以对调，即：PK（IK（X））=X。

在公开密钥密码体制中，最有名的是 RSA 体制。它已被 ISO/TC97 的数据加密技术分委员会 SC20 推荐为公开密钥数据加密标准。请参考图 4-6。

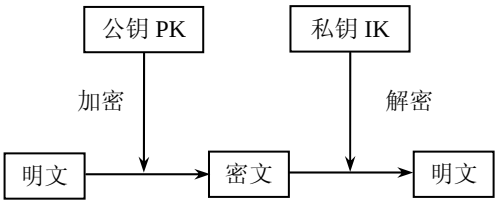

图 4-6　非对称密钥密码体系示意图

实例：RSA 的算法。

1）选取两个足够大的质数 P 和 Q；如：P=101，Q=113。

2）计算 P 和 Q 相乘所产生的乘积 n=P×Q；如：n=11413。

3）找出一个小于 n 的数 e，使其符合与（P−1）×（Q−1）互为质数；如：取 e=3533。

4）另找一个数 d，使其满足（e×d）mod[(P−1)×(Q−1)]=1（其中 mod 为相除取余）；如：取 d=6597。

5）（n，e）即为公开密钥；（n，d）即为私用密钥。

6）将明文 X 分组，$X=X_1X_2\cdots X_r$（$X_i<=n$）。

7）加密：$Y_i=X_i\times e$（mod n），得密文 $Y=Y_1Y_2\cdots Y_r$ 如：明文 c=5761，密文 m=9226。

8）明文 c=m×e（mod n）而密文 m=c×d（mod n），即无论哪一个质数先与原文加密，均可由另一个质数解密。但要用一个质数来求出另一个质数是非常困难的。

2. 数字摘要

采用单向 Hash 函数对文件进行变换运算得到摘要码，并把摘要码和文件一同送给接收方，接收方接到文件后，用相同的方法对文件进行变换计算，用得出的摘要码与发送来的摘要码进行比较来断定文件是否被篡改。请参考图 4-7。

3. 数字信封

数字信封（也称为电子信封）并不是一种新的加密体系，它只是把两种密钥体系结合起来，获得了非对称密钥技术的灵活和对称密钥技术的高效。请参考图 4-8。

数字信封使网上信息传输的保密性得以解决。发送方采用对称密钥加密信息，然后将此对称密钥用接收方的公开密钥加密之后，将它和信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开信息。安全性能高，保证只有规定的接收方才能阅读信的内容。

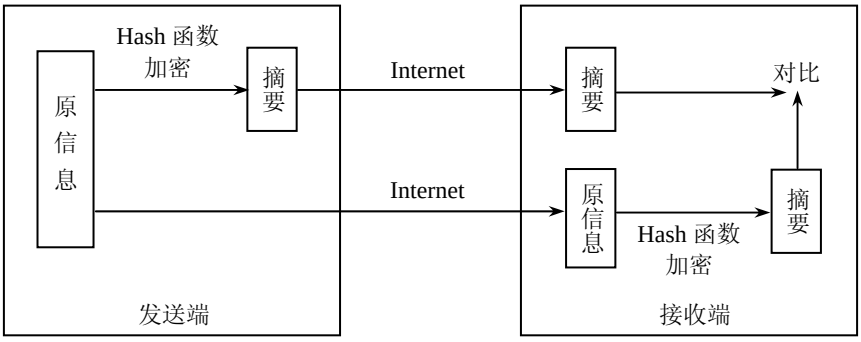

图 4-7　数字摘要体系示意图

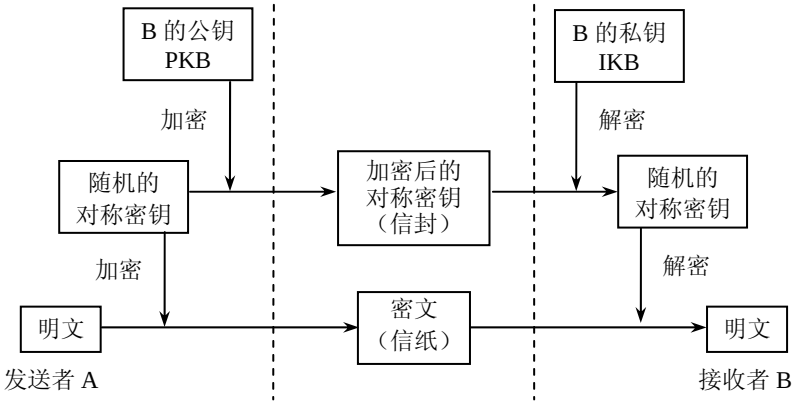

图 4-8　数字信封体系示意图

4. 数字签名

数字签名技术是实现交易安全的核心技术之一，它的实现基础就是加密技术。这里介绍数字签名的基本原理。

以往的书信或文件是根据签名或印章来证明其真实性的。但在计算机网络中传送的报文又如何盖章呢？这就是数字签名所要解决的问题。数字签名必须保证以下几点：

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）接收者不能伪造对报文的签名。

现在已有多种实现数字签名的方法，但采用公开密钥算法要比常规算法更容易实现。下面就来介绍这种数字签名。

发送者 A 用其秘密解密密钥 IKA 对报文 X 进行运算，将结果 IKA（X）传送给接收者 B。B 用已知的 A 的公开加密密钥得出 PKA（IKA（X））=X。因为除 A 外没有别人能具有 A 的解密密钥 IKA，所以除 A 外没有别人能产生密文 IKA（X）。这样报文 X 就被签名了。

假若 A 要抵赖曾发送报文给 B。B 可将 X 及 IKA（X）出示给第三者。第三者很容易用 PKA 去证实 A 确实发送消息 X 给 B。反之，如果是 B 将 X 伪造成 X'，则 B 在第三者面前出示 IKA（X'）。这样就证明 B 伪造了报文。可以看出，实现数字签名也同时实现了对报文来源

的鉴别。

但是上述过程只是对报文进行了签名。对传送的报文 X 本身却未保密。因为截到密文 IKA（X）并知道发送者身份的任何人，通过查问手册即可获得发送者的公开密钥 PKA，因而能够理解报文内容。请参考图 4-9。

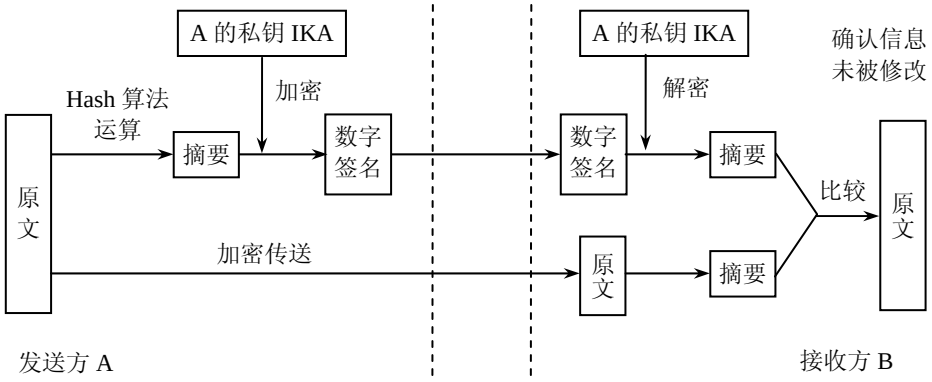

图 4-9　数字签名体系示意图

5. 数字时间戳

数字时间戳技术就是对电子文件签署的日期和时间进行安全性保护和有效证明的技术，它是由专门的认证机构来加的，并以认证机构收到文件的时间为依据。请参考图 4-10。

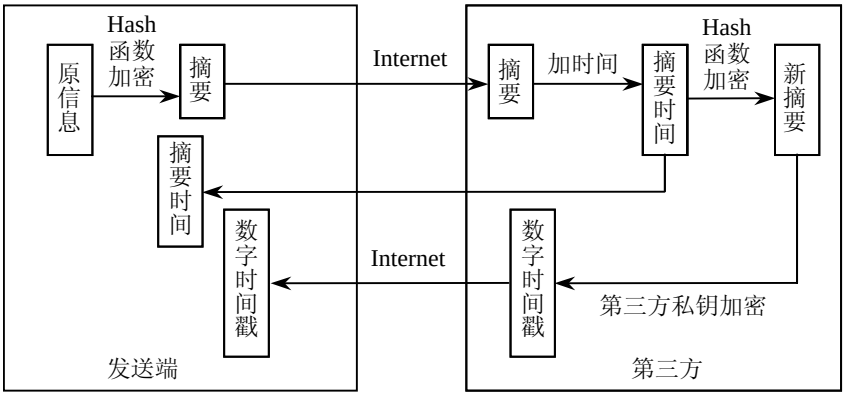

图 4-10　数字时间戳体系示意图

6. 密钥的管理

对称密钥加密方法致命的弱点就是它的密钥管理十分困难，因此它很难在电子商务实践中得到广泛应用。在这一点上，公开密钥加密方法占有绝对优势。不过，无论实施哪种方案，密钥管理都是要考虑的问题。当网络扩大、用户增多时尤其如此。一家专门从事安全性咨询公司 Cypress Consulting 的总裁 CyArdoin 说：“在所有加密方案中，都必须有人来管理密钥。”

目前，公认的有效方法是通过密钥分配中心 KDC 来管理和分配公开密钥。每个用户只保存自己的私有密钥和 KDC 的公开密钥 PKA。用户通过 KDC 获得其他用户的公开密钥。首先，A 向 KDC 申请公开密钥，将信息（A，B）发给 KDC。KDC 返回给 A 的信息为（CA，CB），

其中，CA=IKAS（A，PKA，T1），CB=IKAS（B，PKB，T2）。CA 和 CB 称为证书（Certificate），分别含有 A 和 B 的公开密钥。KDC 使用其解密密钥 IKAS 对 CA 和 CB 进行签名，以防止伪造。时间戳 T1 和 T2 的作用是防止重放攻击。最后，A 将证书 CA 和 CB 传送给 B。B 获得了 A 的公开密钥 PKA，同时也可检验自己的公开密钥 PKB。

4.3 安全电子交易技术

4.3.1 SSL 协议

SSL 协议是 Netscape 公司在网络传输层之上提供的基于 RSA 和保密密钥的用于浏览器和 Web 服务器之间的安全连接技术。它被视为 Internet 上 Web 浏览器和服务器的标准安全性措施。SSL 提供了用于启动 TCP/IP 连接的安全性“信号交换”。这种信号交换导致客户和服务器同意将使用的安全性级别，并履行连接的任何身份验证要求。它通过数字签名和数字证书可实现浏览器和 Web 服务器双方的身份验证。在用数字证书对双方的身份验证后，双方就可以用保密密钥进行安全的会话了。如图 4-11 所示。

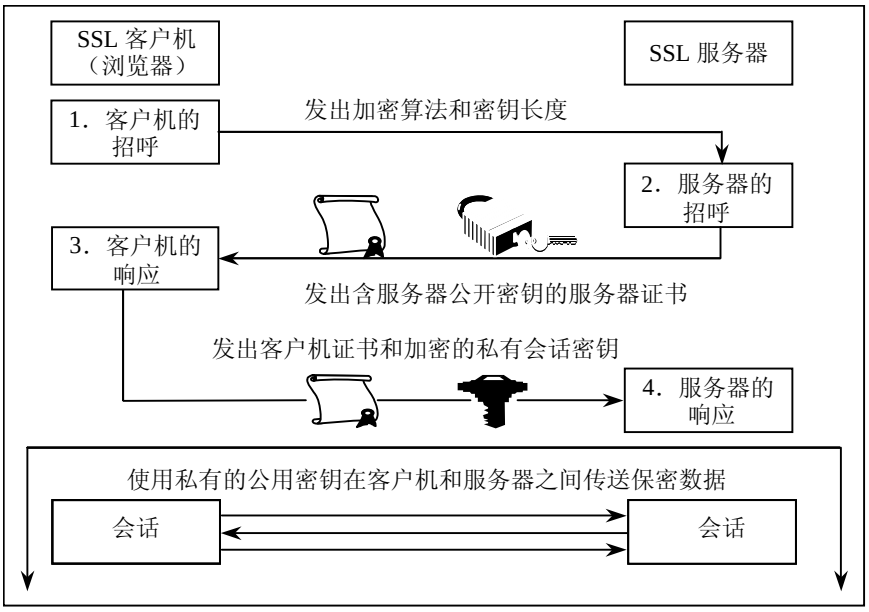

图 4-11 建立 SSL 会话体系示意图

SSL 协议在应用层收发数据前，协商加密算法、连接密钥并认证通信双方，从而为应用层提供了安全的传输通道；在该通道上可透明加载任何高层应用协议（如 HTTP、FTP、TELNET 等）以保证应用层数据传输的安全性。SSL 协议独立于应用层协议，因此在电子交易中被用来安全传送信用卡号码。

中国目前多家银行均采用 SSL 协议，如在中国的电子商务系统中能完成实时支付，招行一网通采用的就是 SSL 协议。从目前实际使用的情况看，SSL 还是人们最信赖的协议。实现 SSL 协议的是 HTTP 的安全版名为 HTTPS。如图 4-12 所示。

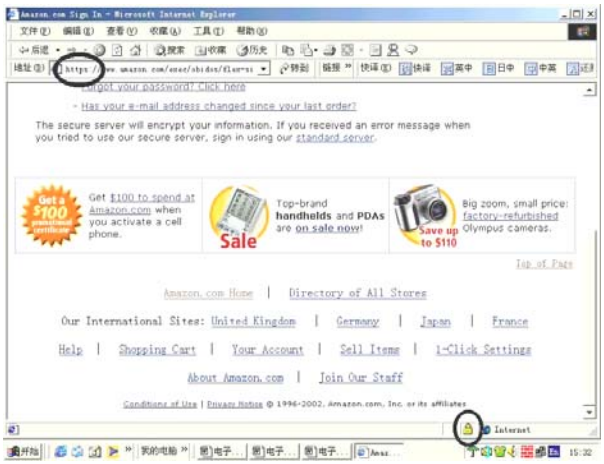

图 4-12　HTTPS 协议的使用

图 4-13 显示在 ecoin 上登录（Login）用户名时即进入 SSL 安全连接。

图 4-13　在 ecoin 上连接交换敏感信息的页面

这时浏览器发出安全警报，开始建立安全连接，参见图 4-14 中左侧窗口的验证安全证书，再参见图 4-14 的右侧窗口，用户单击“确定”按钮即进入安全连接。

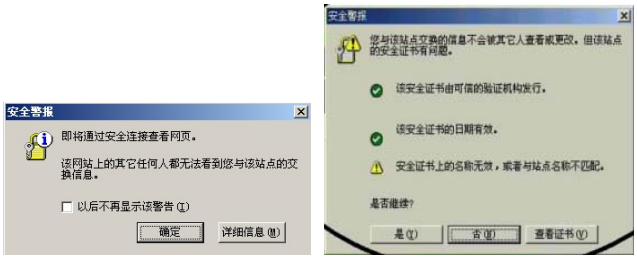

图 4-14　浏览器开始建立安全连接及浏览器验证服务器安全证书

图 4-15 显示在 ecoin 上的安全连接已经建立，浏览器右下角状态栏的锁型图案表示用户通过网页传输的用户名和密码都将通过加密方式传送。

图 4-15　显示在 ecoin 上的安全连接已经建立

当加密方式传送结束后，浏览器会离开交换敏感信息的页面，自动断开安全连接，如图 4-16 所示。

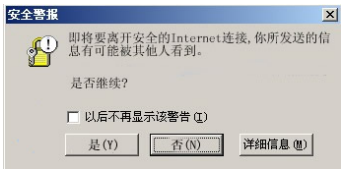

图 4-16　离开交换敏感信息的页面

SSL 当初并不是为支持电子商务而设计的，所以在电子商务系统的应用中还存在很多弊端。它是面向连接的协议，在涉及多方的电子交易中，只能提供交易中客户与服务器间的双方认证，而电子商务往往是用户、网站、银行三家协作完成，SSL 协议并不能协调各方间的安全传输和信任关系；还有购货时用户要输入通信地址，这样将可能使得用户收到大量垃圾信件。因此，为了实现更加完善的电子交易，MasterCard 和 Visa 以及其他一些业界厂商制订并发布了 SET 协议。

4.3.2　SET 协议

SET 协议是针对开放网络上安全、有效的银行卡交易，由 Visa 和 Mastercard 联合研制，为 Internet 上卡支付交易提供高层的安全和反欺诈保证。

SET 协议保证了电子交易的机密性、数据完整性、身份合法性和抗否认性。

SET 是专门为电子商务而设计的协议，虽然它在很多方面优于 SSL 协议，但仍然不能解决电子商务所遇到的全部问题。

1. SET 的作用

SET（Secure Electronic Transaction，安全电子交易）协议是维萨（Visa）国际组织、万事达（MasterCard）国际组织创建，结合 IBM、Microsoft、Netscape、GTE 等公司制定的电子商务中安全电子交易的国际标准。其主要目的是解决信用卡电子付款的安全保障性问题：

- 保证信息的机密性，保证信息安全传输，不被窃听，只有收件人才能得到和解密信息。

- 保证支付信息的完整性，保证传输数据完整地接收，在中途不被篡改。
- 认证商家和客户，验证公共网络上进行交易活动的商家、持卡人及交易活动的合法性。
- 广泛的互操作性，保证采用的通讯协议、信息格式和标准具有公共适应性。从而可在公共互联网络上集成不同厂商的产品。

2. SET 的应用流程

电子商务的工作流程与实际的购物流程非常接近。从顾客通过浏览器进入在线商店开始，一直到所定货物送货上门或所定服务完成，然后账户上的资金转移，所有这些都是通过 Internet 完成的，如图 4-17 所示。

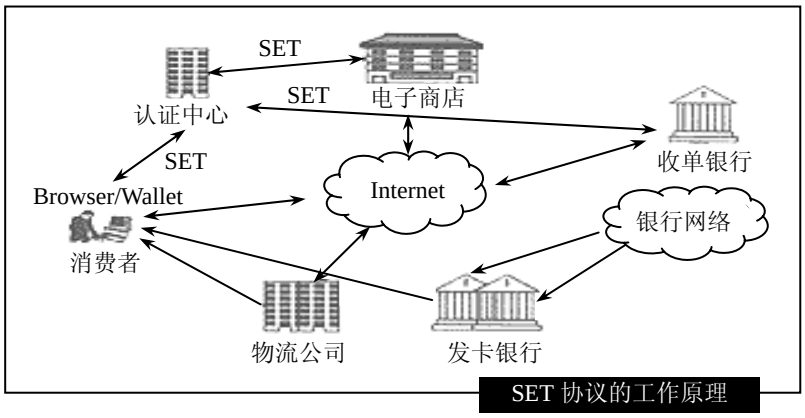

图 4-17　SET 协议体系示意图

其具体流程为：

（1）持卡人在商家的 WEB 主页上查看在线商品目录、浏览商品。

（2）持卡人选择要购买的商品。

（3）持卡人填写定单，定单通过信息流从商家传过来。

（4）持卡人选择付款方式，此时 SET 开始介入。

（5）持卡人发送给商家一个完整的定单及要求付款的指令。在 SET 中，定单和付款指令由持卡人进行数字签名。同时利用双重签名技术保证商家看不到持卡人的账号信息。

（6）商家接受定单后，向持卡人的金融机构请求支付认可。通过 Gateway 到银行，再到发卡机构确认，批准交易。然后返回确认信息给商家。

（7）商家发送定单确认信息给顾客。顾客端软件可记录交易日志，以备将来查询。

（8）商家给顾客装运货物或完成订购服务。到此为止购买过程已经结束。商家可以立即请求银行将货款从购物者的账号转移到商家账号，也可以等到某一时间，请求成批划账处理。

（9）商家从持卡人的金融机构请求支付。在认证操作和支付操作中间一般会有一个时间间隔。

前 3 步与 SET 无关，从第 4 步开始 SET 起作用。在处理过程中，通信协议、请求信息的格式、数据类型的定义等 SET 都有明确的规定。在操作的每一步，持卡人、商家、网关都通过 CA 来验证通信主体的身份，以确认对方身份。

3. SET 技术概要

（1）加密技术。

SET 采用两种加密算法进行加密、解密处理，其中密钥加密是基础，公钥加密是应用的核心。

用同一个密钥来加密和解密数据。加密的主要算法是 DES，例如加密银行卡持卡人的个人识别代码（PIN）；公开密钥要求使用一对密钥，一个公开发布，另一个由收信人保存。发信人用公开密钥加密数据，收信人则用私用密钥去解密。解密的主要算法是 RSA，例如加密支付请求数据。加密过程可保证不可逆，必须使用私用密码才能解密。

（2）数字签名。

金融交易要求发送报文数据的同时发送签名数据作为查证。这种电子数字签名是一组加密的数字。SET 要求用户在进行交易前首先进行电子签名，然后进行数据发送。

（3）电子认证。

电子交易过程中必须确认用户、商家及所进行的交易本身是否合法可靠。一般要求建立专门的电子认证中心（CA）以核实用户和商家的真实身份以及交易请求的合法性。认证中心将给用户、商家、银行等进行网络商务活动的个人或集团发电子证书。

（4）电子信封。

金融交易所使用的密钥必须经常更换，SET 使用电子信封来传递更换密钥。其方法是由发送数据者自动生成专用密钥，用它加密原文，将生成的密文连同密钥本身一起再用公开密钥手段传送出去。收信人再解密后同时得到专用密钥和用其加密后的密文。这样保证每次传送都可以由发送方选定不同的密钥进行交易。

根据 SET 标准设计的软件系统必须经过 SET 验证才能授权使用。首先进行登记，再进行 SET 标准的兼容性试验，目前已经有多家公司的产品通过了 SET 验证。

4.3.3 PKI 协议

公开密钥基础设施（PKI——Public Key Infrastructure）是一种以公钥加密技术为基础技术手段实现安全性的技术。PKI 由认证机构、证书库、密钥生成和管理系统、证书管理系统、PKI 应用接口系统等基本成分组成。

公开密钥基础设施的优点：

- 透明性和易用性。
- 可广展性。
- 操作性强。
- 支持多应用。
- 支持多平台。

作为网络环境的基础设施，PKI 具有良好的性能，是一个比较完整的安全体系。电子商务建设过程中涉及的许多安全问题都可由 PKI 解决。

本章小结

国际标准化组织 ISO 对网络安全的定义，它是指为数据处理系统建立和采取的科技和管理的安全保护，以保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和显露。

Internet 带来了两种不同的安全威胁。一种威胁是来自文件下载；另一种是网络化趋势加

重了病毒的威胁。首先应该考虑在何处安装病毒防治软件。在企业中，重要的数据往往保存在位于整个网络中心结点的文件服务器上，这也是病毒攻击的首要目标。为保护这些数据，网络管理员必须在网络的多个层次上设置全面保护措施。

防火墙（FireWall）是一种隔离控制技术，在某个机构的网络和不安全的网络（如 Internet）之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止专利信息从企业的网络上被非法输出。防火墙是一种被动防卫技术，由于它假设了网络的边界和服务，因此对内部的非法访问难以有效地控制。因此，防火墙最适合于相对独立的与外部网络互连途径有限、网络服务种类相对集中的单一网络。从实现原理上分，防火墙技术包括四大类：网络级防火墙（也叫包过滤型防火墙）、应用级网关、电路级网关和规则检查防火墙。

按照全面的安全保护要求，认证和识别确保参与加密对话的人确实是其本人。厂家依靠许多机制来实现认证，从安全卡到身份鉴别。安全卡安全保护能确保只有经过授权的用户才能通过个人计算机进行 Internet 网上的交互式交易；身份鉴别则提供一种方法，用它生成某种形式的口令或数字签名，交易的另一方据此来认证他的交易伙伴。用户管理的口令通常是前一种安全措施；硬件/软件解决方案则不仅正逐步成为数字身份认证的手段，同时它也可以被可信第三方用来完成用户数字身份（ID）的相关确认。

数据加密技术从技术实现上分为软件和硬件两方面。按作用不同，数据加密技术主要分为数据传输、数据存储、数据完整性鉴别以及密钥管理技术四种。

SSL 协议是 Netscape 公司在网络传输层之上提供的基于 RSA 和保密密钥的用于浏览器和 Web 服务器之间的安全连接技术。SET 协议是针对开放网络上安全、有效的银行卡交易，由 Visa 和 Mastercard 联合研制的，为 Internet 上卡支付交易提供高层的安全和反欺诈保证。

思考题

1．计算机网络病毒的类型有哪些？
2．布署一种防病毒软件的实际操作包括几个步骤？
3．从实现原理上分，防火墙技术包括哪几个大类？
4．网络安全检测工具的种类有哪些？
5．认证主要有几种方法？
6．介绍几种最常见的加密体制的技术实现机制。
7．阐述建立 SSL 会话体系的过程。
8．SET 的应用流程？
9．SET 技术包括哪些？
10．公开密钥基础设施的优点有哪些？

实训题

有关网络安全的问题

有关数据显示，网上银行的用户已有近千万，每年通过网上银行流通的资金超过千亿。美国 Ponemon Institute 于当地时间 2004 年 9 月 29 日公布了以美国消费者为对象实施的关于网

页仿冒（Phishing）的调查结果。76%的消费者感觉欺骗（Spoofing）和网页仿冒行为在增加，其中的 35%每星期至少收到一封假冒电子邮件。该公司推测，整个美国这方面的经济损失大约为 5 亿美元。该调查是由从事在线隐私业务的 TRUSTe 和从事电子结算业务的 NACHA 赞助实施的。

该调查以 1335 名美国因特网用户为对象实施，结果每 10 人中有 7 人回答曾经受骗访问过假冒网站。另外，15%以上的用户提供了包括信用卡号码、活期存款账户以及社会保险号码在内的个人信息。占总数 2%的回答者由于网页仿冒攻击受到经济损失。大部分受害的回答者是在网页仿冒行为发生后两个星期内遭受实际损失的。

因特网用户在遭遇不愉快的经验后对电子邮件和网站产生怀疑，他们希望针对这些问题采取某种措施。64%的回答者表示，企业及其他团体对于欺骗及网页仿冒行为没有采取任何措施，这是令人无法接受的。96%的回答者希望企业研究出能够认证电子邮件和网站的新技术。

针对商业网站的一系列恶性攻击已经打击了消费者对网络的信心。网络安全专家指出，大量迹象表明网络黑客行为逐渐趋于攫取利益，如对银行的袭击等。Deloite Touche 的一份调查报告显示，100 家顶极金融机构中 83%的机构遭受过黑客袭击，而前一年这一比例仅为 39%。其中遭到黑客攻击的机构中有 40%蒙受了经济损失。

微软的 Hotmail 免费服务系统每天都接手 35 亿封垃圾邮件，约占其邮件总数的 80%。而且，用户反映大部分邮件被邮件病毒和能够自动传播的蠕虫病毒感染。

网络安全公司 Cyota 说：“网络用户对网上交易日趋警惕。”针对 650 个网上银行用户的一项最新调查显示，74%的用户担心被欺骗而不愿进行网上购物。Cyota 营销副总裁阿米尔·奥拉德（Amir-Orad）说：“最大的损失不是金钱，而是顾客对网络的信心。”

微软的 Windows 操作系统不断曝出新的安全漏洞，而目前高达 90%的网络用户都使用微软的操作系统，这就更加令人担忧。技术精湛的黑客现在可以在数周内，甚至数日内就能发现 Windows 系统的新漏洞，而一年前，黑客需要几个月才能做到这一点。尽管微软每月都发布安全补丁，但是公司和家庭用户却做不到及时更新。

安全公司 NCircle 的首席执行官阿贝·克莱恩菲尔德（Abe Kleinfeld）表示：“对一家大公司而言，及时更新安全补丁是一个非常繁冗的过程。”

以上原因导致各种网络病毒和蠕虫病毒得以继续感染那些联网的公司和家庭电脑。一旦一台 PC 成了黑客们为所欲为的天堂，黑客们就可以任意传输垃圾邮件，侵入私人网络，以及盗窃他人身份谋取暴利。

防毒公司赛门铁克最近发布 2004 上半年“网络安全威胁研究报告”（注），对全球企业及家庭、个人电脑做了半年度的回顾，电子商务及小型企业成为主要攻击目标。根据这份报告，2004 年上半年电子商务（e-commerce）及小型企业分别以 16%及 10%分居网络攻击目标产业的一、二名。在 2003 年下半年两者分别只有 4%及 3%。

全球电子商务日趋成熟的结果，为电子商务公司，大至 eBay、小至个人在雅虎奇摩开设的拍卖专区等，都有可能成为攻击的受害者，尤其是后者数量众多，一旦被入侵网站服务器（Web Server），一切交易记录及信息将显露无疑。

小型企业之所以成为攻击对象，部分原因和过去最大的攻击目标——金融业强化防护有关。如银行、证券、保险业等大型企业，开始注重电子交易及网站安全，导致黑客转而攻击较不设防的小型企业。小型企业往往也是安全意识较薄弱的一群，因此也没有足够的安全预算。

而和电子商务相关的是 Web 应用的安全。IE 或 IIS 的漏洞以及 Web 应用的瑕疵导致电子商务网站交易信息被任意存取。例如，信息隐码攻击（SQL Injection）就是可以在输入任意字串的 Web 应用中搞鬼，一旦不幸中标，就可让有心人士存取该网站服务器甚至数据库。

漏洞安全日益严重。2004 年上半年，赛门铁克报告有 1237 个新漏洞，平均每周有 48 个新漏洞被发现。其中 96% 是属于中度到高度风险，其中有 46% 被列为高度风险。而在所有漏洞中，超过一半不用撰写程序就可以发动攻击。前述的 Web 应用漏洞，也从去年下半年占总漏洞数量的 31% 提升为 38.7%。

另一个骇人的趋势是，漏洞公诸于世到该漏洞的相关攻击时间差平均只差 5.8 天，比前半年的报告天数（7 天）更为缩短。这显示黑客撰写攻击源代码的速度不断加快，相对地，一个未加修补的漏洞的风险更高。

赛门铁克也提出未来可能的信息安全忧患：

（1）首先，网络钓鱼（Fishing）是未来数月最重大的威胁之一。网络钓鱼的研究统计、自保方法、商业解决方案，以及各国政府应对方法，CNET 新闻网站有多次报道，在此不在赘述。

（2）间谍程序也会在未来攻击上扮演重要角色。特别是对允许 HTTP 的流量进出的公司网络而言，这意味着众多间谍程序可能借此渠道发送。因为有些封包包含能够自我更新的源代码，所以间谍程序越来越难卸载。

（3）恶意程序变种。今年的 Netsky、MyDoom 及 Bagle 等被认为背后具有组织性的支持，不断撰写变种。恶意源代码变种会改变蠕虫本身，并通过不断复制，导致各代蠕虫之间产生着不同的形式，而且许多传统的扫描技术可能无法侦测出这些进化的蠕虫变种。

（4）宽带分享器及网络装置。2004 年上半年，赛门铁克安全漏洞数据库发现 20 多个周边设备的漏洞，种类从允许远端破坏、重新设定到远端黑客甚至可以拥有系统管理者的权限。这也打破硬件装置“非常”安全的看法；虽然硬件装置的嵌入式操作系统不用担心 Windows 的安全问题，但是它们仍然有漏洞让黑客乘虚而入，一些本来协助防护网络安全的产品，像防火墙、入侵侦测产品，也不能免于这个隐忧。

国内随着 ISP 调降费用，宽带网络将会日渐普及。未来家庭甚至都会购买宽带分享器，同时提供 PC 及机上盒、PS2 等信息家电联网。相对于思科、Checkpoint 等大厂会定期公布弱点及修补程序，国内联网设备厂商往往都还没有注意到这件事，这也让国内产品的用户，特别是家庭用户可能陷于攻击的风险之中而不知。

这个趋势可能会促使用户开始重视硬件韧体更新，以便修补漏洞，进一步迫使国内厂商重视弱点及修补程序的更新服务。

（5）移动装置成为攻击目标。曾有分析师预测，掌上设备甚至 VoIP 电话都可能成为病毒制造者的攻击目标。这个预言最终实现。一只名为 Cabir 的病毒是专门针对 Symbian 智能手机的病毒。这是一只“概念验证”（Proof of Concept）病毒，证明蓝牙装置也会有安全疑虑，不过却没有造成什么损害。

它会通过蓝牙传输协议传给另一只手机。不过前提是对方使用者同意接收、执行程序，因此主要还是利用人性的弱点。但王岳忠指出蓝牙是一种短距离的传输装置，在办公室内通常用于同事之间，未来出现造成有重大灾害的病毒后果可能不堪设想。“同事之间往往是相互信任的，因此不太会去质疑对方传来的文件是有问题的。”

（6）P2P/IM（Instant Messenging）。同样愈来愈普及的 P2P/IM（即时通讯）/IRC/CIFS（文

件分享）等，将成为新兴的传染对象及途径。

（7）互联网相关的 IE、Web 应用，则已是最受欢迎的攻击对象。

【资料来源】：新浪科技讯　时间：2004-08-04

随着网络的发展，一系列侵犯网络安全和信息安全的恶性事件不断地给人们敲响警钟。

根据上述资料谈谈你对网络安全诸多要素的认识。如网络的安全标准及实施、网络受到侵犯及受害程度、识别和过滤不良信息、确保重要信息的私密性和完整性、防止外界有害信息的入侵和传播、防止黑客入侵、保护个人隐私或企业的商业秘密、防治病毒的传染、保证电子商务的安全性、合法性和确认网络上交易双方的身份等十个方面。