第 1 章　网络空间信息安全概论

本　章　提　要

本章首先阐述网络空间信息安全的重要意义，指出信息安全是国家安全的重要基础，然后列出一些网络空间面临的安全问题，如电子邮件的安全问题、域名系统的安全威胁、IP 地址的安全问题、Web 站点的安全问题等，简要介绍了本课程的主要内容，即病毒防范技术、远程控制与黑客入侵、网络信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵检测技术、网络数据库安全与备份技术、信息隐藏与数字水印技术、网络安全测试工具及其应用，又介绍了网络空间信息安全与网络信息安全的区别，最后介绍了网络空间信息安全的七大趋势。

1.1　网络空间信息安全的重要意义

进入信息社会，信息已经成为一种非常重要的资源，它的安全与否已经影响到个人、企业甚至国家的根本利益。网络空间信息安全是一个涉及网络技术、通信技术、密码技术、信息安全技术、计算机科学、应用数学、信息论等多种学科的边缘性综合学科。网络空间信息安全是国家安全的重要基础，网络信息在国民经济建设、社会发展、国防和科学研究等领域的作用日益重要。实际上，网络的快速普及与发展、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。确保网络空间信息安全至关重要，没有网络空间信息的安全就谈不上网络信息的应用。当今，由于计算机互联网的迅速发展和广泛应用，它打破了传统的时间和空间的局限性，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。计算机网络和通信是促进信息化社会发展的最活跃的因素。然而，任何事物的发展都具有两重性。由于计算机互联网的国际化、社会化、开放化、个性化的特点，使它在向人们提供网络信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。网络空间信息安全问题已威胁到国家的政治、经济和国防等领域。这是因为对互联网的非法侵入或人为的故意破坏，将会轻而易举地改变互联网上的应用系统或导致网络瘫痪，从而使网络用户在军事、经济、政治上造成无法弥补的巨大损失。因此，很早就有人提出了“ 信息战 ”的概念并将信息武器列为继原子武器、生物武器和化学武器之后的第四大武器。网络信息的泄露、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等对网络信息安全已构成重大威胁。如果这些问题不解决，国家安全会受到威胁，电子政务、电子商务、网络银行、网络科研、远程教育、远程医疗等都将无法正常开展，个人的隐私信息也得不到保障。

网络空间是一个虚拟的空间，用规则管理起来，我们称之为“ 网络空间 ”。虚拟空间包含了三个基本要素：第一个是载体，也就是通信信息系统；第二个是主体，也就是网民、用户；第三个是构造一个集合，用规则管理起来，我们称之为“ 网络空间 ”。网络空间是人运用信息通信系统进行交互的空间，其中信息技术通信系统包括各类互联网、电信网、广电网、物联网、在线社交网络、计算系统、通信系统、控制系统、电子或数字信息处理设施等。人间交互指信息通信技术活动。网

络空间安全涉及网络空间中的电子设备、电子信息系统、运行数据、系统应用中存在的安全问题，分别对应这四个层面：设备、系统、数据、应用。

网络空间信息安全包括两个部分：防治、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的各种通信系统及其承载的数据不受损害；防止对这些信息通信技术系统的滥用所引发的政治安全、经济安全、文化安全、国防安全。一个是保护系统本身，另一个是防止利用信息系统带来其他的安全问题。所以针对这些风险，要采取法律、管理、技术、自律等综合手段来应对，而不能像过去一样信息安全主要依靠技术手段。

1.2 网络空间面临的安全问题

网络空间面临的安全问题包括 Internet 安全问题、电子邮件的安全、域名系统的安全问题、IP 地址的安全问题、Web 站点的安全问题、文件传输的安全问题、社会工程学的安全问题。

1.2.1 Internet 安全问题

Internet 是全球最大的信息网络，它的发展促进了国家的政治、军事、文化和人们生活水平的提升，甚至改变了人们的生活、学习和工作方式。Internet 是一个开放系统。窃密与破坏已经从个人、集团的行为上升到国家的信息战行为。其不安全的问题日显突出。据 CERT/CC 统计，在历年的 Internet 网络安全案件中，其安全威胁来自黑客攻击和计算机病毒。Internet 的安全来自内因和外因的各种因源。

(1)站点主机数量的增加,无法估计其安全性能。网络系统很难动态适应站点主机数量的突增，系统网管功能升级困难也难以保证主机的安全性。

(2) 主机系统的访问控制配置复杂、软件的复杂等，没有能力在各种环境下进行测试，UNIX 系统从 BSD 获得网络部分代码。而 BSD 源代码可轻易获取，导致攻击者易侵入网络系统。

(3) 分布式管理难于预防侵袭，一些数据库用口令文件进行分布式管理，又允许系统共享数据和共享文件，这就带来不安全因素。

(4) 验证环节虚弱。Internet 中的许多事故源于虚弱的静态口令，易被破译，且易于解密或通过监视信道窃取口令。TCP/IP 和 UDP 服务也只能对主机地址进行验证，而不能对指定的用户进行验证。

(5) Internet 和 FTP 的用户名及口令的 IP 包易被监视与窃取。使用 Internet 或 FTP 连接到远程主机上的账户时，在 Internet 上传输的口令是没有加密的，攻击者通过获取的用户名和口令的 IP 包登录到系统。

(6) 攻击者的主机易冒充成被信任的主机。这种主机的 IP 地址是被 TCP 和 UDP 信任的，导致主机失去安全性。攻击者用客户 IP 地址取代自己的 IP 地址或构造一条攻击的服务器与其主机的直接路径，客户误将数据包传送给攻击者的主机。

一般 Internet 服务安全内容包括 E-mail 安全、文件传输（FTP）服务安全、远程登录（Telnet）安全、Web 浏览服务安全和 DNS 域名安全、设备的物理安全以及社会工程学的安全问题。

1.2.2 电子邮件（E-mail）的安全问题

E-mail 即电子邮件，是一种用电子手段提供信息交换的通信方式，也是全球网上最普及的服务方式，数秒内通过 E-mail 传遍全球，它加速了信息交流。E-mail 除传递信件之外，还可以传送文件（当作附件）、声音、图形等信息。

E-mail 不是“终端到终端”的实时服务，而是“存储转发式”服务，它非实时通信，而发送者可随时随地发送邮件，将邮件存入对方电子邮箱，并不要求对方接收者实时在场收发邮件，其优点是不受时间、空间约束。

E-mail 邮件系统的传输过程包括邮件用户代理（Mail User Agent，MUA）、邮件传输代理（Mail Transfer Agent，MTA）和邮件接收代理（Mail Delivery Agent，MDA）三部分。用户代理是一个用户端发信和收发的程序，负责将信件按一定的标准进行包头，然后送到邮件服务器。传输代理负责信件的交换和传输，将信件传送到邮件主机，再交给接收代理。接收代理按收信人的地址，根据简单邮件传输协议将信件传递到目的地。一般采用 Sendmail 程序来完成此工作。接收代理的 POP（Post Office Protocol）网络邮局协议或网络中转协议能使用户在自己的主机上读取这份邮件。E-mail 服务器是向全体开放的，故有一个“路由表”，列出了其他 E-mail 服务器的目的地地址。当服务器读取信头时，如果不是发给自己的，会自动转发到目的地的服务器。

E-mail 的正常服务靠的是 E-mail 服务协议。有以下几种 E-mail 相关协议。

（1）SMTP。

简单邮件传输（Simple Mail Transfer Protocol，SMTP）是邮件传输协议。经过它传递的电子邮件都是以明文形式进行的，但这种明文传输很容易被中途窃取、复制或篡改。

（2）ESMTP。

ESMTP（Extended SMTP）指扩展型 SMTP。其主要有不易被中途截取、复制或篡改的功能。

（3）POP。

POP3 是邮局协议，其在线工作，有邮件保留在邮件服务器上允许用户从邮件服务器收发邮件的功能。POP3 是以用户当前存在邮件服务器上的全部邮件为对象进行操作的，并一次性将它们下载到用户端计算机中。但用户不需要的邮件也下载了。

（4）IMAP4。

Internet 消息访问协议版本 4（Internet Message Access Protocol，IMAP4）为用户提供了有选择地从邮件服务器接收邮件的功能。IMAP4 在用户登录到邮件服务器之后，允许采取多段处理方式，查询邮件，用户只读取电子信箱中的邮件信头，然后下载指定的邮件。

（5）MIME。

MIME（Multipurpose Internet Mail Extensions）协议的功能是将计算机程序、声音和视频等二进制格式信息先转换成 ASCII 文本，然后利用 SMTP 传输这些非文本的电子邮件，也可随同文本电子邮件发出。

E-mail 的安全漏洞有以下几种。

（1）窃取 E-mail。从浏览器向 Internet 上另一方发送 E-mail 时，要经过许多路径上的网络设备，故入侵者可在路径上窃取 E-mail 或伪造 E-mail。

（2）Morris 内有一种会破坏 Sentmail 的指令。这种指令可使其执行黑客发出的命令，故 Web 提供的浏览器更容易受到侵袭。

（3）E-mail 轰炸，E-mail Spamming 和 E-mail 炸弹。E-mail 炸弹（End Bomb 和 KaBoom）能把攻击目标加到近百个 E-mail 列表中。Up Yours 是最流行的炸弹程序，它使用最少的资源，又隐藏自身攻击者的源头而进行攻击。E-mail 轰炸使同一收件人会不停地接到大量同一内容的 E-mail，使电子信箱挤满而不能工作。E-mail Spamming 是同一条信息被传给成千上万的不断扩大的用户，如果一个人用久了 E-mail Spamming，那么所有用户都会收到这封信。E-mail 服务器如果收到很多 E-mail，服务器会脱网，导致系统崩溃，不能服务。

（4）E-mail 欺骗。E-mail 伪称来自网络系统管理员，要求用户将口令改变为攻击者的特定字符串，并威胁用户，如果不按此处理，将关闭用户的账户。

（5）虚构某人名义发出 E-mail。由于任何人都可以与 SMTP 协议的端口连接，故攻击者可以虚构某人名义利用与 SMTP 协议连接的端口发出 E-mail。

（6）电子邮件病毒。由于 Outlook 存在安全隐患，可让攻击者编制一定的代码使病毒自动执行，病毒多以 E-mail 附件形式传给用户，一旦用户点击该附件，计算机就会中毒。故不要打开不明的邮件，如果要打开附件，应先用防毒软件扫描一下，确保附件无病毒。E-mail 为计算机病毒最主要的传播媒介。

E-mail 的安全措施包括以下几种。

（1）在邮件系统中安装过滤器，在接收任何 E-mail 之前，先检查（过滤）发件人的资料，删去可疑邮件，不让它进入邮件系统。

（2）防止 E-mail 服务器超载，超载会降低传递速度或不能收发 E-mail。

（3）如有 E-mail 轰炸或遇上 E-mail Spamming，就要通过防火墙或路由器过滤来自这个地址的 E-mail 炸弹邮包。

（4）防止 E-mail 炸弹指删除文件或在路由的层次上限制网络的传输。另一种方法是写一个 Script 程序，当 E-mail 连接到自己的邮件服务器时，它就会捕捉到 E-mail 炸弹的地址，对邮件炸弹的每一次连接，它都会自动终止其连接，并回复一个声明指出触犯法律。

（5）严禁打开 E-mail 附件中的可执行文件（.EXE、.COM）及 Word/Excel 文档，因为这些多是病毒“特洛伊木马”的有毒文件。

1.2.3 域名系统的安全问题

域名系统（Domain Name System，DNS）是一种用于 TCP/IP 应用程序的分布式数据库，它的作用是提供主机名称和地址的转换信息。网络用户通过 UDP 协议与 DNS 域名服务器进行通信，而服务器在特定的 53 端口监听，并返回用户所需要的相关信息，这是正向域名解析的过程，而反向域名解析是一个查询 DNS 的过程。当用户向一台服务器请求服务时，服务器会根据用户的 IP 地址反向解析出其对应的域名。

域名系统的安全威胁有以下几种。

（1）DNS 会查漏内部的网络拓扑结构，故 DNS 存在安全隐患。整个网络架构中的主机名、主机 IP 列表、路由器名、路由器 IP 列表、计算机所在位置等可以被轻易窃取。

（2）攻击者控制了 DNS 服务器后，就会篡改 DNS 的记录信息，利用被篡改的记录信息达到入侵整个网络的目的，使到达原目的地的数据包落入攻击者控制的主机。

（3）DNS 服务器有其特殊性，在 UNIX 中，DNS 需要 UDP 53 和 TCP 53 的端口，它们需要使用 root 执行权限，这样防火墙很难控制对这些端口的访问，导致入侵者可窃取 DNS 服务器的管理员权限。

（4）DNS ID 欺骗行为：黑客伪装的 DNS 服务器提前向客户端发送响应数据包，使客户端的 DNS 缓存里域名所对应的 IP 变成黑客自定义的 IP，于是客户端被带到黑客设定的网站。

域名系统的威胁解除办法：遇到 DNS 欺骗，先禁止本地连接，然后启用本地连接即可消除 DNS 缓存。如果在 IE 中使用代理服务器，DNS 欺骗就不能进行，因为这时客户端并不会在本地进行域名请求。如果访问的不是网站主页，而是相关子目录的文件，则在自定义的网站上不会找到相关的文件。所以，禁用本地连接，再启用本地连接就可以清除 DNS 欺骗。

1.2.4 IP 地址的安全问题

IP 地址的安全威胁有以下几种。

（1）盗用本网段的 IP 地址，但会记录下物理地址。在路由器上设置静态 ARP 表，可以防止在

本网段盗用 IP。路由器会根据静态 ARP 表检查数据，如果不能对应，则不进行处理。

（2）IP 电子欺骗：IP 欺骗者通过 RAW Socket 编程，发送带有伪造的源 IP 地址的 IP 数据包，让一台机器来扮演另一台机器达到的目的，获得对主机未授权的访问。即使设置了防火墙，如果没有配置对本地区域中资源 IP 包地址的过滤，这种 IP 欺骗仍然奏效。当黑客进入系统后，黑客绕过口令及身份验证，专门等候合法用户连接登录到远程站点，一旦合法用户完成其身份验证，黑客就可控制该连接。这样，远程站点的安全就被破坏了。

IP 欺骗攻击的防备有以下几种办法。

（1）通过对包的监控来检查 IP 欺骗。可用 netlog 或类似的包监控工具来检查外接口上包的情况，如发现包的两个地址——源地址和目的地址都是本地域地址，就意味着有人试图攻击系统。

（2）安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网资源地址包的通过。当然也应禁止（过滤）带有不同的内部资源地址内部包通过路由器到其他网络中，这就防止内部的用户对其他站点进行 IP 欺骗。

（3）将 Web 服务器放在防火墙外面有时更安全。如果路由器支持内部子网的两个接口，则易引发 IP 欺骗。

（4）在局部网络的对外路由器上加一个限制条件，不允许声称来自内部网络包通过，也能防止 IP 欺骗。

1.2.5 Web 站点的安全问题

Web 服务器有以下安全漏洞。

（1）安全威胁类来源有以下几种。

①外部接口。

②网络外部非授权访问。

③网络内部的非授权访问。

④商业或工业间谍。

⑤移动数据。

（2）入侵者会重点针对访问攻击某个数据库、表、目录，达到破坏数据或攻击数据的目的。

（3）进行地址欺骗、IP 欺骗或协议欺骗。

（4）非法偷袭 Web 数据，如电子商务或金融信息数据。

（5）伪装成 Web 站点管理员，攻击 Web 站点或控制 Web 站点主机。

（6）服务器误认闯入者是合法用户，而允许其访问。

（7）伪装域名，使 Web 服务器向入侵者发送信息，而客户无法获得授权访问的信息。

常用的 Web 站点安全措施有以下几种。

（1）将 Web 服务器当作无权限的用户运行，很不安全，故要设置权限管理。

（2）将敏感文件放在基本系统中，再设置二级系统，所有敏感文件数据都不向 Internet 开放。

（3）要检查 HTTP 服务器使用的 Applet 和脚本，尤其是与客户交互作用的 CGI 脚本，以防止外部用户执行内部指令。

（4）建议在 Windows NT 上运行 Web 服务器，并检查驱动器和共享的权限，将系统设为只读状态。

（5）采用 Macintosh Web 服务器更为安全，但又缺少 Windows NT 的一些设置特性。

（6）要克制 daemons 系统的软件安全漏洞。daemons 会执行不要执行的功能，如控制服务、网络服务、与时间有关的活动及打印服务。

（7）为防止入侵者用电话号码作为口令进入 Web 站点，要配备能阻止和覆盖口令的收取机制

及安全策略。

（8）不断更新、重建和改变 Web 站点的连接信息，一般 Web 站点只允许单一种类的文本作为连接资源。

（9）假设 Web 服务器放置在防火墙的后面，就可将“ Wusage ”统计软件安装在 Web 服务器内，以控制通过代理服务器的信息状况，这种统计工具能列出站点上往返最频繁的用户名单。

（10）安装在公共场所的浏览器，以防被入侵者改变浏览器的配置，并获得站点机要信息、IP 地址、DNS 入口号等，故要做防御措施。

1.2.6 文件传输的安全问题

文件传输协议（File Transfer Protocol，FTP）是为用户在 Internet 上主机之间进行收发文件提供的协议。FTP 使用客户机/服务器模式。当使用客户端程序时，用户的命令要求 FTP 服务器传送一个指定文件，服务器会响应发送命令，并传送这个文件，存入用户机的目录中。FTP 传送条件是用户拥有 FTP 服务器的权限。FTP 可通过 CERN 代理服务器访问该服务器或直接访问该服务器。

目前，FTP 的安全问题是 FTP 自身的安全问题及协议的安全功能如何扩展。即便使用安全防火墙，黑客仍有可能访问 FTP 服务器，故 FTP 存在安全问题。

FTP 的安全漏洞有以下几种。

（1）代理 FTP 中的跳转攻击。代理 FTP 是 FTP 规范 PR85 提供的一种允许客户端建立的控制连接，是在两台 FTP 服务器间传输文件的机制。可以不经过中间设备传给客户端，再由客户端转给另一个服务器，这就减少了网络流量，但攻击者可以发出一个 FTP “ PORT ” 命令给目标 FTP 服务器，其中包括该被攻击主机的网络地址和与命令及服务相对应的端口号。这样，客户端就能命令 FTP 服务器发送数据给被攻击的服务器。由于通过第三方连接的，使跟踪攻击者出现难度。其防范措施有：①禁止使用 PORT 命令，而通过 PASV 命令来实现传输，缺点是损失了使用代理 FTP 的能力；②服务器不打开数据连接到小于 1024 的 TCP 端口号，因为 PR85 规定 TCP 端口从 0～1023 是留给用户服务器的端口号，而 1024 以上的服务才是由用户自定义的服务。

（2）FTP 软件允许用户访问所有系统中的文件，且 FTP 文件系统存在可写区域可供攻击者删改文件。

（3）地址被盗用。基于网络地址的访问，会使 FTP 服务器的地址易被盗用，攻击者冒用组织内的机器地址，从而将文件下载到组织外未授权的机器上，防范措施是加上安全鉴别机制。

（4）用户名和密码被猜测。为了防止用户名和密码被猜测，FTP 服务器要限制大于 5 次的查询尝试，停止设备的 5 次以上尝试的控制连接。此时，应给用户一个响应返回码 421，表示服务器不可用，即将关闭控制连接。

（5）端口盗用。

因为用户要获得一个 TCP 端口号，才能连接上一个 FTP 服务器，故端口号易被盗用。从而使黑客盗取合法用户的文件或从授权用户发出的数据流中伪造文件。为防止端口盗用，可以采取随机性分配端口号。

FTP 的安全措施有以下几种。

（1）未经授权的用户禁止进行 FTP 操作，FTP 使用的账号必须在 password 文件中有记载，并且它的口令不能为空。凡是被 FTP 服务器拒绝访问的账号和口令都记录在 FTP 的保护进程 FTP 的 /ete/FTPuser 文件中，凡在此文件出现的用户将拒绝访问。

（2）保护 FTP 使用的文件和目录。

① FTP\bin 目录的所有者设为 root，此目录主要放置系统文件，设为用户不可访问的文件。

② FTP\exe 目录的所有者设为 root，此目录存放 group 文件和 password 文件，设为只读属性，

并将文件 password 中用户加密过的口令删除，但不删除文件中已加密的口令。

③ FTP\pub 目录的所有者设为 FTP，设为所有用户均可读和可写，以保证 FTP 合法用户的正常访问。

④ FTP 的主目录的所有者设为“ FTP ”，主目录设为所有用户均不可写，以防止用户删除主目录文件。注意，设为 FTP 与设为“ FTP ”有不同的含义。

1.2.7 社会工程学的安全问题

网络信息保护中采用的技术和最终对安全系统的操作都是人来完成的。所以从网络信息安全对安全策略的依赖性，已经知道保护的信息对象、所要达到的保护目标是人通过安全策略确定的。因此，在网络信息安全系统的设计、实施和验证中也不能离开人，人在网络信息安全管理中占据着中心地位。特别是网络内部客户，不正确地使用系统，其可以轻而易举地跳过技术控制。例如，计算机系统一般是通过口令来识别用户的。如果用户提供正确的口令，则系统自动认为该用户是授权用户。假设一个授权用户把其用户名/口令告诉了其他人，那么非授权用户就可以假冒这个授权用户，而且无法被系统发现。

非授权用户攻击一个机构的网络计算机系统是危险的。而一个授权的网络内部用户攻击一个机构的网络计算机系统将更加危险。因为内部人员对机构的计算机网络系统结构、操作员的操作规程非常清楚，而且通常知道足够的口令跨越安全控制，而这些安全控制已足以把外部攻击者挡在“门”外了。可见，内部用户的越权使用是一个非常难应对的问题。

如果系统管理员在系统安全的相关配置上出现错误，或未能及时查看安全日志，或用户未正确采用安全机制保护信息，都将会使机构的信息系统防御能力大大降低。没有培训的员工通常会给机构的信息安全带来另一种风险。例如，没有培训员工不知道文件数据备份到磁盘上之前需要做一下验证，当系统遭到攻击后，其员工可能才发现其所备份的文件无法读出来。这是由于错误的流程造成了数据的丢失。由此可见，对使用者的技术培训和安全意识教育是非常重要的。网络信息安全一般不会给组织机构带来直接的经济效益。安全虽然能限制损失，但建设初期是需要花费一定的经费的。认识问题比较严重的是，有的组织机构一般认为在安全上投资是一种浪费，而且为系统添加安全特色通常会使原先简单的操作变得复杂而降低处理效率，这种情况通常会延续到安全问题带来的损失已经发生的时候。

组织机构只有建立起网络信息安全责任和权力基础，网络信息安全才能与机构的其他工作一样正常展开。然而，组织机构开展网络信息安全建设，起初可能会面临一系列问题。例如，首先是缺乏专业人才，或仅有的人才不是专职工作的。其次，网络信息安全建设需要资金支持，需要进行安全需求论证、请人设计和实施，需要培训运行人员，需要建立规章制度等。

在一个组织机构中，对任职人员的行为进行适当的记录是一项保障网络信息安全行之有效的方法。因为网络信息安全不仅要求组织和内部人员有安全技术知识、安全意识和领导层对安全的重视，还必须制定一整套明确的责任，明确审批权限的安全管理制度，以及专门的安全管理机构，从根本上保证所有任职人员的规范化使用和操作。

此外，法律会限制网络信息安全保护中可用的技术以及技术的使用范围，因此决定安全策略或选用安全机制的时候需要考虑法律或条例的规定。

例如，中华人民共和国国家密码管理委员会颁布的《商用密码管理条例》（1999 年）规定，在中国，商用密码属于国家密码，国家对商用密码的科研、生产、销售和使用实行专控经营。

也就是说，使用未经国家批准的密码算法，或使用国家批准的算法但未得到国家授权认可的产品都属于违法行为。因此，当采用密码算法保护本单位的商用信息时，需要采用国家授权的产品。

在现代社会里，人们的行为习惯和社会道德都会对网络空间信息安全产生影响。一些技术方法

或管理办法在一个国家或区域可能不会有问题，但在另一个地方可能会受到抵制。例如，密钥托管在一些国家实施起来可能不会很艰难，但有些国家曾因为密钥托管技术的使用被认为侵犯了人权而被起诉。信息安全的实施与所处的社会环境有紧密的联系，不能鲁莽照搬他人的经验。

1.3 网络空间信息安全的主要内容

随着信息化进程的深入和网络的飞速发展，我国现在已建设了大量的信息化系统，并成为国家关键基础设施，它们支持着电子政务、电子商务、电子金融、电子投票、网络通信、网络合作研究、网络教育、网络医疗和社会保障等方方面面。网络化、信息化、数字化的特点使这些系统均与保密或敏感网络信息有关，运作方式有别于传统模式，因此，这些设施的安全维护显得格外重要。要保证网络电子信息的安全性和有效性，除了需要根据知识经济的发展，制定出相适应的政策、法规和管理规范外，还需要通过网络空间信息安全技术来提供安全保障。网络空间信息安全是构建整个社会网络化、信息化、数字化的根本保证。

现代网络技术的广泛应用大大提高了人类活动的质量和效率，但如同许多新技术的应用一样，网络技术也是人类为自己锻造的一柄双刃剑，善意的应用将造福于人类，恶意的应用则将给社会带来危害。所以，我们在考虑网络空间信息安全的保障总体规划上，不仅要在网络空间信息安全技术上统筹计划，还要强调网络信息保障研究跨学科的性质。更重要的是加强网络空间信息安全教育与管理，强调其系统规划和责任，重视对网络空间信息系统使用的法律与道德规范问题，将法律、法规和各种规章制度融合到网络空间信息安全解决方案之中。总之，网络空间信息安全保障和网络空间信息安全的本质在于思想观念上的主动防御而不是被动保护。网络空间信息安全保障涉及管理、制度、人员、法律和技术等方面。因此，解决网络信息安全的基本策略是综合治理。网络信息安全研究所涉及的内容相当广泛，包括网络空间信息设施的安全性、网络空间信息传输的完整性（防止信息被未经授权的篡改、插入、删除或重传）、网络空间信息自身的保密性（保证网络空间信息不泄露给未经授权的人）、网络信息的可控性（对网络空间信息和网络空间信息系统实施安全监控管理，防止非法用户利用网络空间信息和网络空间信息系统）、网络空间信息的不可否认性（保证发送和接收网络空间信息的双方不能事后否认他们自己所做的操作行为）、网络空间信息的可用性（保证网络空间信息和网络空间信息系统确实能为授权者所用，防止由于计算机病毒或其他入侵行为造成系统的拒绝服务）、网络信息人员的安全性和网络信息管理的安全性等。本书有侧重地对下列问题予以讨论和介绍。

1.3.1 病毒防治技术

随着计算机的应用与推广，计算机技术已经渗透到社会的各个领域，伴随而来的计算机病毒传播问题也引起人们的关注。网络计算机病毒可以渗透到信息社会的各个领域，对信息社会造成严重威胁。20 世纪 70 年代中叶，计算机病毒开始出现在美国的一些科幻小说中，使生活在信息社会中的人们颇感新奇。然而，曾几何时，这个人们臆想中的“幽灵”已经活生生地活动在世界各地的计算机系统中，并对信息系统的安全构成了严重的威胁。世界上第一个计算机病毒，准确地说应该是第一个“病毒”雏形，源于 20 世纪 60 年代初美国贝尔实验室的 3 个年轻的程序员编写的一个名为“磁芯大战”的游戏，游戏通过复制自身来摆脱对方的控制。

1983 年 11 月，在国际计算机安全学术研讨会上，美国计算机专家首次将病毒程序在 VAX/750 计算机上进行了实验，世界上第一个计算机病毒就这样诞生在实验室中。

20 世纪 80 年代后期，巴基斯坦有一对以编程为生的兄弟，他们为了打击那些盗版软件的使用

者，设计出了一个名为“巴基斯坦”的病毒，这就是世界上流行的第一个真正的病毒。

总地来说，计算机病毒的发展经历了以下 5 个阶段。

第一个阶段为原始病毒阶段，产生于 1986—1989 年，由于当时计算机的应用软件少，而且大多单机运行，因此病毒没有大量流行，种类也很有限，病毒的清除工作相对来说较容易。

第二个阶段为混合型病毒阶段，产生于 1989—1991 年，是计算机病毒由简单发展到复杂的阶段。计算机局域网开始应用与普及，给计算机病毒带来了第一次流行高峰。

第三个阶段为多态性病毒阶段。防病毒软件查杀此类病毒非常困难。这个阶段病毒技术开始向多维化方向发展。

第四个阶段为网络病毒阶段。从 20 世纪 90 年代中后期开始，随着国际互联网的发展壮大，依赖互联网传播的邮件病毒和宏病毒等大量涌现，病毒传播速度快、隐蔽性强、破坏性大。

第五个阶段为主动攻击型病毒。这类病毒利用操作系统的漏洞进行进攻型的扩散，并不需要任何媒介或操作，用户只要接入互联网就有可能被感染，此类病毒的危害性更大。

迄今为止，世界上已发现的计算机病毒已有数万种，给全球经济造成的损失每年高达数十亿美元。可以预见，随着计算机、网络运用的不断普及、深入，防范计算机病毒将越来越受到人们的高度重视。

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。可见，计算机病毒是一种人为的用计算机高级语言写成的可存储、可执行的计算机非法程序。因为这种非法程序隐蔽在计算机系统可存储的信息资源中，能像微生物学所称的病毒一样，利用计算机信息资源进行生存、繁殖和传播，影响和破坏计算机系统的正常运行，所以人们形象地把这种非法程序称为“计算机病毒”。计算机病毒是一种特殊程序，因此病毒程序的结构决定了病毒的传染能力和破坏能力。从程序结构上来看，计算机病毒通常由 3 部分组成：引导模块，将病毒从外存引入内存，激活传染模块和表现模块；传染模块，负责病毒的传染和扩散，将病毒传染到其他对象上；表现模块，计算机病毒中最关键的部分，实现病毒的破坏作用，如删除文件、格式化硬盘、显示或发声等。计算机病毒主要呈现以下特征：传染性、非授权性、隐蔽性、潜伏性、破坏性、不可预见性、可触发性。

计算机病毒有以下特点：一是攻击隐蔽性强，病毒可以无声无息地感染计算机系统而不被察觉，待发现时，往往已造成严重后果；二是繁殖能力强，计算机一旦染毒，可以很快复制许多病毒文件，目前的三维病毒还会产生很多变种；三是传染途径广，可通过软盘、有线和无线网络、硬件设备等多渠道自动侵入计算机中，并不断蔓延；四是潜伏期长，病毒可以长期潜伏在计算机系统中而不发作，待满足一定的条件后，就激发破坏；五是破坏力大，计算机病毒一旦发作，轻则干扰系统的正常运行，重则破坏磁盘数据、删除文件，导致整个计算机系统的瘫痪；六是针对性强，计算机病毒的效能可以准确地加以设计，满足不同环境和时机的要求。

计算机病毒的广泛传播，推动了反病毒技术的发展，新的反病毒技术的出现，又迫使计算机病毒更新其技术。两者相互激励，螺旋式上升地不断提高各自的水平，在此过程中涌现出许多计算机病毒新技术，采用这些技术的目的是使计算机病毒广泛传播。计算机病毒的发展呈现以下趋势。

（1）病毒传播方式不再以存储介质为主要的传播载体，网络成为计算机病毒传播的主要载体，使用计算机网络逐渐成为计算机病毒发作条件的共同点。

（2）传统病毒日益减少，计算机病毒变形（变种）的速度极快并向混合型、多样化发展，网络蠕虫成为最主要和破坏力最大的病毒类型。

（3）运行方式和传播方式将更加多样化，更具有隐蔽性。

（4）尽管目前 Windows 10 比其他版本的 Windows 系统安全，但随着其日益流行，它将成为黑客的主要攻击目标。

（5）针对 OS X 和 UNIX 等其他系统的病毒数量明显增加。

（6）跨操作系统的病毒将会越来越多。

（7）计算机病毒技术与黑客技术将日益融合，出现带有明显病毒特征的木马或者木马特征的病毒。

（8）物质利益将成为推动计算机病毒发展的最大动力。

长期以来，人们设计计算机的目标主要是追求信息处理功能的提高和生产成本的降低，而对于安全问题则重视不够。计算机系统的各个组成部分、接口界面、各个层次的相互转换，都存在着不少漏洞和薄弱环节。全球万维网（WWW）使“地球一村化”，为计算机病毒创造了实施的空间。新的计算机技术在电子系统中不断应用，为计算机病毒的实现提供了客观条件。国外专家认为，分布式数字处理、可重编程嵌入计算机、网络化通信、计算机标准化、软件标准化、标准的信息格式、标准的数据链路等都使计算机病毒侵入成为可能。

现代信息技术的巨大进步已使空间距离不再遥远，“相隔天涯，如在咫尺”，但也为计算机病毒的传播提供了新的“高速公路”。计算机病毒可以附着在正常文件中通过网络进入一个又一个系统，国内计算机感染一种“进口”病毒已不再是什么大惊小怪的事情了。在信息国际化的同时，计算机病毒也在国际化。因此，计算机病毒防范的对策和方法根据计算机病毒的组成、特点和传播途径，可分为以下措施。

（1）给计算机安装防病毒软件，各种防病毒软件对防止病毒的入侵有较好的预防作用。

（2）写保护所有系统盘，不要把用户数据或程序写到系统盘上，对系统的一些重要信息做备份。一般至少做出 CMOS、硬盘分区表和引导区记录等参数的备份（可用 Debug 或 Norton Utilities Disk Tool 等），有些病毒很猖獗，如 CMOS 病毒，一旦感染，可能使所有硬盘参数丢失，如果没有这些参数备份，计算机则可能完全崩溃。

（3）尽量使用硬盘引导系统，并且在系统启动时即安装病毒预防或疫苗软件。例如，在系统启动时，在 Windows 98 的启动栏中装入 Vsafe.com、Norton、Scan 或 LANDesk Virus Protect。

（4）对公用软件和共享软件的使用要谨慎，禁止在机器上运行任何游戏盘，因游戏盘携带病毒的概率很高。禁止将软盘带出或借出使用，必须要借出的软盘归还后一定要进行检测，无毒后才能使用。

（5）对来历不明的软件不要未经检查就上机运行。要尽可能使用多种最新查毒、杀毒软件来检查外来的软件。同时，应经常用查毒软件检查系统、硬盘上有无病毒。

（6）使用套装正版软件，不使用或接收未经许可的软件。

（7）使用规范的公告牌和网络，不要从非正规的公告牌中卸载可执行程序。

（8）对已联网的微机，注意访问控制，不允许任何对微机的未授权访问。

（9）计算机网络上使用的软件要严格检查，加强管理。

（10）不忽视任何病毒征兆，定期用杀毒软件对机器和软盘进行检测。

总之，对于计算机病毒要以预防为主，尽量远离病毒感染源，只有这样才能给计算机一个洁净而安全的生存环境。

1.3.2 远程控制与黑客入侵

一般认为，计算机系统的安全威胁主要来自黑客的攻击，现代黑客从以系统为主的攻击转变为以网络为主的攻击，而且随着攻击工具的完善，攻击者不需要专业的知识就可以完成复杂的攻击过程。首先是远程控制，它只是通过网络来操纵计算机的一种手段而已，只要运用得当，操纵远程的计算机也就如同操纵眼前正在使用的计算机一样。远程控制在网络管理、远程协作、远程办公等计算机领域有着广泛的应用，它进一步克服了由于地域性的差异而带来的操作中的不便性，使网络的效率得到了更大的发挥。其实，远程控制的具体操作过程并不复杂，关键是要选好适合远程控制

的软件工具，远程控制就是一把双刃剑，若利用不当，会造成很大的安全隐患。

计算机中的远程控制技术，始于磁盘操作系统时代，只是那个时代由于计算机性能和技术比较低，网络不发达，市场没有更高的要求，所以远程控制技术没有引起更多人的注意。但是，随着网络的高度发展，出于计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。远程控制一般支持下面的网络方式：LAN、WAN、拨号方式、互联网方式。此外，有的远程控制软件还支持通过串口、并口、红外端口对远程机的控制。传统的远程控制软件一般使用 NetBEUI、NetBIOS、IPX/SPX、TCP/IP 等协议来实现远程控制。随着网络技术的快速发展与普及，目前很多远程控制软件提供通过 Web 页面以 Java 技术来控制远程网络计算机的服务。

黑客源于英语动词 hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数计算机使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”由这些定义中，还看不出贬义的意味。

在 20 世纪的 60—70 年代，“黑客”也曾经专用来形容那些有独立思考意识的计算机“迷”，如果他们在软件设计上做了一件非常漂亮的工作，或者解决了一个程序难题，同事们经常高呼“hacker”。

他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。“黑客”能使更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。于是“黑客”就被定义为“技术娴熟的具有编制操作系统级软件水平的人”。

许多处于 UNIX 时代早期的“黑客”云集在麻省理工学院和斯坦福大学，正是这样一群人建成了今天的“硅谷”。后来某些具有“黑客”水平的人物利用通信软件或者通过网络非法进入他人系统，截获或篡改计算机数据，危害信息安全。于是“黑客”开始有了“计算机入侵者”或“计算机捣乱分子”的恶名。入侵者是那些利用网络漏洞破坏网络的人。他们往往做一些重复的工作（如用暴力法破解口令），也具备广泛的计算机知识，但与黑客不同的是他们以破坏为目的。这些群体成为“骇客”。当然，有一种人介于黑客与入侵者之间。 到了 20 世纪的 80、90 年代，计算机越来越重要，大型数据库也越来越多，同时，信息越来越集中在少数人的手里。这样一场新时期的“圈地运动”引起了黑客们的极大反感。黑客认为，信息应共享而不应被少数人垄断，于是将注意力转移到涉及各种机密的信息数据库上。而这时，计算机化空间已私有化，成为个人拥有的财产，社会不能再对黑客行为放任不管，而必须采取行动，利用法律等手段来进行控制。

典型的黑客会使用如下技术隐藏其真实的 IP 地址：利用被侵入的主机作为跳板；在安装 Windows 的计算机内利用 WinGate 软件作为跳板；利用配置不当的 Proxy 作为跳板。 黑客总是寻找那些被信任的主机。这些主机可能是管理员使用的机器，或者一台被认为很安全的服务器。黑客会检查所有运行 nfsd 或 mountd 的主机的 NFS 输出。往往这些主机的一些关键目录（如/usr/bin、/etc 和/home）可以被那台被信任的主机侵入。

Finger Daemon 也可以被用来寻找被信任的主机和用户，因为用户经常从某台特定的主机上登录。黑客还会检查其他方式的信任关系。例如，其可以利用 CGI 的漏洞，读取/etc/hosts.allow 文件等。

黑客会选择一台被信任的外部主机进行尝试。一旦成功侵入，黑客将从这里出发，设法进入内部的网络。但这种方法是否成功要看内部主机和外部主机间的过滤策略。攻击外部主机时，黑客一般会运行某个程序，利用外部主机上运行的有漏洞的 daemon 窃取控制权。有漏洞的 daemon 包括 Sendmail、IMAP、POP3 各个漏洞的版本，以及 RPC 服务中的 statd、mountd、PCNFSD 等。有时，攻击程序必须在与被攻击主机相同的平台上进行编译。

一旦计算机被黑客入侵，那么被入侵的计算机将没有任何秘密可言，因此我们要加强网络安

全防范意识，学习并掌握一些基本的安全防范措施，尽量使其免受黑客的攻击。

1.3.3 网络信息密码技术

网络信息密码技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机交叉的一门新兴学科。随着计算机网络和计算机通信技术的发展，网络信息密码技术得到了前所未有的重视并迅速地发展和普及起来。密码作为运用于军事和政治斗争的一种技术，历史悠久，无论是在古希腊时代还是在现代都发挥了非常重要的作用。现代密码学不仅用于解决信息的保密性，还用于解决信息的完整性、可用性、可控性和不可抵赖性等。可以说，密码是保护网络信息安全的最有效的手段，密码技术也是保护网络信息安全的关键技术。过去密码的研制、生产、使用和管理都是在封闭的环境下进行的。20 世纪 70 年代以来，随着经济、社会和信息技术的发展，密码应用范围日益扩大，社会对密码的需求愈加迫切，密码研究领域不断拓宽，密码研究也从专门机构扩展到社会和民间，密码技术得到了空前发展。

密码技术是保障信息安全的最基本、最核心的技术措施和理论基础。密码技术不仅在保护国家秘密信息中具有重要的、不可代替的作用，同时，也广泛应用于电子邮件、政府信息上网、网上招生录取、网上购物、网络银行、数字化网络电视、网络远程教育、远程合作诊断等领域。密码通信模型由明文空间、密文空间、密钥空间、加密算法、解密算法 5 个模块组成，安全密码体制根据应用性能对网络信息提供秘密性、鉴别性、完整性、不可否认性等功能。常见密码的破解方法有唯密文攻击法、已知明文攻击法、选择文攻击法。到目前为止，已经公开发表的各种加密算法已有数百种。若以密钥为分类标准，可将密码系统分为对称密码 （又称为单钥密码或私钥密码）和非对称密码 （又称为双钥密码或公钥密码）。若以密码算法对明文的处理方式为标准，则可将密码系统分为序列密码和分组密码系统。在私钥密码体制中，发送方和接收方使用同一个秘密密钥，即加密密钥和解密密钥是相同或等价的。除了以代换密码和转轮密码为代表的古典密码之外，比较著名的私钥密码系统有美国的 DES 及其各种变形，如 Triple DES、GDES、NewDES，欧洲的 IDEA，日本的 FEAL-N、LOKI-91、Skipjack、RC4、RC5 等。其中数据加密标准（Data Encryption Standard，DES）为美国国家标准局（现美国国家标准与技术研究所）公布的商用数据加密标准，几十年来得到了广泛的应用。

对称密码体系中主要有三大密码标准：数据加密标准、高级加密标准和序列加密算法。数据加密标准是 20 世纪 70 年代由 IBM 公司设计和修改的、经美国国家标准局（NBS）审阅的一种分组加密算法，即对一定大小的明文或密文进行加密或解密工作，其工作模式分为电子密码本、密码分组链和密码反馈，并可以通过多次使用 DES 或要求多于 56 位的密钥增强安全性。高级加密标准是用于替代 DES 的，并要求新算法必须允许 128、192、256 位密钥长度，不仅能够在 128 位输入分组上工作，还能在各种不同硬件上工作，速度和密码强度同样也要被重视。在加密算法上，AES 算法密钥长度限制为 128 位，算法过程由 10 轮循环组成，每一轮循环都有一个来自于初始密钥的循环密钥，由 4 个基本步骤组成：字节转换、移动行变换、混合列变换、加循环密钥，而解密算法则是加密的逆过程。

在公钥密码体制中，接收方和发送方使用的密钥互不相同，即加密密钥和解密密钥不相同，加密密钥公开而解密密钥保密，而且几乎不可能由加密密钥推导出解密密钥。比较著名的公钥密码系统有 RSA 密码系统、椭圆曲线密码系统、背包密码系统、McEliece 密码系统、Diffie-Hellman 密码系统、零知识证明的密码体制和 ElGamal 密码等。理论上，最为成熟完善的公钥密码体制是 RSA 算法，以及 Diffie-Hellman、ElGamal 和 Merkle-Hellman 公钥体制。最有影响的公钥密码体制是 RSA 和 ECC，它们能够抵抗到目前为止已知的所有密码攻击。RSA 密码体制的安全性基于大整数素因子分解的困难性。ECC 密码系统的安全性基于求解椭圆曲线离散对数问题的困难性。ECC 被认为

是下一代最有前途的密码系统。

在“密码管理”方面主要讨论密码的生成、空间、发送、验证、更新、存储密钥的管理机制。其中，密码的生成是算法安全性的基础；非线性密钥空间可假设能将选择的算法加入到防篡改模块中，要求有特殊保密形式的密钥，从而使能偶然碰到正确密钥的可能性降低；在密钥发送时需要分成许多不同的部分，然后用不同的信道发送，即使截获者能收集到密钥，仍可保证密钥安全性；密钥验证需要根据信道类型判断是发送者传送还是伪装发送者传送；密钥更新可采用从旧密钥中产生新密钥的方法改变加密数据链路的密钥。

1.3.4 数字签名与验证技术

随着 Internet 的发展与应用的普及，除了需要保护用户通信的私有性和秘密性，使非法用户不能获取、读懂通信双方的私有信息和秘密信息之外，在许多应用中，还需要保证通信双方的不可抵赖性和信息在公共信道上传输的完整性。数字签名（Digital Signatures）、身份验证和信息验证等技术可以解决这些问题。

数字签名的概念最早由 Whitfield Diffie 和 Martin Hellman 于 1976 年提出，其目的是使签名者对电子文件也可以进行签名并且无法否认，验证者无法篡改文件。简单地说，所谓数字签名就是附加在数据单元上的一些数据，或者对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人（如接收者）伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。各种数字签名方案先后被提出：Rivest、Shamir 和 Adleman 于 1978 年提出了基于 RSA 公钥密码算法的数字签名方案；Shamir 于 1985 年提出了一种基于身份识别的数字签名方案；ElGamal 于 1985 年提出了一种基于离散对数的公钥密码算法和数字签名方案； Schnorr 于 1990 年提出了适合智能卡应用的有效数字签名方案；Agnew 于 1990 年提出了一种改进的基于离散对数的数字签名方案；NIST 于 1991 年提出了数字签名标准；1992 年，Scott Vanstone 首先提出椭圆曲线数字签名算法。1993 年以来，针对实际应用中大量特殊场合的签名需要，数字签名领域转向对特殊签名和多重数字签名的广泛研究阶段。

基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。其包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou- Quisquarter、Schnorr、Ong-Schnorr-Shamir、DES/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及法律问题，美国基于有限域上的离散对数问题制定了自己的数字签名标准。数字签名技术是不对称加密算法的典型应用。数字签名的应用过程如下：数据源发送方使用自己的私钥对数据校验和其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在公钥与私钥管理方面，数字签名应用与加密邮件 PGP 技术正好相反。在数字签名应用中，发送者的公钥可以很方便地得到，但其私钥需要严格保密。

数字签名主要的功能是保证信息传输的完整性、发送者的身份验证、防止交易中的抵赖发生。数字签名通过一套标准化、规范化的软硬结合的系统，使持章者可以在电子文件上完成签字、盖章，与传统的手写签名、盖章具有完全相同的功能。其主要解决电子文件的签字盖章问题，用于辨识电子文件签署者的身份，保证文件的完整性，确保文件的真实性、可靠性和不可抵赖性。同时，依据《中华人民共和国电子签名法》使用户所签署文档具有法律效力，大大提高了用户在电子商务、电

子政务中的办事效率和安全性，同时也为实现无纸化办公扫除了障碍，大大节省了办公耗材等。

在现代生活中，当人们在住宿、求职、银行存款时，通常要出示自己的身份证来证明自己的身份。但是，如果警察要求你出示身份证以证明你的身份，按照规定，警察必须首先出示自己的证件来证明自身的身份。前者是一方向另一方证明身份，而后者则是对等双方相互证明自己的身份。网络信息验证技术是网络信息安全技术的一个重要方面，它用于保证通信双方的不可抵赖性和信息的完整性。在 Internet 深入发展和普遍应用的时代，网络信息验证显得十分重要。例如，在网络银行、电子商务等应用中，对于所发生的业务或交易，人们可能并不需要保密交易的具体内容，但是交易双方应当能够确认是对方发送(接收)了这些信息,同时接收方还能确认接收的信息是完整的，即在通信过程中没有被修改或替换。

一般的，网络身份验证可分为用户与主机间的验证和主机与主机之间的验证。用户与主机之间的验证可以基于如下一个或几个因素来完成。

（1）用户所知道的东西，如口令、密码等。

（2）用户拥有的东西，如印章、智能卡（如信用卡等）。

（3）用户所具有的生物特征，如指纹、声音、视网膜、签字、笔迹等。

下面对这些方法的优劣进行比较。

基于口令的验证方式是一种最常见的技术,但是存在严重的安全问题。它是一种单因素的验证，安全性依赖于口令，口令一旦泄露，用户即可被冒充。

基于智能卡的验证方式，智能卡具有硬盘加密功能，有较高的安全性。每个用户持有一张智能卡，智能卡存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息。进行验证时，用户输入 PIN（个人身份识别码），智能卡验证 PIN，成功后，即可读出秘密信息，进而利用该信息与主机之间进行验证。基于智能卡的验证方式是一种双因素的验证方式（PIN+智能卡），即使 PIN 或智能卡被窃取，用户仍不会被冒充。

基于生物特征的验证方式以人体唯一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机的强大功能和网络技术进行图像处理和模式识别。该技术具有很好的安全性、可靠性和有效性，与传统的身份确认手段相比，无疑产生了质的飞跃。当然，身份验证的工具应该具有不可复制及防伪等功能，使用者应依照自身的安全程度需求选择一种或多种工具进行。但目前这种技术并不成熟，而且需要用户增加成本，以使生物特征测定所需要的设备和计算机网络中的身份识别系统集成起来，同时，这种技术在身份验证的速度、方便性等方面还有很多实际问题需要解决。另外，这种技术也并非能够解决所有问题，攻击者依然可能设法破坏或者绕过计算机网络中的身份识别机制从而获得权限，因此，其他方面的安全措施依然十分重要。

1.3.5 网络安全协议

网络协议是网络上所有设备（网络服务器、计算机及交换机、路由器、防火墙等）之间通信规则的集合，它定义了通信时信息必须采用的格式和这些格式的意义。大多数网络采用分层的体系结构，每一层都建立在它的下层之上，向它的上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。一台设备上的第 n 层与另一台设备上的第 n 层进行通信的规则就是第 n 层协议。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。网络安全协议就是在协议中采用了若干的密码算法协议——加密技术、验证技术、保证信息安全交换的网络协议。它运行在计算机通信网或分布式系统中，为安全需求的各方提供了一系列步骤。

一般的，网络安全协议具有以下 3 种特点。

（1）保密性：即通信的内容不向他人泄露。为了维护人们的个人权利，必须确定通信内容发给

所指定的人，同时必须防止某些怀有特殊目的的人的“窃听”。

（2）完整性：把通信的内容按照某种算法加密，生成密码文件进行传输。在接收端对通信内容进行破译，必须保证破译后的内容与发出前的内容完全一致。

（3）验证性：防止非法的通信者进入。进行通信时，必须先确认通信双方的真实身份。甲乙双方进行通信，必须确认甲乙是真正的通信人，防止除甲、乙以外的人冒充甲或乙的身份进行通信。为了保证计算机网络环境中信息传递的安全性，促进网络交易的繁荣和发展，各种信息安全标准应运而生。SSL、SET、IPSec 等都是常用的安全协议，为网络信息交换提供了强大的安全保护。

常用的安全协议有 SSH（安全外壳协议）、PKI（公钥基础结构）、SSL（安全套接字层协议）、SET（安全电子交易）、IPSec（网络协议安全）等。

（1）SSH 是 Secure Shell Protocol 的缩写。它是由 Network Working Group 所制定的协议。通过它可以加密所有传输的数据，攻击者想通过 DNS 欺骗和 IP 欺骗的方法是无法入侵系统的。SSH 可以将要传输的数据在传输之前进行压缩，从而加快传输的速度。

（2）PKI 是 Public Key Infrastructure 的缩写，是提供公钥加密和数字签名服务的系统或平台，目的是管理密钥和证书。一个机构通过采用 PKI 框架管理密钥和证书可以建立一个安全的网络环境。

PKI 是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构和关于公开密钥的安全策略等基本成分共同组成。PKI 是利用公钥技术实现电子商务安全的一种体系，是一种基础设施，网络通信、网上交易是利用它来保证安全的。从某种意义上讲，PKI 包含了安全验证系统，即安全验证系统——CA/RA 系统是 PKI 不可缺少的组成部分。

PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性，数据的机密性是指数据在传输过程中，不能被非授权者偷看，数据的完整性是指数据在传输过程中不能被非法篡改，数据的有效性是指数据不能被否认。一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解 PKI 是怎样管理证书和密钥的。

（3）SSL 是 Secure Sockets Layer 的缩写，是一种安全协议，它为网络（如互联网）的通信提供私密性。SSL 使应用程序在通信时不用担心被窃听和篡改。SSL 实际上是共同工作的两个协议：“SSL 记录协议”（SSL Record Protocol）和“SSL 握手协议”（SSL Handshake Protocol）。

SSL 是网景（Netscape）公司提出的基于 Web 应用的安全协议，它包括服务器验证、客户验证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。对于电子商务应用来说，使用 SSL 可保证信息的真实性、 完整性和保密性。但由于 SSL 不对应用层的消息进行数字签名，因此不能提供交易的不可否认性，这是 SSL 在电子商务中使用的最大不足。鉴于此，网景公司在从 Communicator 4.04 开始的所有浏览器中引入了一种被称作“表单签名”的功能，在电子商务中，可利用这个功能来对包含购买者的订购信息和付款指令的表单进行数字签名，从而保证交易信息的不可否认性。综上所述，在电子商务中采用单一的 SSL 协议来保证交易的安全是不够的，但采用“SSL+表单签名”模式能够为电子商务提供较好的安全性保证。

（4）SET 是 Secure Electronic Transaction 的缩写，即安全电子交易，是由美国 VISA 和 MasterCard 两大信用卡组织提出的应用于 Internet 上的以信用卡为基础的电子支付系统协议。它采用了公钥密码体制和 X.509 数字证书标准，主要在 B to C 模式中保障支付信息的安全性。SET 协议本身比较复杂，设计比较严格，安全性高，它能保证信息传输的机密性、真实性、完整性和不可否认性。SET 协议是 PKI 框架下的一个典型实现，也在不断升级和完善。

由于 SET 提供了消费者、商家和银行之间的验证，确保了交易数据的安全性、完整可靠性和不可否认性，特别是保证不将消费者银行卡号暴露给商家等，因此它成为了目前公认的信用卡/借

记卡的网上交易的国际安全标准。

IPSec 是 IP Security 的缩写。由于 Internet 是全球最大的、开放的计算机网络，TCP/IP 协议族是实现网络连接和互操作性的关键，但在最初设计 IP 协议时并没有充分考虑其安全性。为了加强 Internet 的安全性，Internet 安全协议工程任务组研究制定了一套用于保护 IP 层通信的安全协议。

1.3.6 无线网络安全机制

从 20 世纪 90 年代以来，移动通信和 Internet 是信息产业发展最快的两个领域，它们直接影响了亿万人的生活，大大地改变了人类的生活方式。移动通信使人们可以在任何时间、任何地点和任何人进行通信，Internet 使人们可以获得丰富多彩的信息。那么如何把移动通信和 Internet 结合起来，使任何人、任何地方都能联网呢？无线网络的出现解决了这个问题。

所谓无线网络，就是利用无线电波作为信息传输的媒介构成的无线局域网（Wireless LAN，WLAN），与有线网络的用途十分类似，最大的不同在于传输媒介的不同，利用无线电技术取代网线，可以和有线网络互为备份。

目前，无线网络可分为以下几类。

（1）无线个人网：主要用于个人用户工作空间，典型距离覆盖几米，可以与计算机同步传输文件，访问本地外围设备，如打印机等。目前，主要技术包括蓝牙（Bluetooth）和红外（IrDA）。

（2）无线局域网：主要用于宽带家庭、大楼内部及园区内部，典型距离覆盖几十米至上百米。目前，其主要技术为 802.11 系列。

（3）无线 LAN-to-LAN 网桥：主要用于大楼之间的联网通信，典型距离为几千米，许多无线网桥采用 802.11b 技术。

（4）无线城域网和广域网：覆盖城域和广域环境，主要用于 Internet 访问，但提供的带宽比无线网络技术要低很多。

在无线网络领域，常见的是 IEEE 802.11 标准。IEEE 802.11 是 IEEE 最初制定的一个无线网络标准，主要用于解决办公室局域网和校园网、用户与用户终端的无线接入。

IEEE 802.11 是由 IEEE 最初制定的无线局域网标准系列：1999 年 9 月 IEEE 802.11b 出台，其通信速率为 11Mb/s，工作在 2.4GHz 的无线频段；随后推出的 IEEE 802.11a 的工作频段为 5.4GHz，通信速率提高到 54Mb/s; 2001 年底 IEEE 802.11g 的推出又旨在解决 IEEE 802.11a 和 IEEE 802.11b 在工作频段上不兼容而不易过渡的问题。无论是在国外还是在国内，IEEE 802.11 无线局域网技术都可以称得上是 IT 业界发展最快的一种技术。常见的无线网络标准有以下 3 种。

（1）IEEE 802.11a：使用 5GHz 频段，传输速率 54Mb/s，与 802.11b 不兼容。

（2）IEEE 802.11b：使用 2.4GHz 频段，传输速率 11Mb/s。

（3）IEEE 802.11g：使用 2.4GHz 频段，传输速率 54Mb/s，可向下兼容 802.11b，目前 IEEE 802.11b 最常用，但 IEEE 802.11g 更具下一代标准的实力。

对不同的无线网络技术，有着不同的安全级别要求。一般的，安全级别可分为四级。第一级，扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据。第二级，采取网络隔离及网络验证措施。第三级，设置严密的用户口令及验证措施，防止非法用户入侵。第四级，设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容。

针对无线网络的安全问题，采取的常见措施如下：第一，运用服务区标识符（SSID）；第二，运用扩展服务集标识号（ESSID）；第三，物理地址过滤；第四，连线对等保密（WEP）；第五，使用虚拟专用网络（VPN）；第六，端口访问控制技术（802.1x）。

计算机无线联网方式是有线联网方式的一种补充，它是在有线网的基础上发展起来的，使联网的计算机可以自由移动，能快速、方便地解决以有线方式不易实现的信道连接问题。然而，由于无

线网络采用空间传播的电磁波作为信息的载体，因此与有线网络不同，辅以专业设备，任何人都有条件窃听或干扰信息，因此在无线网络中，网络安全是至关重要的。

各种无线网络的运用必将越来越进步与普遍，所以只要有资料信号在无线中传送，安全的保护机制将是首先要面对的问题，唯有确保万无一失的数据传输，才能满足人们在一定的区域内实现不间断移动办公的要求，为用户创造了一个安全自由的空间，这也将为服务商带来无限的商机。

1.3.7 访问控制与防火墙技术

信息安全的门户是访问控制与防火墙技术。访问控制技术过去主要用于单机状态，但如今随着网络技术的发展，该项技术也得到了长足的进步，而防火墙技术则是用于网络安全的关键技术之一。只要网络世界存在着利益之争，那么就必须要“自立门户”，即拥有自己的网络防火墙。

访问控制是通过一个参考监视器来进行的。每次用户对系统内目标进行访问时，都由它来进行调节。用户对系统进行访问时，参考监视器查看授权数据库，以确定准备进行操作的用户是否确实得到了可进行此项操作的许可。而数据库的授权则是由一个安全管理器负责管理和维护的，管理器以组织的安全策略为基准来设置这些授权。访问控制策略包括自由访问控制策略、强制性策略、角色策略。强制性和自由访问控制策略都很有用，但它们并不能满足许多实际需要。角色访问策略成功地替代了严格的传统的强制性控制并提供了自由控制中的一些灵活性。有效地分散式授权行政管理还可以使用改进的一些技术。

将计算机和网络安全更紧密地统一起来，发展信息安全是非常必要的。访问控制策略尽管在这方面已取得了很大进步，却还在发展之中。为此，必须引入防火墙技术。

一般而言，安全防范体系具体实施的第一项内容就是在内网和外网之间构筑一道防线，以抵御来自外部的绝大多数攻击，完成这项任务的网络边防产品就是防火墙。下面来看看防火墙的发展现状和发展趋势。

自从 1986 年美国 Digital 公司在 Internet 上安装了全球第一个商用防火墙系统以来，它们就提出了防火墙的概念，防火墙技术得到了飞速的发展。第二代防火墙也称为代理服务器，它用来提供网络服务级的控制，起到外部网络向被保护的内部网络申请服务时中间转接的作用，这种方法可以有效地防止对内部网络的直接攻击，安全性较高。第三代防火墙有效地提高了防火墙的安全性，称为状态监控功能防火墙，它可以对每一层的数据包进行检测和监控。随着网络攻击手段和信息安全技术的发展，新一代的功能更强大、安全性更强的防火墙已经问世，这个阶段的防火墙已超出了原来传统意义上防火墙的范畴，已经演变成一个全方位的安全技术集成系统，被称之为第四代防火墙，它可以抵御目前常见的网络攻击手段，如 IP 地址欺骗、特洛伊木马攻击、Internet 蠕虫、口令探寻攻击、邮件攻击等。

在目前采用的网络安全的防范体系中，防火墙占据着举足轻重的地位，因此市场对防火墙的设备需求和技术要求都在不断提升。

防火墙的发展趋势如下。

（1）高速化。目前防火墙一个很大的局限性是速度不够。应用 ASIC、FPGA 和网络处理器是实现高速防火墙的主要方法，其中以采用网络处理器最优。实现高速防火墙，算法也是一个关键，因为网络处理器中集成了很多硬件协处理单元，因此比较容易实现高速。对于采用纯 CPU 的防火墙，就必须有算法支撑，如 ACL 算法。

（2）多功能化。多功能也是防火墙的发展方向之一，鉴于目前路由器和防火墙价格都比较高，组网环境也越来越复杂，一般用户总希望防火墙可以支持更多的功能，以满足组网和节省投资的需要。

（3）更安全化。未来防火墙的操作系统会更安全。随着算法和芯片技术的发展，防火墙会更多

地参与应用层分析，为应用提供更安全的保障。

1.3.8 入侵检测技术

随着网络应用范围的不断扩大，对网络的各类攻击与侵害也与日俱增。无论政府、商务，还是金融、媒体的网站都在不同的程度上受到了入侵与侵害。网络安全已成为国家与国防安全的重要组成部分，同时也是国家网络经济发展的关键。据统计，信息窃贼在过去 5 年中以 250%的速度增长，99%的大公司发生过较大的入侵事件。世界著名的商业网站，如 Yahoo、Buy、EBay、Amazon、CNN 都曾被黑客入侵，造成巨大的经济损失，甚至连专门从事网络安全的 RSA 网站也受到了黑客的攻击。

入侵是指任何企图危及资源的完整性、机密性和可用性的活动。入侵检测（Intrusion Detection），顾名思义，就是对入侵行为的发觉，它通过对计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统所采用的技术可分为特征检测与异常检测两种。

特征检测又称为 Misuse Detection，这种检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。其难点在于如何设计模式既能够表达“ 入侵 ”现象又不会将正常的活动包含进来。

异常检测的假设是入侵者活动异常于正常主体的活动。根据这个理念建立主体正常活动的“ 活动简档 ”，将当前主体的活动状况与“ 活动简档 ”相比，当违反其统计规律时，认为该活动可能是“ 入侵 ”行为。异常检测的难题在于如何建立“ 活动简档 ”以及如何设计统计算法，从而不把正常的操作作为“ 入侵 ”或忽略真正的“ 入侵 ”行为。

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。特征检测是对已知的攻击或入侵的方式做出确定性的描述，形成相应的事件模式。统计模型常用异常检测，在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。用专家系统对入侵进行检测，经常是针对有特征的入侵行为。据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中 95%属于使用入侵模板进行模式匹配的特征检测产品，其他是采用概率统计的统计检测产品与基于日志的专家知识库系统产品。

经过几年的发展，入侵检测产品开始步入快速的成长期。一个入侵检测产品通常由两部分组成：传感器与控制台。传感器负责采集数据（网络包、系统日志等）、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持 Windows NT 平台。从技术上看，这些产品基本上分为以下几类：基于网络的产品和基于主机的产品。混合的入侵检测系统可以弥补一些基于网络与基于主机的片面性缺陷。此外，文件的完整性检查工具也可看作一类入侵检测产品。

随着科学技术的发展，入侵的手段与技术也有了飞速的发展，如入侵的综合化、分布化和主体间接化，入侵攻击的规模夸大、攻击对象的转移等都对入侵检测技术提出了更高的要求。今后，入侵检测技术要朝智能化、分布化等方向发展。入侵检测技术的智能化：所谓的智能化就是利用现阶段常用的神经网络、模糊技术、遗传算法等方法，加强入侵检测的辨识能力。如现有的专家系统，特别是具有自学习能力的专家系统，实现了知识库的不断更新与扩展，使设计的入侵检测系统的防范能力不断增强，具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也已有报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。

分布式入侵检测技术：它是针对分布式网络攻击的检测方法，通过收集、合并来自多个主机的审计数据和检查网络通信，能够检测出多个主机发起的协同攻击。全面的安全防御方案：使用