第5章 计算机信息安全

本章学习目标

- 掌握信息安全的定义。
- 理解数据加密、数字签名、数字证书的概念。
- 了解防火墙的概念。
- 熟悉计算机病毒的预防和消除。

21世纪是信息技术快速发展的一个世纪，随着Internet在全世界日益普及，人类已经进入信息化社会。计算机与网络技术为信息的获取和使用提供了越来越先进的手段，同时也为好奇者和入侵者打开了方便之门，于是信息安全问题也越来越受关注。目前的网络和信息传播途径中蛰伏着诸多不安全因素，信息文明还面临着诸多威胁和风险。个人担心隐私泄露，企业和组织担心商业秘密被窃取或重要数据被盗，政府部门担心国家机密信息泄露。信息系统的安全性不仅关系到金融、商业、政府部门的正常运作，更关系到军事和国家的安全。信息安全已成为国家、政府、部门、组织、个人都必须重视的问题。

5.1 信息安全的概述

信息安全是指信息系统的硬件、软件和数据不因为偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行、信息服务不中断。信息安全的本质和目的就是保护合法用户使用系统资源和访问系统中存储的信息的权利和利益，保护用户的隐私。

5.1.1 信息安全的定义

从技术角度看，计算机信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种学科的边缘性综合学科。

当前常见的有关计算机系统安全的称谓有：信息安全、信息系统安全、网络安全、网络信息安全、网络系统安全、网络信息系统安全、信息网络安全、信息网络系统安全、计算机安全、计算机信息系统安全等。这些称谓从字面上看，有的差别不大，有的相去甚远。所有这些称谓都是指确保在计算机网络环境下信息系统的安全运行以及信息系统中所存储、传输和处理的信息的安全保护，或者简单地描述为系统安全运行和信息安全保护。

信息安全包括两个方面，一方面是信息本身的安全，即在信息传输过程中是否有人把信息截获，尤其是重要文件的截获，造成泄密，此方面偏重于静态信息保护。另一方面是信息

系统或网络系统本身的安全,一些人出于恶意或好奇进入系统使系统瘫痪,或者在网上传播病毒,此方面着重于动态意义描述。

事实上,信息及信息系统的安全与人、应用及相关计算环境是紧密相关的,不同场合对信息的安全有不同的需求。例如,电子合同的签署要求具有不可抵赖性,而电子货币的安全又要求不可追踪性,这两者是截然相反的要求。又如,有人可能认为把文件放到公共目录服务器上是最安全的,而另外一些人则可能认为将文件保存到自己的计算机上并使用口令保护才是安全的,这种人们在特定应用环境下对信息安全的要求叫做安全策略。

综上分析,信息安全可以定义为:信息安全是研究特定应用环境下,依据特定的安全策略,对信息及信息系统实施防护、检测和恢复的科学。

5.1.2 信息安全的要素

计算机信息安全包括物理安全、运行安全、数据安全、内容安全4个方面。

1. 物理安全

物理安全主要是指因为主机、计算机网络的硬件设备、各种通信线路和信息存储设备等物理介质造成的信息泄露、丢失或服务中断等不安全因素,主要涉及网络与信息系统的机密性、可用性、完整性、生存性、稳定性、可靠性等基本属性。

它所面对的威胁主要包括电源故障、通信干扰、信号注入、人为破坏、自然灾害、设备故障等,主要的保护方式有加扰处理、电磁屏蔽、数据检验、容错、冗余、系统备份等。

2. 运行安全

运行安全是指对网络与信息系统的运行过程和运行状态的保护,主要涉及网络与信息系统的真实性、可控性、可用性、合法性、唯一性、可追溯性、占有性、生存性、稳定性、可靠性等。

它所面对的威胁包括非法使用资源、系统安全漏洞利用、网络阻塞、网络病毒、越权访问、非法控制系统、黑客攻击、拒绝服务攻击、软件质量差、系统崩溃等,主要的保护方式有防火墙与物理隔离、风险分析与漏洞扫描、应急响应、病毒防治、访问控制、安全审计、入侵检测、源路由过滤、降级使用、数据备份等。

3. 数据安全

数据安全是指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护,使得在数据处理层面保障信息依据授权使用,不被非法冒充、窃取、篡改、抵赖。数据安全主要涉及信息的机密性、真实性、实用性、完整性、唯一性、不可否认性、生存性等。

它所面对的威胁包括窃取、伪造、密钥截获、篡改、冒充、抵赖、攻击密钥等,主要的保护方式有加密、认证、非对称密钥、完整性验证、鉴别、数字签名、秘密共享等。

4. 内容安全

内容安全是指对信息在网络内流动中的选择性阻断,以保证信息流动的可控能力。在此,被阻断的对象可以是通过内容能够判断出来的会对系统造成威胁的脚本病毒、因无限制

扩散而导致消耗用户资源的垃圾类邮件、导致社会不稳定的有害信息等。内容安全主要涉及信息的机密性、真实性、可控性、可用性、完整性、可靠性等。

它所面对的难题包括信息不可识别(因加密)、信息不可更改、信息不可阻断、信息不可替换、信息不可选择、系统不可控等,主要的处置手段是密文解析或形态解析、流动信息的裁剪、信息的阻断、信息的替换、信息的过滤、系统的控制等。

5.2　信息安全基础

随着网络的普及与发展,人们十分关心在网络上交换信息的安全性,普遍认为密码技术是解决信息安全保护的一个最有效的方法。事实上,现在网络上应用的保护信息安全的技术(如数据加密技术、数字签名技术、消息认证与身份识别技术、防火墙技术以及反病毒技术)都是以密码技术为基础的。电子商务中应用的各种支付系统(如智能卡)也是基于密码技术来设计的,可以说密码技术是信息安全技术的基础,加密、数字签名、认证等都与密码技术有密切的关系。

5.2.1　数据加密

数据加密技术是为了提高信息系统及数据的安全性和保密性,防止秘密数据被外部破坏所采用的主要技术之一。数据加密的基本思想就是伪装信息,使非法接入者无法理解信息的真正含义。借助加密手段,信息以密文的方式归档存储在计算机中,或通过网络进行传输,即使发生非法截获数据或数据泄露事件,非授权用户也不能理解数据的真正含义。

1. 加密与解密的概念

用某种方法伪装消息以隐藏它的内容的过程称为加密,经过加密的消息称为密文,而密文转变为明文的过程称为解密,如图 5.1 所示。

图 5.1　数据加密、解密过程

数据加密技术的术语:

(1) 明文:需要传输的原文。

(2) 密文:对原文加密后的信息。

(3) 加密算法:将明文加密为密文的变换方法。

(4) 解密算法:将密文解密为明文的变换方法。

(5) 密钥:控制加密结果的数字或字符串。

发送方用加密密钥,通过加密设备或算法,将信息加密后发送出去。接收方在收到密文后,用解密密钥将密文解密,恢复为明文。如果传输中有人窃取,他只能得到无法理解的密文,从而对信息起到保密作用。

2. 现代密码体制

密码体制是指实现加密和解密功能的密码方案,从密钥使用策略上,可分为对称密码体制(Symmetric Key Cryptosystem)和非对称密码体制(Asymmetric Key Cryptosystem)两种。

1) 对称加密算法

对称算法有时又叫传统密码算法,就是加密密钥能够从解密密钥中推算出来,反过来也成立。在对称加密技术中,文件的加密和解密使用的是同一密钥。这些算法也叫秘密密钥算法或单密钥算法,它要求发送者和接收者在安全通信之前,商定一个密钥。对称算法的安全性依赖于密钥,泄漏密钥就意味着任何人都能对消息进行加密/解密。

对称密码算法有两种类型:分组密码(Block Cipher)和流密码(Stream Cipher,或称序列密码)。分组密码一次处理一个输入块,每个输入块生成一个输出块。流密码对单个输入元素进行连续处理,同时产生连续单个输出元素。分组密码将明文消息划分成固定长度的分组,各分组分别在密钥的控制下变换成等长度的密文分组。分组密码的工作原理如图 5.2 所示。

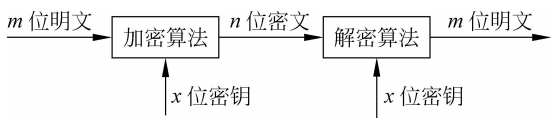

图 5.2 对称密钥加、解密过程

2) 非对称加密算法

非对称算法的设计原理为:用作加密的密钥不同于用作解密的密钥,而且解密密钥不能根据加密密钥计算出来(至少在合理假定的有限时间内)。非对称算法也叫做公开密钥算法,是因为加密密钥能够公开,即陌生者能用加密密钥加密信息,但只有用相应的解密密钥才能解密信息。在这些系统中,加密密钥叫做公开密钥,解密密钥叫做私有密钥。

公开密钥和私有密钥是成对出现的,使用公开密钥加密的数据,只有使用对应的私有密钥才能解密;使用私有密钥加密的数据,只有使用对应的公开密钥才能解密。

5.2.2 数字签名

数字签名的概念最早是在 1976 年由美国斯坦福大学的 W. Diffie 和 M. Hellman 提出的,其目的是使签名者对文件进行签署且无法否认该签名,而签名的验证者无法篡改已被签名的文件。1978 年,麻省理工学院 Rivest、Shamir 和 Adleman 给出了数字签名的具体应用方案。

数字签名(Digital Signature)是在数字文档上进行的身份认证技术,类似于纸张上的手写签名,是无法伪造的。它利用数据加密技术,按照某种协议来产生一个反映被签署文件的特征和签署人特征,以保证文件的真实性和有效性的数字技术。另外,利用数字签名,也可核实接收者是否有伪造、篡改数字文件的行为。

1. 数字签名的作用

1）信息传输的保密性

交易中的商务信息均有保密的要求。如果信用卡的账号和用户名被别人获悉，就可能被盗用；订货和付款的信息被竞争对手获悉，就可能丧失商机，因此在电子商务的信息传播中一般都有加密的要求。

2）交易者身份的可鉴别性

网上交易的双方很可能素昧平生，相隔千里。对于商家要确认客户端不是骗子，而客户也要相信网上的商店不是一个玩弄欺诈的黑店，因此能方便而可靠地确认对方的身份是网上交易的前提。为顾客或用户开展服务的银行、信用卡公司和销售商店，为了做到安全、保密、可靠地开展服务活动，都需要进行身份认证工作。对有关的销售商店来说，他们不知道顾客的信用卡号码，只能把信用卡的确认工作完全交给银行来完成。银行和信用卡公司可以采用各种保密与识别方法来确认顾客的身份是否合法、确认订货和订货收据信息，同时还要注意防止发生拒付款等问题。

3）数据交换的完整性

交易的文件是不能被修改的。例如订购黄金，供货方在收到订单后，发现金价大幅上涨了，如果他能改动订单内容，将订购数 1 吨改为 1 克，则可大幅受益，而订货方就会因此而蒙受损失。因此电子交易文件也要做到不可修改，以保障交易的严肃性和公正性。

4）发送信息的不可否认性

由于商情的千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益。例如订购黄金，订货时金价较低，但收到订单后，金价上涨了，如果供货方能否认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。因此电子交易通信过程的各个环节都必须是不可否认的。

5）信息传递的不可重放性

在数字签名中，如果采用了对签名报文添加流水号、时戳等技术，可以防止重放攻击。例如在日常生活中，A 向 B 借了钱，同时写了一张借条给 B；当 A 还钱的时候，肯定要向 B 索回他写的借条并撕毁，不然，恐怕他会再次挟借条要求 A 还钱。

2. 数字签名的用途

在网络应用中，数字签名比手工签字更具优越性，数字签名是进行身份鉴别与网上安全交易的通用实施技术。当然，网络环境还有很多其他威胁，要由其他专门技术解决，如防火墙技术、反病毒技术、入侵检测技术等。在网络应用中，凡是要解决伪造、抵赖、冒充、篡改与身份鉴别的问题，都可运用数字签名来处理。

数字签名的设计目标：

（1）签名的比特模式依赖于消息报文；

（2）数字签名对发送者来说是唯一的，能够防止伪造和抵赖；

（3）产生数字签名的算法必须相对简单、易于实现，且能够在存储介质上备份；

（4）对数字签名的识别、证实和鉴别也必须相对简单，易于实现；

（5）无论攻击者采用何种手法，伪造数字签名在计算上是不可行的。

5.2.3 数字证书

数字证书如同我们日常生活中使用的身份证,它是持有者在网络上证明自己身份的凭证。在一个电子商务系统中,所有参与活动的实体都必须用证书来表明自己的身份。

1. 数字证书的定义

证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。证书一方面可以用来向系统中的其他实体证明自己的身份,另一方面由于每份证书都携带着证书持有者的公钥,所以证书也可以向接收者证实某人或某个机构对公开密钥的拥有,同时也起着公钥分发的作用。

数字证书采用公钥体制,即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所有的私有密钥(私钥),用它进行解密和签名;同时设定一把公共密钥(公钥)并由本人公开,为一组用户所共享,用于加密和验证签名。

当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,这样信息就可以安全无误地到达目的地了。通过数字手段保证加密过程是一个不可逆过程,即只有用私有密钥才能解密。公开密钥技术解决了密钥发布的管理问题,用户可以公开其公开密钥,而保留其私有密钥。

2. 常用的数字证书

数字证书必须具有唯一性和可靠性。为了达到这一目的,需要采用很多技术来实现。常用的数字证书有如下几种。

1) SPKI(Simple Public Key Infrastructure)

SPKI 是由 IETF SPKI 工作组指定的一系列技术和参考文档,包括 SPKI 证书格式。SPKI 证书又叫授权证书,主要目的是传递许可权。目前只有很少的 SPKI 证书应用需求,而且缺乏市场需求。

2) PGP(Pretty Good Privacy)

PGP 是一种对电子邮件和文件进行加密与数字签名的方法。它规范了在两个实体间传递信息、文件和 PGP 密钥时的报文格式。

PGP 证书与 X.509 证书之间存在着显著不同,它的信任策略主要是基于个人而不是企业。因此,虽然在 Internet 上的电子邮件通信中得到了一定范围内的应用,但对企业内部网来说,却不是最好的解决方案。

3) SET (Secure Electronic Transaction)

SET 安全电子交易(SET)标准定义了在分布式网络上进行信用卡支付交易所需的标准。它采用了 X.509 第三版公钥证书的格式,并指定了自己私有的扩展。非 SET 应用无法识别 SET 定义的私有扩展,因此非 SET 应用无法接受 SET 证书。

4) 属性证书

属性证书是用来传递一个给定主体的属性以便于灵活、可扩展的特权管理。属性证书不是公钥证书,但它的主体可以结合相应公钥证书通过“指针”来确定。

3. 数字证书的验证

数字证书的验证，是验证一个证书的有效性、完整性、可用性的过程。证书验证主要包括以下5方面的内容。

(1) 验证证书签名是否正确有效，这需要知道签发证书的CA的公钥。

(2) 验证证书的完整性，即验证CA签名的证书散列值与单独计算的散列值是否一致。

(3) 验证证书是否在有效期内。

(4) 查看证书撤销列表，验证证书没有被撤销。

(5) 验证证书的使用方式与任何生命的策略及使用限制一致。

数字证书的用途很广泛，它可以用于方便快捷安全地发送电子邮件、访问安全站点、网上招标投标、网上签约、网上订购、网上公文的安全传送、网上办公、网上缴费、网上缴税、网上购物等安全电子事务处理和安全电子交易活动。

5.3　计算机病毒的防治

计算机病毒(Computer Viruses)是一种人为蓄意制造的，以破坏为目的的程序。从1984年第一个病毒“小球”诞生以来，计算机病毒不断翻新。计算机病毒防治工作的基本任务是在计算机的使用管理中，利用各种行政和技术手段，防止计算机病毒的入侵、存留、蔓延。

5.3.1　计算机病毒的概念

“病毒”一词来源于生物学。计算机病毒最早是由美国加州大学的Fred Cohen提出的。他在1983年编写了一个小程序，这个程序可以自我复制，能在计算机中传播。该程序对计算机并无害处，能潜伏于合法的程序当中，传染到计算机上。

计算机病毒有很多种定义，国外最流行的定义为：计算机病毒是一段附着在其他程序上的、可以实现自我繁殖的程序代码。在《中华人民共和国计算机信息系统安全保护条例》中的定义是：“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数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。从广义上说，凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。

计算机病毒寄生于其他应用程序或系统的可执行部分，通过非法入侵而隐藏在可执行程序或数据文件中。当计算机运行时，它可以把自身精确复制或有修改地复制到其他程序体内，从而破坏用户的系统及数据文件，占用系统资源，具有相当大的破坏性。

5.3.2　计算机病毒的特点与分类

目前，计算机病毒到底有多少，各种说法不一。但不管怎样，计算机病毒的数量确实在不断地增加，而且它们种类不一，感染目标和破坏行为也不尽相同。对计算机病毒进行分类、研究计算机病毒的特点是为了更好地了解计算机病毒，找到防治方法，使计算机免遭病毒的侵害。

1. 计算机病毒特点

计算机病毒是一段特殊的程序,除了与其他程序一样,可以存储和运行外,计算机病毒还有寄生性、传染性、潜伏性、隐藏性、破坏性等特征。

1) 寄生性

计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

2) 传染性

计算机病毒不但本身具有破坏性,更有害的是具有传染性,一旦病毒被复制或产生变种,其速度之快令人难以预防。传染性是病毒的基本特征。

3) 潜伏性

有些病毒像定时炸弹一样,让它什么时间发作是预先设计好的。例如“黑色星期五”病毒,不到预定时间一点都觉察不出来,等到条件具备的时候一下子就爆炸开来,对系统进行破坏。

4) 隐藏性

计算机病毒具有很强的隐藏性,有的可以通过病毒软件检查出来,有的根本就查不出来,有的时隐时现、变化无常,这类病毒处理起来通常很困难。

5) 破坏性

计算机中毒后,可能会导致正常的程序无法运行,把计算机内的文件删除或受到不同程度的损坏。通常表现为增加、删减、改变、移动。

2. 病毒类型

按照计算机病毒的诸多特点及特性,其分类方法有很多种,所以同一病毒按照不同的分类方法可能被分到许多不同的类别中。公认的分类方法如下。

1) 按照病毒寄生方式分类

(1) 引导型病毒

引导型病毒是一类专门感染硬盘主引导扇区和软盘引导扇区的病毒。引导型病毒隐藏得很隐蔽,不以文件的形式存在,不能用类似 Del 这样的命令来删除。引导型病毒一般分为主引导区病毒和引导区病毒。

常见的主引导型病毒有“石头病毒”、“INT60 病毒”等;常见的引导区病毒有“小球病毒”和“Brain 病毒”等。

(2) 文件型病毒

文件型病毒主要是干扰可执行文件(如 Windows 系统中的 exe 文件和 dll 文件等),被感染的可执行文件在执行的同时,病毒被加载并执行其传播和破坏操作。

(3) 混合型病毒

混合型病毒,顾名思义就是既能感染引导区,又能感染文件的病毒。此类病毒不是文件型病毒和引导型病毒的简单相加,它通过引导型病毒的方法驻留内存,然后修改 INT8、监视 INT21 的地址是否改变。如果地址改变,则说明 DOS 系统已经加载,这样就可以通过修改 INT21 从而运行病毒。混合型病毒的目的是为了综合利用多种传染渠道进行传染和破

坏，如木马、蠕虫、后门等都是混合型病毒。

(4) 变形病毒

病毒传染到目标后，病毒自身代码和结构在空间上、时间上具有不同的变化。这一类病毒使用一个复杂的算法，使自身每传播一份都具有不同的内容和长度。它们一般是由一段混有无关指令的解码算法和被改变过的病毒体组成的。

(5) 宏病毒

它是利用高级语言——宏语言编制的病毒，与前几种病毒存在很大的区别。宏病毒充分利用宏命令的强大系统调用功能，实现某些涉及系统底层操作的破坏。宏病毒仅向Word、Excel、Access 和 PowerPoint 等办公自动化程序编制的文档进行传染，而不会传染给可执行文件。

2) 按照计算机病毒的破坏情况分类

(1) 良性计算机病毒

良性病毒是指不包含对计算机系统产生直接破坏作用代码的计算机病毒。这类病毒为了表现其存在，只是不停地进行传播，并不破坏计算机内的数据。但它使系统资源急剧减少，可用空间越来越少，最终导致系统崩溃。

良性病毒又可分为无危害病毒和无危险病毒。前者是指除了传染时减少磁盘的可用空间外，对系统没有其他影响。后者是指在传播过程中不仅减少内存和硬盘空间，还伴随显示图像、发出声音等。

(2) 恶性计算机病毒

恶性病毒是指包含损伤和破坏计算机系统的操作，在其传染激发时会对系统产生直接破坏作用的计算机病毒。例如破坏磁盘扇区，格式化磁盘导致数据丢失等。这些代码都是刻意写进病毒的，是其本性之一。

恶意病毒可分为危险型病毒和非常危险型病毒。危险型病毒是指破坏和干扰计算机系统的操作，从而造成严重的错误。非常危险型病毒主要是删除程序、破坏数据、清除系统内存和操作系统中重要的信息。

3) 按照传播媒介分类

(1) 单机病毒

单机病毒的载体是磁盘或光盘。常见的传播途径是通过软盘或光盘传入硬盘，感染系统后，再传染给其他系统。

(2) 网络病毒

网络病毒的传播媒介是网络。当前，因特网在世界上迅速发展，上网已成为计算机使用者的时尚，随着网上用户的增加，网络病毒的传播速度更快、范围更广、造成的危害更大。网络病毒往往造成网络堵塞，修改网页，甚至与其他病毒结合修改或破坏文件。

4) 按计算机病毒的链接方式分类

(1) 源码型病毒

该病毒攻击高级语言编写的程序，在高级语言所编写的程序编译前插入到源程序中，经编译成为合法程序的一部分。

(2) 嵌入型病毒

这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插

入的方式链接。这种计算机病毒是难以编写的,一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术,将给当前的反病毒技术带来严峻的挑战。

(3) 外壳型病毒

外壳型病毒将其自身包围在主程序的外面,对原来的程序不做修改,这种病毒最为常见,易于编写,也易于发现,一般测试文件的大小即可察觉。

(4) 译码型病毒

译码型病毒隐藏在微软 Office、AmiPro 文档中,如宏病毒、脚本病毒等。

(5) 操作系统型病毒

这种病毒用自身的程序加入或取代部分操作系统进行工作,具有很强的破坏力,可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

5) 按病毒攻击的操作系统分类

(1) DOS 病毒

DOS 病毒是针对 DOS 操作系统开发的病毒。目前几乎没有新制作的 DOS 病毒,由于 Windows 9x 病毒的出现,DOS 病毒几乎绝迹。但 DOS 病毒在 Windows 9x 环境中仍可以进行感染活动,因此若执行染毒文件,Windows 9x 用户的系统也会被感染。通常使用杀毒软件能够查杀的病毒中一半以上都属于 DOS 病毒,可见 DOS 时代病毒的泛滥程度。但这些众多的病毒中除了少数几个让用户胆战心惊的病毒之外,大部分病毒都只是制作者出于好奇或对公开代码进行一定变形而制作的病毒。

(2) Windows 病毒

Windows 病毒主要指针对 Windows 9x 操作系统的病毒。现在的计算机用户一般都安装 Windows 系统,Windows 病毒一般感染 Windows 9x 系统,其中最典型的病毒有 CIH 病毒。但这并不意味着可以忽略操作系统是 Windows NT 系列的计算机。一些 Windows 病毒不仅在 Windows 9x 上能感染,还可以感染 Windows NT 上的其他文件。

(3) 其他系统病毒

对于攻击 Linux、UNIX、OS2、Macintosh 及嵌入式系统的病毒,由于系统本身的复杂性,这类病毒数量不是很多,但对于当前的信息处理也产生了严重的威胁。

5.3.3 计算机病毒的防范

计算机病毒防范,是指通过建立合理的计算机病毒防范体系和制度。对于计算机病毒,需要树立以防为主,清除为辅的观念,防患于未然。防范计算机病毒的关键是做好预防工作,发现计算机病毒入侵,及时采取有效的手段阻止计算机病毒的传播和破坏。其主要工作包括预防、检测和清除等。

1. 计算机病毒的预防

计算机病毒的传染是通过一定途径实现的,为此要以预防为主,制订出一系列的安全措施,堵塞计算机病毒的传染途径,降低病毒的传染几率。而且即使受到传染,也可以立即采取有效措施将病毒消除,使病毒造成的危害降低到最低限度。对用户来说,抗病毒最有效的方法是备份,抗病毒最有效的手段是病毒库升级要快。

1）从管理上预防病毒

从管理上预防病毒、控制病毒的入侵，主要从以下几个方面进行：

（1）机器要有专人负责管理。

（2）尽量不要用软盘、U盘、移动硬盘或其他移动存储设备启动计算机，而用本地硬盘启动。同时尽量避免在无防毒措施的计算机上使用可移动存储设备。

（3）对所有系统软盘、工具软盘、程序软盘要进行写保护。

（4）对于外来的机器和软件要进行病毒检测。

（5）不使用来历不明的软件，也不要使用非法解密或复制的软件。

（6）谨慎地使用公用软件和共享软件。

（7）对游戏程序要严格控制。

（8）定期检测磁盘上的系统区和文件并及时消除病毒。

（9）系统中的数据盘和系统盘要定期进行备份，数据备份是保证数据安全的重要手段，可以通过比照文件大小、检查文件个数、核对文件名来及时发现病毒，也可以在文件损失后尽快恢复。

（10）网络上的计算机用户，要遵守网络的使用规定，不能随意在网络上使用外来软件。

2）从技术上预防病毒

前面讲述的管理措施能够在一定程度上预防和抑制计算机病毒的传播，但它是以牺牲数据共享的灵活性而换得的系统安全，这会给使用者带来一定程度的不便。因而要形成一种在管理方法、技术措施及安全性上都合理的折中方案，达到计算机系统资源的相对安全和充分共享，而且不影响计算机的运行效率。在技术手段上对病毒的预防有硬件保护和软件预防两种方法。

任何计算机病毒对系统的入侵都是利用内存提供的自由空间及操作系统所提供的相应的中断功能来达到传染目的的。因此，可以通过增加硬件设备来保护系统，此硬件设备既能监视内存中的常驻程序，又能阻止对外存储器异常的写操作，这样就能实现对计算机病毒预防的目的。目前，普遍使用的防病毒卡就是一种硬件保护手段，将它插在主板的I/O插槽上，在系统的整个运行过程中密切监视系统的异常状态。

防病毒的另一种方法是使用计算机病毒疫苗来进行软件预防。计算机病毒疫苗是一种能够监视系统运行，并在发现某些病毒入侵时防止或禁止病毒入侵，当发现非法操作时及时警告用户或直接拒绝这种操作的不具备传染性的可执行程序。

2. 计算机病毒的检测

计算机病毒的检测通常采用手工检测和自动检测两种方法。

1）手工检测

手工检测是指通过一些软件工具（DEBUG、PCTOOLS、NU等）提供的功能进行病毒的检测。这种方法比较复杂，需要检测者熟知机器指令和操作系统，因而无法普及。它的基本过程是利用工具软件，对易遭病毒攻击和修改的内存及磁盘的有关部分进行检查，通过与在正常情况下的状态进行对比分析，判断是否被病毒感染。用这种方法检测病毒，费时费力，但可以检测识别未知病毒，以及检测一些自动检测工具不能识别的新病毒。

2) 自动检测

自动检测是指通过病毒诊断软件来识别一个系统是否含有病毒的方法。自动检测相对比较简单,一般用户都可以进行。这种方法可以方便地检测大量的病毒,但是,自动检测工具只能识别已知病毒,对未知病毒不能识别。

两种方法比较而言,手工检测方法操作难度大、技术复杂,它需要操作人员有一定的软件分析经验以及对操作系统有较深入的了解。自动检测方法操作简单、使用方便,适合于一般的计算机用户使用。但是,由于计算机病毒的种类较多,再加上不断出现病毒变种,所以自动检测方法不可能检测所有未知的病毒,这时只能用手工方法进行病毒的检测。其实,自动检测也是在手工检测成功的基础上把手工检测方法程序化后得到的。因此,手工检测病毒是最基本和最有力的工具。

3. 计算机病毒的清除

1) 清除病毒的原理

清除计算机病毒要建立在正确检测病毒的基础之上。清除病毒主要应做好以下工作:

(1) 清除内存中的病毒。

(2) 清除磁盘中的病毒。

(3) 病毒发作后的善后处理。

2) 清除病毒的方法

由于计算机病毒不仅干扰受感染的计算机的正常工作,更严重的是继续传播病毒、泄密和干扰网络的正常运行。因此,如果发现计算机被病毒感染了,则应立即清除掉。通常用人工处理或反病毒软件两种方式进行清除。

(1) 人工清除法

人工处理的方法有用正常的文件覆盖被病毒感染的文件;删除被病毒感染的文件;重新格式化磁盘,但这种方法有一定的危险性,容易造成对文件数据的破坏。还可以借助工具软件打开被感染的文件,从中找到并摘除病毒代码,使文件复原。这种方法是专业防病毒研究人员用于清除新病毒时采用的,不适合一般用户。

(2) 杀毒软件清除法

反病毒软件是专门用于对病毒防堵、清除的工具。采用反病毒软件清除法对病毒进行清除是一种较好的方法。这种方法对于大多数计算机用户来说是首要选择,用户只需按照杀毒软件的菜单或联机帮助操作即可轻松杀毒。该方法适合于查杀已知的计算机病毒,并且要求用户对杀毒软件的病毒库进行及时更新、升级。这些反病毒软件操作简单、行之有效,但对某些病毒的变种不能清除,需使用专门的反病毒软件进行清除。

目前,国内外有很多杀毒软件,比较流行的有 360 杀毒、小红伞、卡巴斯基、Avast、瑞星、NOD32、诺顿、金山、江民、McAfee。由于目前的杀毒软件都具有病毒防范和拦截功能,能够以快于病毒传播的速度发现、分析并部署拦截,因此安装杀毒软件是最有效的防范病毒感染的方法。

5.4　防火墙技术

随着因特网的发展，网络的安全越来越成为网络建设中的关键技术，企业级组织为确保内部网络及系统的安全，均设置不同层次的信息安全解决机制，而防火墙（Firewall）就是各企业及组织在设置信息安全解决方案中最常被优先考虑的安全控管机制。

5.4.1　防火墙的定义

防火墙一词来源于早期的欧式建筑，它是建筑物之间的一道矮墙，用来防止发生火灾时火势的蔓延。在计算机网络中，防火墙通过对数据包的筛选和屏蔽，可以防止非法的访问进入内部或外部计算机网络。

1. 防火墙的概念

防火墙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重要信息从企业的网络上被非法输出。我国公安安全行业标准中对防火墙的定义为："设置在两个或多个网络之间的安全阻隔，用于保证本地网络资源的安全，通常是包含软件部分和硬件部分的一个系统或多个系统的组合。"

防火墙作为网络防护的第一道防线，它由软件和硬件设备组合而成，它位于企业或网络群体计算机与外界网络的边界，限制着外界用户对内部网络的访问以及管理内部用户访问外界网络的权限。

防火墙是一种必不可少的安全增强点，它将不可信任网络同可信任网络隔离开，如图 5.3 所示。防火墙筛选两个网络间所有的连接，决定哪些传输应该被允许，而哪些应该被禁止。

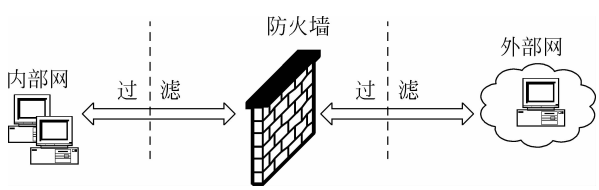

图 5.3　防火墙示意图

2. 防火墙的特性

防火墙是放置在两个网络之间的一些组件，防火墙一般有以下三个特性：

（1）所有的通信都经过防火墙。

（2）防火墙只放行经过授权的网络流量。

（3）防火墙能经受得住对其本身的攻击。

防火墙主要提供以下 4 种服务。

（1）服务控制：确定可以访问的网络服务类型。

(2) 方向控制：特定服务的方向流控制。

(3) 用户控制：内部用户、外部用户所需的某种形式的认证机制。

(4) 行为控制：控制如何使用某种特定的服务。

5.4.2 防火墙的分类

防火墙的分类方法很多，可以分别从采用的防火墙技术、软/硬件形式、性能以及部署位置等标准来划分。

1. 按防火墙软硬件形式分类

1) 软件防火墙

软件防火墙运行于特定的机器上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关，俗称“个人防火墙”。软件防火墙就像其他的软件产品一样，需要先在计算机上安装并配置才可以使用。

2) 硬件防火墙

这里说的硬件防火墙是指所谓的硬件防火墙，之所以加上“所谓”二字是针对芯片级防火墙说的，它们最大的差别在于是否基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙。它们都基于 PC 架构，也就是说，它们和普通家用的 PC 没有太大区别。

3) 芯片级防火墙

芯片级防火墙基于专门的硬件平台，没有操作系统。专有的 ASIC 芯片促使它们比其他种类的防火墙速度更快、处理能力更强、性能更高。厂商有 NetScreen、FortiNet 和 Cisco 等。这类防火墙由于是专用 OS(操作系统)，因此防火墙本身的漏洞比较少，不过价格相对比较昂贵。

2. 按防火墙技术分类

1) 包过滤(Packing Filtering)型防火墙

包过滤防火墙是工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则从数据流中被丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采用特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是路由器集成的；之所以有效，是因为它能在很大程度上满足绝大多数企业的安全要求。

2) 应用代理(Application Proxy)型防火墙

应用代理型防火墙工作在 OSI 参考模型的最高层，即应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

应用代理型防火墙的最突出的优点就是安全。由于它工作在最高层，因此它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过

滤。应用代理型防火墙的最大缺点就是速度相对比较慢，当用户对内、外部网络网关的吞吐量要求比较高时，代理防火墙就会成为内、外部网络之间的瓶颈。

3. 按防火墙结构分类

按防火墙结构分类，防火墙主要分为单一主机防火墙、路由器集成式防火墙和分布式防火墙三种。

1）单一主机防火墙

单一主机防火墙是最为传统的防火墙，独立于其他网络设备，它位于网络边界。这种防火墙其实与一台计算机结构类似，包括 CPU、内存、硬盘、主板等基本组件，且主板上也有南、北桥芯片。它与普通计算机最主要的区别就是一般防火墙都集成了两个以上的以太网卡，因为它需要连接一个以上的内、外部网络。

2）路由器集成式防火墙

原来单一主机的防火墙由于价格非常昂贵，仅有少数大型企业才能承受得起，为了降低企业网络投资，现在许多种高档路由器中都集成了防火墙功能。例如 Cisco IOS 防火墙系列，但这种防火墙通常是较低级的包过滤型。这样，企业就不用再同时购买路由器和防火墙，大大降低了网络设备购买成本。

3）分布式防火墙

随着防火墙技术的发展及应用需求的提高，原来作为单一主机的防火墙现在已发生了许多变化。最明显的变化就是现在许多中、高档的路由器中已集成了防火墙功能，有的防火墙已不再是一个独立的硬件实体，而是由多个软、硬件组成的系统，这种防火墙俗称“分布式防火墙”。分布式防火墙不再是只位于网络边界，而是渗透于网络的每一台主机，对整个内部网络的主机实施保护。

4. 按防火墙的应用部署位置分类

如果按防火墙的应用部署位置分类，防火墙可以分为边界防火墙、个人防火墙和混合式防火墙三大类。

1）边界防火墙

边界防火墙是最为传统的防火墙类型，它们位于内、外部网络的边界，所起的作用是对内、外部网络实施隔离，保护边界内部网络。这类防火墙一般都是硬件类型的，价格较贵、性能较好。

2）个人防火墙

个人防火墙安装于单台主机中，防护的也只是单台主机。这类防火墙应用于广大的个人用户，通常为软件防火墙，价格最便宜，性能也最差。

3）混合式防火墙

混合式防火墙可以说就是“分布式防火墙”或者“嵌入式防火墙”，它是一整套防火墙系统，由若干个软、硬件系统组成，分布于内、外部网络边界和内部各主机之间，既对内、外部网络之间的通信进行过滤，又对网络内部各主机间的通信进行过滤。它属于最新的防火墙技术之一，性能最好，价格也最贵。

5. 按防火墙性能分类

如果按防火墙的性能分类,目前可以分为百兆级防火墙和千兆级防火墙两类。

5.4.3 黑客

网络发展到今天,黑客们为了相互区别自封了三顶帽子,即“黑帽子”、“白帽子”和“灰帽子”。一般来说,以入侵他人计算机系统为乐趣并进行破坏的人,被称为“黑帽子”,Cracker指的也是这种人;入侵系统进行安全研究并主动帮助别人修补漏洞的网络安全人员,被称为“白帽子”;而“灰帽子”是指那些发现系统漏洞,并在公开场合探讨这些漏洞和安全防范措施的计算机技术爱好者。

1. 黑客的定义

黑客一词源于英文 Hacker,原指热衷于计算机技术、水平高超的计算机专家,尤其是程序设计人员,也有人把他们比作“侠客”。黑客是那些检查系统完整性和安全性的人,他们非常精通计算机硬件和软件知识,并有能力通过新的方法剖析系统。黑客通常会去寻找网络中的漏洞,但是往往并不去破坏计算机系统。正是因为黑客的存在,人们才会不断了解计算机系统中存在的安全问题。

入侵者(Cracker,有人翻译成“骇客”)是那些利用网络漏洞破坏系统的人,他们往往会通过计算机系统漏洞来入侵。他们具有广泛的计算机知识,但与黑客不同的是他们以破坏为目的。真正的黑客应该是一个负责任的人,他们认为破坏计算机系统是不正当的。但是现在 Hacker 和 Cracker 已经混为一谈,人们通常将入侵计算机系统的人统称为黑客。

2. 黑客的主要行为

黑客利用漏洞来做以下几个方面的工作。

1) 获取系统信息

有些漏洞可以泄露系统信息,暴露敏感资料(如银行客户账号),黑客们利用系统信息进入系统。

2) 入侵系统

通过漏洞进入系统内部,取得服务器上的内部资料,甚至完全掌管服务器。

3) 寻找下一个目标

一个胜利意味着下一个目标的出现,黑客会充分利用自己已经掌管的服务器作为工具,寻找并入侵下一个相似的系统。

3. 黑客的预防措施

常用的黑客预防措施有如下几种:

1) 防火墙技术

使用防火墙来防止外部网络对内部网络的未经授权的访问,建立网络信息系统的对外安全屏障,以便对外部网络与内部网络交流的数据进行检测,符合的予以放行,不符合的则拒之门外。

2）安全监测与扫描工具

经常使用安全监测与扫描工具作为加强内部网络与系统的安全防护性能和抗破坏能力的主要手段，用于发现安全漏洞及薄弱环节。当网络或系统被黑客攻击时，可用该软件及时发现黑客入侵的迹象，并进行处理。

3）网络监控工具

使用有效的控制手段抓住入侵者。经常使用网络监控工具对网络和系统的运行情况进行实时监控，用于发现黑客或入侵者的不良企图及越权使用，及时进行相关处理，防患于未然。

4）备份系统

经常备份系统，以便在被攻击后能及时修复系统，将损失减少到最低程度。

5）防范意识

加强安全防范意识，有效地防止黑客的攻击。

5.5　信息安全与职业道德

由于计算机网络的开放性和方便性，人们可以轻松地从网上获取信息或者向网络发布信息，同时也很容易干扰其他网络活动和参加网络活动的其他人的生活。因此，要求网络活动的参加者具有良好的品德和高度的自律，努力维护网络资源，保护网络的信息安全，树立和培养健康的网络道德，遵守国家有关网络的法律法规。

5.5.1　信息安全的法律法规

信息系统的规划、设计、建设、使用、管理和维护等环节都是基于计算机系统、通信系统、网络系统的平台，信息安全设计的问题也必然与此相关。

1. 信息网络的规划与建设

任何一个信息系统都不是孤立的，而是相互关联的，规模宏大，极其复杂。为了克服在信息系统规划与建设中存在的各种问题，用法律法规进行规划是十分必要的。在立法时，特别关注这些问题是必要的：建立统一的组织领导机构；符合国家整体建立利益；统筹规划、统一协调；网络的标准化与开放性原则等。因此，有必要通过行政立法，强制性贯彻实施信息系统安全技术与安全管理等措施，强化信息系统安全。

2. 信息系统的运行与管理

信息系统的运行与管理受到各国政府和公众的普遍关注。充斥在网络中的有害信息，包括危害国家安全、社会安定，扰乱公共秩序，侵犯他人合法权益，破坏文化传统、伦理道德、有伤风化的信息，在社会上产生很多不良影响。因此，控制网络中的有害信息是信息系统管理与经营中的一项重要任务。

3. 数据保护

随着信息技术的发展，众多的数据被各类信息系统收集和存储，且可经由网络进行传输

和查看。因此,保护数据安全,要保证数据的安全可靠与正当使用,同时确保数据拥有者的权益不受损害,如何避免不准确或不当使用用户的数据给其造成损失也是必须考虑的问题。

4. 电子商务

电子商务是信息网络的一个新的重要应用方面。电子商务中不但涉及电子数据交换、电子资金划拨等,还包括消费者合法权益保护以及税收等。

由于网上交易时,供销双方并不见面,网上购物质量保证、售后服务、退货、退款、顾客投诉等的处理安全不同于常规交易情况。随着电子商务的开展,消费者合法权益受到损害的案件越来越多,这反映了网上交易与消费者合法权益保护相应立法的落后。

5. 计算机犯罪

随着信息系统的广泛应用,计算机犯罪成为信息社会的主要犯罪形式之一。计算机犯罪的主要表现是侵犯信息系统的各种资源,包括硬件、软件以及系统中存储和传输的数据,达到窃取钱财、信息、情报以及破坏或恶作剧等目的。因此,许多国家已经修改刑法或制定计算机犯罪的法规,以便更有力地打击计算机犯罪。

6. 计算机取证

计算机取证是一个对受侵计算机系统进行扫描和破解,以对入侵事件进行重建的过程。也就是针对计算机入侵与犯罪,进行证据获取、保存、分析和出示。从技术角度看,计算机取证是分析硬盘、光盘、zip 磁盘、U 盘、内存缓冲和其他形式的存储介质以发现犯罪证据的过程。

计算机取证在打击计算机和网络犯罪中起着十分关键的作用,它的目的是将犯罪者留在计算机中的“痕迹”作为有效的诉讼证据提供给法庭,以便将犯罪嫌疑人绳之以法。

5.5.2 计算机职业道德规范

职业道德是指为了适应各种职业要求所产生的道德规范,是指人们在从事不同的工作过程中所应遵循的行为规范和准则的总和。计算机职业作为一种特殊的职业,具有与其他职业不同的特点,所以有着与众不同的职业道德规范和行为准则。对从事计算机职业的工作人员有许多特殊的要求,每一个计算机从业人员都应该遵守这些职业道德和行为准则。

(1) 爱岗敬业、诚实守信、办事公道、服务群众、奉献社会是社会主义职业道德的基本规范,作为一名合格的职业计算机工作人员都应该遵守这些通用的职业道德和行为准则。

(2) 每一位计算机职业从业人员都应该遵守国家有关法律规定,这是计算机专业人员职业道德的最基本要求。

(3) 自觉维护计算机安全,不破坏和损伤他人的计算机系统设备及资源,不制造和有意传播病毒程序,采取预防措施防范病毒。

(4) 不得利用国际互联网制作和传播破坏宪法和法律、破坏国家统一、扰乱社会秩序、损害国家机关信誉、侮辱或诽谤他人的信息。

(5) 不利用电子邮件进行广播型的宣传;未经允许不私自阅读他人的通信文件,如电子邮件;不能通过破解他人的口令到他人的计算机中窥探。

（6）在工作中尊重各类著作权人的合法权利。

5.6　本章小结

随着信息化建设的不断深入，复杂应用系统和计算机网络的广泛应用，特别是政府上网工程和电子商务的开展，信息系统的安全问题日益显得重要。由于网络系统的开放性、互联性和资源共享性，以及网络协议本身先天的缺陷和安全漏洞，使得网络极易受到“黑客”、病毒、恶意软件的攻击，给信息系统带来各种各样的安全问题。本章介绍了信息安全的基本概念，信息安全的相关技术和措施，如数据加密、数字签名、数字证书、防火墙等，以及计算机病毒的防治技术。

习题 5

1. 什么是信息安全？
2. 什么是数字签名和数字证书？
3. 什么是数据加密？
4. 什么是计算机病毒？
5. 计算机病毒的特点是什么？
6. 计算机病毒的分类有哪几种？
7. 什么是防火墙？
8. 黑客的入侵技术？
9. 计算机病毒的预防需注意哪些问题？
10. 消除计算机病毒的方法有哪些？