前　言

随着国际互联网事业的发展，电子商务作为一种全新的商业模式正愈来愈深入地影响着当今人们的经济生活。然而，人们在欣喜地享用这些高科技成果的同时，却不得不对另一类普遍存在的社会问题产生了越来越多的顾虑和不安，这就是商务网站的安全问题。1988 年 11 月发生的“蠕虫”事件，使人们第一次意识到计算机网络的安全问题同网络的其它技术一样，应该作为今后计算机网络发展的必须研究的课题。

本书是作者结合自己的有关商务网站的研究成果，加上多年的教学经验精心编写而成。这套教材以理论和实践相结合，基础知识和相关领域的最新研究成果相结合为特色，内容新颖，实践性强。它是为高等院校、职业技术院校的电子商务、经济管理或计算机应用专业编写的教材，也可作为同类成人教育的培训用书，更是电子商务、计算机工作者的专业参考用书。

为了便于读者更好地理解电子商务安全技术，本书作者从三个方面介绍了相关内容。首先介绍了网络安全技术和信息安全技术的基础知识，然后在此基础上，结合实例阐述了电子商务安全技术。

本书由周景学任主编，并负责全书的大纲设计和统稿，具体编写分工是周景学（第 3、4、5、6 章）及朱琦（第 1 章及 2 章的 1、2、3、5、6、7、8、9、10 节），孟雪梅（第 2 章第 4 节及第 8 章），王玉芹（第 7 章），金明俊（第 9 章）。王玉芹协助主编进行统稿和绘图。杨振宇教授审阅。

由于编写时间仓促，编者水平有限，书中如有错误和不足之处，敬请读者批评指正，并向参考文献的各位作者、本书审阅者和有关单位的同仁一并致谢。

编　者

2001 年 3 月

第一部分 网络安全技术

第1章 网络安全基础

§1.1 计算机网络的组成与特点

1.1.1 网络的组成

计算机网络是一个非常复杂的系统，由许多计算机软件、硬件及各种通讯设备组成，为了方便学习和理解，我们对常见的术语(概念)作一简单介绍。

1.服务器。目前，在网络中尤其是局域网中，其访问控制方式大都是集中控制型，服务器(Server)是网络的中枢，一般是由一个或几个比较高档的速度较快、存储容量较大的微机担任，服务器运行的情况直接影响整个网络的效率。它的作用一般有以下几个方面：

(1)运行网络操作系统，通过网络操作系统来控制和协调各工作站的运行，处理和响应各工作站发出的服务申请。

(2)存储和管理网络中的共享资源。网络服务器中存储这种用来共享的数据库、各种应用程序等软件资源；另外，如打印机、扫描仪、大容量硬盘、快速 CD－ROM 等硬件资源也常常通过服务器来共享。因此，按网络服务器的功能可以把服务器分为文件服务器(FS)、打印服务器、通信服务器等几类。一个网络中，至少有一个文件服务器用来存放网络操作系统及应用软件和共享资源等。在小的网络中，一般没有专用的打印服务器和通信服务器，而用文件服务器来提供相应的服务，因此经常把文件服务器简称为服务器。网络操作系统对这些资源进行管

理,使整个工作站能共享这些资源。

(3)网络管理员在网络服务器上对各工作站上用户的活动能够进行控制和监视,从而可以有效地保证网络安全和网络资源的充分利用。总之,随着网络规模的不断加大和复杂化,服务器的作用和地位也在变化,重要性也进一步加强。多服务器网络是网络发展的一个趋势。而另一方面对等网络的发展,将促使网络服务器概念的淡化。

2.工作站。工作站 WS(Work Station)又常称为客户机(Client),是局域网中共享网络资源的计算机。一个这样的计算机被称为一个工作站点或一个服务器,工作站计算机的档次可以稍低一些,但常因网络操作系统的不同需有不同的配置。用户在工作站上通过执行命令或应用程序,向服务器申请服务。如申请网络打印、网络通信或共享其它网络资源等。工作站一般通过用户的形式上网,不同的用户在网络上有不同的权限,从而所能共享的资源也有所不同。当用户不需网络服务时,可将工作站作为普通微机使用。工作站本身的硬盘和打印机称为本地硬盘和本地打印机,一般不能为网络用户共享,除非进行专门的设置才行。没有磁盘的工作站称为无盘工作站。无盘工作站可以大大降低建网成本,提高网络可靠性,易于管理,因此,在教学网络中经常使用。无盘工作站的网卡必须有用于远程复位的 PROM 模块,用于引导工作站到服务器上查找引导文件,启动工作站。

3.网络操作系统。网络操作系统 NOS(Network Operating System)是网络的核心部分,对整个网络资源和网络用户进行管理、协调和控制,为网络中的工作站提供各种网络服务,以实现网络资源共享和网络数据通信。

网络操作系统由多种系统软件和网络协议组成,所有的网络功能都是通过网络操作系统来实现的。网络操作系统有别于单机操作系统如 DOS 等,它一般是多任务、多用户的,可以根据用户的需要作不同的配置调整,同时满足不同用户的需要。目前,常见的网络操作系统有:UNIX、NetWare 和 Windows NT。UNIX 网络操作系统可以在各种类型机如微机、小型机、大型机上运行,从 UNIX 发展而来的 Linux 是一种代码开放的新型网络操作系统,性能稳定,安全性高,易于开发出基于其上的应用软件;NetWare 是一种面向微机、占世界计算机网络市场相当比重的网络操作系统;Windows NT 是微软公司新推出的可运行在微机和网络中的面向分布式图形应用的网络操作系统。

4.实体。实体(Entity)是计算机网络中每一层的活动元素。实体即可以是软件实体,也可以是硬件实体。不同网络计算机上的同一层的实体叫做对等实体(Peer Entity)。

5.服务。即网络服务(Service),泛指网络中计算机的处理和共享能力。服务在形式上是由一组原语(Primitive)(或操作)来描述的,这些原语供用户和其它实体访问该服务。

6.协议。协议(Protocol)是计算机网络中实现通信必需有的一些规则,对速率、传输代码、代码结构、传输控制步骤、出错控制等制定标准。它帮助实体之间、网络之间的相互理解和正确进行通信。协议通常由三部分组成:一是语义部分,用于决定双方对话的类型;二是语法部分,用于决定双方对话的格式;三是变换规则,用于决定通信双方的应答关系。常用的协议有 TCP/IP 协议、Novell 公司的 IPX 协议、微软公司的 NetBEUI 协议等。其中 TCP/IP 协议是为美国 ARPA 网(Internet 的前身)设计的:TCP 是传输控制协议,规定一种可靠的数据信息传递服务;IP 又称互联网协议,是支持网络间互联的数据协议。计算机网络协议都是用一个分层

的方式来进行设计的。

7.对等机和对等网络。对等机(Peer to Peer Network)既可作为服务器使用,也可用作工作站,而不需一个专用的服务器,每台工作站都可以有绝对的自主权,可相互交换文件。对等网络也可以称为点对点网络,它允许每一台计算机都处于对等机的角色,它以均衡式的数据存储和资源共享为基础。目前,流行的对等网络操作系统有:Novell 公司的 NetWare Lite 和微软公司的 Windows for Workgroups 等。

1.1.2 网络的分类

计算机网络的类型繁多、性能各异,根据不同的分类规则,可以分为不同类型的计算机网络。例如,按通信距离可分为广域网和局域网;按信息交换方式可分为电路交换网、分组交换网和综合交换网;按通信介质可分为双绞线网,同轴电缆网、光纤网和卫星网等;按传输带宽可分为基带网和宽带网;按网络拓扑结构分可分为星形网、树形网、环形网及总线网。根据计算机网络覆盖的面积和处理机相隔的距离不同,可以得到如表 1-1 所示的分类。这些分类都是为了从不同角度来研究计算机网络技术。

表 1-1

计算机网络分类

分布距离	处理机位置	分类
0.1m	电路板	数据流
1m	系统	多处理机
10m	房间	局域网
100m	校园	局域网
1km	建筑物	局域网
10km	城市	广域网
100km	国家	广域网
1000km	洲	广域网
10000km	行星	广域网互联

这里仅简单介绍广域网和局域网的概念。

1.广域网 WAN(Wide Area Network)。广域网称为远程网。广域网最根本的特点就是其处理机分布范围极广,一般从数公里到上万公里。因此网络所涉及的范围可分为市、省、国家、洲乃至整个地球。广域网的这个特点决定了它的一系列特性。单独建造一个广域网是极不经济和不现实的,所以常常借助传统的公共通信(电话、电报)网来实现。此外,广域网的分布不规则,使得网络的通信控制比较复杂。尤其是使用公共传输网,要求连到网上的任何用户都必需严格遵守各种标准和规范。例如我国于 1989 年开通的公用数据网 CNPAC,它对于外部用户提供的界面采用了国际标准,这就是 CCITT 制定的 X.25 协议。这个协议规定了采用分组方式工作和公用数据连接的数据终端设备 DTE(Data TerminaL Equipment)和数据电路端结设备(Data Circuit-Terminating Equipment)之间的接口。这里所说的接口是广义的,泛指界

面的意思，并不是特指相邻层次的接口。

2.局域网 LAN(LocaL Area Network)。对于局域网，美国电子电气工程师协会 IEEE 的局部地区网络标准委员会曾提出如下定义——局部地区网络在下列方面与其它的数据网络不同：通信一般被限制在中等规模的地理区域内，例如一座办公楼，一个仓库或一所学校；能够依靠中等到较高数据传输率的物理通信信道，而且这种信道具有始终一致的低误码率；局部地区网是专用的，由单一组织机构所使用。

局域网的类型繁多，从广义上可以将它分为 3 类：

- 局部地区网络(Local Area Network，缩写为 LAN)；
- 高速局域网络(High Speed Local Network，缩写为 HSLN)；
- 用户交换局域网络(Private Branch Exchange，缩写为 PBX)。

表 1－2 是三种网络的主要特性说明。

表 1－2

局域网分类

特性	LAN	HSLN	PBX
传输介质	双绞线　同轴电缆　光纤	同轴电视电缆 CATV	双绞线
拓朴结构	总线　树形　环形	总线	星形
传输速率 (Mbps)	1－20	50	0.0096－0.064
最大距离(km)	25	1	1
交换技术	包交换	包交换	线路交换
可连接设备	100～1000	10	100～1000
连接费用(元)	500～5000	40000～50000	250～1000

从计算机网络技术来讲，局域网是指采用 IEEE 或 1SO 的局域网络协议的网络。这套协议对应于 ISO－OSI 模型的最低的两层。而以太网、令牌环网、FDDI 光纤分布式数据接口等，都属于这套协议的范畴。

正是由于这套协议的限定，局域网一般都具有以下特点：

- 传输线路都是专线。媒体是粗同轴电缆、细同轴电缆、双绞线和光缆等。光缆主要用于建筑物之间的连接，或作为总线，且使用方式不同于长途通信。
- 传输速率高。例如，高速以太网和 FDDI 传输速率可达 100Mbps，而目前的广域网高的也只能达到每秒几十千位。
- 传输距离短。计算机规模小，一般为微机。近些年来，服务器(Server)虽然已有高档化的趋势，但客户机(Client)仍大多采用微机。
- 网络用途单一。选用的高层协议简单，另外建网的费用也相对低一些。

表 1－3 列出了 WAN 和 LAN 的性能比较。

表 1-3

LAN 和 WAN 性能比较

分类	传输速率	传输介质	应用范围	典型网络
WAN	64KB/S	卫星,微波	国家网	英国 EPPS
广域网	44.184MB/S	无线电	国际网	中国 CNADAC
LAN	10MB/S	电话,DDS	公司,企事业单位	清华大学校园网
局域网	100MB/S	光纤,同轴电缆	校园网	TDNET

随着计算机技术、通信技术以及计算机网络技术的发展,局域网、广域网的界域愈来愈模糊,估计今后的计算机网络将是局域网和广域网的连接。

1.1.3 网络的特点

一个计算机系统连入网络之后,具有共享资源、提高可行性、分担负荷和实现管理等特点,另外,还可以在一定程度上节省软硬件的开销。据预测,今后计算机网络将具有以下特点:

1.开放式的网络体系结构,使不同软硬件环境、不同网络协议之间可以互联,真正达到资源共享、数据通信和分布处理的目标。

2.向高性能发展,追求高速、高可靠性和高安全性。采用多媒体技术,提供文本、声音、图像等综合性服务。

3.计算机网络智能化提高了网络的性能和综合的多功能服务,并更加合理地进行网络各种业务的管理,真正以分布和开放的形式面向用户提供服务。

另外,还应达到易用性和个性化,使用户能在尽量短的时间内尽快掌握网络的具体使用;个性化的设置,使网络更能为用户服务,提供更好的服务。

§1.2 网络面临的安全威胁

1.2.1 易受攻击的目标

计算机系统的脆弱性表现在它极易受攻击和侵害,它的抗打击力和防护力很弱。外界对计算机(硬、软件)有意或无意的攻击可使其不能正常工作。

1.易受环境和灾害的影响。温湿度、供电、火灾、水灾、静电、灰尘、雷电、强电磁场、电磁脉冲等,均会破坏数据和影响它的正常工作。

2.易受攻击。计算机病毒于 20 世纪 70 年代中期开始曾在科幻小说中描述过,但不久就出现在计算机系统中,并对计算机安全构成严重威胁,目前病毒的应用正在向军用方面发展。美军就正在进行病毒直接注入、间接注入的研究,并进行了以无线方式,经空间把计算机病毒注入敌方的飞机、军舰、武器系统、通信设备中去的试验。1988 年美国计算机系统发生的一次蠕虫病毒事件使 18 万台计算机阻塞,6000 台计算机瘫痪,大量数据因死机而丢失,经济损失上亿美元。

1991 年美军在海湾战争中第一次针对信息系统使用了计算机病毒武器。美国国家安全局研制出一种 AF/91 的病毒，侵入到伊拉克的军用计算机网，使伊军的指挥系统失灵，削弱了伊军战斗力。

3. 易被偷取或修改信息。计算机有共享资源的特点，这就使犯罪者可进入系统窃取信息、修改数据、盗窃他人存款、获取资金。

传统的贪污方法一般要涂改银行票据，制作假支票等，而计算机犯罪只须修改计算机内的信息即可达到目的，并且作案可在很短的时间内不留痕迹地完成。

例如，某银行营业部微机操作员利用职务之便，制造假账户，晚上趁机房无人之机，利用微机向假账户非法输入 87 万元，并修改源程序，使总账虚平，进行贪污。

又如，中国工商银行某县支行城市信用社的某计算机记账员，曾在短短的 68 天中利用计算机贪污挪用了 47 万元。

据报导，在美国等西方国家，每年通过计算机窃走的金钱已高达上百亿美元。

犯罪者可采用非法手段进入系统，收集和窃取信息，打开数据库，偷窃或篡改数据库资料等。犯罪者可利用计算机网络的脆弱性，通过通信线路从终端设备上窃取重要信息。例如，在同一条通信线路上加装终端，冒充合法使用者，窃取系统中的重要信息。此外，犯罪者还可采用截获电磁波、远距离摄影、激光窃听等高技术手段，进行不直接接触计算机系统的远距离窃收，再经放大还原处理，得到重要信息。

从安全保密的角度讲，计算机信息系统关系着党和国家的安危。一旦敌方利用计算机的脆弱性窃取了这些重要信息，将严重危害国家的安全，在战争时期甚至会决定战争的胜负。历史上的“中途岛战役”和“山本五十六之死”均是由于密码被破译而造成重大损失的范例。特别是随着国际互联网的发展，成千上万的用户通过计算机与互联网相连，敌对势力可通过互联网搜集、处理和破坏国家的政治、经济、军事、科技等信息，从而引发一系列政治、经济和社会问题。

1.2.2 几种攻击

字典中将安全定义为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。本节探讨将数据置于危险境地的几种情况，用“安全威胁”这一术语特指能被利用或用来对数据进行未授权访问的状态或行为。

安全威胁的类型，分布式系统的安全威胁至少可以说是富有挑战性的。正在使用的各式各样的系统使得对机构内部所有的系统采用统一的安全措施变得实际上是不可能的。在网络上进行集中安全管理实质上是一种折衷方案。例如你或其他的过程需要通过线缆发出信息以执行安全措施，但线缆传输本身就使整个系统变得不再可靠。

图 1－1 显示了安全威胁的几种基本类型。在下列各节中将逐个对它们进行简短的分析。

1. 物理威胁。物理安全是一个相当简单的概念：不要让任何别的什么人拿到你有的东西，也不让他们窥视你的东西。最常见的物理威胁参见图 1－2。

(1)偷窃。在执法理论中有一个学派认为，你如果想抓住罪犯你就必须像罪犯那样思考，不要低估了那些使用直截了当的方法获取所需东西的窃贼们的勇气。如果他们想要什么他们负担不起的东西，他们就把它偷来；如果他们需要钱，他们就会偷点什么东西并把它卖掉；如果

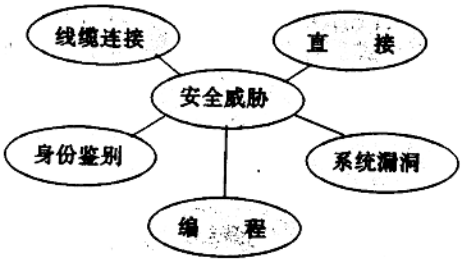

图 1-1 安全威胁基本类型

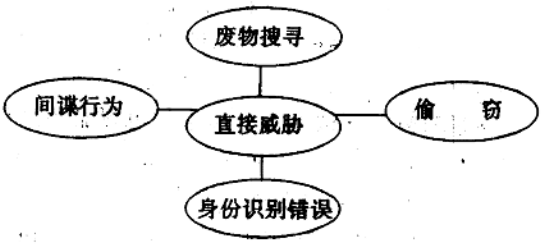

图 1-2 最常见的物理威胁

他们想要的在保险箱里，他们就偷保险箱；如果他们想要偷的东西在计算机里，他们就将整台计算机偷走。

当然，从计算机中获取信息的另一个办法是通过监视器读取。那么，怎样才能使用一台监视器呢？如果采用直截了当的方法，就是砸开锁或把钥匙偷来，打开门，目不斜视地走到监视器前。这种办法不是很有创造性，但很管用。

(2)废物搜寻。在废物中搜寻，希望能找到一些打印出来的材料或废弃的软盘，这是消磨掉整个晚上或整个周末的好办法。如果能和你的心上人一起来做就更好了，有的人可能认为这个办法很聪明，有的人则把这称为拣破烂，还有些人称之为环境和人格的完美结合。说得够多了，但这种情况的确会发生。

(3)间谍行为。请不要回避这个问题，实际上你可能自己就在什么时候做过这种事，就算不是有意的。你看别人在键盘上敲密码并暗记在心里，这种情形常发生在你帮别人排除故障时。在这种时候可能需要登录并退出上百次。也许这不算是真正的间谍行为，但真的有人会注意这些事情来使自己获利。

你可能真的没做的事情是深夜在竞争对手的建筑物外走来走去，透过窗户往里看，读在黑暗中闪烁的陌生人的监视器上的信息。工业间谍是确实存在的，甚至政府也时不时地卷入这些行动中。这当然有些令人不安，但也是见怪不怪的事。商业机构为了省钱或获取有价值的机密，什么不道德的事情都会做得出来。

(4)身份识别错误。你需要一本护照，一本驾驶执照，一份出生证明或一个加密的安全卡吗？随便哪里都有人可以为你做一个。真的能够做这种事情的人至少需要一点点勇气、技术才能和狡猾。

在这种办法中，直截了当的手法遇到了老练和技巧。能犯下这种罪行的人一般都相当严肃

地对待他们的计划并知道他们要找的东西是什么。因此，他们对你的数据构成了巨大的威胁。

2.线缆连接。计算机网络的使用对数据造成了新的安全威胁(见图 1－3)。下面将讨论一些比较常见的问题。

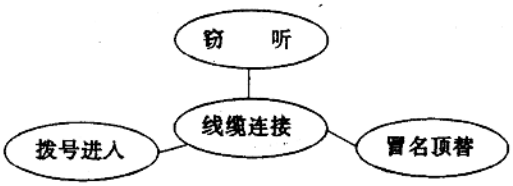

图 1－3　线缆连接威胁

(1)窃听。分布式计算机的特征是各种分立的计算机通过一些媒介相互通讯。因此，自然而然地，你可以"倾听"会话过程并借此收集信息。这种电子窃听甚至并不需要窃听设备一定要安装在线缆上。有时候通过检测从连线上发射出来的电磁辐射就能拾取所要的信号，为了使机构内部的通讯有一定的保密性，可以使用加密手段来防止信息轻易地被解密。

(2)拨号进入。任何拥有一个调制解调器和一个电话号码的人都可以试着通过远程拨号访问你的网络，特别是他有一个从你的机构中的某个人那里偷来的账户时。

(3)冒名顶替。术语假冒是指一台机器在网络上看起来像是另一台机器的能力，就好比是"罪恶的双胞胎"。这种办法实现起来并不容易，而且一般说明有机构内部的、了解网络和操作过程的人也卷了进去。

3.身份鉴别。身份鉴别是指计算机借以决定你是否有权在服务器上要求或提供某些服务的过程。今天，如果没有身份鉴别，在 LAN 系统上就不会有安全。常见的身份鉴别安全威胁如图 1－4 所示。

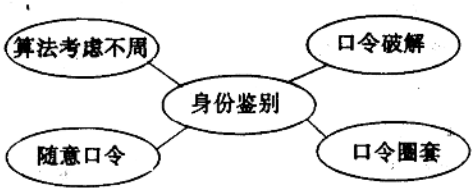

图 1－4　身份鉴别安全威胁

(1)口令圈套。口令圈套是计算机行业中真正聪明的诡计之一，和上面谈到的冒名顶替有关。有人写出并编译一个代码模块，运行起来和登录屏幕一模一样。该代码被插入到正常的登录过程之前。最终用户看到的只是两个登录屏幕，一个接一个。第一次登录显然失败了，所以用户被要求输入用户名和口令。实际上，第一次登录并未失败，它将登录数据，如用户名和口令写入了一个数据文件以便今后使用。

(2)口令破解。破解计算机上的口令就像是想出自行车密码锁的数字组合是什么一样。像在其它领域中一样，此中高手自然比业余爱好者有高得多的技巧和成功率。

(3)算法考虑不周。口令输入过程要想正常地工作必须满足一组条件。这个过程是由某地方的新人编写的，并且采用了某些算法。这些算法对某种输入组合也许不能正常工作。在一些已知的案例中，机灵的非法闯入者聪明地用超长的字符串破坏了那些口令算法，成功地进

入了系统。

(4)随意口令。像许多安全折衷措施导致的问题一样,随意口令需要有一个内部漏洞。说起来很简单,公司内部的什么人建立了一个虚设的账户或修改了一个已有的隐含账户的口令,这样,任何知道那个账户的用户名和口令的人都可以访问该机器了。

4.编程。真正有趣而且恶毒的安全漏洞源于程序代码见图1-5所示。有些时候这些攻击是良性的,只是测试一下,看看那些代码是否工作。大多数时候则是毁灭性的,会摧毁数据。因此,计算机病毒同时威胁到系统安全和数据完整性。

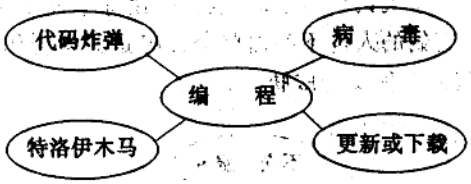

图1-5 编程安全威胁

(1)病毒。病毒是能通过把自己的一个拷贝附着于机器中的另一个程序上的一段代码。通过这种方式,病毒可以进行自我复制,并随着它所附着的那个程序在机器之间传播。这种传播可以通过从BBS上下载文件来进行,也可以通过购置的磁盘来进行,或通过任何将新的资料输入机器的过程来进行。一些最烦人的病毒问题是由于在进行过热缩包装的商品软件安装盘中含有病毒,当软件安装好了时,机器就染上了病毒。

在过去的几年中出现过许多很著名的病毒。最重要的病毒之一——Internet蠕虫,并不是一个真正意义上的病毒。Internet蠕虫开始时是有人想探索一下,看是否可以写一段代码,使其能够进入Internet,并在整个网络上进行传播。利用已知的UNIX安全漏洞,该代码传遍了整个网络,获得了令人眩目的成功,也使Internet上的许多系统遇到了严重的性能下降问题。该代码并不是蓄意想破坏,但不幸的是,通过侵入系统中大量进行自我复制,将存储器空间用完,它的确起到了一些破坏作用。尽管如此,Internet蠕虫暴露了在Internet和分布式计算系统中存在的严重安全问题,总的来说,可能还是功大于过。

(2)代码炸弹。大多数最具杀伤力的病毒是代码炸弹。代码炸弹的原理是到了设定的日期和钟点,或在机器中发生了某种操作步骤,代码炸弹就被触发并开始干坏事。

代码炸弹不必像病毒那样四处传播。有大量系统程序员将代码炸弹写入机器的案例。侏罗纪公园的小说和电影中的那个贪婪的程序员,Michael Crichton扮演的那个,用一个代码炸弹关掉了电子安全系统,这样他就可以偷取恐龙的DNA并将其转卖给侏罗纪公园的竞争对手。在实际生活中,人们已多次使用了类似的办法。他们是这样做的:在系统软件中编写一个代码炸弹,使其产生一个没有什么人能轻易地找出来的软件漏洞。有朝一日,该代码炸弹被触发后,这个不走正道的程序员会被请回来修正这个错误,并马上成了英雄,赚了一大笔钱。这种高技术的敲诈的受害者甚至不知道他们被敲诈了。就算他们起了疑心也无法证实自己的猜测。

(3)特洛伊木马。特洛伊木马是包括病毒、代码炸弹、蠕虫和诸如此类的恶意代码的通称。就像这个名称所暗示的,一个特洛伊木马程序使自己被安装到不知情的人的机器上,并按它不知其名的编制者的意图行事。特洛伊木马经常会摧毁数据。有时它伪装成你的系统上已有的

程序,有时它创建新的用户名和口令。

(4)更新或下载。不要和特洛伊木马相混淆了,有些计算机系统允许通过调制解调器进行固件和操作系统更新。曾有过非法闯入者解开了这种更新方法,使用访问权限代码并对系统进行了非法更新的案例。

5.系统漏洞。系统漏洞也被称为陷阱。陷阱通常是由操作系统开发者有意设置的,这样他们就能在用户失去了对系统的所有访问权时仍能进入系统。例如,VMS操作系统中隐藏了一个维护 ID 和口令,这样软件工程师就可以在用户忘掉了自己的账号或口令时进入系统进行维修。但有时这些陷阱是由系统错误引起的,也就是说除了发现它们的人外没有人知道它们是如何工作的。甚至发现它们的人也不明白整个过程是如何工作的,而是只知道结果。图 1-6 总结了由系统漏洞引起的各种安全威胁。

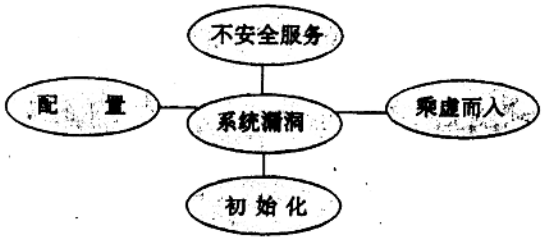

图 1-6　系统漏洞安全威胁

(1)乘虚而入。乘虚而入是指这种情况:一个用户停止与另一个系统的通讯,但由于某种原因仍使另一个系统上的一个端口处于激活状态。紧接着,另一个用户通过同一个端口开始与另一个系统通讯,这样他就不必通过任何申请使用端口的安全检查了。

(2)不安全服务。有时操作系统的一些服务程序可以绕过机器的安全系统。前面有关病毒的威胁中提到的 Internet 蠕虫,就是曾利用了 Berkeley UNIX 系统中三个这样的可绕过机制。

(3)配置和初始化。试想你不得不关掉一台服务器以便维修它的一个子系统。几天后,当你重新启动该服务器时,一大群用户却向你抱怨,说他们的文件丢失或被篡改了。发生了什么事情呢?这有可能是在系统重新初始化时,安全系统却没有被正确地初始化。这样就留下了安全漏洞使其他的什么人可以利用,而他们的确利用了这个机会。有些类似的问题在特洛伊木马程序修改了系统的安全配置文件时也会发生。

1.2.3　网络是否安全

下面是建议采用的可以为你的系统提供适当安全的方法的一个简短清单,以决定你的网络是否安全。左边的一列是建议采取的方法,右边的一列指出该方法是能够在系统上实现,还是一种必须向机构雇员传达的雇员守则。

修补系统漏洞	系统
病毒检查	系统
直接安全	守则

空闲机器守则	守则
废品处理守则	守则
口令守则	守则
加密	系统
执行身份鉴别	系统
Internet 防火墙	系统
捕捉闯入者	系统

1.修补系统漏洞。如果你在系统中发现了一个漏洞,你可能会想请人修补它。显然,今后你也许会因为这个漏洞被堵上了而陷入麻烦,因为你也许会需要利用这个漏洞才能重新排除进入系统的那些故障,但你经常会请生产商那边的什么人来为你做这样的事吗?这总比让别的什么人发现这个漏洞,利用它访问你的系统,并将数据偷走或损坏要强些吧?

2.病毒检查。病毒检查是一个像备份和不间断电源那样对你来说极为重要的术语,市场上有许多检查病毒的产品可以帮助你免受病毒的侵害。病毒检查软件在 LAN 客户机和服务器上都可以运行。如果你觉得自己易于受到病毒的攻击,你可以将自己置于多个反病毒产品结成的战略同盟的保护下。

3.直接安全。在大多数人没法看见的上锁的房间里的设备比放在大庭广众之下的设备要安全得多。在那种人来人往的地方谁都可以走近设备,研究它,并暗想把它放在他们的地下办公室将会是多么雅致呀!尽管设备室不会被布置成展览厅,但对你、你的同事和任何想用该设备的人来说,真正值得注意的事情是闲杂人员在你们工作时不应在场。

4.空闲机器守则。在人员离开机器时,屏幕保护程序和键盘锁定口令必须执行。尽管每个人都喜欢新的屏幕保护程序,但好像大多数人都不喜欢键盘锁。至少应该有一条这样的守则,就是在晚上和周末机器必须关掉。

5.废品处理守则。你怎样丢弃垃圾?撕碎?消磁?可能真的需要用这些措施来处理纸上的或磁记录介质上的机密文件,以打消你附近的高技术垃圾搜寻者的企图。

6.口令守则。你多久进行一次强制性口令变更?这件工作应该定期进行(口令不能重复使用,也不能像姓氏或电话号码这样的东西一样使用)。

7.加密。加密是对数据进行编码。进行编码加密的数据,如果不先进行解码,数据就不可用。这种措施可以防止别人将文件拷贝到别处去进行阅读。在 Internet 上对信用卡信息进行加密被认为是为减少信用卡欺诈行为并促进电子贸易所需的最主要的功能。

所有加密算法的弱点是所用的算法总有一天会被人破解。苏联解体后这种可能性就更大了。来自冷战双方的大批数学家都拥有从事解密工作所需的高超技巧、专门的知识和多年的经验。

8.执行身份鉴别。现在你怎么才能知道谁在你的网络上做什么呢?你也许没有直接访问另一台机器,但你正在运行的某个程序也许在你不知道的情况下却正在访问那台机器。有可能那些想偷偷地访问你的系统的人知道这种情况,并知道如何利用它。执行身份鉴别可以保证会话过程另一端的人或程序有合法的访问权,而这对许多机构而言是极其重要的。Kerberos 是 UNIX 环境中执行这种功能的产品。

9. Internet 防火墙。如果你想上 Internet，请安装一个防火墙程序。对系统复杂性的认识比你多的网络黑客实在是太多了。

10. 捕捉闯入者。通过使用一种能识别那些黑客并确定他们所处的位置的程序可以扭转与他们打交道时所处的不利局面。具体办法是使闯入者认为他们已经真的进入了你的系统，与此同时你却正在努力追踪他们的节点号码。

§1.3 网络安全的服务与机制

国际和各国际标准化组织，都对网络安全十分关注。ISO 制定了网络安全体系结构，针对网络系统受到的威胁，该体系结构提出了对等实体鉴别、访问控制、数据保密、数据完整性、数据源鉴别及禁止否认等六类安全服务，并建议采用以下 8 种安全机制来实现安全服务。

(1)加密机制；
(2)数据鉴别机制；
(3)访问控制机制；
(4)数据完整性机制；
(5)交换鉴别机制；
(6)业务量填充机制；
(7)路由控制机制；
(8)公证机制。

§1.4 让网络更安全

1.4.1 安全问题

计算机网络的广泛应用已经对经济、文化、教育与科学的发展产生了重要影响，同时也不可避免地带来了一些新的社会、道德、政治与法律问题。大量的商业活动与大笔资金正在通过计算机网络在世界各地快速地流通，这已经对世界经济的发展产生了重要、积极的影响，同时也面临着严峻的挑战。计算机犯罪正在引起社会的普遍关注，而计算机网络是被攻击的重点。计算机犯罪是一种高技术型犯罪，由于其犯罪的隐蔽性，在此对计算机网络安全构成了很大的威胁。在国际上，计算机犯罪案件正在以每年 100% 的速率增长；在 1nternet 网上，“黑客”(hacker)攻击事件则以每年 10 倍的速率增长；计算机病毒从 1986 年发现首例以来，10 年间正以几何级数增长，目前已经发现了 2 万多种病毒，它对计算机网络带来了很大的威胁。美国国防部的计算机系统曾经受到非法闯入者的攻击，美国金融界为此每年损失金额近百亿美元。因此，计算机网络的安全问题已引起人们的普遍重视。

作为网络用户，他们都希望在任何一个地方的任何一台计算机上，都可以十分方便地访问网络中任何一台计算机上的信息资源。特别是在 Internet 上，人们希望能在学校、企业或家庭的个人计算机上漫游 Internet 世界，这会给人们带来无穷的乐趣。但是，这对于将自己的 In-

ternet 连入 Internet 的各企业网络管理人员来说无疑是一场恶梦。因为大多数公司都有一些重要的在线信息，如贸易秘密、产品开发计划、市场策略、财政分析资料等，泄露这些经济情报对一家公司来说无疑是一种致命的危险。在 Internet 的安全性讨论中，人们把对 Internet 构成的威胁分成两类：有意造成的危害和无意造成的危害。

有意危害 Internet 安全的主要有三种人：故意破坏者(Hackers)、不遵守规则者(Vandals)和刺探秘密者(crackers)。

故意破坏者企图通过各种手段去破坏网络资源与信息，例如涂抹别人的主页、修改系统配置，造成系统瘫痪；不遵守规则者企图访问不允许他访问的系统，他可能仅仅是到网中看看，找些资料，也可能想盗用别人的计算机资源(如 CPU 时间)；刺探秘密者的企图非常明确，即通过非法手段侵入他人系统，以窃取商业秘密与个人资料。

除泄露信息对企业网构成威胁之外，还有一种危险是有害信息的侵入。有人在网上传播一些不健康的图片、文字，或散布不负责任的消息。一些不遵守网络使用规则的用户，可能通过玩一些电子游戏将病毒带入系统，轻者造成信息出现错误，使得一些应用程序不能使用，严重的将会造成网络瘫痪。显然，要设计一个成功的网络系统，就必须针对网络安全构成威胁的各种因素，研究确保网络信息系统安全的机制。网络安全机制涉及到网络安全策略与数据加密、数字签名、第三方确认、Internet 防火墙(Firewall)等安全技术。

1.4.2 使网络物理上更安全

网络物理安全指用以保护网络计算机硬件和存储介质的装置和工作程序。由于计算机和其它物理物体之间的相似之处，因此网络物理安全是网络计算机安全的最重要的方面，这是最好理解的。

像打字机和家具一样，计算机也是偷窃者的目标，一张软盘完全可以装在口袋里带走。但是不同于打字机和家具，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

实际上目前有许多确保安全的设备。比如在计算机下面安装将计算机固定在桌子上的安全托盘，用高强度电缆在计算机的机箱中穿过等。还有就是要加强计算机机房的管理，如门卫；出入者身份检查；下班锁门以及实施各种硬件安全手段等预防措施。

网络物理安全还包括防止损害计算机，如不要将咖啡溅在磁盘上，不要猛力震动硬盘等。备份(Backups)也是保证安全的一项重要措施。

“备份”的意思是指在另一个地方制作一份拷贝。这个拷贝或备份将保留在一个安全的地方，一旦失去原件，就能使用备份。应该有规律地备份以便使用户避免由于硬件故障导致的数据损失。备份对防卫人为破坏(Human Subverter)也至关重要。如果计算机被偷，数据的惟一的拷贝还在备份上，这是可以在另一台计算机上恢复的。如果计算机黑客攻破计算机系统里并抹掉所有文件，备份将能把它们恢复，假定这个计算机黑客确实无法获得备份或者知道备份的存在。

但是，备份也是潜在安全问题。间谍把它当成偷窃的目标，因为备份含有秘密信息的精确拷贝。确实，备份给计算机系统提供更大安全性，因为偷窃含有工作数据的介质比偷窃备份更

引人注目。

由于备份存在安全漏洞，一些计算机系统允许用户的特别文件不进行系统备份。这样的行动是因为备份磁带被偷的损失比由于设备故障失去数据的损失更大。

1.4.3 制作安全的链路层

链路层加密是密码保护最透明的形式。事实上，它常常通过外部加密盒实现，因此，即使是设备驱动程序也不知道它的存在，更别说应用程序了。

顾名思义，这种形式的加密是为了保护一个单独的链路。它既有优点也有弱点。优点是它非常强有力，因为(对一定类型的硬件)整个数据包是加密的，包括源地址和目的地址。这能抗御流量分析，一种能明智地识别出谁与谁在通信的攻击。在一定环境下，如点到点链路加密，甚至流量的存在性都可以伪装。

然而，链路加密有一个严重的弱点：它一次只能保护一个链路。报文在通过其他链路的时候，仍然会暴露。即使它们也被加密器保护起来，报文在交换节点仍容易受到伤害。关键看敌人是谁，这可能成为一个严重的缺陷。

如果希望严密保护本地通信(即在共享的同轴电缆上)或保护少量极脆弱的线路，应选择链路加密。

卫星线路是一个典型的例子，因为跨洋电缆线路随时可以切换为基于卫星的备用线路。

1.4.4 网络层安全很重要

对 Internet 层的安全协议进行标准化的想法早就有了。在过去十年里，已经提出了一些方案。例如，“安全协议 3 号(SP3)”就是美国国家安全局以及标准技术协会作为“安全数据网络系统(SDNS)”的一部分而制定的。“网络层安全协议(NLSP)”是由国际标准化组织为“无连接网络协议(CLNP)”制定的安全协议标准。“集成化 NLSP(I－NLSP)”是美国国家科技研究所提出的包括 IP 和 CLNP 在内的统一安全机制。SwIPe 是另一个 Internet 层的安全协议，由 Ioannidis 和 Blaze 提出并实现原型。所有这些提案的共同点多于不同点。事实上，他们用的都是 IP 封装技术。其本质是，纯文本的包被加密，封装在外层的 IP 报头里，用来对加密的包进行 Internet 上的路由选择。到达另一端时，外层的 IP 报头被拆开，报文被解密，然后送到收报地点。

Internet 工程特遣组(IETF)已经特许 Internet 安全协议(IPSEC)工作组对 IP 安全协议(IPSP)和对应的 Internet 密钥管理协议(IKMP)进行标准化工作。IPSP 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制不仅能在目前通行的 IP(IPv4)下工作，也能在 IP 的新版本(IPng 或 IPv6)下工作。该体制应该是与算法无关的，即使加密算法替换了，也不对其它部分的实现产生影响。此外，该体制必须能实行多种安全政策，但要避免给不使用该体制的人造成不利影响。按照这些要求，IPSEC 工作组制订了一个规范：认证头 AH(Authentication Header)和封装安全有效负荷 ESP(Encapsulating Security Payload)。简言之，AH 提供 IP 包的真实性和完整性，ESP 提供机要内容。

IP AH 指一段消息认证代码 MAC(Message Authentication Code)，在发送 IP 包之前，它

已经被事先计算好。发送方用一个加密密钥算出 AH，接收方用同一或另一密钥对之进行验证。如果收发双方使用的是单钥体制，那他们就使用同一密钥；如果收发双方使用的是公钥体制，那他们就使用不同的密钥。

IP ESP 的基本想法是对整个 IP 包进行封装，或者只对 ESP 内上层协议的数据(运输状态)进行封装，并对 ESP 的绝大部分数据进行加密。在管道状态下，为当前已加密的 ESP 附加了一个新的 IP 头(纯文本)，它可以用来对 IP 包在 Internet 上作路由选择。接收方把这个头取掉，再对 ESP 进行解密，处理并取掉 ESP 头，再对原来的 IP 包或更高层协议的数据就像普通的 IP 包那样进行处理。

AH 与 ESP 体制可以合用，也可以分用。不管怎么用，都逃不脱传输分析的攻击。我们不太清楚在 Internet 层上，是否真有经济有效的对抗传输分析的手段，不过，在 Internet 用户里，真正把传输分析当回事儿的也是寥寥无几。

大多数 IPSP 及其相应的密钥管理协议的实现均基于 Unix 系统。任何 IPSP 的实现都必须跟对应协议的源码纠缠在一起，而这源码又能在 Unix 系统上使用，其原因大概就在于此。但是，如果要想在 Internet 上更广泛地使用和采纳安全协议，就必须有相应的 MS－DOS 或 Windows 版本。而在这些系统上实现 Internet 层安全协议所直接面临的一个问题就是，PC 上相应的实现 TCP/IP 的公共源码资源什么也没有。为克服这一困难，Wagner 和 Bellovin 实现了一个 IPSEC 模块，它像一个设备驱动程序一样工作，完全处于 IP 层以下。

Internet 层安全性的主要优点是它的透明性，就是说，安全服务的提供不需要应用程序、其它通信层次和网络部件做任何改动。它的最主要的缺点是：Internet 层一般对属于不同进程和相应条例的包不作区别，对所有去往同一地址的包，它将按照同样的加密密钥和访问控制策略来处理。这可能导致提供不了所需的功能，也会导致性能下降。针对面向主机的密钥分配的这些问题，RFC 1825 允许(甚至可以说是推荐)使用面向用户的密钥分配，其中，不同的连接会得到不同的加密密钥。但是，面向用户的密钥分配需要对相应的操作系统内核作比较大的改动。

虽然 IPSP 的规范已经基本制订完毕，但密钥管理的情况千变万化，要做的工作还很多。尚未引起足够重视的一个重要的问题是在多播 (Multicast)环境下的密钥分配问题，例如，在 Internet 多播骨干网(MBone)或 IPv6 网中的密钥分配问题。

简言之，Internet 层是非常适合提供基于主机对主机的安全服务的。相应的安全协议可以用来在 Internet 上建立安全的 IP 通道和虚拟私有网。例如，利用它对 IP 包的加密和解密功能，可以简捷地强化防火墙系统的防卫能力。事实上，许多厂商已经这样做了。RSA 数据安全公司已经发起了一个倡议，来推进多家防火墙和 TCP/IP 软件厂商联合开发虚拟私有网。该倡议被称为 S－WAN(安全广域网)倡议。其目标是制订和推荐 Internet 层的安全协议标准。

1.4.5 安全的传输层、会话层和应用层

1.4.5.1 传输层的安全性

在 Internet 应用编程序中，通常使用广义的进程间通信(IPC)机制来同不同层次的安全

协议打交道。比较流行的两个 IPC 编程界面是 BSD Sockets 和传输层界面(TLI),在 Unix 系统 V 命令里可以找到。

在 Internet 中提供安全服务的首先一个想法便是强化它的 IPC 界面,如 BSD Sockets 等,具体做法包括双端实体的认证,数据加密密钥的交换等。Netscape 通信公司遵循了这个思路,制定了建立在可靠的传输服务(如 TCP/IP 所提供)基础上的安全套接层协议(SSL)。SSL 版本 3(SSLv3)于 1995 年 12 月制定。它主要包含以下两个协议:

• SSL 记录协议。它涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSL v3 提供对数据认证用的 MD5 和 SHA 以及数据加密用的 R4 和 DES 等的支持,用来对数据进行认证和加密的密钥可以通过 SSL 的握手协议来协商。

• SSL 握手协议。用来交换版本号、加密算法、(相互)身份认证并交换密钥。SSL v3 提供对 Deffie－Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一实现在 Fortezza Chip 上的密钥交换机制的支持。

Netscape 通信公司已经向公众推出了 SSL 的参考实现(称为 SSLref)。另一免费的 SSL 实现叫做 SSLeay。SSLref 和 SSLeay 均可给任何 TCP/IP 应用提供 SSL 功能。Internet 号码分配当局(IANA)已经为具备 SSL 功能的应用分配了固定端口号,例如,带 SSL 的 HTTP (https)被分配以端口号 443,带 SSL 的 SMTP(ssmtp)被分配以端口号 465,带 SSL 的 NNTP (snntp)被分配以端口号 563。

微软推出了 SSL 版本 2 的改进版本,叫做 PCT(私人通信技术)。至少从它使用的记录格式来看,SSL 和 PCT 是十分相似的。它们的主要差别是它们在版本号字段的最显著位(The Most Significant Bit)上的取值有所不同:SSL 该位取 0,PCT 该位取 1。这样区分之后,就可以对这两个协议都给以支持。

1996 年 4 月,IETF 授权一个传输层安全(TLS)工作组着手制定一个传输层安全协议(TLSP),以便作为标准提案向 IESG 正式提交。TLSP 将会在许多地方酷似 SSL。

我们已经看到,Internet 层安全机制的主要优点是它的透明性,即安全服务的提供不要求应用层做任何改变。这对传输层来说是做不到的。原则上,任何 TCP/IP 应用,只要应用传输层安全协议,比如说 SSL 或 PCT,就必定要进行若干修改以增加相应的功能,并使用(稍微)不同的 IPC 界面。于是,传输层安全机制的主要缺点就是要对传输层 IPC 界面和应用程序两端都进行修改。可是,比起 Internet 层和应用层的安全机制来,这里的修改还是相当小的。另一个缺点是,基于 UDP 的通信很难在传输层建立起安全机制来。同网络层安全机制相比,传输层安全机制的主要优点是它提供基于进程对进程的(而不是主机对主机的)安全服务。这一成就如果再加上应用级的安全服务,就可以再向前跨越一大步了。

1.4.5.2 会话层不提供安全服务(略)

1.4.5.3 应用层的安全性

网络层(传输层)的安全协议允许为主机(进程)之间的数据通道增加安全属性。本质上,这意味着真正的(或许再加上机密的)数据通道还是建立在主机(或进程)之间,但却不可能区分在同一通道上传输的一个个具体文件的安全性要求。比如说,如果一个主机与另一个主机之间建立起一条安全的 IP 通道,那么所有在这条通道上跑的 IP 包就都要自动地被加密。同