商务电脑

现用现查

商务电脑安全技术

主编：李　勇

台海出版社

商务电脑现用现查系列丛书

商务电脑安全技术

刘远宁　　编著

台海出版社

目　录

第一部分　概　述

第二部分　计算机反病毒技术

第三部分 计算机网络安全技术

第一部分　概　述

第一章　计算机系统安全简介

1.1　计算机安全常识

1.1.1　计算机安全的重要性

众所周知，社会的发展需要信息和信息交流，人们几乎无时无刻不和信息打交道。然而，信息的价值真正被人们所认识还是在今天。据统计，在19世纪，知识和信息每50年翻一番；20世纪初约每30年翻一番；20世纪50年代后期约每10年翻一番；而90年代只需3年就翻一番了。这种信息量的急剧增加，使得用手工方式进行信息处理已不能适应需要，必须要有更先进的科学技术来收集、处理、存储和传输信息。而计算机正是这种技术的杰出代表，它的出现使得信息科学技术有了飞速发展，对社会发展产生了深远的影响。

计算机技术的高度发展为人类提供了高度的自动化和现代化，计算机网络的不断扩大，迅速地向着国际化方向发展，为人类社会的更高速、更高效、更广泛的信息交流提供了条件，过去人们想象不到的许多事情今天都已经变成了现实。特别是到了90年代，计算机应用已经渗透到政治、经济、军事、科学文化和家庭生活等社会的各个领域，计算机已经成为各发达国家社会生活中的重要工具，实现了社会计算机化，改变着社会生产方式和社会的其它活动方式，朝着社会信息化进军。

随着计算机应用的广泛深入，计算机信息系统日益在整个社会活动中发挥着巨大作用，逐步实现自动指挥与控制、生产、管理、办公自动化。原先由人承担的繁重工作，逐步由计算机代替，生产和工作效率大为提高。计算机信息系统也逐步成为一个国家和政府机构运转的命脉和整个社会活动的支柱。

由此，社会的计算机化产生了一种新的社会资产，即计算机资产。

计算机资产由两大部分构成：

(1) 一是计算机信息系统资源，即硬件、软件、实体及其相关文件资料，系统相关配套设备和设施、系统服务，甚至计算机业务工作人员等。系统资源具有相当高的价值和使用价值；

(2) 二是计算机信息系统生产和拥有的信息资源，或者叫由系统处理、存储、传输的电子信息资源。包括钱、财、物，以及各种有价值的数据，如统计报表、科学技术资源、计划、决策、秘密文件、情报、公民个人的隐私数据等。

如果说系统资源是国家的重要财富，而信息资源则是国家的重要战略资源。谁拥有它，谁就掌握了战略主动权。由此，我们不论从计算机资产的属性，还是从它的社会价值方面看，都会深刻地认识到计算机安全的重大战略意义。

在计算机问世之初，计算机数量还相当少，计算机被视作一种珍贵的财产，所以如何保证软件技术不被窃用是十分重要的。后来，随着计算机技术的发展，计算机从科学计算

的领域中走出来，而成为一种事务处理机。当计算机用于管理和商业后，它便成了直接影响组织的生存及发展的重要财富。

在计算机应用尚由专人管理和以主机为主的集中式网络时代，由于信息的流通受到严格的管制，懂得计算机技术的人又不多，因此，计算机应用只有简单的安全性问题。80年代以后，分布式网络日渐普及，跨国境计算机网络应用逐渐建立起来，计算机程序的设计技术迅速普及到大众，而相对的计算机管理技术、网络中的信息交换控制、程序及资源共享秩序与伦理道德、计算机使用者应遵守的法律及人们的基本的价值观念均未得到同步提高，计算机文化及文明远远滞后于计算机技术的应用，这种情况就为今天的计算机犯罪的产生和发展提供了温床。

由此可见，随着计算机和计算机网络的普及，人类信息资源作为一种社会财富得到充分合理的利用，这时人类的意识形态也应包括计算机部分，从而就要求与之相适应的制度及组织机构亦应得到相应的发展和完善，如法律、法规道德及教育等等。

1.1.2 计算机安全的脆弱性

前面我们列举了计算机有许多强大的功能，但是，也存在着某些缺陷。因此，计算机资源最易受自然和人为有害因素的影响。下面我们来看一看你身边的计算机系统安全吗？

其实，我们周围的计算机系统的安全是非常脆弱的。

我们说计算机系统的安全是脆弱的，那么，它的脆弱因素又包括哪些内容呢？

●数据输入部分：数据通过输入设备输入系统进行处理，数据易被篡改或输入假数据。

●编程部分：用语言写成机器能处理的程序，这种程序可能会被篡改或盗窃。

●软件部分：计算机系统离开软件就是一堆废铁，一旦软件被修改或破坏，就会损害系统功能，以至整个系统瘫痪。

●数据库部分：数据库存有大量的各种数据，有的数据资料价值连城，如果遭到破坏，损失是难以估价的。

●操作系统：操作系统是管理系统运行、保证数据安全、协调处理业务和联机运行的关键部分，如被破坏就等于破坏了系统功能。

●输出部分：经处理后的数据要在这里译成人能阅读的文件，并通过各种输出设备输出，信息有可能被泄露或被截取。

●通信部分：信息或数据要通过它在计算机之间或主机与终端及网络之间传送，通信线路一般是电话线，专线，微波，光缆，前三种线路上的信息易被截取。

●硬件部分：即除软件以外的所有硬设备，这些电子设备最容易被破坏或盗窃。

●电磁波辐射：计算机设备本身就有电磁辐射问题，也怕外界电磁波的辐射和干扰，特别是自身辐射带有信息，容易被别人接收，造成信息泄漏。

●辅助保障系统：水、电、空调中断或不正常会影响系统运行。

●存取控制部分：安全存取控制功能还比较弱。

●自然因素主要是：火、电、水、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲等危害。这些危害有的会损害系统设备，有的则会破坏数据，甚至毁掉整个系统和数据。

●人为因素是：安全管理水平低、人员技术素质差、操作失误或错误、违法犯罪行为

等。

以上计算机的不安全因素说明，计算机自身的脆弱性十分严重。现在计算机已经应用到国家重大要害部门或涉及全国性的大型信息系统之中，如果某个关键部分出了问题，不但系统内可能产生灾难性的“多米诺”连锁反应，而且会造成严重的政治、经济损失，如果系统中的重要数据遭破坏或某些敏感信息被泄露，其后果也是不堪设想的。

探讨计算机安全的实质是分析对计算机资源存在着的各种各样的威胁，以及找出如何对付这些威胁的有效措施。

从造成这些威胁的人员来说，由于对计算机的接近程度不一样，大致可以分四类：

●外部人员：不能进入计算机中心或机房的人员。

●物理存取人员：这类人员能进入计算机中心但没有多少上机的权利。

●系统存取人员：这类人员通常是计算机中心的普通用户，他们在系统里拥有的权利不是太多。

●编程特权人员：这类人员能在计算机上编制自己的程序，通常是指那些系统编程人员和系统维护人员。

从对计算机系进行攻击的手段来说，计算机可能面临以下威胁：

●搭线窃听：在计算机的通信线路上，搭上一个侦听设备，从而获得线路上传输的机密信号。

●重叠：在终端的合法用户登机键入口令时，重叠在该用户之上，从而达到非法目的。

●电磁辐射：通过接受计算机系统辐射出的信号而获得机密信息。

●口令猜测：通过猜测口令而进入到网络系统中。

●密文分析：通过分析线路上传输的加密信息而得到明文。

●流量分析：通过观察通信线路上的信息流量，得到信息的源点和终点、发送频率、报文长度等，从而推断出信息的某些重要特性。

●转向：攻击者可利用自己对系统软件的了解，将自己由普通用户工作方式转为监控方式。

●缓冲区：攻击者直接从输入缓冲区中获得口令等机密信息。

●特权位：在有的机器里，特权位是存放在用户的地址空间里的，攻击者可能修改这些特权位，做系统管理人员才能做的事。

●电子邮件：在传送给别人的电子邮件中插入一些控制信息，达到获得接收者的文件拷贝等目的。

●特洛伊木马：修改某些程序，使得这些程序仍能正常工作，看上去没有问题，实际上其中隐藏着一些破坏性的指令。

●逻辑炸弹：一种只有当特定事件出现才进行破坏的程序。

●意大利香肠术：这是对财务系统进行的攻击。它从每个客户的帐目中偷出一点点钱，客户往往不注意这种微弱损失，而攻击者将众多客户的钱加在一起，其数目就可观了。

●滥用实用程序：有些机器上的实用程序可以被修改以满足不同的需要，攻击者利用实用程序达到自己的目的。

●病毒：实际上是一种逻辑炸弹，不同之处在于它不断地繁殖其自身。

1.1.3 计算机安全的定义

面对计算机应用中出现的一系列安全问题，各国计算机安全专家和学者对计算机安全进行了大量的研究，并且取得了许多进展，但总的来看，计算机安全水平与计算机应用水平相差太远，对计算机安全的研究还不够。

历史已证明，建立一个科学的学科体系对于学科本身的发展有着巨大的推动作用。目前随着对计算机安全研究的不断深入，一个新学科——计算机安全学正在形成，它的形成和发展必然会对计算机安全起指导作用。

要建立计算机安全学学科体系，首先必须明确计算机安全的定义，因为只有这样才能界定计算机安全学的内容。“计算机安全”译自英文“Computer Security”。

国际标准化委员会(ISO International Sandards Organization)的定义是：

“为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭破坏、更改、显露。”这个定义比其他人提出的定义准确，但仍不够完备。它偏重于静态，没有包含运行发挥效益，所以应当包含动态意义。

我国公安部计算机管理监察司的定义是：

“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害”。

计算机安全内容的层次包括以下几个方面：

●计算机安全技术：包括识别用户术、存取核权术、存储器管理术、电磁辐射、屏蔽技术、加密术、反窃听术、防复制术、容错术、审计术、报警术、安全评价术、维护术。

●计算机安全管理：包括安全组织、人事、运行管理、数据与介质管理、机房管理与出入控制、脆弱性分析、风险分析与应急计划、维护。

●计算机安全产品：包括低辐射设备、安全操作系统、安全数据库系统、安全通信设备、加密设备、可信计算机、不停顿计算机、不停顿电源。

●计算机犯罪与侦查：包括计算机犯罪分类、计算机犯罪手段、计算机犯罪心理、计算机犯罪的侦查与取证。

●计算机安全法律：包括保密法(涉及国家秘密)、数据法(涉及个人隐私)、计算机犯罪惩治法(刑事)、计算机安全法、软件产业法、过境数据安全法。

●计算机安全监察：包括安全监督、安全标准与规范、安全检测与质量鉴定、安全监察。

●计算机安全理论与政策：包括计算机安全理论基础、计算机安全与社会、计算机安全相关因素、计算机安全政策、计算机安全试验方法。

1.2 计算机犯罪

1.2.1 计算机犯罪的含义

到目前为止，国际上对计算机犯罪问题尚未形成一个公认的定义。计算机犯罪也许只是人类社会发展过程中一个暂时性的犯罪名称。因为人类从来没有把作案工具称作犯罪的先例，包括作案中使用率最高的刀枪也是如此。也有人把计算机犯罪叫做智能犯罪或科