吴多胜 王 杰 王 帆 等编著

# 网络安全从入门到精通

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

# 网络安全从入门到精通

吴多胜　王　杰　王　帆　等编著


電子工業出版社

**Publishing House of Electronics Industry**

北京 • BEIJING

## 内 容 简 介

随着网络的日益普及，网络安全防范的重要性和必要性也愈加突出。为了便于读者理解网络安全方面的原理，本书采用通俗易懂的方式介绍了网络安全涉及的知识。同时本书还提供了大量的实例和插图。本书旨在帮助普通计算机用户了解网络安全领域的相关知识，建立安全意识，对保证网络系统的安全具有实际的指导意义。本书从实用的角度出发，内容翔实、有章可循、行文流畅、讲解清晰，具有很强的可读性和实际操作性，必能让读者获益匪浅。

本书适用于一切希望了解和学习网络安全的读者使用，既可作为普通计算机用户上网指导方面的参考书，也可作为网络安全培训教材。



**图书在版编目(CIP)数据**

网络安全从入门到精通 / 吴多胜，王杰，王帆等编著.北京：电子工业出版社，2008.10
ISBN 978-7-121-07326-7

Ⅰ. 网… Ⅱ.①吴…②王…③王… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2008）第 135228 号

责任编辑：李红玉
特约编辑：马振萍
印　　刷：北京天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
　　北京市海淀区翠微东里甲 2 号　邮编：100036
开　　本：787×1092　1/16　印张：24　字数：610 千字
印　　次：2008 年 10 月第 1 次印刷
定　　价：43.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

计算机的普及和应用为人们的生活带来了方便。互联网技术的不断发展，使世界成为一个整体，人们可以通过网络学习、购物、交流。可以说，互联网的迅猛发展为人们带来了前所未有的便利。然而，网络也不是完美无缺的，网络给人们带来惊喜的同时，也带来了威胁。

目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题，关于网络安全的书籍也层出不穷。其实网络安全不仅仅是技术问题，也是社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和法律等多种手段进行综合治理。

本书是作者在信息系统安全方面教学和科研实践的基础上，参考了大量国内外文献资料充实整理而成。旨在使计算机应用、信息系统使用和维护的工程人员，以及大中专院校相关专业的师生重视网络的安全问题，更多地了解和掌握这门学科的基本原理、方法、技术和工具。全书共分 10 章，围绕计算机网络所涉及的安全问题，讲述了各种相关的安全技术以及具体应用。第 1 章介绍了网络安全威胁的相关概念；第 2 章介绍了操作系统的发展以及各操作系统的安全性及其漏洞和防范措施；第 3 章介绍了网络通信协议及其安全；第 4 章介绍了计算机病毒及其防治；第 5 章介绍了木马蠕虫、网页恶意代码的相关知识及其防范措施；第 6 章介绍了网络攻击、入侵检测以及防范措施；第 7 章介绍了 IE 的具体设置和防火墙的相关内容；第 8 章介绍了 Windows XP 和 Windows Vista 系统的具体设置；第 9 章介绍了网络病毒及其防护；第 10 章介绍了针对个人计算机用户在具体使用网络时应该采取的相关防范措施。

本书由吴多胜、王杰、王帆和李海龙等合作编写。在本书的写作与出版过程中，作者得到了王杰同志的鼎立支持和帮助，感谢他的热情帮助。同时要特别感谢李海龙同志的支持和帮助，他为本书的写作和出版付出了辛勤的劳动。

由于计算机网络安全技术涉及内容广泛，相关技术发展十分迅速，加上作者水平有限，书中的错误和不足之处在所难免，恳请有关专家和广大读者批评指正。

# 目 录

## 入 门 篇

## 提 高 篇

# 入　门　篇

# 第 1 章　网络安全概述

计算机技术的普及和应用为人们的生活带来了方便。互联网技术的不断发展，使人们享受到了前所未有的便利。然而，网络给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等严重威胁着网络的安全，也给人们的工作和生活带来了诸多烦恼。为保障我国网络基础设施的安全，国家安全部、公安部等明确要求使用国产的网络安全产品来确保我国网络的安全。因此，网络安全的理论及其应用技术的研究，不仅受到学术界以及工业界的关注，同时也受到各国政府的高度重视，网络的安全和保密技术成为了当今网络技术的一个重要研究课题。

## 1.1　网络安全简述

网络安全是一门新兴的交叉性学科，综合运用了数学、物理、生物、通信及计算机技术等诸多学科的基础理论和最新研究成果，同时还涉及政治、法律、军事等复杂层面。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据，提高网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题，网络信息的保密性、完整性、可用性、真实性和可控性等相关技术问题都成为网络安全研究的重要课题。下面就对这几方面进行说明。

（1）保密性：信息的安全性，即不能将信息泄露给非授权用户。

（2）完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）可控性：能够对信息进行控制，保护其完整性和可用性，对信息的传播及内容具有控制能力。

网络安全包括物理安全、逻辑安全、操作系统安全和网络连接安全。

### 1.1.1 物理安全

在信息安全体系中，物理安全就是要保证信息系统有一个安全的物理环境，对接触信息系统的人员有一套完善的技术控制手段，且充分考虑到自然事件对系统可能造成的威胁并加以规避。简单的说，物理安全就是保护信息系统的软硬件设备、设施以及其他媒体免遭地震、水灾、火灾、雷击等自然灾害，人为破坏或操作失误，以及各种计算机犯罪行为导致破坏的技术和方法。在信息系统安全中，物理安全是基础。如果物理安全得不到保证，如计算机设备遭到破坏或被人非法接触，那么其他的一切安全措施就都只是空中楼阁。

（1）防盗

网络的硬件和软件设备与其他的物品一样，具有自身非常重要的价值，因此成为偷窃者窃取信息的首选目标，软硬盘、主板等都是计算机的关键部件，是窃贼窃取实物的首选。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。

（2）防火

防火是计算机网络中心安全的头等大事，由于计算机机房和中心设有许多线路和电器设备，因此发生火灾的原因一般是由于电器原因、人为事故或外部火灾蔓延引起的。电器设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎，吸烟、乱扔烟头等，使充满易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

（3）防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。它还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。因此机房和网络中心必须采取防静电措施，采用防静电设备进行装饰，以防止由于静电而产生不安全因素。

（4）防雷击

随着科学技术的发展，电子信息设备的广泛应用，对现代闪电保护技术提出了更高、更新的要求，利用传统的常规避雷针，已不能满足微电子设备的要求，而且带来很多弊端。利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃引爆的主要原因。

雷击防范的主要措施是，根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点做分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多级层保护。

（5）防电磁泄漏

抑制和防止电磁泄漏（即 TEMPEST 技术）是物理安全策略的一个主要问题。目前主要防护措施有两类：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，这类防护措施又可分为以下两种：一是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对

机房的下水管、暖气管和金属门窗进行屏蔽和隔离；二是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。从 20 世纪 80 年代开始，美国市场上出现了一种符合 TEMPEST 标准的军用通信设备，并逐渐形成商品化、标准化生产。TEMPEST 技术是综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及多个学科领域。

### 1.1.2　逻辑安全

计算机的逻辑安全是计算机安全的最基本要求。可以通过设置口令字、文件授权、账号存取等方法来实现。防止计算机黑客的入侵主要依赖计算机的逻辑安全。

可以限制登录的次数或对试探操作加上时间限制；可以用软件来保护存储在计算机文件中的信息，该软件限制了其他人存取其他人的文件。直到该文件的所有者明确准许其他人可以存取该文件时为止。限制存取的另一种方式是通过硬件完成，接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如多次登录或请求别人的文件。

### 1.1.3　操作系统安全

操作系统是计算机应用的核心，因此操作系统的安全关系到计算机用户的程序、数据等的安全。由于同一计算机可以安装几种不同的操作系统，如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以便于防止他们相互干扰。例如，多数的多用户操作系统，不会允许一个用户删除属于另一个用户的文件，除非第二个用户明确地授予允许权限。

### 1.1.4　网络连接安全

网络连接的安全性是进行网络通信的最基本保证，网络连接安全涉及的方面很多，技术广泛，具体可以归结为以下两方面的安全服务：

（1）访问控制服务：用来保护计算机和连网资源不被非授权使用。

（2）通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。例如，基于互联网或 WWW 的电子商务就必须依赖并广泛采用通信安全服务。

## 1.2　安全威胁

安全威胁是指对安全的一种潜在的侵害。计算机硬件资源易受自然灾害和人为破坏；软件资源和数据信息易受计算机病毒的侵扰，以及非授权用户的复制、篡改和毁坏。计算机硬件工作时的电磁辐射以及软硬件的自然失效、外界电磁干扰等均会影响计算机的正常工作。通信链路易受自然灾害和人为破坏。采用主动攻击和被动攻击可以窃听通信链路的信息，并非法进入计算机网络获取敏感信息。网络的安全威胁通常分为网络的内部安全威胁和外部安全威胁。我国的计算机以及因特网技术发展比较晚，广泛而普遍地应用主要集中在最近几年，一些先进的软硬件技术都受制于人，相对欧美国家，我国的计算机和网络安全相对要复杂得多。

### 1.2.1 内部威胁

内部安全威胁如图 1-1 所示，主要有操作系统的脆弱性、计算机系统的脆弱性以及 TCP/IP 协议的脆弱性等方面。

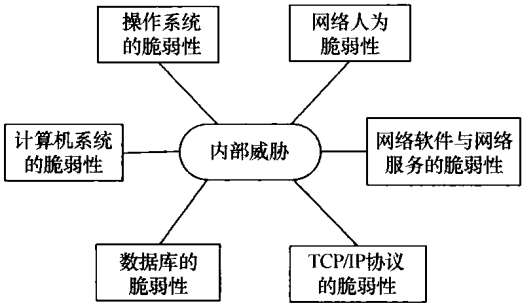


图 1-1 内部威胁

1. 操作系统的脆弱性

无论哪一种操作系统，其体系结构本身就是不安全的一种因素。由于操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务都可以用打补丁的方法升级和进行动态连接。这种方法该产品的厂商可以使用，“黑客”成员也可以使用，而这种动态连接也是计算机病毒产生的温床。因此，这种使用打补丁与渗透开发的操作系统是不可能从根本上解决安全问题的。在 UNIX 系统中黑客采用的攻击手法便是一个很有说服力的例证。但是，操作系统支持的程序动态连接与数据动态交换是现代系统集成和系统扩展的必备功能，因此，这是相互矛盾的两个方面。

操作系统不安全的另一个原因在于它可以创建进程，即使在网络的结点上同样也可以进行远程进程的创建与激活，更令人不安的是被创建的进程具有可以继续创建进程的权力，这一点加上操作系统支持在网络上传输文件、在网络上加载程序，二者结合起来就构成可以在远端服务器上安装“间谍”软件的条件。如果把这种“间谍”软件以打补丁的形式“打”入合法用户上，尤其是“打”在特权用户上，那么，系统进程与作业监视程序就根本监测不到“间谍”软件的存在。

对一个设计上不够安全的操作系统，事后采用增加安全特性或打补丁的办法是一项很艰巨的任务，特别是对引进的国外设备，在没有详细技术资料的情况下，其工作更加复杂。

操作系统的主要功能包括：进程控制和调度、信息处理、存储器管理、文件管理、输入输出管理、资源管理、时间管理等。操作系统的安全是深层次的安全，主要的安全功能包括：存储器保护（限定存储区和地址重定位，保护存储的信息）、文件保护（保护用户和系统文件，防止非授权用户访问）、访问控制、用户认证（识别请求访问的用户权限和身份）。

操作系统的安全漏洞主要有：

（1）输入/输出（I/O）非法访问

在某些操作系统中，一旦 I/O 操作被检查通过之后，该操作系统就继续执行下去而不再检查，从而造成后续操作的非法访问。某些操作系统使用公共的系统缓冲区，任何用户都可以搜索这个缓冲区，如果此缓冲区没有严格的安全措施，那么其中的机密信息（用户的认证数据、

身份识别号、口令等）就有可能被泄露。

（2）访问控制的混乱

安全访问强调隔离和保护措施，但是资源共享则要求公开和开放，这是矛盾的。如果在设计操作系统时没能够处理好这两者之间的关系，就可能会出现因为界限不清造成操作系统的安全问题。

（3）不完全的中介

完全的中介必须检查每次访问请求以进行适当的审批。而某些操作系统省略了必要的安全保护，比如，仅检查一次访问或没有全面实施保护机制。

（4）操作系统后门

某些操作系统为了安装其他公司的软件包而保留了一种特殊的管理程序功能。尽管此管理功能的调用需要以特权方式进行，但是并未受到严密的监控，缺乏必要的认证和访问权的限制，有可能被用于安全访问控制，从而形成操作系统后门。

为了建立安全的操作系统，首先，必须构造操作系统的安全模型（单级安全模型、多级安全模型、系统流模型等）和不同的实施方法。其次，应该采用诸如隔离、核化（最小特权等）和环结构（开放设计和完全中介）等安全科学的操作系统设计方法。再者，还需要建立和完善操作系统的评估标准、评价方法和测试质量。

2. 计算机系统的脆弱性

计算机系统的脆弱性主要来自于操作系统的不安全，在网络环境下还来自于通信协议的不安全性。美国对计算机安全规定了级别，有的操作系统属于 D 级，这一级别的操作系统根本就没有安全防护措施，如 DOS、Windows 3.1 和 Windows 98 等操作系统就属于这一类，它们只能用于一般的桌面计算机，而不能用于对安全性要求高的服务器。UNIX 系统和 Windows NT 达到了 C2 级别，安全性远远强于 Windows 98 操作系统，而且主要用于服务器上。但这种系统仍然存在着安全漏洞，因为这两种系统中都存在超级用户（root 在 UNIX 中，Administrator 在 Windows NT 中），如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会有超级用户带来的问题。现在许多系统都使用静态口令来保护系统，但口令还是有很大的被破解的可能性，而且不好的口令维护制度会导致口令被人偷去。失去口令也就意味着安全系统的全面崩溃。

世界上没有能长久运行的计算机，计算机可能会因为硬件或软件故障而停止运转，或被入侵者利用并造成损失。硬盘故障、电源故障和芯片的故障都是人们应考虑的问题。软件故障则可能出现在操作系统中，也可能出现在应用软件当中。

3. 数据库的脆弱性

数据库是从操作系统的文件系统基础上派生出来的，用于大量数据的管理系统。数据库的全部数据都记录在存储媒体上，并由数据库管理系统（DBMS）统一管理。DBMS 为用户及应用程序提供一种访问数据的方法，并对数据库进行组织、管理以及维护和恢复。数据库系统的安全策略，部分由操作系统来完成，部分由强化 DBMS 自身安全措施来完成。数据库系统存放的数据往往比计算机系统本身的价值大得多，必须加以特别保护。

从操作系统的角度看，DBMS 是一种应用程序，而数据库是一种数据文件。为了防止数据库中的数据受到物理破坏而不能恢复到原来的系统中，应当对数据库系统采取定期备份所有文

件的方法来保护系统的完整性。

DBMS 是在操作系统的基础之上运行的应用程序，是为多个用户共享的应用软件。因此，不能允许它具有通向操作系统的可信途径。DBMS 必须具有独立的用户身份认证机制，以便构成双重保护。有时，还可以对使用数据库的时间、地点加以限制，甚至要求用户只能在指定时间、指定终端上对数据库系统进行指定的操作。

有些数据库将原始数据以明文形式存储于数据库中，这是不够安全的。实际上，高明的入侵者可以从计算机系统的内存中导出所需的信息，或者采用某种方式打入系统，从系统的后备存储器上窃取或篡改数据。因此，必要时应该对存储数据进行加密保护，数据库的加密应该采用独特的加密方法和密钥管理方法，因为数据的生命周期一般较长，密钥的保存时间也相应较长。

4. TCP/IP 协议的脆弱性

协议是两个或多个参与者为完成某种任务或功能而采取的一系列有序步骤。在网络信息系统中，协议使得不了解的双方能够相互配合并保证公平性。协议可以为通信者建立、维护和解除通信联系，实现不同机型互联的共同约定。协议的基本特点是：预先建立（在使用前事先设计好）、相互约定（协议的所有参加者要约定按顺序执行的步骤）、无歧义（不应使参加者由于误解而不能执行其步骤）、完备的（对每一种可能发生的情况都有预防措施）。

通信网的运行机制基于通信协议。不同结点之间的信息交换按照事先约定的固定机制，通过协议数据单元来完成。对每个结点来说，所谓通信，只是对接收到的一系列协议数据单元产生响应，而对从网上传来的信息真实性或从结点发给网中其他结点的真实性均无法提供保证。高速信息网在技术上以传统电信网为基础，是通过改革传输协议发展而来的，因此，各种传输协议之间的不一致性，也会大大影响信息的安全质量。

TCP/IP 协议是 20 世纪 90 年代以来发展最为迅速的网络协议。尽管 TCP/IP 技术取得了巨大的成功，但也越来越暴露出它的不足之处。在设计初期，TCP/IP 通信协议并没有考虑到安全性问题，而且用户和网络管理员没有足够的精力专注于网络安全控制，加上操作系统和应用程序越来越复杂，开发人员不可能测试出所有的安全漏洞，连接到网络上的计算机系统就可能受到外界的恶意攻击和窃取。众所周知，Robert Morries 是在 VAX 机上用 C 语言编写的一个 Guess 软件，根据对用户名的搜索，猜测机器口令的程序从 1988 年 11 月开始在网络上传播以后，几乎每年都给因特网造成巨大损失。在异种机型资源共享的背后，是既令黑客心动，又让网络安全专家头痛的种种漏洞和缺陷，例如：脆弱的认证机制、容易被窃听或监视、易受欺骗、有缺陷的 LAN 服务和相互信任的主机、复杂的设置和控制、基于主机的安全不易扩展、IP 地址的不保密性等。另外，计算机网络系统都使用的 FTP、E-mail、NFS 等都包含着许多影响信息安全的因素，存在许多漏洞。

5. 网络软件与网络服务的脆弱性

网络软件和网络服务的脆弱性主要有两个方面的因素。一是，协议和服务所设计的交互机制可能存在漏洞；二是，由于其规模的复杂性和人的局限性，软件实现也必然存在各种可能的漏洞。这与前面分析的操作系统漏洞的成因是一致的。此外，网络软件和网络服务的不当的使用方法，也会带来许多隐患。

口令是网络信息系统中最常用的安全与保密措施之一。如果用户采用了适当的口令，那么

他的信息系统安全性将得到大力加强。但是，实际上，网络用户中谨慎设置口令的用户却很少。这给计算机内信息的安全保护带来了很大的隐患。曾有人在 Internet 上选择了几个网点，用字典攻击法在给出用户名的条件下，测出 70%的用户口令只用了 30 多分钟，80%用了 2 小时，83%用了 48 小时。

网络信息系统的设计安全性再强，如果用户选择的口令不当，仍然存在被破坏的危险。用户对口令的选择，存在着以下几个误区：

●用“姓名+数字”作口令：许多用户用自己或与自己有关的人的姓名再加上其中某人的生日等作口令。

● 用单个的单词或操作系统（如 DOS 等）的命令作口令。

● 多个主机用同一个口令，一个主机口令被窃会影响多台主机的安全。

● 只使用一些小写字母作为口令，这样使字典攻击法攻破的概率大增。

以上 4 个口令设置的误区，将给信息保密与网络安全带来隐患，网络用户和管理员应切实注意自己的口令设置，不给网络黑客留下可乘之机。

6. 网络人为威胁

网络信息的安全与保密所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。人为威胁则通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，造成不可估量的经济损失和政治上的损失。

人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故）；另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。

虽然人为的偶然事故没有明显的恶意企图和目的，但它会使信息受到严重破坏。最常见的偶然事故有：操作失误、意外损失、编程缺陷、意外丢失、管理不善、无意破坏等。

人为的恶意攻击是有目的的破坏。恶意攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息，如修改、删除、伪造、添加、重放、乱序、冒充、传送病毒等；被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦听、截获、窃取、破译和业务流量分析及电磁泄露等。

由于人为恶意攻击有明显企图，其危害性相当大，给国家安全、知识产权和个人信息带来巨大的威胁。人为恶意攻击具有以下特性：

（1）智能性

从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，许多人都是具有一定社会地位的部门业务主管。他们在攻击前都经过了周密的预谋和精心策划。

（2）严重性

涉及到金融资产的网络信息系统恶意攻击，往往会由于资金损失巨大，而使金融机构、企业蒙受重大损失，甚至破产，同时，也给社会带来动荡。如美国资产融资公司计算机欺诈案，涉及金额达 20 亿美元之巨，犯罪影响震荡全美。在我国也发生过数起计算机盗窃案，金额在数万到数百万人民币，给国家金融资产带来严重损失。

（3）隐蔽性

人为恶意攻击的隐蔽性很强，不易引起怀疑，做案的技术难度大。一般情况下，其犯罪的证据，存在于软件的数据和信息资料之中，若无专业知识，很难获取侦破证据。相反，犯罪行为人却可以很容易地毁灭证据。计算机犯罪的现场也不像传统犯罪现场那样明显。

（4）多样性

随着计算机互联网的迅速发展，网络信息系统中的恶意攻击也随之发展变化。出于经济利益的巨大诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻击手段日新月异。新的攻击目标包括偷税漏税、利用自动结算系统洗钱以及在网络上进行盈利性的商业间谍活动等等。

国际互联网上以人为恶意攻击为代表的高新技术犯罪的另一大发展趋势是网络犯罪集团化。由于网络上的安全机制不断加强，今后的网络犯罪将需要比今天高得多的技术力量，这种客观要求加上网络上日益增长的经济利益将诱使计算机犯罪集团（尤其是跨国犯罪集团）将黑手伸向网络通信系统。届时，传统犯罪活动和网络犯罪的融合将对各国司法当局和国际反犯罪机构提出更大的挑战。

以下是一些有代表性的恶意攻击：

（1）信息战

信息战是一种以获得信息权为目标的无硝烟的战争。信息战可以说是一种国家行为的恶意攻击。信息战的攻击目标包括各种军事命令、通信系统、能源、运输和金融等与国家的政治、经济、文化密切相关的系统。在和平时期，信息战处于绝对隐蔽状态。但是，一旦战争爆发，信息战将出其不意地发挥出巨大的破坏力。美军在伊拉克实施的“沙漠风暴”战争便是典型的信息战例。

（2）商业间谍

商业间谍，即利用国际联网收集别国的重要商业情报，其目标是获得有价值的信息、能力、技术和对自身有利的谈判地位。在多数情况下，商业间谍属于一种集团行为的恶意攻击。除了以信息战为代表的国家行为恶意攻击和以商业间谍为代表的集团行为恶意攻击之外，还有众多的个人行为或者小团体行为的恶意攻击。此类恶意攻击数量巨大，目的复杂。有的恶意攻击者来自窃贼、骗子、敲诈犯、毒犯、犯罪组织成员和其他有犯罪行为的人。有的恶意攻击者来自黑客、恶意竞争者、心怀不满的工作人员、个人仇敌等。此类恶意攻击的典型代表有：

① 窃听

在广播式网络信息系统中，每个结点都能读取网上的数据。对广播网络的基带同轴电缆或双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得窃听网上的数据或非授权访问很容易，且不易被发现。

② 流量分析

流量分析能通过对网上信息流的观察和分析推断出网上的数据信息，比如有无传输，传输的数量、方向、频率等。因为网络信息系统的所有结点都能访问全网，所以流量分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

③ 破坏完整性

破坏完整性，即有意或无意地修改、破坏信息系统，或者在非授权和不能监测的方式下对

数据进行修改。

④ 重发

重发是重复一份报文或报文的一部分，以便产生一个被授权效果。当攻击结点拷贝发到其他结点的报文，并在其后重发它们时，如果网络系统不能监测重发，接收结点将依据此报文的内容接受某些操作。例如，报文的内容是关闭网络的命令，则将会出现严重的后果。

⑤ 假冒

当一个实体假扮成另一个实体时，就发生了假冒。一个非授权结点，或一个不被信任的、有危险的授权结点都能冒充一个授权结点，而且不会有多大困难。很多网络适配器都允许网帧的源地址由结点自己来选取或改变，这就使假冒变得较为容易。

⑥ 拒绝服务

当一个授权实体不能获得对网络资源的访问，或当紧急操作被推迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议而引起，如传输了错误的信号或在不适当的时候发出了信号，还可能是由超载而引起的。

⑦ 资源的非授权使用

资源的非授权使用，即与所定义的安全策略不一致的使用。因常规技术不能限制结点收发信息，也不能限制结点侦听数据，因此，一个合法结点能访问网络上的所有数据和资源。

⑧ 干扰

干扰，即由一个结点产生数据来扰乱提给其他结点的服务。干扰能由一个已经损坏的并还在继续传送报文的结点所引起，或由一个已经被故意改变成具有此效果的结点所引起。频繁的、令人讨厌的电子邮件信息是最典型的干扰形式之一。

⑨ 病毒

目前，全世界已经发现了几十万种计算机病毒，并且最新的病毒还在不断出现。随着计算机技术的不断发展以及人们对计算机系统和网络的依赖程度的增加，计算机病毒已经构成了对计算机系统和网络的严重威胁。

### 1.2.2　外部威胁

单台计算机的威胁相对而言比较简单，而且属于网络系统中的威胁，网络系统的威胁是极富挑战性的，因为在网络系统中可能存在许多种类的计算机和操作系统，所以采用统一的安全措施是很不容易的，而对网络进行集中安全管理则是一种好方案，外部威胁如图 1-2 所示。

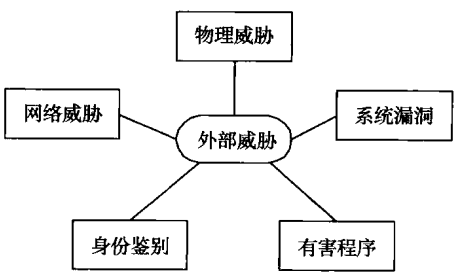


图 1-2　外部威胁

1. 物理威胁

物理安全是指用以保护计算机硬件和存储介质的装置和工作程序。其作用是不要让别人拿走或偷窥自己的资料。常见的物理安全问题有偷窃、废物搜寻和间谍活动等，物理安全是计算机安全最重要的方面。

（1）偷窃

网络安全中的偷窃包括偷窃设备、偷窃信息和偷窃服务等内容。如果想偷的信息在计算机里，那一方面可以将整台计算机偷走。另一方面，也可以通过网络将信息盗走，甚至还可以利用摄像等手段进行窃取。

（2）废物搜寻

废物搜寻包含两个方面的内容：其一就是在废物（如一些打印出来的材料或废弃的软盘）中搜寻所需要的信息；其二是在微型计算机上，从未删除有用信息的软盘或硬盘上或者是回收站等地方搜寻可能获得的有用资料。

（3）间谍活动

间谍活动是人们不能忽视的一种因素，现在商业间谍很多，而且一些商业机构可能会为击败对手而采取任何不道德的手段，有时政府也有可能卷入这种间谍活动当中。

（4）身份识别错误

和假证件、假证书对社会的危害一样．非法建立文件或记录，企图作为有效的正式生产的文件或记录，如对具有身份鉴别特征物品（如护照、执照、出生证明或加密的安全卡）进行伪造，均属于身份识别发生错误的范畴。这种行为对网络数据构成了巨大的威胁。

物理威胁如图 1-3 所示。

2. 网络威胁

（1）计算机网络的使用对数据造成了新的安全威胁，首先在物理上存在着电子窃听。分布式计算机的特征是各种独立的计算机通过一些媒介相互通信，而且局域网一般是广播式的，也就是人人都可以收到发向任何人的信息，只要把网卡模式设置成混合模式（Promiscuous）即可。当然也可以通过加密来解决这个问题，但现在强大的加密技术还没有在网络上广泛使用，况且密码也是有可能被破解的。

（2）现在很流行拨号入网，由于调制解调器也存在安全问题，所以入侵者就可能通过电话线入侵到用户网络当中。

（3）在因特网上存在着很多冒名顶替的现象，而这种冒名顶替的形式也是多种多样的，如：某公司可能会谎称一个站点是他们公司站点、在通信中有的人可能冒充别人或冒充从另一台机器访问某站点。

网络威胁如图 1-4 所示。

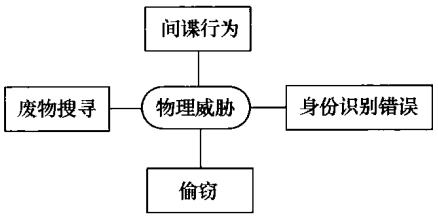


图 1-3　物理威胁

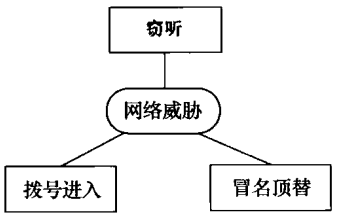


图 1-4　网络威胁