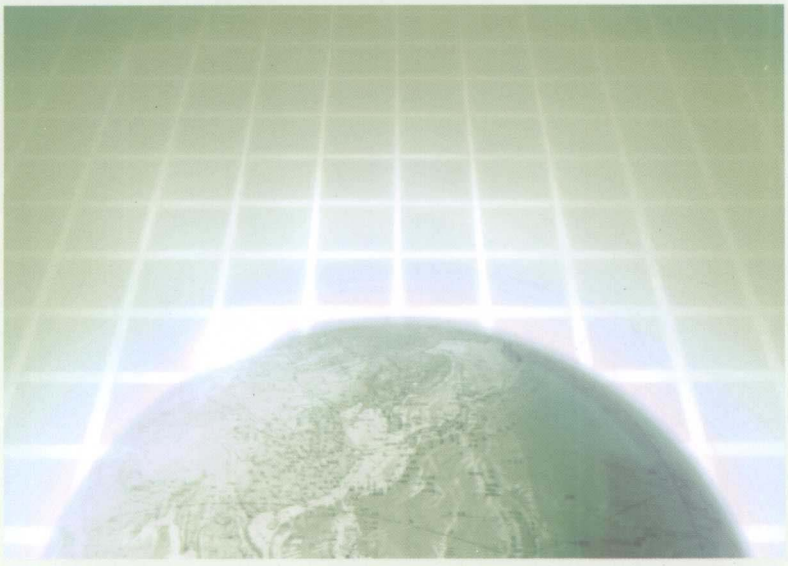
高等学校规划教材

GAODENG XUEXIAO GUIHUA JIAOCAI

网络信息安全技术基础与应用

主　编　庞淑英

副主编　方娇莉　潘晟旻

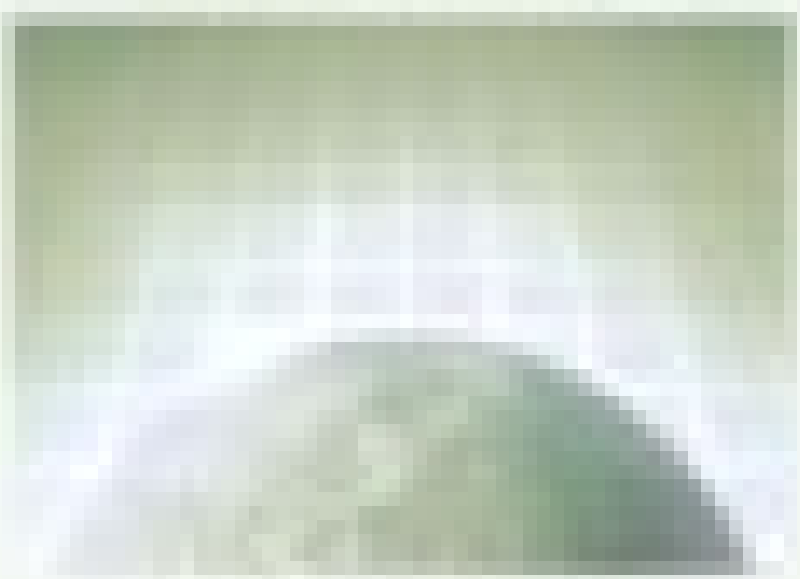


冶金工业出版社

http://www.cnmip.com.cn

网络信息安全技术基础与应用

[redacted]



[redacted]

高等学校规划教材

网络信息安全技术基础与应用

主　编　庞淑英

副主编　方娇莉　潘晟旻

北　京

冶金工业出版社

2009

内 容 提 要

本书系统、科学地介绍了网络信息安全的基础理论和应用。全书共分为 5 章，主要包括信息安全技术基础、TCP/IP 技术应用、操作系统安全技术、网络信息系统的攻防技术和网络信息实体环境安全技术等内容。书中还附有与内容相配套的上机实验指导内容，所有实验均经过编者上机检验，具备很强的可操作性。

本书内容紧凑翔实、语言简练、实用性强，可作为高等院校、各类职业学校及培训机构作为网络信息安全方面的教材，也可作为相关领域专业科研人员的参考书。

图书在版编目（CIP）数据

网络信息安全技术基础与应用 / 庞淑英主编. —北京：冶金工业出版社，2009.3

高等学校规划教材

ISBN 978-7-5024-4709-0

Ⅰ. 网… Ⅱ. 庞… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 026195 号

出 版 人 曹胜利

地 址 北京北河沿大街嵩祝院北巷 39 号，邮编 100009

电 话 (010) 64027926 电子信箱 postmaster@cnmip.com.cn

责任编辑 宋 良 陈慰萍 美术编辑 李 心 版式设计 张 青

责任校对 王贺兰 责任印制 李玉山

ISBN 978-7-5024-4709-0

北京兴华印刷厂印刷；冶金工业出版社发行；各地新华书店经销

2009 年 3 月第 1 版，2009 年 3 月第 1 次印刷

787mm × 1092mm 1/16；13 印张；341 千字；195 页；1-4000 册

21.00 元

冶金工业出版社发行部 电话：(010) 64044283 传真：(010) 64027893

冶金书店 地址：北京东四西大街 46 号(100711) 电话：(010) 65289081

前　言

当前，我国信息化建设、网络技术集成已进入高速发展阶段，网络与信息安全技术在各行业中的重要作用日趋显现，信息安全产业已成为国家安全、政治稳定、经济发展等具有生存性和保障性支撑作用的关键产业。论述网络信息安全的书籍在国内外已有大量出版，但它们大多定位于水平考试或短期培训的层面，而为高等院校非计算机专业本科生、专科生编写的教材还较少。在信息技术高速发展的今天，只有既懂信息技术，又懂网络信息安全技术的学生，才有可能利用网络技术在各个学科领域进行安全而全面的探索和交流，才有可能在今后的工作岗位中拓展自己，为用人单位所接受。本书正是顺应这种需求，立足于网络信息安全技术的基本原理及实际应用，辅以丰富的操作实践，力求提高学生的理解能力、动手能力以及主动学习的兴趣而编写的。

本书在出版之前曾多次作为讲义用于云南省信息安全社会培训，有着较坚实的应用基础，并在多年的实际教学过程中，不断对本书的结构和内容进行修改，形成较为完善、实用的体系。

本书取材新颖，内容涉及广泛，注重理论与实践相结合。所选择的案例和实验深入浅出，紧密结合当前主流网络应用方向，可操作性强，在时下各学校的计算机实验环境下易于实现。

全书共分5章，涵盖了网络信息系统安全技术的基本理论、TCP/IP技术应用、操作系统安全技术、网络攻击和防御技术、实体安全技术分析等方面的内容，并附有配套的实验指导。本书各章节的结构规划、内容选择、审核和修改由庞淑英完成，其中第1章由田春瑾编写；第2章和第5章由潘晟旻编写；第3章由王凌编写；第4章由方娇莉编写；实验部分由付湘琼编写；全书统稿和校正工作由庞淑英、方娇莉和潘晟旻共同完成。

由于作者水平所限，书中不妥之处诚请读者指正。

编　者

2009年1月

目　录

1 信息安全技术基础

【内容提示】本章主要介绍信息安全技术研究的内容，分析信息系统安全所涉及的问题、面临的威胁和风险，并围绕安全体系结构模型、信息安全标准、信息与网络安全组件、安全策略的制定与实施等技术基础问题展开讨论。

1.1 概述

信息系统是以计算机和数据通信网络为基础的应用管理系统。目前，越来越多的信息系统应用于金融、贸易、商业和企业等领域。这在给人们带来极大方便的同时，也为那些不法分子利用计算机信息环境进行犯罪提供了可能。据不完全统计，全球每年因利用计算机系统进行犯罪所造成的经济损失高达上千亿美元。

网络信息系统在成为支撑多行业开展业务的重要平台的同时，面临着不同动机的威胁者发动的不同类型攻击的可能，如信息泄露、恶意代码、垃圾邮件、网络恐怖主义等。因此，多协议、多系统、多应用、多用户组成的网络环境，复杂性高，存在难以避免的安全脆弱性。

1.1.1 信息安全技术研究内容

一切影响计算机网络安全的因素和保障计算机网络安全的措施，都是计算机网络安全技术的研究内容。信息安全技术研究的主要内容如下：

（1）实体安全。实体安全又称物理安全，是指包括环境、设备和记录介质在内的所有支持网络系统运行的总体安全。实体安全主要包括计算机设备、通信线路及设施、建筑物等的安全；预防地震、水灾、火灾、飓风、雷击等的措施；满足设备正常运行环境要求；防止电磁辐射、泄漏；媒体的安全备份及管理等。

（2）软件系统安全。软件系统安全主要是针对所有计算机程序和文档资料，保证它们免遭破坏和非法复制。软件安全技术还包括掌握高安全产品的质量标准，对自己开发使用的软件建立严格的开发、控制、质量保障机制，保证软件满足安全保密技术标准要求，确保系统安全运行。

（3）加密技术。信息安全最重要的自动工具是加密。通常使用两种形式的加密，即对称加密和非对称加密。

（4）网络安全防护。网络安全防护主要是针对计算机网络面临的威胁和网络的脆弱性而采取的防护技术，如安全服务、安全机制及其配置方法、动态网络安全策略、网络安全设计的基本原则等。

（5）数据信息安全。数据信息安全对于系统的稳定性越来越重要。其安全保密主要是指为保证计算机系统的数据库、数据文件以及数据信息在传输过程中的完整、有效、使用合法，免遭破坏、篡改、泄露和窃取等威胁和攻击而采取的一切技术、方法和措施，包括备份技术、压缩技术、数据库安全技术等。

（6）认证技术。与保密性同等重要的安全措施是认证。在最低程度上，消息认证是确保一个消息来自合法用户的手段。此外，认证还能够保护信息免受篡改、延时、重放和重排序，

涉及的内容包括访问控制、散列函数、身份认证、消息认证、数字签名、认证应用程序。

（7）病毒防治技术。计算机病毒对信息系统安全的威胁已成为一个重要的问题。要保证信息系统的安全运行，除了采用服务安全技术措施外，还要专门设置计算机病毒检查、诊断、杀除设施，并采取成套的、系统的预防方法，以防止病毒的再入侵。

（8）防火墙与隔离技术。防火墙与隔离技术是静态安全防御技术，是保护本地计算机资源免受外部威胁的一种标准方法。

（9）入侵检测技术。入侵检测技术是动态安全技术的核心技术，是防火墙的合理补充。入侵检测技术帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时防范。

1.1.2　信息安全的属性

信息安全是指信息在产生、传输、处理和存储的过程中不被泄露或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。

信息安全保密以信息系统的可靠性为前提，基本属性是可靠性和安全性，具体属性叙述如下：

（1）保密性（Confidentiality）。所谓保密性，是指利用密码技术对敏感信息进行加密处理，同时采取抑制、屏蔽措施防止电磁泄漏，保证信息只有合法用户才能利用，而不会被泄漏给非授权的个人和实体。即保证信息不泄漏给未经授权的人。

（2）完整性（Integrity）。所谓完整性，是指防止信息在存储或传输过程中被非法复制、修改、丢失和破坏，以保证信息的正确性、有效性和一致性。保证信息完整性是信息安全的又一基本要求，即防止信息被未经授权的人（实体）篡改，保证真实的信息从真实的信源无失真地到达真实的信宿。

（3）可用性（Availability）。所谓可用性，一方面是指要防止未授权者进入系统访问，窃取或破坏信息资源，另一方面是指保护及保证合法用户有权访问并能够访问信息及信息系统。即保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝服务或为敌手所用。

（4）可控性（Controllability）。所谓可控性，是指合法机构能对信息及信息系统进行合法监控，防止不良分子利用安全保密设备来从事反对政府或破坏社会安全等犯罪活动。政府及管理监控机关可以依法侦探犯罪分子的保密通信，同时保护合法用户的个人隐私，即对信息及信息系统实施安全监控管理。

（5）不可否认性（Incontestable）。所谓不可否认性，是指无论合法的还是非法的用户，一旦对某些受保护的信息进行了处理或其他操作，它都要留下自己的信息，以备日后查证。即保证信息行为人不能否认自己的行为。

1.1.3　信息安全技术的基本功能

信息安全技术应具备防御、监测、应急、恢复等基本功能，下面分别简要叙述。

（1）网络安全防御。网络安全防御是指采取各种手段和措施，使网络系统具备阻止、抵御各种已知网络威胁的功能。

（2）网络安全监测。网络安全监测是指采取各种手段和措施，使网络系统具备监测、发

现已知或未知的网络威胁的功能。

（3）网络安全应急。网络安全应急是指针对网络系统中的突发事件，采取各种手段和措施，使网络系统具备及时响应、处置网络攻击的功能。

（4）网络安全恢复。网络安全恢复是指针对已经发生的网络灾害事件，采取各种手段和措施，使网络系统具备恢复网络系统运行的功能。

1.2 信息安全涉及的问题

信息安全问题涉及很多方面的问题。当提到网络传输的信息安全时，人们总是会立即联想到加密、防黑客、反病毒等专业技术问题。实际上，网络环境下的信息安全不仅涉及技术问题，而且涉及法律政策问题和管理问题。技术问题虽然是最直接的保证信息安全的手段，但离开了法律政策和管理的基础，即使有最先进的技术，信息安全也得不到保障。

1.2.1 法律法规问题

要使信息安全运行和传递，需要必要的法律建设，以法制来强化信息安全。这主要涉及网络规划与建设的法律，网络管理与经营的法律，信息安全的法律，用户（自然人或法人）数据的法律保护，电子资金划转的法律认证，计算机犯罪与刑事立法，计算机证据的法律效力等法律问题。同时，还要有法必依，有法必行。

法律是信息安全的第一道防线。如果没有这些法律的建设和实施，网络将不能规范、协调的运营管理，数据将得不到有效的保护，电子资金的划转将产生法律上的纠纷，网络将受到黑客的攻击而攻击者又受不到惩罚。仅仅这些问题的发生，就会使网络无法安全地传递信息，无法起到信息传递通道的作用。

1.2.2 管理问题

管理问题包括三个层次的内容：组织建设、制度建设和人员意识。组织建设问题是指有关信息安全管理机构的建设。信息安全管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统的评估、安全认证等多方面的内容，因此只靠一个机构是没法解决这些问题的。在各信息安全管理机构之间，要有明确的分工，以避免“政出多门”和“政策撞车”现象的发生。明确了各机构的职责之后，还需要建立切实可行的规章制度，以保证信息安全。如对人的管理，需要解决多人负责、责任到人的问题，任期有限的问题，职责隔离的问题，最小权限的问题等。有了组织机构和相应的制度，还需要领导的高度重视和群防群治。这需要进行信息安全意识的教育和培训。

1.2.3 技术问题

影响计算机网络环境下信息安全的技术问题包括通信安全技术和计算机安全技术两个方面。

保证通信安全所涉及的技术有信息加密技术、信息确认技术及网络控制技术等。保证计算机安全所涉及的技术主要有容错计算机技术、安全操作系统和计算机反病毒技术等。

（1）容错计算机技术。容错计算机的基本特点是有稳定可靠的电源、预知故障、保证数据的完整性和数据恢复等。当任何一个可操作的子系统遭到破坏后，容错计算机能够继续正常运行。

（2）安全操作系统。操作系统是计算机工作的平台。一般的操作系统在一定程度上都具

有访问控制、安全内核和系统设计等安全功能。但是微软视窗系统的“NSA 密钥”则在很大程度上危害着用户的信息安全。所谓 NSA 密钥，是指 1998 年有人发现视窗系统中存在用途等详情不清的第二把密钥。1999 年 8 月，加拿大 Cryotonym 公司首席科学家 Andrew Femandes 宣布这第二把密钥叫做 NSAKey。而 NSA 就是美国国家安全局的简称，也就是说微软在每一份视窗系统中都安装了一个“后门”，专供 NSA 在需要时侵入全世界用户的电脑。

（3）计算机反病毒技术。计算机病毒其实是一种在计算机系统运行过程中能够实现传染和侵害的功能程序，是影响计算机安全不容忽视的重要因素。

反病毒技术的发展过程可划分如下：

第一代反病毒技术采取单纯的病毒特征诊断，但是对加密、变形的新一代病毒无能为力。

第二代反病毒技术采用静态广谱特征扫描技术，可以检测变形病毒，但是误报率高，杀毒风险大。

第三代反病毒技术将静态扫描技术和动态仿真跟踪技术相结合。

第四代反病毒技术基于病毒家族体系的命名规则，采用多位 CRC 校验和扫描机理、启发式智能代码分析模块、动态数据还原模块（能查出隐蔽性极强的压缩加密文件中的病毒）、内存解毒模块、自身免疫模块等先进解毒技术，能够较好地完成查毒解毒的任务。

1.2.4　其他问题

信息安全产业发展的问题也是影响网络环境下信息安全的一个很重要的因素。保证网络环境下的信息安全，涉及很多信息安全产品和服务，如防火墙、安全操作系统、相应的信息安全软件等。如果一个国家的信息安全产品都是依靠国外进口，那么就很难保证一些涉及国家经济安全信息的安全应用。因为如果出口国完全掌握着信息安全产品的核心技术，就很容易侵入进口国的网络系统，得到进口国的机密信息。信息安全的另一个问题是信息安全产品和技术的标准及其标准化。制定行业标准是保证行业发展的重要基础，在信息安全产品和技术方面，如果没有统一的标准，那么将无法度量和测评各种信息安全产品和技术。

1.3　信息系统的安全威胁与风险分析

1.3.1　脆弱性分析

信息资产及其安全措施在安全方面的不足和弱点导致的脆弱性常常被称为漏洞或薄弱点。系统自身的脆弱和不足，是构成信息系统安全问题的内部根源。

（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。而这种动态连接是计算机病毒产生的温床，该产品的厂商可以使用，“黑客”成员也可以使用。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 系统中黑客所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。

（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 Window 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 Unix 服务器。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。

（3）协议安全的脆弱性。当前，计算机网络系统所使用的 TCP/IP 协议以及 FTP、E-mail、NFS 等都包含着许多影响信息安全的因素。众所周知，Robert Morries 在 VAX 机上用 C 编写的一个 Guess 软件，根据对用户名的搜索，猜测机器密码口令的程序从 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。黑客通常采用 Sock、TCP 预测或远程访问（RPC）直接扫描等方法对防火墙进行攻击。

（4）数据库管理系统安全的脆弱性。由于数据管理系统（DBMS）对数据库的管理是建立在分级管理的概念上的，因此 DBMS 的安全性也不高。而且 DBMS 的安全必须与操作系统的安全配套，这无疑是一个先天不足。

（5）人性的脆弱性。网络是信息资源得以利用的基础，并将成为人们获取信息的基本手段；同时人们对网络的依赖给国民经济和国家安全也带来了巨大隐患。网络和信息时代给我们带来技术进步和生活便利的同时，也给国民经济和国家安全带来了巨大隐患。信息网络受攻击，形成对信息社会的攻击；人性的脆弱性，同样会引发信息社会的脆弱性。安全专家都同意这样一种观点：狡猾的电脑黑客往往利用社交工程学的概念来进行欺诈。他们利用人类与生俱来的信任他人、乐意助人以及对未知事物的好奇心等弱点，通过 E-mail、伪造的 Web 网站、向特定的用户提几个简单的问题等伎俩，骗取公司的保密资料或从个人用户那里骗取网上购物的信用卡号、用户名和密码，达到入侵网络信息系统的目的，使得那些采用各种先进技术的安全防护措施形同虚设。

另一方面，不管是什么样的网络系统都离不开人的管理，但现实中又特别缺少高素质的网络管理员，缺少信息安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控等等必备防范措施。这都造成了信息系统的脆弱性。

1.3.2 安全威胁分析

信息安全的威胁可能来自一个物体、一个人或者来自不断对资产表现出危险的实体，这里将损害信息安全的行为统称做安全性威胁。信息安全的管理人员必须清楚所处机构、人员、应用程序、数据以及信息系统所面临的各种各样的威胁，才能更好地理解互联世界中诸多的威胁。

单台计算机的威胁相对而言比较简单，而且包含在网络系统的威胁中，所以在这里只讨论网络系统的威胁。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的方案。本节对构成信息系统安全威胁的因素、类型进行叙述。

1.3.2.1 构成威胁的因素

影响信息系统的因素很多。有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用。归结起来，针对信息系统的威胁主要有以下三个因素。

（1）环境和灾害因素。温度、湿度、供电、火灾、水灾、地震、静电、灰尘、雷击、强电磁

场、电磁脉冲等，均会破坏数据和影响信息系统的正常工作。灾害轻则造成业务工作混乱，重则造成系统中断，甚至造成无法估量的损失。如 1999 年 8 月吉林省某电信业务部门的通信设备被雷击中，造成了惊人的损失；还有某铁路计算机系统遭受雷击，造成设备损坏、铁路运输中断等。

（2）人为因素。人为因素可分为有意和无意。有意的是指人为的恶意攻击、违纪、违法和犯罪。这是信息系统所面临的最大威胁。无意的是指人为的无意失误，如操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将已有的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

人为的无意失误和各种各样的误操作都可能造成严重的不良后果，典型的错误有文件的误删除、输入错误的数据等。

（3）系统自身因素。计算机网络安全保障体系应尽量避免天灾造成的计算机危害，控制、预防、减少人祸以及系统本身原因造成的计算机危害。尽管近年来计算机网络安全技术取得了巨大的进展，但计算机网络系统的安全性比以往任何时候都受到更大的威胁。主要表现在它极易受到攻击和侵害，它的抗打击力和防护力很弱。

1）计算机硬件系统的故障。由于生产工艺或制造商的原因，计算机硬件系统本身有故障而引起系统的不稳定、电压波动的干扰等。信息系统在工作时，向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2）软件组件。软件组件的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及代码过长，将不可避免地导致软件存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别。

3）网络和通信协议。安全问题最多的网络和通信协议是基于 TCP/IP 协议族的 Internet 及其通信协议建立的。TCP/IP 协议最初设计的应用环境是美国国防系统的内部网络，这一网络环境是互相信任的，而且支持 Internet 运行的 TCP/IP 协议族原本只考虑互联互通和资源共享的问题，并未考虑也无法兼容解决来自网际中的大量安全问题。当其推广到全社会的应用环境之后，信任问题发生了。因此，Internet 充满安全隐患就不难理解了。

1.3.2.2　安全威胁类型

网络系统包含各类不同的资产，由于其具有的价值不同，因此受到的威胁也不同。表 1-1 是网络系统受到的非自然的威胁主体类型实例。

表 1-1　非自然的威胁主体类型实例

威胁主体类型	威胁主体描述
国　家	以国家安全为目的，由专业信息安全人员实现，如信息战
黑　客	以安全技术挑战为目的，由具有不同安全技术熟练程度的人员组成
恐怖分子	以强迫或恐吓为手段，企图实现不当愿望
网络犯罪	以非法获取经济利益为目的，非法进入网络系统，出卖信息或修改信息记录
商业竞争对手	以市场竞争为目的，主要是搜集商业情报或损害对手的市场影响力
新闻机构	以收集新闻信息为目的非法获取有关新闻事件中的人员信息或背景材料
不满的内部工作	以报复、泄愤为目的，破坏网络安全设备或干扰系统运行
内部粗心工作人员	因工作不专心或技术不熟练而导致网络系统受到危害，如误配置等

根据威胁主体的自然属性，可将威胁分为自然威胁和人为威胁。自然威胁有地震、雷击、洪水、火灾、静电、鼠害和电力故障等。人为威胁分为：

（1）盗窃类型的威胁：如偷窃设备、窃取数据、盗用计算资源等。

（2）破坏类型的威胁：如破坏设备和数据文件、引入恶意代码等。

（3）处理类型的威胁：如插入假的输入、隐瞒某个输出、电子欺骗、非授权改变文件、修改程序和更改设备配置等。

（4）操作错误和疏忽类型的威胁：如数据文件的误删除、误存和误改、磁盘误操作等。

从威胁对象来分类，可以将威胁划分成物理安全威胁、网络通信威胁、网络服务威胁、网络管理威胁，分别阐述如下。

（1）物理安全威胁。网络物理安全是整个网络系统安全的前提。物理安全威胁主要有地震、水灾、火灾等造成的整个系统的毁灭；电源故障造成设备断电，甚至导致操作系统引导失败或数据库信息丢失；设备被盗、被毁造成数据丢失或信息泄露；电磁辐射可能造成数据信息被窃取，等等。

（2）网络通信威胁。网络通信威胁有线路窃听、篡改网上传输信息、中断网络通信或滥用网络通信带宽、非法访问网络设备等。常见网络通信威胁的实际案例有网络嗅探器，简称 sniffer；TCP 通信会话劫持；利用漏洞远程破坏网络设备、重设配置、获得网络管理访问权限等。

（3）网络服务威胁。假冒内部合法用户身份进行非法登录，窃取网络服务。攻击者通过发送大量虚假请求包到网络服务器，造成网络服务器超负荷工作，甚至造成系统瘫痪。例如分布式拒绝服务攻击，简称 DDoS。威胁者虚构和仿冒知名网站的页面或登录界面，骗取网上用户的敏感信息，如银行账号、会员号信息等。

（4）网络管理威胁。网络管理威胁有多种形式，如误用管理权、安全配置不当、泄露敏感用户名及口令等，这些都将对网络安全构成很大的威胁。

1.3.3 安全风险分析

风险分析（Risk Analysis）是信息系统安全管理中的一个重要问题。它不但是信息系统建设初期应该考虑的问题，而且也是在系统生命周期的全过程都应关注的问题。这对系统最初设计时应该采取什么安全防护措施起到指导作用，并且对检查修订安全防护措施提供有效的帮助。

1.3.3.1 进行安全风险分析的原因

在信息系统安全管理中，考虑风险就是要考虑由于人为的或自然的威胁因素可能对信息系统造成的危害以及由此可能带来的损失。

如图 1-1 所示，我们建立一个信息系统，希望使用它为我们创造财富。但是，它可能由于

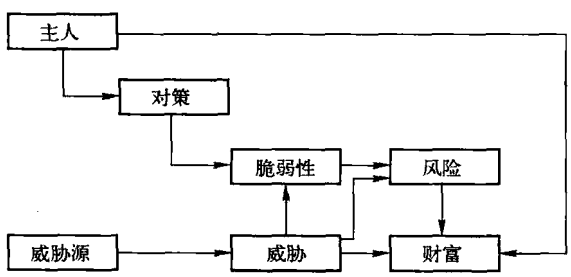


图 1-1 风险对系统的影响