21世纪

高等学校精品规划教材

信息安全技术基础

张浩军　杨卫东　谭玉波　等编著

中国水利水电出版社
www.waterpub.com.cn

21世纪高等学校精品规划教材

信息安全技术基础

张浩军　杨卫东　谭玉波　等编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

随着计算机和网络应用的普及，信息安全已经成为关系国家政治稳定、经济发展、军事对抗的重要问题。本书面向实际应用，全面介绍了信息安全保障体系和防御体系，信息安全基本概念、理论背景，以及各种信息安全技术的实现机理，解读信息安全技术的典型应用，帮助读者树立信息安全工程思想。

全书共分 11 章，分为四大模块：信息安全工程基本思想、密码学、基于密码技术的安全服务、非密码网络安全防御技术。

本书在编写上强调实用性和系统性，适合大专院校计算机、通信、电子商务等相关专业的信息安全课程使用，也可以作为从事计算机、网络工程项目建设与运行维护的技术人员的参考书。

本书配套提供相关电子资源，包括 PPT 形式电子教案以及编著者所在单位教学中的网络资源。读者可从中国水利水电出版社网站或万水书苑上免费下载，网址：http://www.waterpub.com.cn/softdown/或 http://www.wsbookshow.com。

图书在版编目（CIP）数据

信息安全技术基础 / 张浩军等编著. -- 北京 : 中国水利水电出版社, 2011.10
21世纪高等学校精品规划教材
ISBN 978-7-5084-8940-7

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息系统－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2011)第172582号

策划编辑：雷顺加　责任编辑：张玉玲　加工编辑：孙　丹　封面设计：李　佳

书　名	21 世纪高等学校精品规划教材 **信息安全技术基础**
作　者	张浩军　杨卫东　谭玉波　等编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市鑫金马印装有限公司
规　格	184mm×260mm　16 开本　12 印张　289 千字
版　次	2011 年 10 月第 1 版　2011 年 10 月第 1 次印刷
印　数	0001—4000 册
定　价	22.00 元

前　言

信息作为一种资源和交流的载体，在现代社会发展中发挥着重要作用。信息在产生、加工、传递和使用过程中面临着各种安全威胁，信息可能丢失，可能被非授权用户获取、使用。随着计算机和网络应用的普及，人们的生活和工作越来越离不开计算机和计算机网络，随之而来的信息安全问题也更加突出。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，病毒通过网络肆虐，网络资源可能被滥用等，这些已经成为影响国家政治稳定、经济发展、军事对抗的重要方面。信息安全已成为国家、政府、部门、组织、个人都非常重视的问题。

信息安全涉及计算机科学与技术、密码学、数学、通信工程等学科专业领域，已成为一门交叉学科。同时，信息安全保障不仅是一个技术问题，还涉及人、管理、制度、法律等众多层面。本书为读者介绍信息安全技术的基本背景、原理与应用，本书编写不求大而全，而是突出网络环境下的信息安全保障体系的建立和相关技术，面向实用，力求向读者诠释“什么是信息安全”、“如何构建信息安全保障体系”、“信息安全有哪些主要技术和如何应用”等问题。

本书适合计算机、通信、电子商务等大专院校相关专业的信息安全课程使用，也可以作为从事计算机、网络工程项目建设与运行维护的技术人员的工具参考书。本书面向应用，全面地介绍了实现和保障信息安全的各种技术和手段，透视了各种信息安全技术的实现机理与方法，帮助读者掌握信息安全基本概念，建立起对信息安全较全面的、系统的认识，掌握信息安全技术应用，解决实际工作中的信息安全工程问题。同时，本书编者希望与读者一起对这些技术的设计开发理念、创新思想进行剖析，产生共鸣，启发我们的创新思维。

本书以网络环境下的信息安全保障技术为主线，力求全面刻画信息安全保障体系，介绍安全保障与防御的各种具体技术，重点突出以密码技术为基础的安全机制与服务。本书共分11章。第1章描述常见的信息安全威胁实例，通过列举一些影响深刻的典型信息安全案例，归纳出信息安全事件分类，为读者建立起信息安全的基本概念，圈定信息安全问题的讨论范畴。第2章从信息本身、信息载体、信息环境角度总结信息安全范畴，刻画保密性、完整性、鉴别性等信息安全属性；介绍信息安全保障体系结构，并给出闭环式具有动态适应性的信息安全防御模型；介绍信息安全等级保护与风险评估的相关标准与过程；为读者建立起信息安全工程思想与方法。密码技术是实现信息安全服务中保密性、完整性、鉴别性、抗抵赖性等安全属性的基础性关键技术。第3章介绍密码术的基本概念和发展，数据保密通信模型，抽象介绍对称密码体制、公钥密码体制、数字签名体制，以及基于密码技术实现消息完整性保护和认证等服务，最后简单介绍密码技术的理论支撑——计算复杂理论。第4章详细介绍两种典型对称密码算法DES、AES的实现，并简单介绍了IEDA、RC4等其他几个著名的对称密码算法，介绍了分组密码工作模式，使读者了解现代对称加解密算法的实现机理，掌握对称密码的应用。第5章详细介绍著名的RSA、ElGamal和基于椭圆曲线的公钥密码算法，使读者了解公钥密码算法的实现机理，掌握公钥密码的应用，以及密码技术应用中必须解决的密钥分发与管理问题。第6章介绍了对称密钥管理，详细介绍了基于数字证书的公钥密码中的密钥管理技术——公钥基础

设施 PKI，密码技术使得在开放的网络环境下实现实体认证和数据保密通信成为可能。第 7 章介绍基于密码技术实现网络环境下数据安全通信的典型协议——虚拟专用网协议 IPSec 和传输层安全 TLS 协议，以解释在网络层、传输层不同协议层上实现对等实体相互认证以及数据保密通信的方法。第 8 章以特殊的无线局域网 WLAN 环境为背景，介绍了典型的 IEEE 802.11 定义的健壮网络安全以及我国 WAPI 无线局域网的安全基础架构。第 9 章介绍非密码的网络防御技术、包括基于主机和端口的扫描技术、隔离内外网络的防火墙技术、基于模式及规则匹配的入侵检测技术，以及建立诱导系统发现攻击和系统脆弱性的蜜罐技术、第 10 章介绍数字隐藏和数字水印技术。第 11 章介绍基于信任模型的可信计算技术，重点介绍可信计算平台的工作原理和实现。

本书由河南工业大学张浩军教授、杨卫东博士、谭玉波博士、王峰博士共同编写。其中张浩军编写第 4～6 章和第 8 章，并负责全书统稿；杨卫东编写第 1～3 章；谭玉波编写第 7、10、11 章；王峰编写第 9 章。此外，范学辉、赵保鹏、齐庆磊、吴勇、易红、赵玉娟、程立、王雪涛、尹辉、程凤娟、王晓松、李国平等在本书的编写、素材整理、校对等过程中做了大量工作，在此表示感谢。本书编写工作受到河南省青年骨干教师资助计划、河南工业大学高层次人才引进计划项目（150269）、河南省精品课程“计算机网络技术”、河南省教育科学“十一五”规划 2010 年度课题等项目资助。

本书编者诚挚欢迎广大读者和各界人士批评指正本书中的错误和不妥之处并提出宝贵的建议，欢迎就相关技术问题进行切磋交流，作者联系方式：zhj@haut.edu.cn。

编　者

2011 年 8 月

目　　录

第 1 章　绪论

本章学习目标

本章介绍了信息安全问题的产生及其重要性、信息系统面临的威胁及分类，通过本章的学习，读者应该掌握以下内容：

- 信息安全基本概念和范畴。
- 信息及信息系统面临的安全威胁。
- 安全事件的分类。

1.1　信息安全问题及其重要性

在网络世界中我们的信息安全吗?

信息作为一种资源和交流的载体，具有普遍性、共享性、增值性、可处理性和多效用性，对人类社会发展具有特别重要的意义。当然，我们这里讨论的是计算机中存储和处理的、在网络中传递的信息——以各种形式存在的数据。信息安全的实质就是要保护信息系统和信息网络中的信息资源免受各种类型的威胁、干扰和破坏。保护信息安全性应贯穿信息生命周期的各个环节——信息的产生、存储、处理、传递、使用等，以及保护信息各种形态的安全性。

什么是信息系统（Information System）呢？按照信息安全事件分类分级指南（GB/Z20986-2007）国家标准定义，信息系统是由计算机及其相关和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。信息安全事件（Information Security Incident）则指由于自然或者人为以及软硬件本身缺陷或故障，对信息系统造成危害，或对社会造成负面影响的事件。因此，保障信息安全就是要查找、防范、阻断引起危害和影响的潜在威胁。因此，信息安全是指信息系统的硬件、软件及系统中的数据受到保护，不受偶然的因素或者恶意的行为而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。

随着计算机、网络的日益广泛应用，人们的生活和工作越来越离不开计算机和计算机网络，人们把繁多且复杂的事情托付给计算机来完成，敏感信息正在通过脆弱的通信线路在计算机系统之间传送，隐私信息在计算机内存储或在计算机之间交换，机密的电子商务信息正在被不安全地存储和传送，个人隐私信息正在被无数的恶意软件窥视，所有这一切让我们使用计算机和网络时心惊胆战，问题的关键是如何防范非授权用户非法获取（非授权访问）这些敏感（重要）信息。然而网络的开放性、自主/自由性、无组织性使这些信息安全问题更为突出。

我们经常可以听到或看到各种信息安全事件的报道，例如，使用聊天软件、访问挂马网站导致用户的账户等敏感信息泄露，网上交易遭遇虚假商家致使资金被骗，病毒和木马泛滥，影响我们的计算机系统正常工作或窃取我们的私密信息。最近几年，个人隐私通过网络外泄的几率正在增加，“日记门”、人肉搜索，人人都有可能因为隐私泄露而在网络上一夜“走红”。

先让我们看一些近期发生的信息安全重大事件。

“维基解密”风波

2010 年上演的愈演愈烈的“维基解密”风波，更加暴露信息安全问题的严峻。2010 年维基解密网站（WikiLeaks）连续三次大规模公开美国军事外交机密，包括 9 万份阿富汗战争文件、40 万份伊拉克战争文件、25 万份秘密外交电报，对美国军方机构的“情报安全和运作安全”构成了严重的威胁。2009 年，该网站公布了超过 1000 封英格兰东安格利亚大学气候研究所的邮件内容，邮件内容显示，气候学家擅自更改对自己研究不利的气候数据，以证明全球气候变暖主要是由人类活动造成的，此事导致人们对全球变暖理论产生怀疑，影响极其恶劣，外界纷纷指责科学家操纵研究结果的行为。

Stuxnet 蠕虫攻击伊朗核电厂事件

2010 年最受安全产业关注的议题恐怕是 Stuxnet 蠕虫（国内译成“震网”、“超级病毒”或“超级工厂”）攻击伊朗核电厂，大多数 Stuxnet 的攻击目标出现在伊朗，引发意图破坏核设施的阴谋论说。毫无疑问的是，Stuxnet 是一款高度精良的恶意软件，其开发动用了大量时间、金钱、人力等方面资源，就冲击度而言，多数的使用者并未受到明显的影响，Stuxnet 虽然散布到世界上许多的系统中，但对几乎所有受到感染的系统来说，它并不是个大问题，它既不偷盗数据、不促销假防病毒软件，也不会大量传送垃圾信息，而是以特定供货商的系统监控与数据抓取软件 Simatic WinCC SCADA（Supervisorg Control And Data Acqusition）平台作为攻击目标。该系统主要被用作工业控制系统，能够监控工业生产、基础设施或基于设施的工业流程。类似的系统在全球范围内被广泛地应用于输油管道、发电厂、大型通信系统、机场、轮船甚至军事设施中。Stuxnet 蠕虫利用了 Windows 的四个零日攻击漏洞（撰写本书时微软已发布漏洞修复公告），Stuxnet 蠕虫利用这些安全漏洞攻破工业控制系统。赛门铁克提供证据称，Stuxnet 蠕虫的攻击目标是用于控制马达速度的频率转换器驱动程序。有媒体称这个蠕虫真正的目标是攻破核计划，因为许多 Stuxnet 蠕虫的感染事件都发生在伊朗，人们推测这个蠕虫主要把伊朗当作一个可能的目标。

国内网络安全现状

（下面的数据引自《南方都市报》）再转向国内，网络与信息安全形式不容乐观。安徽省通信管理局互联网安全处负责人对新闻媒体称，2010 年全省每个月都有几百家网站被黑客攻破。江苏省公安厅网监总队案件侦查科介绍，近年来，网络违法犯罪无论是破获案件数还是抓获犯罪分子数都呈上升趋势。从破获的案件看，案件类型在不断翻新。其中，网络诈骗、盗窃案件在网络犯罪案件中占了八成以上，仅江苏 2010 年网络诈骗立案就超过 2000 起，包括股票类网站诈骗、购物网站诈骗、中奖诈骗、虚假信息视频聊天诈骗等多种类型。网络盗窃则发展到利用钓鱼网站虚假页面盗窃支付平台密码进而转移支付资金，以及用木马植入电脑替换支付链接直接将受害人的钱财转移至犯罪分子账户的盗窃新形式。来自国家互联网应急中心（CNCERT）和中国互联网络信息中心的年度报告显示，2010 年上半年，CNCERT 接收 4780 次网络安全事件报告，同比增加 105%。而在过去一年，中国半数网民曾遭遇过网络安全事件，

全年处理安全事件所支出的服务费用共计153亿元人民币，网民对网络的安全感开始降低。

“维基解密”暴露了信息安全保障的严重问题，网络上各种类型的攻击、破坏甚至犯罪呈上升趋势。针对日益严峻的网络安全事件，为了遏制黑客袭扰不断升级的现象，美国联邦政府实施了代号为“爱因斯坦”的网络安全工程，整个项目将持续数年。美国国土安全部表示，本次接受改造的互联网接入系统不仅涉及军方网站，未来美联邦政府雇员的所有网络活动（如浏览网页和收发电子邮件）都将使用特别打造的安全网络。届时，美国联邦政府设在互联网上的2400多处“接入点”将处于严密保护之下，从而防止黑客盗取各类敏感信息。不过，此举也引发了一些人的顾虑，并担心它可能会侵害联邦政府雇员的隐私权。

“Stuxnet蠕虫攻击事件”显现了计算机病毒、蠕虫等恶意软件更为严峻的威胁，病毒等恶意软件对计算机系统或信息系统的攻击并不少见，但一般目的是盗窃用户账号或其他隐私信息，或者影响用户系统正常工作，或者破坏文件、应用软件等。而Stuxnet蠕虫攻击具有僵尸网络等更多种恶意软件的特性，且针对性极强。有人称Stuxnet预告了恶意软件威胁影响“真实世界”机构新时代的来临，这也许有些言过其词了。其实，早在2003年，Slammer蠕虫就打击了俄亥俄州一个核能机构，并关闭了一个监视系统。而DOWNAD\Conficker蠕虫攻击了多个高知名度机构，如医院（甚至影响了MRI磁核共振造影）、执法单位，甚至是军事机构。从Stuxnet事件中我们可以看到，Stuxnet攻击的“软”目标皆未受到良好的防护，可能正是因为它们位于网络的“内部”，被认为其区域防护已足够了，然而事实证明，往往网络的安全性取决于其最弱的环节。Stuxnet事件提示了企业控制内部网络系统中的计算机和网络都需要全面强化。

而国内统计的信息安全事件及其造成的危害与损失越来越突出。信息安全事件不仅危及公共安全、政治稳定、企业竞争，更关系到广大网民的切身利益。近年来，以微软操作系统为首的操作系统以及各种应用软件漏洞已经成为病毒木马发起攻击的主要途径，包括Adobe、IE等使用量很大的知名软件都经常被病毒木马利用。

由此可见，信息安全问题已经成为上至国家、政府、企业、组织，下至每个使用计算机和网络的个人都需要关注和面对的现实问题。

1.2 信息安全威胁实例

在使用信息产品和基础设施时，我们面临哪些威胁?

上面我们列举了一些重大信息安全事件，以及身边发生的许多信息安全实例。不难看出，信息在存储、处理和交换过程中，都存在泄密或被截获、窃听、篡改、伪造的可能性，信息系统面临着其所涉及的各个环节的安全保护问题，包括信息的载体，如计算机、手机等终端设备，以及构成网络通信基础设施的各种网络设备和服务平台等。

那么，我们在使用信息系统时，到底面临哪些安全问题呢？或者说面临哪些威胁呢？直观地看，作为一个计算机用户或单位的网络管理员可能会担心如下的安全威胁：

- 我的计算机是否感染了病毒或木马？——造成系统工作不稳定，工作速度缓慢，经常出现死机，而此时我又忘记保存正在录入的文档，系统内数据或文件莫名奇妙丢失，系统中的重要口令、文件或数据被通过网络传输出去，系统经常从网络中下载莫名其

妙的文件等。

- 我在网络中传输的数据是否会被别人看到、截获（拦截）、篡改？——我通过网络把一份重要文件传递给一位商业伙伴，文件能安全、正确地被接收吗？
- 我从网络中接收到的数据确实来自我所信任或期望的发送者吗？我能确信接收到的数据是正确的（没有被篡改、不是伪造的）吗？

一个假想的例子：

假设某大学张教授准备通过网络给王教授发送一份期末考试试卷的电子文档，而我们的某一位同学李某是一位计算机天才、网络技术高手，他试图通过网络截获这份考卷。我们的张教授会担心以下问题：试卷通过网络传输，是否会被李同学监听到并看到试卷的全部或部分内容（保密性问题）；试卷在传输过程中是否被李同学篡改过（完整性问题），他把不会做的题目换成了简单的题目；王教授能够确定这份试卷来自张教授而不是李同学调换的往届试卷（可认证性）吗；张教授发送了这份试卷但事后否认此事，或者王教授接收到这份试卷事后否认已经收到了这份试卷（不可否认性或抗抵赖性）。天哪，张教授最后决定亲自上门把试卷送到王教授手中。

这些问题是我们在使用网络传输数据时需要考虑的，当然在具体应用中还有其他安全问题需要一并考虑，如网络上电子交易中的匿名性、可追溯性、公平性保障等。

- 我单位内部网络是否遭到入侵？单位内部服务器（面向内部应用）是否受到非法访问（非授权人员访问）？我单位内部数据库系统是否受到非法访问？数据是否被窃取或篡改？内部应用软件（如内部 OA 系统）是否被非法使用？
- 我单位的对外服务器是否受到破坏或干扰？服务器是否能够对外提供正常而稳定的服务？我单位网站的主页是否被篡改，主页文件是否被替换，网站上是否被非法外挂恶意代码？
- 我的计算机是否会被盗？保存有重要数据的移动硬盘或 U 盘丢失了怎么办？
- 我的办公室是否会漏水？供电不稳定或打雷会不会导致我的计算机损坏？
- 如果发生地震或洪水，我的办公楼如果倒塌了，我的计算机损坏了，重要的数据就会丢失。

上面列举了我们使用计算机和网络等信息系统时可能面临的一些安全威胁，也是我们在使用、管理我们的计算机、网络、软件、系统时需要认真考虑并加以防范的安全需求。

1.3 信息安全事件分类

上面列举了一些典型的安全威胁，如何系统地进行分类呢？信息安全事件分类分级指南（GB/Z20986-2007）国家标准中将信息安全事件分为 7 个基本分类，每个基本类型又分为若干子类，这些安全事件分类可以概括我们可能面临的信息安全问题，可以更系统地分析我们面临的安全事件。

1. 有害程序事件

有害程序事件是指蓄意制造、传播有害程序（或称恶意代码、恶意软件），或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序，危害系统中的数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行的程

序。有害程序事件又包括以下 7 个子类：

（1）计算机病毒事件。指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或在计算机程序中插入的一组计算机指令或者程序代码，它可以破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制。

（2）蠕虫事件。指蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序。

（3）特洛伊木马事件。指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能。

（4）僵尸网络事件。是指利用僵尸工具软件形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序。

（5）混合攻击程序事件。指蓄意制造、传播混合攻击程序，或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其他系统的有害程序，可能兼有计算机病毒、蠕虫、木马、僵尸网络等多种特征。混合攻击程序事件也可以是一系列有害程序综合作用的结果，例如一个计算机病毒或蠕虫在侵入系统后安装木马程序，进而可能构建僵尸网络等。

（6）网页内嵌恶意代码事件。指蓄意制造、传播网页内嵌恶意代码，或是因受到网页内嵌恶意代码影响而导致的信息安全事件。网页内嵌恶意代码是指内嵌在网页中，未经允许由浏览器执行，影响信息系统正常运行的有害程序。

（7）其他有害程序事件。指不包含在以上 6 个子类之中的有害程序事件。

实际中，病毒、蠕虫、木马等有害程序有融合的趋势，即现在攻击者往往综合多种技术构造有害程序，因此有时通称恶意代码。

2. 网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件又包括以下 7 个子类：

（1）拒绝服务攻击事件。指利用信息系统缺陷或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，以影响信息系统正常运行为目的的信息安全事件。

（2）后门攻击事件。指利用软硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施攻击信息安全事件。

（3）漏洞攻击事件。指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。

（4）网络扫描窃听事件。指利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件。

（5）网络钓鱼事件。指利用欺骗性的计算机网络技术，使用户泄漏重要信息而导致的信息安全事件。例如，利用欺骗性电子邮件获取用户银行账号和密码等。

（6）干扰事件。指通过技术手段对网络进行干扰，或对广播电视有线或无线传输网络进

行插播、对卫星广播电视信号非法攻击等导致的信息安全事件。

（7）其他网络攻击事件。指不包含在以上 6 个子类之中的网络攻击事件。

应该注意的是，这里所指的软硬件系统包括网络中的终端设备（如计算机、服务器、智能终端等），也包括网络通信设备（如路由器、交换机、防火墙等）。

3. 信息破坏事件

信息破坏事件是指通过网络或其他技术手段造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件又包括以下 6 个子类：

（1）信息篡改事件。指未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件。

（2）信息假冒事件。指通过假冒他人信息系统收发信息而导致的信息安全事件，例如网页假冒等导致的信息安全事件。

（3）信息泄漏事件。指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件。

（4）信息窃取事件。指未经授权的用户利用可能的技术手段恶意主动获取信息系统中的信息而导致的信息安全事件。

（5）信息丢失事件。指因误操作、人为蓄意或软硬件缺陷等因素使信息系统中的信息丢失而导致的信息安全事件。

（6）其他信息破坏事件。指不包含在以上 5 个子类之中的信息破坏事件。

4. 信息内容安全事件

信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括以下 4 个子类：

（1）违反宪法和法律、行政法规的信息安全事件。

（2）针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件。

（3）组织串联、煽动集会游行的信息安全事件。

（4）其他信息内容安全事件。

网络舆情及监测

互联网被公认为是“第四媒体”，成为反映社会舆情的主要载体之一。网络环境下的舆情信息来源包括新闻评论、BBS、博客、聚合新闻等。网络舆情表达快捷、信息多元、方式互动，具备传统媒体无法相比的优势。舆情是指在一定的社会空间内，围绕中介性社会事件的发生、发展和变化，民众对社会管理者产生和持有的社会政治态度。它是较多群众关于社会中各种现象、问题所表达的信念、态度、意见和情绪等表现的总和。网络舆情形成迅速，对社会影响巨大。

网络的开放性和虚拟性决定了网络舆情具有以下特点：直接性，通过 BBS、新闻点评和博客网站，网民可以立即发表意见，下情直接上达，民意表达更加畅通；突发性，网络舆论的形成往往非常迅速，一个热点事件的存在加上一种情绪化的意见，就可以成为点燃一片舆论的导火索；偏差性，由于发言者身份隐蔽，并且缺少规则限制和有效监督，网络自然成为一些网民发泄情绪的空间。在现实生活中遇到挫折、对社会问题片面认识等，都会利用网络得以宣泄。因此，在网络上更容易出现庸俗、灰色的言论。

因此，网络是把“双刃剑”，在提供下情上达的便捷方式的同时，也对国家政治安全和文

化安全构成了严重威胁，例如通过网络实施政治文化侵蚀，观念、生活方式可以便捷地渗透，网上思想舆论阵地的争夺战日趋激烈；传统的政治斗争手段在网上将以更高效的方式实现，利用网络串联、造谣、煽动将比在现实中容易得多，也隐蔽得多。

2010 年我国网络舆论关注度高的有重大灾难和事故、食品药品安全、卫生疫情防控、突发恐怖事件、生态环境污染等，如王家岭矿难、玉树地震、舟曲泥石流、上海特大火灾、金浩茶油致癌、山西问题疫苗、河南商城蜱虫咬人、校园袭童案、南京塑料厂爆炸、新疆阿克苏爆炸、大连漏油事故等。重大灾难和事故吸引全社会的关注，往往反映出社会矛盾的杂糅状态。2010 年度网络热点事件仍然集中在官民关系、警民关系、贫富关系、医患关系、城乡关系、劳资关系等，如辽宁庄河千人市政府下跪事件、“我爸是李刚”事件、安徽马鞍山局长打人、广州“咆哮哥”、山东新泰 23 岁副局长、湖南凤凰少女坠楼案、宝马反复碾压男童案、超女王贝整容致死事件、重庆大学生拒绝“农转非”、富士康员工跳楼事件等。

5. 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为地使用非技术手段有意或无意地造成信息系统破坏而导致的信息安全事件。设备设施故障又包括以下 4 个子类：

（1）软硬件自身故障。指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件。

（2）外围保障设施故障。指由于保障信息系统正常运行所必需的外部设施出现故障而导致的信息安全事件，例如电力故障、外围网络故障等导致的信息安全事件。

（3）人为破坏事故。指人为蓄意地对保障信息系统正常运行的硬件、软件等实施窃取、破坏造成的信息安全事件，或由于人为的遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏，影响信息系统正常运行的信息安全事件。

（4）其他设备设施故障。指不包含在以上 3 个子类之中的设备设施故障而导致的信息安全事件。

6. 灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括由水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

“911 恐怖袭击事件”引发的数据灾难

美国东部时间 2001 年 9 月 11 日上午，恐怖分子劫持的 4 架民航客机撞击美国纽约世界贸易中心和华盛顿五角大楼，美国纽约地标性建筑世界贸易中心双塔建筑被完全摧毁。此次恐怖袭击不仅造成两栋 400 米摩天大厦的坍塌，使 2000 余名无辜者不幸罹难，还彻底毁灭了数百家公司所拥有的重要数据。坐落在纽约的世贸中心，曾经是美国乃至全球财富的象征，在这座建筑群中，聚集了众多全球一流的大公司，不少是银行、证券和 IT 行业的翘楚，如世界著名的摩根-斯坦利公司、AT&T 公司、SUN 公司、瑞士银行等。在此次灾难之后的废墟中，深埋着 800 多家公司和机构的重要数据，其中许多公司的数据，特别是那些没有进行备份的数据永远无法恢复。国外的一项调查表明，因灾难而丢失关键数据，并且在几天内不能恢复关键业务的企业将会从市场上消失。对于依赖计算机系统运作的金融、电信、保险、民航、铁路和制造业而言，系统停机的可忍受时间更短。

随着大厦的轰然坍塌，无数人认为摩根-斯坦利将成为这一恐怖事件的殉葬品之一。然而，

该公司竟然奇迹般地宣布，全球营业部第二天可以照常工作。摩根-斯坦利公司之所以能够在9月12日恢复营业，其主要原因是它不仅像一般公司那样在内部进行数据备份，而且在新泽西州建立了灾备中心，并保留着数据备份。911恐怖袭击事件发生后，摩根-斯坦利公司立即启动新泽西州灾难备份中心，从而保障了公司全球业务的不间断运行。正是数据备份和远程容灾系统在关键时刻挽救了摩根-斯坦利公司，同时也在一定程度上挽救了美国的金融行业。然而许多其他企业并没有像摩根-斯坦利公司一样幸运。（摘自《金融电子化》2004年第3期）

7. 其他事件

其他事件是指不能归为以上6个基本分类的信息安全事件。

上述安全事件不是相互独立的，有的事件可能需要依赖其他事件而发生，或借助其他手段实施。如信息泄漏事件可能是借助病毒、蠕虫、特洛伊木马等有害的恶意软件获得敏感信息，也可能通过网络监听或者漏洞攻击等手段实施而获得非授权的信息访问。

显然，单一的保护措施很难完整地保证信息安全，必须综合应用各种保护措施，即通过技术、管理、行政的手段实现信源、信号、信息等各个环节的保护，以达到信息安全的目的。

信息安全事件的分级主要考虑三个要素：信息系统的重要程度、系统损失和社会影响。

（1）信息系统的重要程度是指信息系统所承载的业务对国家安全、经济建设、社会生活的重要性，以及业务对信息系统的依赖程度，可以将一个信息系统划分为特别重要、重要和一般三类。

（2）系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏导致系统业务中断，从而给事发组织造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失。

（3）社会影响是指信息安全事件对社会造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响，划分为特别重大、重大、较大和一般的社会影响。

谈到信息安全或网络安全，很多人自然而然地联想到黑客，实际上，黑客只是实施网络攻击或导致信息安全事件的一类主体，很多信息安全事件并非由黑客（包括内部人员或还称不上黑客的人）所为，同时也包括自然环境等因素带来的安全事件。因此，有必要阐明一下黑客的定义。

什么是黑客？

黑客一词，源于英文Hacker，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙，对这些人的正确英文叫法是Cracker，有人翻译成“骇客”。

*The New Hacker's Dictionary*一文中对Hacker的解释：那些喜欢发掘程序系统内部实现细节并延展自己的能力的人，这与只满足于学习有限知识的人是截然不同的；那些狂热地沉浸在编程乐趣中的人，他们喜爱编程而不仅仅在理论上谈及编程的人；那些能够体会侵入他人系统价值的人；那些擅长快速编程的人；特定程序的专家，经常使用这种程序或在上面工作，如UNIX黑客；一个专家或某领域热衷者，例如，可能是一个天文学黑客；一个喜欢智力挑战、创造性地突破各种环境限制的人；一个恶意的爱管闲事、在网络上逡巡溜达试图发现敏感信息的人。

有人这样区分黑客和骇客：黑客们建设，而骇客们破坏。这里我们不讨论到底哪种定义更准确，因为实施网络攻击或信息系统攻击的人的目的不同，很难用“好人”与“坏人”来区分，所以只要是有意窥探、干扰或破坏他人信息系统的人，我们更愿意使用攻击者（Attacker）来描述。

1.4　本书内容组织与使用指南

信息安全涉及计算机技术、网络技术、通信技术、密码技术、应用数学、信息论等技术与理论，已由数学、计算机科学与技术和通信工程等交叉形成了一门综合性学科。国内许多高校开设了信息安全本科专业，许多高校在计算机科学与技术、通信工程等硕士、博士点下开设信息安全方向。研究领域涉及现代密码学、计算机系统安全、计算机与通信网络安全、信息系统安全、电子商务/电子政务系统安全、信息隐藏与伪装等。

本书旨在介绍信息安全领域涉及的基础技术，主要面向计算机、通信、电子商务等本科专业，通过一门信息安全课程的学习，了解信息安全相关基础知识、技术，建立信息安全工程思想。本书在内容组织上力求知识的连贯性、关联性，便于读者形成系统性认识，较全面地了解和掌握信息安全保障涉及的技术，同时方便读者对感兴趣的技术领域进一步拓展学习。

本书的内容组织与体系：

第 1 章介绍信息安全问题产生的背景、定义和涵盖的内容。通过介绍典型的信息安全事件，使读者了解信息安全事件的分类，了解在使用信息系统时可能面临的安全威胁。

第 2 章从信息本身、信息载体、信息环境角度总结信息安全范畴，刻画保密性、完整性、鉴别性等信息安全属性；介绍信息安全保障体系结构，并给出闭环式具有动态适应性的信息安全防御模型；介绍信息安全等级保护与风险评估的相关标准与过程；为读者建立起信息安全工程思想与方法。

第 3 章介绍密码技术基本概念和发展。密码技术是实现信息安全服务中保密性、完整性、鉴别性、抗抵赖性等安全属性的基础性关键技术。本章介绍数据保密通信模型；抽象介绍对称密码体制、公钥密码体制和数字签名体制，以及如何基于密码技术实现消息完整性保护和认证等服务；最后简单介绍密码技术的理论支撑——计算复杂理论。

第 4 章详细介绍两种典型对称密码算法 DES、AES 的实现；简单介绍了 IEDA、RC4 等其他几个著名的对称密码算法；讨论了分组密码工作模式，使读者了解现代对称加解密算法的实现机理，掌握对称密码的应用。

第 5 章详细介绍著名的 RSA、ElGamal 和基于椭圆曲线的公钥密码算法，使读者了解公钥密码算法的实现机理，掌握公钥密码的应用。

第 6 章围绕密码技术应用中密钥分发与管理这一关键问题，介绍了对称密钥管理，详细介绍了基于数字证书的公钥密码中的密钥管理技术——公钥基础设施 PKI。

第 7 章介绍基于密码技术实现网络环境下数据安全通信的典型协议——虚拟专用网协议 IPSec 和传输层安全 TLS 协议。IPSec 和 TLS 分别在网络层、传输层不同协议层上运用密码技术在开放的网络环境下实现对等实体相互认证以及数据保密通信。

第 8 章以特殊的无线局域网 WLAN 环境为背景，介绍了典型的 IEEE 802.11 定义的健壮网络安全，以及我国 WAPI 无线局域网安全基础架构。

第 9 章介绍非密码的网络防御技术，包括基于主机和端口的扫描技术、隔离内外网络的防