全国高等院校应用型创新规划教材 计算机系列

计算机网络安全教程

付忠勇 赵振洲 乔明秋 主 编
刘亚琦 李焕春 胡晓凤 副主编

- 以基础知识—实用技术—项目实训为主线
- 理论与实际应用紧密结合，通过经典案例的讲解突出实用性
- 每章精心设置“小型案例实训”，旨在培养学生的实践能力
- 配备免费教学资源——电子课件、实验相关的软件及习题答案

清华大学出版社

全国高等院校应用型创新规划教材·计算机系列

计算机网络安全教程

付忠勇　赵振洲　乔明秋　主　编

刘亚琦　李焕春　胡晓凤　副主编

清华大学出版社

北 京

内 容 简 介

作为高等职业教育的教材，本书在介绍网络安全理论及其基础知识的同时，突出计算机网络安全方面的管理、配置及维护的实际操作手法和手段，并尽量跟踪网络安全技术的最新成果与发展方向。全书主要内容包括网络安全概述、数据加密和认证、常见网络攻击方法与防护、病毒分析与防御、防火墙技术、操作系统安全、Web 安全防范、无线网络安全、网络安全管理、项目实践等。各方面知识内容所占比例为：网络安全理论知识占 40%，操作系统安全知识占 10%，网络安全配置管理，操作维护方面的知识占 50%。

本书内容涵盖了网络安全的基础知识及其管理和维护的基本技能，它既可作为普通高等院校及高职院校安全、信息安全等相关专业的课程教材，也可作为各种培训班的培训教材，是一本覆盖面相当广泛的基础教材。

图书在版编目(CIP)数据

计算机网络安全教程/付忠勇，赵振洲，乔明秋主编. --北京：清华大学出版社，2017
(全国高等院校应用型创新规划教材 • 计算机系列)
ISBN 978-7-302-46175-3

Ⅰ. ①计… Ⅱ. ①付… ②赵… ③乔… Ⅲ. ①计算机—网络—网络安全—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 019944 号

责任编辑： 汤涌涛
封面设计： 杨玉兰
责任校对： 周剑云
责任印制： 宋　林
出版发行： 清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn, 010-62791865
印 装 者： 清华大学印刷厂
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　张：** 19.75　　**字　数：** 474 千字
版　　次： 2017 年 6 月第 1 版　　**印　次：** 2017 年 6 月第 1 次印刷
印　　数： 1～2000
定　　价： 45.00 元

产品编号：066827-01

前　言

随着信息社会的到来，Internet 迅猛发展，网络已经影响到社会生活的各个领域，给人类的生活方式带来了巨大的变革。人们在利用网络实现资源共享、电子商务等社会活动，享受网络给我们带来的便利同时，安全问题也变得日益突出。黑客入侵、网络病毒肆虐，网络系统损害或瘫痪，重要数据被窃取或毁坏等，给政府、企业以及个人带来了巨大的经济损失，也为网络的健康发展造成巨大的障碍。网络信息安全问题已成为网络技术领域的重要研究课题，已经成为一个组织生死存亡或贸易亏盈成败的决定性因素之一，因此信息安全逐渐成为人们关注的焦点。世界范围内的各国家、机构、组织、个人都在探寻如何保障信息安全的问题，各相关部门和研究机构也纷纷投入相当的人力、物力和资金试图来解决信息安全问题。

全书总共分 10 章，主要内容包括网络安全概述、数据加密和认证、常见网络攻击方法与防护、病毒分析与防御、防火墙技术、操作系统安全、Web 安全防范、无线网络安全、网络安全管理、项目实践。本书跟踪计算机网络安全技术的发展方向并吸取相关最新研究成果，主要讲述了网络安全理论及相关基础知识，同时也讲述了计算机网络安全方面的管理、配置及维护的实际操作手法和手段。

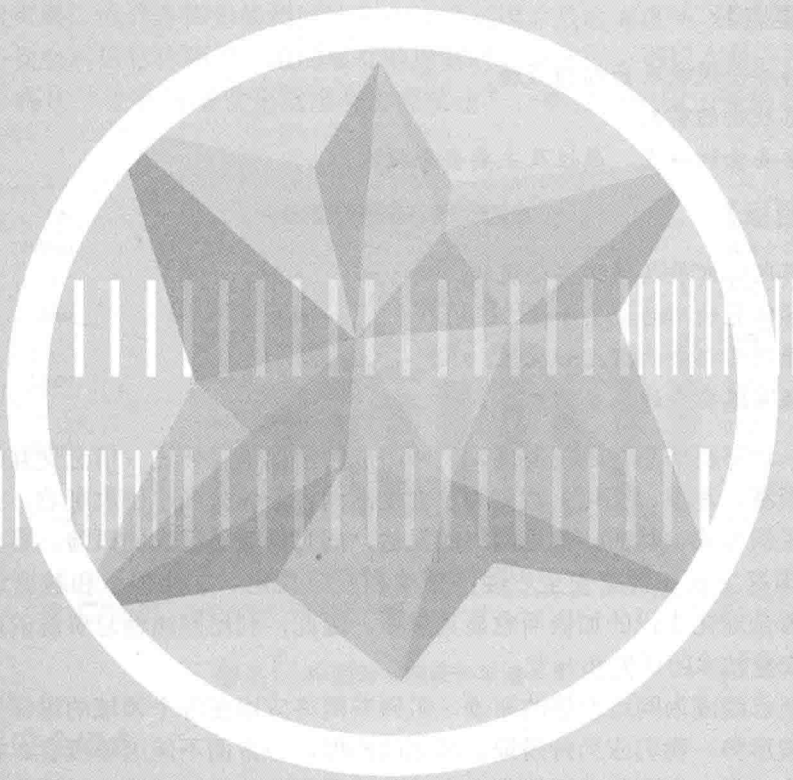
本书内容特色体现在以下 3 个方面：①通俗易懂。计算机网络的技术性很强，网络安全技术本身也比较晦涩难懂，本书力求以通俗的语言和清晰的叙述方式，向读者介绍计算机网络安全的基本理论、基本知识和实用技术。②突出实用。通过阅读本书，读者可掌握计算机网络安全的基础知识，并了解设计和维护网络及其应用系统安全的基本手段和方法。本书在编写形式上突出了应用的需求，每一章的理论内容都力求结合实际案例进行教学，第 10 章还设计了与前述章节内容配套的实训方案，从而为教学和自主学习提供了方便。③选材新颖。计算机应用技术和网络技术的发展是非常迅速的，本书在内容组织上力图靠近新知识、新技术的前沿，以使本书能较好地反映新理论和新技术。

本书由长期工作在教学的第一线的教师编写，他们都具有丰富的教学经验。其中第 1 章和第 9 章由付忠勇编写，第 2、3、4 章由乔明秋编写，第 5 章由李焕春编写，第 6 章由赵振洲编写，第 7 章由胡晓凤编写，第 8 章由刘亚琦编写，第 10 章由上述 6 位老师共同完成。全书由付忠勇、赵振洲负责内容的组织、统稿和审定。

限于水平，疏漏与谬误之处在所难免，恳请专家、同人及广大读者批评指教。

编　者

目录



第 1 章

网络安全概述

【项目要点】

- 网络安全现状及面临的威胁。
- 网络攻击的类别。
- 网络安全的特点、属性及主要安全技术。

【学习目标】

- 了解网络发展及网络安全现状。
- 了解常见的网络攻击手段。
- 掌握网络安全的特点和属性。
- 掌握网络安全的基本要素。

近年来，计算机信息技术的发展，使网络成为全球信息传递、信息交互的主要途径，并在政治、经济、军事、文化、教育等社会生活的各个领域产生巨大影响，迅速改变着人们的生产和生活方式。然而，信息网络的发达，同时伴随着巨大的风险。事实上，网络安全成为关系国家主权和国家安全、经济繁荣和社会稳定、文化传承和教育进步的重大问题，并且随着全球化步伐的加快而愈显其重要。因此，利用网络信息资源的同时，必须加强网络信息安全技术的研究和开发。

网络安全已经成为网络发展的瓶颈，阻碍着网络应用在各个领域的纵深发展。面对网络安全的严峻形势，我们应当持辩证、客观的态度，一方面不能因噎废食、拒绝先进的网络技术和文化，另一方面要对网络的安全威胁给予充分的重视。政府对网络安全技术的研发积极支持，普通网络使用者和网络服务提供商也应该充分认识网络安全及网络管理的重要性，保护好个人、集体和国家利益不受侵害。

构筑信息网络安全防线事关重大，刻不容缓。

1.1 网络安全现状

1.1.1 网络发展

20 世纪末，信息技术领域内最使人振奋的重大事件是互联网的发展，它已遍及 180 多个国家和地区。无论你身在办公室、家里、工地、野外、大街，抑或是你正在旅途中、海边，都可以与互联网亲密接触！无论你是在工作、学习、玩游戏还是炒股票，你都需要互联网！

据《第 37 次中国互联网络发展状况统计报告》统计，截至 2015 年 12 月，中国网民人数已经达到 6.88 亿，网民规模位居世界第一，全年共计新增网民 3951 万人。目前中国的互联网普及率已经达到 50.3%，比上年同期提高了 2.4 个百分点(见图 1-1)。互联网在中国的应用正逐步广泛化，越来越多的人接触到互联网，并从互联网世界获益。根据 CNNIC 统计，接触过互联网的人中，99%都会继续上网。

近几年，网络空间逐渐被视为继陆、海、空、天之后的“第五空间”，成为国际社会关注的焦点和热点。水能载舟，亦能覆舟。网络在方便和丰富人们生活的同时，使得网络

攻击活动有机可乘。世界各国纷纷将网络安全提升到国家战略高度予以重视，我国也不例外。中央网络安全和信息化领导小组的成立恰逢其时，习近平总书记在第一次会议上发表了重要讲话，指出“没有网络安全就没有国家安全”，彰显出我国加强网络安全保障的决心。

图 1-1　中国网民规模和年增长率

1.1.2　网络安全概念

国际标准化组织(ISO)将计算机网络安全定义为：“为数据处理系统建立和采取的技术与管理的安全保护，保护网络系统的硬件、软件及其系统中的数据不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠、正常地运行，网络服务不中断。”

上述计算机安全的定义包含物理安全和逻辑安全两方面的内容，其逻辑安全的内容可理解为我们常说的网络上的信息安全，是指对信息的保密性、完整性和可用性的保护。而网络安全性的含义是信息安全的引申，即网络安全是对网络信息保密性、完整性和可用性的保护。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。

网络安全应具有以下 5 个方面的特征。

- 保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 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。
- 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。
- 可控性：对信息的传播及内容具有控制能力。
- 可审查性：出现安全问题时能提供依据与手段。

当然，网络安全的具体含义会随着“角度”的变化而变化。比如，从用户(个人、企业等)角度，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和

真实性的保护，避免其他人利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用以及非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.1.3 网络安全现状

近年来，随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。国家互联网应急中心发布的《2015 年中国互联网网络安全报告》显示，2015 年互联网应急中心共接收境内外报告的网络安全事件 126 916 起，较 2014 年增长了 125.9%。其中，境内报告网络安全事件 126 424 起，较 2014 年增长了 128.6%；境外报告网络安全事件 492 起，较 2014 年下降 43.9%。发现的网络安全事件中，数量排前三位的类型分别是网页仿冒事件(占 59.8%)、漏洞事件(占 20.2%)和网页篡改事件(占 9.8%)。2015 年，互联网应急中心共成功处理各类网络安全事件 125 815 起，较 2014 年的 56 072 起增长 124.4%。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大的挑战，事实上，资源共享和安全历来是一对矛盾。在一个开放的网络环境中，大量信息在网上流动，这为不法分子提供了攻击目标。而且计算机网络组成形式的多样性、终端分布广和网络的开放性、互联性等特征更为他们提供便利。他们利用不同的攻击手段，获得访问或修改在网中流动的敏感信息，闯入用户或政府部门的计算机系统，进行窥视、窃取、篡改数据。不受时间、地点、条件限制的网络诈骗，其“低成本和高收益”又在一定程度上刺激了犯罪的增长，使得针对计算机信息系统的犯罪活动日益增多。

1.2 网络安全威胁

所谓网络安全威胁，是指对网络和信息的机密性、完整性、可用性在合法使用时可能造成的危害。

从人为(黑客)角度来看，常见的计算机网络安全威胁主要有信息泄露、完整性破坏、拒绝服务攻击、网络滥用。

- 信息泄露：信息泄露破坏了系统的保密性，信息被透露给非授权的实体。常见的能够导致信息泄露的威胁有网络监听、业务流分析、电磁截获、射频截获、人员的有意或无意、媒体清理、漏洞利用、授权侵犯、物理侵入、病毒、木马、后门、流氓软件、网络钓鱼。
- 完整性破坏：可以通过物理侵犯、授权侵犯、病毒、木马、漏洞等方式来实现。
- 拒绝服务攻击：对信息或资源可以合法地访问却被非法的拒绝或者操作延迟等与

时间密切相关的操作。

- 网络滥用：合法的用户滥用网络，引入不必要的安全威胁，包括非法外联、非法内联、移动风险、设备滥用、业务滥用。

常见的计算机网络安全威胁的表现形式主要有窃听、重传、篡改、拒绝服务攻击、行为否认、电子欺骗、非授权访问、传播病毒。

- 窃听：攻击者通过监视网络数据的手段获得重要的信息，从而导致网络信息的泄密。
- 重传：攻击者事先获得部分或全部信息以后，将此信息发送给接收者。
- 篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再将伪造的信息发送给接收者，这就是纯粹的信息破坏，这样的网络侵犯者被称为积极侵犯者。积极侵犯者的破坏作用最大。
- 拒绝服务攻击：攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务。
- 行为否认：通信实体否认已经发生的行为。
- 电子欺骗：通过假冒合法用户的身份来进行网络攻击，从而达到掩盖攻击者真实身份、嫁祸他人的目的。
- 非授权访问：没有预先经过同意，就使用网络或计算机资源，被看作非授权访问。
- 传播病毒：通过网络传播计算机病毒，其破坏性非常高，而且用户很难防范。

当然，除了人为因素，网络安全在很大部分上还由网络内部、安全机制或者安全工具本身的局限性所决定，主要表现在：每一种安全机制都有一定的应用范围和应用环境、安全工具的使用受到人为因素的影响、系统的后门是传统安全工具难于考虑到的地方、只要是程序就可能存在 Bug。而这一系列的缺陷，更加给想要进行攻击的人以方便。因此，网络安全问题可以说是由人所引起的。

1.3　网 络 攻 击

1.3.1　潜在的网络攻击者

潜在的网络攻击者有以下几种情况。

(1) 国家：组织精良并得到很好的财政资助。

(2) 黑客：攻击网络和系统，企图探求操作系统的脆弱性或其他缺陷的人们，如能解密者、行为不良者、剽窃者、电话黑客。

(3) 计算机恐怖分子：国内外代表各种恐怖分子或极端势力的个人或团体。

(4) 有组织犯罪：有组织和财政资助的犯罪团体。

(5) 其他犯罪成员：犯罪群体的其他部分，单独行动的个人。

(6) 国际新闻机构：收集和发布消息，其行为包括收集关于任何人和事的情报。

(7) 商业竞争(工业竞争)：在竞争市场中的国内外公司或集团。

(8) 不满的雇员：对公司或集团不满的人，能够对系统实行内部威胁。

(9) 不小心或未受到良好训练的雇员：缺乏训练、操作失误、对安全认识不足的人。

1.3.2 网络攻击的种类

1. 被动攻击

监视网络上的信息传送，包括监视明文，解密加密不善的通信数据，口令嗅探等。可通过通信量分析获取通信模式。

抵抗：使用 VPN, 加密。

2. 主动攻击

企图避开或打破安全防护，引入恶意代码以及转换数据或破坏系统的完整性。

(1) 修改传输中的数据：如在金融领域，改变交易的数量或将交易转移到别的账户。

(2) 替换：插入数据，重放。

(3) 会话劫持：未授权使用一个已经建立的会话。

(4) 伪装成授权的用户或服务器：通过实施嗅探或其他手段获得用户/管理员信息，然后使用该信息作为一个授权用户登录，同样可对服务器实施攻击。

(5) 获取系统应用和操作系统软件的缺陷：攻击者探求运行操作系统和应用软件中的脆弱性，如 Windows 95 和 Windows NT 都存在许多漏洞。

(6) 攫取主机或网络信任：攻击者通过操作文件使远方主机提供服务，从而攫取传递信任，知名的攻击有 rhost 和 rlogin。

(7) 获得数据执行：攻击者将恶意代码植入看起来无害的供下载的软件和电子邮件中，从而使用户执行该恶意代码。恶意代码可用于破坏和修改文件，特别是包含权限参数和权限值的文件。如 PostScript、Active- X 和微软的 Word 宏病毒等。

(8) 恶意代码插入并刺探：通过先前发现的脆弱性并使用该访问来达到攻击。例如：使用特洛伊木马、陷门。黑客工具如：Rootkit(http://www.rootshell.com 可下载其他很多的黑客工具)，具有总控能力，包括插入脚本，获取根权限。

(9) 拒绝服务：在网络中扩散垃圾包以及向邮件中心扩散垃圾邮件等。

3. 邻近攻击

未授权者在物理上接近网络系统或设备，目的是修改、收集或拒绝访问信息，这种接近可以秘密进入、公开接近或二者皆有之。

(1) 修改数据或收集信息：攻击者获取对系统的物理访问，如 IP 地址、登录的用户名和口令等，从而修改和窃取信息。

(2) 物理破坏：获得对系统的网络访问，导致对系统的物理破坏。

4. 内部人员攻击

这些内部人员要么被授权在信息安全处理系统的物理范围内，要么对信息安全处理系统具有直接访问权，常常是最难检测和防范的。如不明身份的清洁人员(下班后的物理访问)、授权的系统用户和恶意的系统管理员。其攻击方式有以下几种。

(1) 修改数据或安全机制：攻击者常常对信息具有访问权，他们进行未授权操作或破坏数据(他们知道系统布局、有价值的数据在何处以及何种安全防范系统在工作)。

(2) 建立未授权网络连接：对机密网络具有物理访问能力的用户，未授权连接到一个低机密级别或敏感网络中。

(3) 秘密通道：建立未授权的通信路径，用于从本地区域向远程传输盗用信息。

(4) 物理损坏或破坏：攻击者赋予的物理访问权。

对付方法：安全防范意识和训练，审计和入侵检测，关键数据、服务的访问控制，强身份识别与认证。

5. 分发攻击

分发攻击是指在软件和硬件开发出来之后和安装之前这段时间，当它从一个地方传送到另一个地方时，攻击者恶意修改软硬件。

(1) 在制造商的设备上修改软件、硬件：在生产线上流通时，修改软、硬件配置。

(2) 在产品分发时修改软/硬件：在分发期内修改软硬件配置，如在装船时安装窃听设备。

对付方法：在产品中加密签名，严格管理等。

1.4　网络安全的特点及属性

1.4.1　网络安全特点

一个系统是否安全，依赖它所应用的环境、应用的目的、外在的威胁等多种因素；网络安全问题虽然是随着互联网的发展出现的，但似乎和现实安全问题一样，将会是一个永恒的问题，其具有鲜明的特点。

1. 攻击与防守的不对称性

实施网络安全威胁的攻击者，通常会突破网络默认的规则，利用攻击工具或系统软件、应用软件以及协议上的漏洞，或者通过勾结内部人员等达到攻击目的。

攻击是有备而来的，在当前的网络环境下，攻击工具较容易获得，攻击风险低、追踪难。对于防卫人员来说则恰恰相反，意味着必须堵住所有可能的漏洞，否则整个防御就可能毁于一旦。

如果把安全问题比作一段链条，最脆弱的一环可以使整个链条断裂。不断增加的网络复杂性使得安全防护的难度日益增大，100%的绝对网络安全根本难以做到。

攻击可以攻其一点，防守却要全面防御；受到攻击几乎是必然的，而保证安全却是相对的；很多攻击者具有专业知识和经验，而大部分用户却只会基础应用，这是很不对称的。

2. 网络安全的动态特性

网络安全威胁是变化的。

无论我们采取了多么先进的技术来进行安全防范，但随着时间的推移，操作系统、硬件平台、应用软件、网络协议等都会不断更新，在这个过程中，原来存在的一系列安全问

题都发生着变化，如旧的漏洞可能不存在或者不重要了，但新的漏洞又出现了。为了应付新的安全风险，网络安全防范也永远处于动态之中，因此，不可能存在一劳永逸的技术或解决方案。

3．攻击与防御的经济性问题

在网络安全方面，投入的代价既可能是资金、人力，也可能是时间、易用性。

网络安全在很大程度上依赖于投入。为了让信息系统更安全，可能需要使用很多安全设备和技术，雇用许多安全专业人员。所以，拥有的资源越多，就越可能达到更好的安全程度。

但这里就有一个矛盾：假设要保护的资产价值为 M，而安全投入为 m。如果 $m<M$，可能系统的安全程度不够；如果 $m>M$，或者 m 接近 M，则安全投入就失去了意义。同样，这个矛盾对于攻击者也存在，攻击的代价如果超过了攻击者的获益，也是没有意义的。

并且，信息服务的本质是开放性的，或者是部分开放，或者是完全开放。例如，提供检索的搜索引擎、新闻网站、各种公共信息网站是面向所有用户的，企业信息是针对部分对象，如企业与企业之间，企业对用户、企业对内部职员等。而采取各种网络防范措施就意味着限制这种开放性，必然给使用带来不便。

一般情况下，谁拥有的资源(技术能力、专业人员等)更多，谁就更有可能占上风。但很多时候却相反，系统越复杂，漏洞也越多，实施的网络攻击更容易奏效。因此，以合理的代价达到一定程度的网络安全是网络安全策略的出发点。

从这个意义上来讲，各种网络安全技术及措施，其目的是使得攻击的成本加大，增强用户的安全感，并且不至于使系统太烦琐而难以使用。

4．人是网络安全问题的核心

实际上，不管我们采取怎样的安全防护技术，最根本的还是人，安全问题的根源在于人性的弱点，不论是攻击者还是防卫者。

攻击者的动机包括获取利益、好奇心、出名、发泄、政治或军事原因等，这些动机和导致社会问题的动机是一样的。

而对于防卫者来说，弱点则是麻痹和懒惰。每当一场危机来临的时候，如洪水、瘟疫发生时，人们的安全意识会很快上升，甚至会达到风声鹤唳、草木皆兵的程度。遗憾的是，危机一过，人们很快就会恢复到常态，直到下次危机才又被唤醒。

网络安全也一样。可以预料，只要人性的弱点存在，不管安全技术如何发展，安全问题总是存在并不断变化的。唯一能够确定的是，永远没有100%的网络安全。既然如此，我们为什么还要讨论网络安全技术呢？

现实社会中虽然有假钞，信用卡也会被偷窃，但人们仍然在大量使用，这是因为技术进步带来的方便程度超过了可能的损失。人们会在家里安装防盗门、保险柜等，虽然不能万无一失，但大部分情况下仍能起作用，并给人们带来安全感。

因此，通过网络安全技术管理手段，最大限度地减少风险，增加攻击者的成本，给用户带来安全感，并使正常的交易、业务能够进行下去，就是网络安全防御的目标。

安全没有绝对的、统一的标准，因为每个人的利益是不同的，每个组织或单位的利益也是不同的；一个系统是否安全，取决于它所采取的安全措施是否实现了既定的安全政策

(Security Policy)。

网络安全更多地被作为一个技术问题来研究。但是不管这种技术看起来是多么的完善，必须要有人的参与，配合以良好的安全管理措施，才能够较好地发挥作用。因此，建立(健全)安全意识、强化管理更为重要。

1.4.2　安全属性

安全属性的相关术语及其含义如下。

保密性/机密性：信息的内容不被未授权的人获取。

数据完整性：数据传输或存储过程中不被未授权的篡改或破坏。

可用性：即便是在故障或受攻击时也能提供有效的服务。

真实性：通信双方的身份，消息的来源应该真实。

授权与访问控制：合法的用户，有不同的访问权限。

抗抵赖/不可否认：交易双方任何人不能否认已经发生的交易。

可追查性：可以追踪到消息的来源(责任人)。

可生存性/抗毁性：在部分被摧毁的情况下，其余的部分还能够维持运转。

私密性/隐私：个人的隐私信息(比如上网记录)不被泄露。

可控性：对不良信息进行屏蔽的能力。

1.4.3　如何实现网络安全

1. 什么是安全政策

安全政策是一个组织为了实现其业务目标而制定的一组规定，用来规范用户的行为，指导信息资源的保护和管理。

安全政策应该表现为一份或一系列正式的文档。

安全政策规定了用户什么是该做的、什么是不该做的。

2. 安全政策举例

校园网安全政策举例：

① ××大学计算机信息系统及校园网安全与保密管理暂行规定。

② AUP(Accessible Usage Policy)，入网协议。

③ 防火墙政策。

④ 口令政策。

1.5　网络安全技术

1.5.1　网络安全基本要素

1. 双向身份认证

双方通信前证明对方的身份与其声明的一致，建立带有一定保障级别的实体身份。