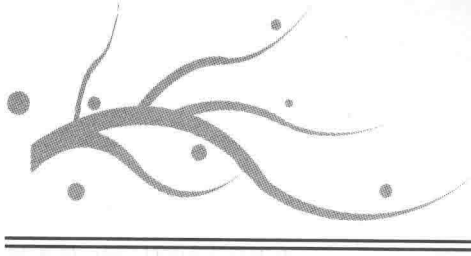
高职高专计算机任务驱动模式教材

网络安全实用项目教程

贾如春　沈　洋　库德来提·热西提　主　编

杨　云　崔　鹏　张晓珲　副主编

清华大学出版社



高职高专计算机任务驱动模式教材

网络安全实用项目教程

贾如春　沈　洋　库德来提·热西提　主　编

杨　云　崔　鹏　张晓珲　副主编

清华大学出版社

北京

内 容 简 介

本书基于“项目导向、任务驱动”的项目化教学方式编写而成，体现了“基于工作过程”的教学理念。

全书在基于全国职业院校技能大赛网络信息安全的项目基础上，融入了基于国家社科学基金科研项目青年项目：基于维哈柯文信息的电子数据司法鉴定问题研究(编号：13CFX055)的成果。从中分解成多个项目的任务环节，其中包括认识网络安全、网络攻击与防护、网络数据库安全、计算机病毒与木马防护、使用 Sniffer Pro 防护网络、数据加密、Windows Server 系统安全、防火墙技术、无线局域网安全和 Internet 安全与应用等内容。

本书可以作为计算机和通信专业的教材，也可作为信息安全专业和从事信息安全研究的工程技术人员的参考书。

图书在版编目(CIP)数据

网络安全实用项目教程/贾如春，沈洋，库德来提·热西提主编. --北京：清华大学出版社，2015
高职高专计算机任务驱动模式教材
ISBN 978-7-302-40759-1

Ⅰ. ①网… Ⅱ. ①贾… ②沈… ③库… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 161825 号

责任编辑：张龙卿
封面设计：徐日强
责任校对：刘　静
责任印制：杨　艳

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,010-62795764

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：19.25　　**字　　数**：438 千字
版　　次：2015 年 9 月第 1 版　　**印　　次**：2015 年 9 月第 1 次印刷
印　　数：1～2500
定　　价：38.00 元

产品编号：066233-01

编审委员会

出版说明

我国高职高专教育经过十几年的发展，已经转向深度教学改革阶段。教育部于2006年12月发布了教高〔2006〕第16号文件《关于全面提高高等职业教育教学质量的若干意见》，大力推行工学结合，突出实践能力培养，全面提高高职高专教学质量。

清华大学出版社作为国内大学出版社的领跑者，为了进一步推动高职高专计算机专业教材的建设工作，适应高职高专院校计算机类人才培养的发展趋势，根据教高〔2006〕第16号文件的精神，2007年秋季开始了切合新一轮教学改革的教材建设工作。该系列教材一经推出，就得到了很多高职院校的认可和选用，其中部分书籍的销售量都超过了3万册。现重新组织优秀作者对部分图书进行改版，并增加了一些新的图书品种。

目前国内高职高专院校计算机网络与软件专业的教材品种繁多，但符合国家计算机网络与软件技术专业领域技能型紧缺人才培养培训方案，并符合企业的实际需要，能够自成体系的教材还不多。

我们组织国内对计算机网络和软件人才培养模式有研究并且有过一段实践经验的高职高专院校，进行了较长时间的研讨和调研，遴选出一批富有工程实践经验和教学经验的双师型教师，合力编写了这套适用于高职高专计算机网络、软件专业的教材。

本套教材的编写方法是以任务驱动、案例教学为核心，以项目开发为主线。我们研究分析了国内外先进职业教育的培训模式、教学方法和教材特色，消化吸收优秀的经验和成果。以培养技术应用型人才为目标，以企业对人才的需要为依据，把软件工程和项目管理的思想完全融入教材体系，将基本技能培养和主流技术相结合，课程设置中重点突出、主辅分明、结构合理、衔接紧凑。教材侧重培养学生的实战操作能力，学、思、练相结合，旨在通过项目实践，增强学生的职业能力，使知识从书本中释放并转化为专业技能。

一、教材编写思想

本套教材以案例为中心，以技能培养为目标，围绕开发项目所用到的知识点进行讲解，对某些知识点附上相关的例题，以帮助读者理解，进而将知识转变为技能。

考虑到是以“项目设计”为核心组织教学，所以在每一学期配有相应的实训课程及项目开发手册，要求学生在教师的指导下，能整合本学期所学的知识内容，相互协作，综合应用该学期的知识进行项目开发。同时，在教材中采用了大量的案例，这些案例紧密地结合教材中的各个知识点，循序渐进，由浅入深，在整体上体现了内容主导、实例解析、以点带面的模式，配合课程后期以项目设计贯穿教学内容的教学模式。

软件开发技术具有种类繁多、更新速度快的特点。本套教材在介绍软件开发主流技术的同时，帮助学生建立软件相关技术的横向及纵向的关系，培养学生综合应用所学知识的能力。

二、丛书特色

本系列教材体现目前工学结合的教改思想，充分结合教改现状，突出项目面向教学和任务驱动模式教学改革成果，打造立体化精品教材。

(1) 参照和吸纳国内外优秀计算机网络、软件专业教材的编写思想，采用本土化的实际项目或者任务，以保证其有更强的实用性，并与理论内容有很强的关联性。

(2) 准确把握高职高专软件专业人才的培养目标和特点。

(3) 充分调查研究国内软件企业，确定了基于 Java 和. NET 的两个主流技术路线，再将其组合成相应的课程链。

(4) 教材通过一个个的教学任务或者教学项目，在做中学，在学中做，以及边学边做，重点突出技能培养。在突出技能培养的同时，还介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

(5) 借鉴或采用项目驱动的教学方法和考核制度，突出计算机网络、软件人才培训的先进性、工具性、实践性和应用性。

(6) 以案例为中心，以能力培养为目标，并以实际工作的例子引入概念，符合学生的认知规律。语言简洁明了、清晰易懂，更具人性化。

(7) 符合国家计算机网络、软件人才的培养目标；采用引入知识点、讲述知识点、强化知识点、应用知识点、综合知识点的模式，由浅入深地展开对技术内容的讲述。

(8) 为了便于教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务资源。在清华大学出版社网站(www. tup. com. cn)免费提供教材的电子课件、案例库等资源。

高职高专教育正处于新一轮教学深度改革时期，从专业设置、课程体系建设到教材建设，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并及时反馈给我们。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育继续出版优秀的高质量的教材。

清华大学出版社

高职高专计算机任务驱动模式教材编审委员会

2014 年 3 月

前　言

一、编写背景

近年来，高等职业技术教育得到了飞速发展，学校急需适合职业教育特点的网络安全课程的实用型教材，减少枯燥难懂的理论，取而代之的是安全建设网络、安全使用网络、安全管理网络等实际操作应用能力的培养与训练。我们基于全国职业院校技能大赛网络信息安全国赛项目，将项目内容分解为多个任务环节，通过任务来实现对相关知识点的理解和学习。

二、本书特点

本书是和四川福立盟信息技术有限公司合作共同编写的“工学结合”的网络安全项目化教材。全书共包含 10 个教学项目，最大的特色是“易教易学”。同时融合了国家社科学基金科研项目青年项目：基于维哈柯文信息的电子数据司法鉴定问题研究（编号：13CFX055）的成果。本书主要特点如下。

1. 体例上有所创新

“教学做一体”，创新编写模式。将“教材—项目案例—工程实践”对接，有机融合项目式教学。全书采用“项目导向、任务驱动”的编写方式，通过工程实例的学习增强读者对知识点和技能点的掌握。

教材大部分章按照“项目导入”→“职业能力目标和要求”→“相关知识点”→“项目实施”→ “拓展提升”→“习题”层次进行组织。

2. 内容上注重实用

全书共有 10 个项目：

项目 1　认识网络安全

项目 2　网络攻击与防护

项目 3　网络数据库安全

项目 4　计算机病毒与木马防护

项目 5　使用 Sniffer Pro 防护网络

项目 6　数据加密

项目 7　Windows Server 系统安全
项目 8　防火墙技术
项目 9　无线局域网安全
项目 10　Internet 安全与应用

三、教学大纲

参考学时 64 学时，其中实践环节为 32 学时，各项目的参考学时参见下面的学时分配表。

章　节	课 程 内 容	学 时 分 配	
		讲授	实训
项目 1	认识网络安全	4	2
项目 2	网络攻击与防护	4	4
项目 3	网络数据库安全	2	4
项目 4	计算机病毒与木马防护	6	6
项目 5	使用 Sniffer Pro 防护网络	4	4
项目 6	数据加密	4	4
项目 7	Windows Server 系统安全	2	2
项目 8	防火墙技术	2	2
项目 9	无线局域网安全	2	2
项目 10	Internet 安全与应用	2	2
课时总计		32	32

四、其他

本书是教学名师、企业工程师和骨干教师共同策划编写的一本工学结合教材。由贾如春、沈洋、库德来提·热西提担任主编，杨云、崔鹏、张晓珲担任副主编。贾如春编写项目 2、项目 9，沈洋编写项目 4，库德来提·热西提编写项目 5、项目 6、项目 8，崔鹏编写项目 1、项目 10，张晓珲编写项目 3、项目 7。杨云编写了大纲以及项目 6 和项目 7 中的部分内容，张晖、金月光、李明生编写了项目 5 的部分内容。

作者 E-mail：yangyun90@163.com。Windows 及 Linux 教师交流群：189934741。

编　者
2015 年 5 月

目 录

项目 1　认识网络安全 …… 1

1.1　项目导入 …… 1
1.2　项目分析 …… 1
1.3　相关知识点 …… 2
1.3.1　网络安全概念 …… 2
1.3.2　典型的网络安全事件 …… 3
1.3.3　信息安全的发展历程 …… 4
1.3.4　网络安全所涉及的内容 …… 5
1.3.5　网络安全防护体系 …… 7
1.3.6　网络安全模型 …… 9
1.3.7　网络安全体系 …… 10
1.3.8　网络安全标准 …… 10
1.3.9　网络安全目标 …… 11
1.4　项目实施 …… 12
任务 1-1　安装和使用 Wireshark …… 12
任务 1-2　TCP 协议的三次握手抓包分析 …… 23
任务 1-3　UDP 协议的抓包分析 …… 26
1.5　拓展提升　网络安全的现状和发展趋势 …… 28
1.6　习题 …… 29

项目 2　网络攻击与防护 …… 31

2.1　项目导入 …… 31
2.2　职业能力目标和要求 …… 31
2.3　相关知识点 …… 32
2.3.1　黑客概述 …… 32
2.3.2　常见的网络攻击 …… 32
2.3.3　社会工程学介绍 …… 38
2.3.4　网络安全解决方案 …… 38

2.4 项目实施 …… 42
任务 2-1 网络信息搜集 …… 42
任务 2-2 端口扫描 …… 42
任务 2-3 口令破解演示实验 …… 47
2.5 习题 …… 50

项目 3 网络数据库安全 …… 52

3.1 项目导入 …… 52
3.2 项目分析 …… 52
3.3 相关知识点 …… 53
3.3.1 数据库安全概述 …… 53
3.3.2 数据库的数据安全 …… 54
3.4 项目实施 …… 56
任务 3-1 数据库备份与恢复实训 …… 56
任务 3-2 SQL Server 攻击的防护 …… 58
任务 3-3 数据库安全检测工具的使用 …… 61
任务 3-4 SQL 注入攻击 …… 63
3.5 拓展提升 数据库安全解决方案 …… 66
3.5.1 SQL Server 数据库的安全保护 …… 66
3.5.2 Oracle 数据库的安全性策略 …… 67
3.6 习题 …… 68

项目 4 计算机病毒与木马防护 …… 69

4.1 项目导入 …… 69
4.2 职业能力目标和要求 …… 69
4.3 相关知识点 …… 69
4.3.1 计算机病毒的起源 …… 69
4.3.2 计算机病毒的定义 …… 70
4.3.3 计算机病毒的分类 …… 70
4.3.4 计算机病毒的结构 …… 72
4.3.5 计算机病毒的危害 …… 74
4.3.6 常见的计算机病毒 …… 75
4.3.7 木马 …… 76
4.3.8 计算机病毒的检测与防范 …… 76
4.4 项目实施 …… 78
任务 4-1 360 杀毒软件的使用 …… 78
任务 4-2 360 安全卫士软件的使用 …… 80
任务 4-3 宏病毒和网页病毒的防范 …… 84

任务 4-4 利用自解压文件携带木马程序 …… 88
任务 4-5 典型木马案例 …… 90
任务 4-6 第四代木马的防范 …… 110
4.5 拓展提升 手机病毒 …… 115
4.6 习题 …… 116

项目 5 使用 Sniffer Pro 防护网络 …… 118

5.1 项目导入 …… 118
5.2 职业能力目标和要求 …… 118
5.3 相关知识点 …… 118
5.3.1 网络嗅探 …… 118
5.3.2 蜜罐技术 …… 119
5.3.3 拒绝服务攻击 …… 120
5.4 项目实施 …… 121
任务 5-1 Sniffer Pro 安装 …… 121
任务 5-2 Sniffer 功能界面 …… 126
任务 5-3 Sniffer Pro 报文的捕获与解析 …… 130
任务 5-4 Web 服务器蜜罐攻防 …… 134
任务 5-5 部署全方位的蜜罐服务器 …… 136
任务 5-6 SYN Flood 攻击 …… 140
5.5 习题 …… 143

项目 6 数据加密 …… 145

6.1 项目导入 …… 145
6.2 职业能力目标和要求 …… 145
6.3 相关知识点 …… 145
6.3.1 密码技术基本概念 …… 145
6.3.2 古典加密技术 …… 146
6.3.3 对称加密及 DES 算法 …… 147
6.3.4 公开密钥及 RSA 算法 …… 152
6.3.5 数字证书 …… 155
6.3.6 公钥基础设施(PKI) …… 156
6.4 项目实施 …… 157
任务 6-1 Windows 7 加密文件系统应用 …… 157
任务 6-2 PGP 加密系统演示实验 …… 161
任务 6-3 Windows Server 2008 证书服务的安装 …… 169
任务 6-4 Windows Server 2008 使用 IIS 配置 Web 服务器上的证书 …… 176
6.5 习题 …… 189

项目 7　Windows Server 系统安全 …… 191
7.1　项目导入 …… 191
7.2　项目分析 …… 191
7.3　相关知识点 …… 191
7.3.1　操作系统安全的概念 …… 191
7.3.2　服务与端口 …… 192
7.3.3　组策略 …… 194
7.3.4　账户与密码安全 …… 195
7.3.5　加密文件系统(EFS) …… 195
7.3.6　漏洞与后门 …… 196
7.4　项目实施 …… 196
任务 7-1　账户安全配置 …… 196
任务 7-2　密码安全配置 …… 199
任务 7-3　系统安全配置 …… 200
任务 7-4　服务安全配置 …… 200
任务 7-5　使用 MBSA 检测和加固 Windows 主机的操作系统 …… 202
任务 7-6　Web 站点服务器安全配置方案 …… 204
任务 7-7　用 SSL 保护 Web 站点服务器 …… 207
任务 7-8　禁用注册表编辑器 …… 210
7.5　拓展提升　Windows 系统的安全模板 …… 210
7.6　习题 …… 213
项目 8　防火墙技术 …… 215
8.1　项目导入 …… 215
8.2　职业能力目标和要求 …… 215
8.3　相关知识点 …… 215
8.3.1　防火墙简介 …… 215
8.3.2　防火墙的实现技术 …… 216
8.3.3　天网防火墙 …… 218
8.4　项目实施 …… 218
任务 8-1　简易防火墙配置 …… 218
任务 8-2　天网防火墙的使用 …… 227
任务 8-3　天网防火墙规则的设置 …… 233
8.5　习题 …… 237
项目 9　无线局域网安全 …… 239
9.1　项目导入 …… 239

9.2 职业能力目标和要求 …… 239
9.3 相关知识点 …… 239
9.3.1 无线网络概述 …… 239
9.3.2 Wi-Fi 在全球范围迅速发展的趋势 …… 240
9.3.3 无线局域网常见的攻击 …… 241
9.3.4 WEP 协议的威胁 …… 241
9.3.5 WEP 缺陷 …… 243
9.3.6 基于 WEP 密钥缺陷引发的攻击 …… 244
9.3.7 对应决策 …… 244
9.3.8 无线安全机制 …… 246
9.3.9 无线 VPN …… 247
9.4 项目实施 …… 248
任务 9-1 无线局域网安全配置 …… 248
任务 9-2 确保无线网安全 …… 250
任务 9-3 无线 VPN 安全设置 …… 251
9.5 习题 …… 255

项目 10 Internet 安全与应用 …… 257

10.1 项目导入 …… 257
10.2 项目分析 …… 257
10.3 相关知识点 …… 257
10.3.1 电子邮件安全 …… 257
10.3.2 Internet 电子欺骗与防范 …… 258
10.3.3 VPN 概述 …… 262
10.4 项目实施 …… 264
任务 10-1 电子邮件安全应用实例 …… 264
任务 10-2 Internet 电子欺骗防范实例 …… 269
任务 10-3 VPN 的配置与应用实例 …… 270
任务 10-4 Internet Explorer 安全应用实例 …… 282
10.5 拓展提升 了解 Internet Explorer 增强的安全配置 …… 285
10.6 习题 …… 290

参考文献 …… 292

项目 1　认识网络安全

1.1　项目导入

近几年来，网络越来越深入人心，它已成为人们学习、工作、生活的便捷工具，并为我们提供了丰富资源，但是我们不得不注意到，网络虽然有强大的功能，但也有会受到攻击而非常脆弱的一面。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元，在我国，每年因网络安全问题也造成了巨大的经济损失，所以网络安全问题是我们决不能忽视的问题。据国外媒体报道，全球计算机行业协会(CompTIA)近日评出了“当前最急需的 10 项 IT 技术”，结果安全和防火墙技术排名首位，这说明安全方面的问题是全世界都急需解决的重要问题，我们所面临的网络安全状况有多尴尬也就可想而知了。

1.2　项目分析

在网络高速发展的今天，人们在享受网络便捷所带来的益处的同时，网络的安全也日益受到威胁。

网络攻击行为日趋复杂，各种方法相互融合，使网络安全防御更加困难。黑客攻击行为组织性更强，攻击目标从单纯地追求“荣耀感”向获取多方面实际利益的方向转移，网上木马、间谍程序、恶意网站、网络仿冒等的出现和日趋泛滥。

智能手机、平板电脑等无线终端的处理能力和功能通用性日益提高，使其日趋接近个人计算机，针对这些无线终端的网络攻击已经开始出现，并将进一步发展。

总之，网络安全问题变得更加错综复杂，影响将不断扩大，很难在短期内得到全面解决。

安全问题已经摆在了非常重要的位置上，网络安全如果不加以防范，会严重地影响到网络的应用。

1.3 相关知识点

1.3.1 网络安全概念

1. 网络安全的重要性

(1) 计算机存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

(2) 随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

(3) 人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转、不可替代的，而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间、核辐射环境等，这些环境都比机房恶劣，出错率和故障的增多必将导致可靠性和安全性的降低。

(4) 随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能出现问题。

(5) 计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

(6) 从认识论的高度看，人们往往首先关注系统功能，然后才被动地从现象注意系统应用的安全问题。因此广泛存在着重应用、轻安全、法律意识淡薄的普遍现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的，这也使得目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。

2. 网络脆弱的原因

(1) 开放性的网络环境：Internet 的开放性，使网络变成众矢之的，可能遭受各方面的攻击；Internet 的国际性使网络可能遭受本地用户或远程用户、国外用户或国内用户等的攻击；Internet 的自由性没有给网络的使用者规定任何的条款，导致用户“太自由了”，自由地下载、自由地访问、自由地发布；Internet 使用的傻瓜性使任何人都可以方便地访问网络，基本不需要技术，只要会移动鼠标就可以上网冲浪，这就给我们带来很多的隐患。

(2) 协议本身的缺陷：网络应用层服务的隐患：IP 层通信的易欺骗性；针对 ARP 的

欺骗性。

(3) 操作系统的漏洞：系统模型本身的缺陷；操作系统存在 BUG；操作系统程序配置不正确。

(4) 人为因素：缺乏安全意识，缺少网络应对能力，有相当一部分人认为自己的计算机中没有什么重要的东西，不会被别人黑，存在这种侥幸心理、重装系统后觉得防范很麻烦，所以不认真对待安全问题，造成的隐患就特别多。

(5) 设备不安全：对于购买的国外的网络产品，到底有没有留后门，我们根本无法得知，这对于缺乏自主技术支撑、依赖进口的国家而言，无疑是最大的安全隐患。

(6) 线路不安全：不管是有线介质、双绞线、光纤还是无线介质，以及微波、红外、卫星、Wi-Fi 等，窃听其中一小段线路的信息是很容易做到的，没有绝对安全的通信线路。

3. 网络安全的定义

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。网络安全包含网络设备安全、网络信息安全、网络软件安全。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。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

4. 网络安全的基本要素

(1) 机密性(保密性)：确保信息不暴露给未授权的实体或进程；防泄密。

(2) 完整性：只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。完整性鉴别机制，保证只有得到允许的人才能修改数据；防止篡改。

(3) 可用性：得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。用访问控制机制阻止非授权用户进入网络。使静态信息可见，动态信息可操作。防止中断。

(4) 可鉴别性(可审查性)：对危害国家信息(包括利用加密的非法通信活动)的监视审计。控制授权范围内的信息流向及行为方式。使用授权机制，控制信息传播范围及内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

(5) 不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

1.3.2　典型的网络安全事件

1995 年，米特尼克闯入许多计算机网络，偷窃了 2 万个信用卡号。他曾闯入“北美空中防务指挥系统”，破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“账户修改密码”，入侵过美国 DEC 等 5 家大公司的网络，造成 8000 万美元的损失。

1999 年，中国台湾省大学生陈盈豪制造的 CIH 病毒在 4 月 26 日发作，引起全球震

撼，有 6000 多万台计算机受害。

2002 年，黑客用 DDos 攻击而影响了 13 个“根 DNS”中的 8 个，作为整个 Internet 通信路标的关键系统遭到严重的破坏。

2006 年，“熊猫烧香”木马致使我国数百万计算机用户受到感染，并波及周边国家。

2007 年 2 月，“熊猫烧香”制作者李俊被捕。

2008 年，一个全球性的黑客组织，利用 ATM 欺诈程序在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。

2009 年，韩国遭受有史以来最猛烈的一次黑客攻击。韩国总统府、国会、国情院和国防部等国家机关，以及金融界、媒体和防火墙企业网站遭受攻击，造成网站一度无法访问。

2010 年，“维基解密”网站在《纽约时报》、《卫报》和《镜报》配合下，在网上公开了多达 9.2 万份的驻阿美军秘密文件，引起轩然大波。

2011 年，堪称中国互联网史上最大泄密事件发生。当年的 12 月中旬，CSDN 网站用户数据库被黑客在网上公开，大约 600 余万个注册邮箱账号和与之对应的明文密码泄露。2012 年 1 月 12 日，CSDN 泄密的两名嫌疑人被刑事拘留。其中一名为北京籍黑客；另一名为外地黑客。

2013 年 6 月 5 日，美国前中情局(CIA)职员爱德华·斯诺顿披露给媒体两份绝密资料，一份资料称：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。另一份资料更加惊人，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。

2014 年 4 月 8 日，“地震级”网络灾难降临，在微软 Windows XP 操作系统正式停止服务的同一天，互联网被划出一道致命裂口——常用于电商、支付类接口等安全极高网站的网络安全协议 OpenSSL 被曝存在高危漏洞，众多使用 HTTPs 的网站均可能受到影响，在“心脏出血”漏洞逐渐修补结束后，由于用户很多软件中也存在该漏洞，黑客攻击目标存在从服务器转身客户端的可能性，下一步有可能出现“血崩”攻击。

1.3.3 信息安全的发展历程

1. 通信保密阶段 ComSec(Communication Security)

通信保密阶段始于 20 世纪 40 年代至 70 年代，又称为通信安全时代，其重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性，主要安全威胁是搭线窃听、密码学分析，主要保护措施是加密技术，主要标志是 1949 年 Shannon 发表的《保密通信的信息理论》、1997 年美国国家标准局公布的数据加密标准(DES)、1976 年 Diffie 和 hellman 在 *New Directions in Cryptography* 一文中所提出的公钥密码体制。

2. 计算机安全阶段

计算机安全阶段始于 20 世纪 70 年代至 80 年代，重点是确保计算机系统中硬件、软