高等院校计算机实验与实践系列示范教材

通信网络安全原理与实践

郑鲲　孙宝岐　等　编著

清华大学出版社

高等院校计算机实验与实践系列示范教材

通信网络安全原理与实践

郑鲲　孙宝岐 等　编著

清华大学出版社
北京

内 容 简 介

本书从理论、技术和实例三方面阐述了网络安全理论，分析了网络安全技术。全书共分15章，在介绍原理的基础上加强了实践内容，包括实验、试验及情境等安全应用环节的设计，力求理论与实践热点结合，突出本书的实用性；本书注重反映网络安全发展趋势，突出新颖性。

本书可以作为网络管理员和计算机用户的参考资料，也可作为高等院校相关课程的教材或参考文献。

图书在版编目(CIP)数据

通信网络安全原理与实践/郑鲲，孙宝岐等编著. --北京：清华大学出版社，2014
高等院校计算机实验与实践系列示范教材
ISBN 978-7-302-35649-3

Ⅰ. ①通… Ⅱ. ①郑… ②孙… Ⅲ. ①通信网－安全技术－高等学校－教材 Ⅳ. ①TN915.08

中国版本图书馆CIP数据核字(2014)第050771号

责任编辑：黄　芝　王冰飞
封面设计：常雪影
责任校对：焦丽丽
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，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：25.75　　字　　数：626千字
版　　次：2014年7月第1版　　印　　次：2014年7月第1次印刷
印　　数：1～2000
定　　价：44.50元

产品编号：056980-01

出版说明

当前，重视实验与实践教育是各国高等教育界的发展潮流，我国与国外教学工作的差距也主要表现在实践教学环节上。面对新的形式和新的挑战，完善实验与实践教育体系成为一种必然。为了培养具有高质量、高素质、高实践能力和高创新能力的人才，全国很多高等院校在实验与实践教学方面进行了大力改革，在实验与实践教学内容、教学方法、教学体系、实验室建设等方面积累了大量的宝贵经验，起到了教学示范作用。

实验与实践性教学与理论教学是相辅相成的，具有同等重要的地位。它是在开放教育的基础上，为配合理论教学、培养学生分析问题和解决问题的能力以及加强训练学生专业实践能力而设置的教学环节；对于完成教学计划、落实教学大纲，确保教学质量，培养学生分析问题、解决问题的能力和实际操作技能更具有特别重要的意义。同时，实践教学也是培养应用型人才的重要途径，实践教学质量的好坏，实际上也决定了应用型人才培养质量的高低。因此，加强实践教学环节，提高实践教学质量，对培养高质量的应用型人才至关重要。

近年来，教育部把实验与实践教学作为对高等院校教学工作评估的关键性指标。2005 年 1 月，在教育部下发的《关于进一步加强高等学校本科教学工作的若干意见》中明确指出："高等学校要强化实践育人的意识，区别不同学科对实践教学的要求，合理制定实践教学方案，完善实践教学体系。要切实加强实验、实习、社会实践、毕业设计（论文）等实践教学环节，保障各环节的时间和效果，不得降低要求。"，"要不断改革实践教学内容，改进实践教学方法，通过政策引导，吸引高水平教师从事实践环节教学工作。要加强产学研合作教育，充分利用国内外资源，不断拓展校际之间、校企之间、高校与科研院所之间的合作，加强各种形式的实践教学基地和实验室建设。"

为了配合开展实践教学及适应教学改革的需要，我们在全国各高等院校精心挖掘和遴选了一批在计算机实验与实践教学方面具有潜心研究并取得了富有特色、值得推广的教学成果的作者，把他们多年积累的教学经验编写成教材，为开展实践教学的学校起一个抛砖引玉的示范作用。

为了保证出版质量，本套教材中的每本书都经过编委会委员的精心筛选和

严格评审，坚持宁缺毋滥的原则，力争把每本书都做成精品。同时，为了能够让更多、更好的实践教学成果应用于社会和各高等院校，我们热切期望在这方面有经验和成果的教师能够加入到本套丛书的编写队伍中，为实践教学的发展和取得成效做出贡献；也衷心地期望广大读者对本套教材提出宝贵意见，以便我们更好地为读者服务。

清华大学出版社

联系人：索梅 suom@tup.tsinghua.edu.cn

FOREWORD 前言

随着网络应用的不断普及，网络中的不安全因素也越来越多，影响到了人们的基本生活，甚至于国家的前途命运。通信网络安全已经成为一个国际关注的问题。

本书以基本原理的应用为中心，理论紧密联系实际，系统地讲述了网络安全所涉及的理论及技术。每章最后都设计了实践内容，规划了任务，通过实战演练帮助读者综合运用书中所讲授的技术进行网络信息安全方面的实践。

在理论介绍的基础上，本书强调了实验实践环节的通用性和可操作性，避免了一些传统网络安全教材操作性不强、理论和实际联系不紧的问题，重点介绍了网络安全领域的新问题和工具的运用。

全书共15章，分别为第1章网络安全概述、第2章TCP/IP基础、第3章数据加密、第4章通信安全、第5章网络攻击、第6章计算机病毒、第7章无线网络安全、第8章操作系统安全、第9章移动存储设备安全、第10章网络设备安全、第11章防火墙技术、第12章入侵检测、第13章Web安全、第14章数据库安全、第15章网络安全风险评估。每章首先讲解技术原理，通过这一部分使读者在理论上有一个清楚的认识，然后是实践部分，选用目前常用的网络安全工具及实验环境，通过对工具的使用与操作，帮助读者理解运用。实践分为实验和试验，实验在合理情境设计的基础上以任务驱动，强调过程；试验在提出任务或假设的基础上不设定具体的过程，强调方法和结果。每章都有各类情境及问题供读者学习和思考，很少有答案唯一的习题，原因是希望读者在学习过程中不被束缚，主动思考，不拘泥于知识经验，在继承中创新。

本书在编写过程中参考了大量国内外文献资料，吸取了很多国内同行专家的先进理念和实践经验。本书所有实践环节均在具体实验环境中测试通过，部分案例来自真实环境。

本书的1.1～1.4节由郑全英编写，2.1～2.2节由徐珍泉编写，第8章Linux实验部分由张红编写，9.1～9.4节由孙俊灵编写，第10章由孙宝岐编写，第13章由刘砚秋编写，第14章由黄静编写，其余各章节及实践部分均由郑鲲编写，最终统稿由郑鲲完成。

限于编者水平，加之网络安全理论与技术不断发展及更新，书中难免有不妥之处，敬请读者批评指正。

编　者

2014年3月

CONTENTS

目录

第 1 章　网络安全概述 …… 1

1.1　网络安全的重要性 …… 1
1.2　网络安全的重要威胁 …… 1
1.2.1　人为疏忽 …… 1
1.2.2　人为的恶意攻击 …… 2
1.2.3　网络软件的漏洞 …… 2
1.2.4　非授权访问 …… 2
1.2.5　信息泄露或丢失 …… 2
1.2.6　破坏数据完整性 …… 3
1.3　网络安全定义及目标 …… 3
1.3.1　网络安全定义 …… 3
1.3.2　网络安全性保护的目标 …… 3
1.4　网络安全的等级 …… 6
1.5　网络安全的层次 …… 7
1.5.1　物理安全 …… 7
1.5.2　安全控制 …… 8
1.5.3　安全服务 …… 8
1.6　国内外信息安全等级认证与评测发展和现状 …… 10
【情境 1-1】　IE 快捷方式加载特定主页 …… 12
【试验 1-1】　通信屏蔽与代理 …… 13

第 2 章　TCP/IP 基础 …… 14

2.1　网络的基础知识 …… 14
2.1.1　计算机网络及其拓扑结构 …… 14
2.1.2　计算机网络的分类 …… 14
2.1.3　OSI 参考模型 …… 16
2.2　TCP/IP 协议 …… 17
2.2.1　TCP/IP 协议及其优点 …… 17
2.2.2　TCP/IP 的体系结构 …… 17

2.2.3 TCP/IP 应用层中的常用协议 …… 19
【实验 2-1】 网络测试工具的使用 …… 20
【情境 2-1】 网页无法打开 …… 27
【情境 2-2】 两台主机只能单方向 ping 通 …… 28
【情境 2-3】 遭受 ARP 攻击无法正常上网 …… 28
【实验 2-2】 网络协议分析 …… 32
【试验 2-1】 一种操作系统指纹识别方法 …… 40

第 3 章 数据加密 …… 41

3.1 数据加密技术 …… 41
3.2 数据加密技术的发展 …… 42
3.3 数据加密算法 …… 42
3.3.1 古典密码算法 …… 42
3.3.2 现代密码体制 …… 44
3.3.3 DES 算法 …… 45
3.3.4 RSA 公开密钥密码体制 …… 50
3.3.5 AES 简介 …… 52
3.3.6 MD5 …… 53
3.3.7 PGP 技术 …… 64
【实验 3-1】 网络软件下载安全性检验 …… 64
【实验 3-2】 PGP 加密应用实验 …… 65

第 4 章 通信安全 …… 71

4.1 安全传输技术简介 …… 71
4.2 IPSec 安全传输技术 …… 71
4.2.1 IPSec VPN 的工作原理 …… 72
4.2.2 IPSec 的实现方式 …… 73
4.3 SSL 安全传输技术 …… 74
4.3.1 SSL 简介 …… 74
4.3.2 SSL 运作过程 …… 74
4.3.3 SSL VPN 的特点 …… 75
4.4 SSL VPN 与 IPSec VPN 技术比较 …… 75
【实验 4-1】 构建 VPN …… 76
【实验 4-2】 配置 VPN 服务器 …… 79
【实验 4-3】 简单的信息隐藏 …… 88

第 5 章 网络攻击 …… 91

5.1 网络攻击技术 …… 91
5.1.1 网络攻击的手段 …… 91

5.1.2 网络攻击的常用工具 …… 100
5.2 网络攻击检测技术 …… 103
5.3 网络安全的防范 …… 104
5.3.1 网络安全策略 …… 104
5.3.2 常用的安全防范技术 …… 109
【实验 5-1】 设置代理服务器 …… 112
【实验 5-2】 X-Scan 漏洞扫描 …… 113
【实验 5-3】 ARP-Killer 实验 …… 117
【实验 5-4】 ARP 攻击的 C 语言实现 …… 118

第 6 章 计算机病毒 …… 122

6.1 计算机病毒产生的原因 …… 122
6.2 计算机病毒的定义及命名 …… 123
6.2.1 计算机病毒的定义 …… 123
6.2.2 计算机病毒的命名 …… 123
6.3 计算机病毒的特征 …… 125
6.4 计算机病毒的症状及危害 …… 127
6.4.1 可能传播病毒的途径 …… 127
6.4.2 计算机病毒的症状 …… 127
6.4.3 计算机病毒造成的危害 …… 129
6.5 反病毒技术 …… 129
6.5.1 反病毒技术的三大内容 …… 129
6.5.2 反病毒技术的发展 …… 130
6.5.3 反病毒技术的划分 …… 130
6.6 病毒的识别与预防 …… 131
6.6.1 判断方法 …… 131
6.6.2 感染病毒后计算机的处理 …… 132
6.6.3 计算机病毒样本的分析方法 …… 133
6.7 蠕虫 …… 134
6.8 木马 …… 135
【实验 6-1】 Word 宏病毒 …… 135
【实验 6-2】 恶意代码攻防 …… 139
【实验 6-3】 可执行程序捆绑及检测 …… 149
【实验 6-4】 清除 DLL 文件中的恶意功能 …… 153

第 7 章 无线网络安全 …… 155

7.1 无线网络的类型 …… 155
7.2 无线网络应用现状 …… 156
7.2.1 无线局域网 …… 156

7.2.2 3G …… 156
7.3 无线网络安全现状 …… 156
7.4 无线局域网安全技术 …… 157
7.4.1 SSID …… 158
7.4.2 MAC 地址过滤 …… 158
7.4.3 802.11 WEP …… 158
7.4.4 802.1x/EAP 用户认证 …… 159
7.4.5 WPA(802.11i) …… 160
7.5 无线网络安全威胁 …… 162
7.6 无线局域网安全措施 …… 164
7.7 无线网络安全测试工具 …… 164
【试验 7-1】 无线网络的搭建与安全检测 …… 168

第 8 章 操作系统安全 …… 169

8.1 操作系统安全概述 …… 169
8.1.1 操作系统安全现状 …… 169
8.1.2 操作系统安全所涉及的几个概念 …… 170
8.1.3 操作系统的安全管理 …… 170
8.1.4 常用的服务器操作系统 …… 172
8.2 Windows 操作系统安全——注册表 …… 173
8.2.1 注册表的由来 …… 173
8.2.2 注册表的作用 …… 174
8.2.3 注册表中的相关术语 …… 174
8.2.4 注册表的结构 …… 174
8.2.5 注册表的维护 …… 176
【实验 8-1】 账户安全配置和系统安全设置 …… 178
【实验 8-2】 注册表的备份、恢复和维护 …… 191
【实验 8-3】 简单批处理应用 …… 199
【实验 8-4】 Linux 文件系统安全 …… 202
【实验 8-5】 Linux 账户安全 …… 208

第 9 章 移动存储设备安全 …… 215

9.1 移动存储设备种类 …… 215
9.1.1 移动存储设备的分类 …… 215
9.1.2 常见的移动存储设备 …… 215
9.2 U 盘存储原理 …… 216
9.2.1 USB 2.0 协议规范 …… 216
9.2.2 USB 3.0 协议规范 …… 216
9.2.3 U 盘的基本工作原理 …… 217

9.2.4 U盘文件系统 …… 217
9.2.5 U盘启动模式 …… 218
9.2.6 U盘量产 …… 219
9.3 autorun.inf文件 …… 219
9.3.1 autorun.inf文件及病毒感染 …… 219
9.3.2 病毒autorun.inf的文件传播 …… 220
9.4 U盘病毒的预防及清除 …… 220
9.4.1 U盘病毒的工作原理 …… 220
9.4.2 U盘病毒的防范 …… 221
9.4.3 U盘病毒的解决方法 …… 222
9.5 U盘数据修复 …… 223
【情境9-1】 U盘内有“固化”的程序或者文件不能删除 …… 224
【情境9-2】 广告U盘的制作 …… 225
【试验9-1】 尝试把一个视频文件转换为EXE文件 …… 228
【试验9-2】 尝试在U盘里安装一个操作系统 …… 228

第10章 网络设备安全 …… 229

10.1 网络设备面临的安全威胁 …… 229
10.1.1 主要网络设备简介 …… 229
10.1.2 网络设备常见的安全隐患 …… 230
10.2 路由器的安全技术 …… 231
10.2.1 路由器存在的安全问题及对策 …… 232
10.2.2 路由器的安全配置 …… 236
10.3 交换机的安全技术 …… 243
10.3.1 交换机存在的安全问题及对策 …… 243
10.3.2 交换机的安全配置 …… 246
【情境10-1】 某公司交换机安全配置——限制访问 …… 247
【情境10-2】 某公司交换机端口安全配置 …… 249
【情境10-3】 网络中拥有核心交换机的VLAN配置 …… 255
10.4 无线网络设备的安全技术 …… 258
10.4.1 无线局域网设备安全存在的问题 …… 258
10.4.2 无线网络常用的安全技术及总体安全策略 …… 259
【实验10-1】 无线接入设备的安全配置 …… 261

第11章 防火墙技术 …… 272

11.1 防火墙概述 …… 272
11.1.1 防火墙的基本概念 …… 272
11.1.2 防火墙的功能 …… 274
11.1.3 防火墙的优缺点 …… 274

11.2 防火墙的工作方式 …… 276
11.2.1 硬件方式 …… 276
11.2.2 软件方式 …… 276
11.2.3 混合方式 …… 277
11.3 防火墙的工作原理 …… 277
11.4 防火墙的设计原则 …… 282
11.5 防火墙的 NAT 功能 …… 283
【实验 11-1】 设计路由器包过滤技术 …… 284
【实验 11-2】 设计企业网络中的路由器 ACL+NAT …… 285

第 12 章 入侵检测 …… 290

12.1 入侵检测的概念 …… 290
12.2 入侵检测系统的分类 …… 291
12.2.1 主机型入侵检测系统 …… 291
12.2.2 网络型入侵检测系统 …… 292
12.2.3 混合型入侵检测系统 …… 293
12.2.4 误用检测 …… 293
12.2.5 异常检测 …… 294
12.3 入侵检测技术的发展方向 …… 295
12.4 主要的 IDS 公司及其产品 …… 296
12.4.1 RealSecure …… 296
12.4.2 NetRanger …… 296
12.4.3 Snort …… 296
【实验 12-1】 Snort 的安装与使用 …… 297
【实验 12-2】 基于 Windows 控制台的入侵检测系统配置 …… 298

第 13 章 Web 安全 …… 304

13.1 概述 …… 304
13.2 Web 安全概念 …… 305
13.2.1 Web 服务 …… 305
13.2.2 Web 架构 …… 305
13.2.3 Web 攻击 …… 306
13.2.4 常见的 Web 攻击种类 …… 307
13.2.5 Web 应用安全与 Web 防火墙 …… 307
13.3 Web 安全专用设置 …… 307
13.4 WWW 攻击与防范 …… 309
13.5 跨站脚本漏洞 …… 310
13.5.1 XSS 的触发条件 …… 311
13.5.2 XSS 转码引发的过滤问题 …… 312

13.5.3 攻击实例 …… 312
13.6 SQL 注入攻击 …… 313
13.7 针对 80 端口的攻击实例 …… 313
13.8 利用 XSS 钓鱼 …… 315
13.9 恶意网页攻击举例 …… 316
【实验 13-1】 Web 安全实验 …… 317

第 14 章 数据库安全 …… 328

14.1 数据库安全概述 …… 328
14.1.1 数据库安全的定义 …… 328
14.1.2 数据库安全受到的威胁 …… 329
14.1.3 数据库安全评估标准 …… 330
14.2 数据库安全实现技术 …… 330
14.3 SQL Server 安全管理 …… 334
14.3.1 SQL Server 安全控制体系 …… 334
14.3.2 服务器层面的安全保护 …… 335
14.3.3 数据库层面的安全保护 …… 337
14.3.4 数据库对象的安全保护 …… 345
14.3.5 SQL Server 安全控制策略小结 …… 349
14.3.6 SQL Server 中的数据加密 …… 350

第 15 章 网络安全风险评估 …… 355

15.1 概述 …… 355
15.2 国内现有风险评估机构 …… 356
15.3 常用风险评估方法 …… 356
15.3.1 风险计算矩阵法 …… 356
15.3.2 风险计算相乘法 …… 358
15.4 风险评估流程 …… 360
15.4.1 风险评估准备工作 …… 360
15.4.2 项目启动 …… 362
15.4.3 风险因素识别 …… 362
15.4.4 风险程度分析 …… 363
15.4.5 风险等级评价 …… 364
15.4.6 控制及规划 …… 365
15.4.7 总结汇报 …… 365
15.4.8 验收 …… 365
15.5 风险评估实施流程图 …… 366
15.6 风险评估工具 …… 366
15.7 风险识别 …… 368

15.7.1 资产识别 …… 368
15.7.2 威胁识别 …… 368
15.7.3 脆弱性识别 …… 371
15.7.4 风险评估结果的确定 …… 372
【实验 15-1】 安全风险检查 …… 377

参考文献 …… 396

第1章 网络安全概述

1.1 网络安全的重要性

安全性是互联网技术中很关键也很容易被忽略的问题。许多组织因为曾经在使用网络的过程中未意识到网络安全的重要性，直到受到了资料安全的威胁后，才开始重视和采取相应的防范措施。因此，在网络广泛使用的今天，更应该了解网络安全，做好防范措施，注重网络信息的保密性、完整性和可用性。

中国国家互联网应急中心发布的《2011年中国互联网网络安全态势报告》显示，目前我国对全球互联网安全威胁低，遭受境外网络攻击持续增多；网上银行面临的钓鱼威胁愈演愈烈；工业控制系统安全事件呈现增长态势；手机恶意程序现多发态势；木马和僵尸网络活动越发猖獗；应用软件漏洞呈现迅猛增长的趋势；DDoS攻击仍然呈现频率高、规模大的特点。

1.2 网络安全的重要威胁

影响计算机网络安全的因素很多，人为的或非人为的，有意的或恶意的，等等，一个很重要的因素是外来黑客对网络系统资源的非法使用，严重威胁着网络的安全。网络安全威胁可以归结为以下几个方面。

1.2.1 人为疏忽

人为疏忽包括失误、失职、误操作等。这些可能是工作人员对安全的配置不当、不注意保密工作、密码选择不够慎重等造成的。比如2012年我国国内某知名证券网站因为人为疏忽，未禁止搜索引擎搜索敏感服务，导致用户资料大量泄露；2010年我国国内某通信公司也是因为人为疏忽未设置文件访问权限，导致用户上传的个人图片可以被其他人随意查看与删除。

1.2.2 人为的恶意攻击

人为的恶意攻击是网络安全的最大威胁，敌意的攻击和计算机犯罪就是这个类别。这种攻击破坏性最强，可能造成极大的危害，可能导致机密数据的泄露。如果涉及的是金融机构，则很可能导致破产，甚至会给社会带来震荡。这种攻击有主动攻击和被动攻击两种。主动攻击有选择性地破坏信息的有效性和完整性。被动攻击是在不影响网络的正常工作的情况下截获、窃取、破译，以获得重要机密信息。而且进行这些攻击行为的大多是具有很高的专业技能和智商的人员，一般需要相当的专业知识才能破解。互联网安全公司赛门铁克发布报告，2011 年 7 月至 2012 年 7 月间，包括恶意软件攻击和钓鱼攻击在内的网络攻击给全球带来了 1110 亿美元的损失。在此期间，全球有 5.56 亿成年网民亲身经历过网络攻击，占到了所有成年网民数量的 46%。360 发布的 2011—2012 年度《中国互联网安全报告》显示，2011 年我国国内日均约 853.1 万台电脑遭到木马病毒等恶意程序攻击，占每天开机联网电脑的比例约为 5.7%。

1.2.3 网络软件的漏洞

网络软件的缺陷和漏洞为黑客提供了攻击机会。软件设计人员为了方便自己而设置的后门，一旦被攻破，其后果也是不堪设想。比如 2012 年 5 月微软发布公告 MS12-029 显示了一个 Microsoft Office 中秘密报告的漏洞，如果用户打开特制的 RTF 文件，该漏洞可能允许远程执行代码，一个成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。近年来，应用软件漏洞呈现迅猛增长的趋势。2011 年，中国国家信息安全漏洞共享平台(CNVD)共收集整理并公开发布信息安全漏洞 5547 个，较 2010 年大幅增加 60.9%。其中，高危漏洞有 2164 个，较 2010 年增加约 2.3 倍。

1.2.4 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序(Exploit)来获取信息系统访问权限。比如 Oracle Database 的组件 PL/SQL Gateway 在访问控制列表的实现上存在漏洞，攻击者可能非授权地访问到被禁止访问的存储过程，从而完全获取数据库的 DBA 权限。

1.2.5 信息泄露或丢失

信息泄露或丢失是指敏感数据被有意或无意地泄露出去或丢失，通常包括信息在传输或保存的过程中丢失或泄露。比如数据明文存储这种方式比较容易导致信息泄露。21 世纪初，我国国内某著名门户网站免费邮件服务器系统升级时，技术人员升级失误删除了邮件，造成了邮件丢失且无法恢复的严重后果。2005 年某银行存有 390 万客户银行账号、历

史支付数据以及社会保障卡号的电脑磁盘在运输途中丢失。2010 年至 2012 年间，我国国内几家知名社区网站分别被曝核心用户数据信息泄露，其中两家分别达到 600 万及 4000 万用户注册的信息包括设置的密码外泄，让人更为吃惊的是这里面 2010 年以前生成的数据大都是采用明文存储形式，给广大用户带来的潜在风险不言而喻。

1.2.6 破坏数据完整性

破坏数据完整性是指以非法手段窃得对数据的使用权，删改、修改、插入或重发某些信息，恶意添加、修改数据，以干扰拥护的正常使用。2008 年某高校招办发现，一些考生的信息被黑客添加到该校录取数据库内。2009 年 6 月，武汉警方披露了一起特大网络招生诈骗案，攻击者雇用黑客攻击高校招生网，篡改网站录取信息，伪造录取通知书，诈骗 8 名学生家长约 300 万元。2011 年有报道说伊朗修改了全球定位系统数据，从而捕获了一架美国无人侦察机。

1.3 网络安全定义及目标

1.3.1 网络安全定义

网络安全是指为保护网络免受侵害而采取的措施的总和。正确地采用网络安全措施，能使网络得到保护，使其正常运行。网络安全具有如下 3 方面内容。

1. 保密性

保密性指网络能够阻止未经授权的用户读取保密信息。

2. 完整性

完整性包括资料的完整性和软件的完整性。资料的完整性指在未经许可的情况下确保资料不被删除或修改。软件的完整性是确保软件程序不会被错误、怀有恶意的用户或病毒修改。

3. 可用性

可用性指网络在遭受攻击时可以确保合法用户对系统的授权访问正常进行。

1.3.2 网络安全性保护的目标

1. 身份真实性

对通信实体身份的真实性进行识别。21 世纪，网络安全最基础和最重要的方面之一就是从防御网络（重点放在防御措施和限制访问的网络）转变到信任网络（允许那些身份通过可靠验证的信任用户访问的网络）。