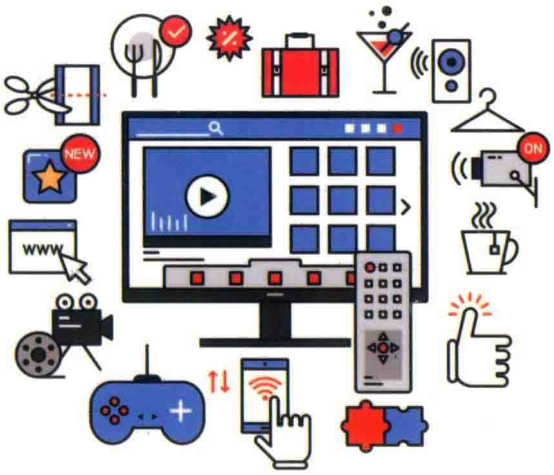
课程 | 实验 | 题库

教育部产学合作协同育人项目成果教材
西普教育研究院 IT 前沿技术方向高校系列教材

“十三五”江苏省高等学校重点教材



Introduction to Information Security

信息安全导论

在线实验 + 在线自测

杨种学 孙维隆 李滢 主编
郑豪 马云涛 林雪纲 邹温林 副主编

实验吧
让实验更简单

-SaaS
开放实验云平台

- 内容新颖，可操作性强，层层深入，简明易懂。
- 从实用角度出发，重点培养动手解决问题的能力。
- 提供体系完整的在线实验，即学即练，书网结合。

扫描书中二维码随时进行在线测试

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

课程 | 实验 | 题库

教育部产学合作协同育人项目成果教材
西普教育研究院 IT 前沿技术方向高校系列教材

“十三五”江苏省高等学校重点教材
（编号：2018-2-010）

Introduction to Information Security

信息安全导论

在线实验 + 在线自测

杨种学 孙维隆 李滢 主编
郑豪 马云涛 林雪纲 邹温林 副主编

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

信息安全导论 ：在线实验+在线自测 / 杨种学，孙维隆，李滢主编. -- 北京 ：人民邮电出版社，2019.2
ISBN 978-7-115-50093-9

Ⅰ. ①信… Ⅱ. ①杨… ②孙… ③李… Ⅲ. ①信息安全－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2018)第259792号

内 容 提 要

本书分为 9 章，主要内容包括信息安全概述、操作系统安全、Web 应用安全、网络安全、物联网安全、移动互联网终端安全、云计算及其安全、大数据及其安全和隐私保护。同时，本书提供在线实验资源，可以帮助学生掌握一定的实战技能。

本书可以作为高校信息安全、网络空间安全和计算机等相关专业的教材，也可作为社会从业人员自学的参考资料。

◆ 主　　编　杨种学　孙维隆　李　滢
副 主 编　郑　豪　马云涛　林雪纲　邹温林
责任编辑　左仲海
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：10.75　　2019 年 2 月第 1 版
字数：239 千字　　2019 年 2 月北京第 1 次印刷

定价：39.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

序 PREFACE

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代，信息就像水、电、石油一样，与几乎所有行业和所有人都相关，成为一种基础资源。信息和信息技术改变着人们的生活和工作方式，如果离开计算机、电视和手机等电子信息设备，人们很难正常生活和工作。信息技术一方面会促进经济的发展，推动社会的前进和人类的进步，另一方面也会伴随着信息破坏、信息侵权、信息污染等不良现象。随着信息技术的不断发展，信息安全已经上升到了国家战略层面，并与社会安全乃至国家安全息息相关。

目前，解决信息安全问题已经刻不容缓，但是我国在相关领域的人才缺口却非常大，加快信息安全人才培养体系建设是发展我国信息安全保障的必备基础和先决条件。基于这种背景，2015 年，经教育部批准，网络空间安全一级学科正式设立，这标志着我国信息安全人才培养进入到了新的阶段。很多高校设置了信息安全、网络空间安全和安全保密等专业，计算机、网络工程、电子商务、电子信息等相关专业也开设了信息安全课程，以此来加强信息安全人才的培养。

开设信息安全课程就需要与之配套的信息安全教材，正是在这种背景下，《信息安全导论》这本书应运而生。本书是由高校一线教师和企业信息安全专家携手组织编写的，在编撰过程中充分发挥了优秀教师的理论专长和信息安全专家的工作经验优势。本书以“理论+实践+知识拓展”为主线，按照“教学做合一”的指导思想，在完成技术讲解的同时，利用“实验吧”里丰富的在线实验资源，通过“图书+网络实训资源”的形式提供了完善的、贴近实际应用的课程体系，并配套了大量在线实操演练案例，帮助读者加深对理论知识的理解，增强实践技能。

本书是高校与企业共同进行信息安全专业课程建设的有益尝试，相信这本书的出版能够为高校信息安全人才培养工作起到良好的示范和帮助作用，能够为我国的信息安全保障事业带来积极的促进作用。

北京航空航天大学网络空间安全学院院长
刘建伟
2018 年 12 月

前 言 FOREWORD

信息是社会发展的重要战略资源。国际上围绕信息获取、使用和控制的斗争愈演愈烈，信息安全变得至关重要，已成为维护国家安全和社会稳定的一个焦点，各国都给予了极大的关注和投入，信息安全已成为信息科学的热点课题之一。

2015年，经教育部批准，网络空间安全一级学科正式设立，这标志着我国对信息安全人才的培养进入了新的阶段。除高校根据该一级学科的建设要求进一步完善人才培养方案之外，从事信息安全实训等相关工作的企业也可与高校协作，帮助学校加强实践环节教学，帮助学生了解知识的应用场景，从而培养出高素质的信息安全人才队伍。

基于上述背景，编者结合多年的网络安全工作经验和教学经验，以“理论+实践+知识拓展”为主线，根据“教、学、做一体化”的教学方法编写了本书。在完成技术讲解的同时，本书利用“实验吧”里丰富的在线实验资源，帮助读者加深对理论知识点的理解，增强实践技能，最后对读者提出相应的自学要求和指导，以达到深入学习相关知识的目的。

本书面向信息安全初学者，力求为读者展示信息安全的技术脉络和基本的知识体系，为读者后续的专业课学习和深造打下基础。因此，本书在内容组织和编写上，遵循如下理念。

（1）具有科学合理的知识体系。本书按照由浅入深的顺序，逐渐引入相关技术与知识，实现技术讲解与训练合二为一，有助于“教、学、做一体化”教学方法的实施。

（2）发挥企业的优势。本书将行业案例与基本的信息安全理论体系相融合来组织全书内容，为读者展示从技术视角出发的信息安全知识体系。

（3）突出前沿性和实用性。随着信息技术的发展，信息安全领域也出现了很多新问题，如移动终端安全、物联网安全、云计算和大数据安全等，本书对这些热点领域面临的安全问题和现有的解决方案均做了介绍。

（4）配备丰富的学习和教学资源。为帮助高校教师使用本书进行教学，本书为教师配备了相关的教学辅助资源。本书通过“图书+网络实训资源”的形式提供了完善的、贴近实际应用的课程体系，并配备了大量的在线实操演练场景，为广大个人用户提供了便捷的网络安全实训服务。

本书由杨种学、孙维隆、李滢任主编，郑豪、马云涛、林雪纲、邹温林任副主编，参与编写的还有时允田、杨志鹏、李彩霞、黄金龙、平立振。此外，在编撰过程中，

徐立丹、王宜海、张洋等人进行了排版和校对，特此表示感谢！

由于编者水平有限，书中不妥之处在所难免，殷切希望广大读者指正。同时，恳请读者一旦发现问题，于百忙之中及时与编者联系，以便尽快更正，编者将不胜感激，E-mail：sunweilong@simpleedu.com.cn。

编　者

2018 年 11 月

平台支撑 PLATFORM SUPPORT

为了让广大读者能够快速入门，本书以实践案例为主线，读者可通过遵循书中案例的操作步骤，完成一个个实践案例，来学习大数据测试技术。同时，北京西普阳光教育科技股份有限公司（简称西普教育）开发的在线教育平台——实验吧（http://www.shiyanbar.com），提供了强大的集成实验环境及海量的在线教学资源，把配套的实验搬到线上，可以让读者更方便地结合本书进行实践。

1. 如何学习本书中的配套实验课程

（1）购买本书后，找到粘贴在本书封底的刮刮卡，刮开并获得学号。

（2）登录实验吧网站（www.shiyanbar.com），完成网站注册。

（3）登录人邮学院在线实验中心（rymooc.shiyanbar.com），输入在实验吧注册的账户及密码，完成登录（见图 1）。

（4）输入刮刮卡中的学号，姓名填写“人邮学院”，单击“保存”按钮，完成绑定（见图 2）。

图 1　登录在线实验平台

图 2　绑定学生信息

（5）完成绑定后，自动登录进入在线实验中心，开始学习本书配套的课程资源。

2. 如何学习本书中的配套练习题

实验吧教研团队为本书配套了丰富的课后练习题，读者通过扫描本书各项目里配套的习题二维码，即可进行在线自测，提交后自动判断正误，并提供正确答案。

目录 CONTENTS

第 1 章　信息安全概述 …… 1

1.1　发生在人们身边的信息安全问题 …… 1
1.2　信息安全的基本认识 …… 2
1.2.1　信息安全的发展历程 …… 2
1.2.2　信息安全的含义 …… 3
1.2.3　信息安全的危害 …… 3
1.2.4　信息安全技术体系 …… 4
1.3　信息安全当前的特点及未来发展趋势 …… 5
1.3.1　信息安全的当前特点 …… 5
1.3.2　信息安全未来发展趋势 …… 6
1.4　本章小结 …… 7
1.5　课堂练习 …… 7
1.6　课后作业 …… 7
1.7　拓展学习 …… 7

第 2 章　操作系统安全 …… 8

2.1　操作系统概述 …… 8
2.1.1　操作系统概述 …… 8
2.1.2　操作系统的功能 …… 9
2.1.3　几种典型的操作系统 …… 11
2.2　操作系统的安全威胁 …… 14
2.2.1　漏洞威胁 …… 14
2.2.2　恶意代码 …… 16
2.2.3　入侵威胁 …… 18
2.3　操作系统的安全防范措施 …… 19
2.3.1　系统漏洞防范措施 …… 19
2.3.2　恶意代码防范措施 …… 20
2.3.3　入侵威胁防范措施 …… 24
2.4　本章小结 …… 27
2.5　课堂练习 …… 27
2.6　课后作业 …… 27
2.7　拓展学习 …… 27

第 3 章　Web 应用安全 …… 28

3.1　Web 应用安全基础 …… 28
3.1.1　Web 常见结构 …… 28
3.1.2　Web 请求流程 …… 29
3.1.3　Web 漏洞扫描 …… 31
3.2　常见的 Web 应用安全漏洞 …… 33
3.2.1　SQL 注入漏洞 …… 34
3.2.2　文件上传漏洞 …… 37
3.2.3　跨站脚本攻击漏洞 …… 39
3.2.4　CSRF 漏洞 …… 42
3.2.5　远程代码执行漏洞 …… 44
3.2.6　数据库提权漏洞 …… 45
3.3　常见 Web 漏洞的防护方法 …… 47
3.3.1　SQL 注入漏洞防护方法 …… 47
3.3.2　文件上传漏洞防护方法 …… 48
3.3.3　XSS 和 CSRF 漏洞防护方法 …… 49
3.3.4　远程代码执行漏洞防护方法 …… 49
3.3.5　UDF 提权漏洞防护方法 …… 49
3.4　本章小结 …… 49
3.5　课堂练习 …… 50
3.6　课后作业 …… 50
3.7　拓展学习 …… 50

第 4 章　网络安全 …… 51

4.1　网络安全概述 …… 51
4.2　网络安全协议 …… 52

4.3 常见的网络攻击方式 …… 54
4.3.1 ARP 欺骗 …… 54
4.3.2 网络欺骗 …… 57
4.3.3 会话劫持 …… 60
4.3.4 分布式拒绝服务攻击（DDoS） …… 63
4.4 常见的网络安全防御手段 …… 67
4.4.1 ARP 欺骗防御手段 …… 67
4.4.2 网络欺骗防御手段 …… 69
4.4.3 会话劫持防御手段 …… 70
4.4.4 DDoS 攻击防御手段 …… 71
4.5 本章小结 …… 73
4.6 课堂练习 …… 73
4.7 课后作业 …… 73
4.8 拓展学习 …… 73
第 5 章 物联网安全 …… 74
5.1 物联网概述 …… 74
5.2 物联网的安全特征与架构 …… 76
5.2.1 物联网感知层安全关键技术 …… 77
5.2.2 物联网网络层安全关键技术 …… 80
5.2.3 物联网处理层安全关键技术 …… 80
5.2.4 物联网应用层安全关键技术 …… 80
5.3 工业物联网及其安全 …… 81
5.3.1 工业物联网概述 …… 81
5.3.2 工业物联网安全 …… 83
5.4 本章小结 …… 85
5.5 课堂练习 …… 86
5.6 课后作业 …… 86
5.7 拓展学习 …… 86
第 6 章 移动互联网终端安全 …… 87
6.1 移动互联网终端概述 …… 88
6.2 移动互联网终端身份认证安全 …… 89
6.2.1 静态密码 …… 89
6.2.2 动态密码 …… 90
6.2.3 指纹密码 …… 92
6.3 移动互联网终端操作系统安全 …… 93
6.3.1 Android 操作系统的安全性 …… 93
6.3.2 iOS 操作系统的安全性 …… 95
6.4 移动互联网终端软件安全 …… 95
6.4.1 移动终端恶意软件 …… 95
6.4.2 移动终端应用恶意行为 …… 97
6.5 移动互联网终端安全防护 …… 98
6.5.1 终端用户面临的威胁 …… 98
6.5.2 防护手段和建议 …… 99
6.6 本章小结 …… 101
6.7 课堂练习 …… 101
6.8 课后作业 …… 101
6.9 拓展学习 …… 101
第 7 章 云计算及其安全 …… 102
7.1 云相关定义 …… 102
7.1.1 云计算 …… 102
7.1.2 云服务 …… 103
7.1.3 云主机 …… 104
7.1.4 云安全 …… 104
7.2 云计算现状、特点及趋势 …… 104
7.2.1 云计算现状 …… 104
7.2.2 云计算特点 …… 105
7.2.3 云计算的发展趋势 …… 106
7.3 云计算的安全隐患及解决方案 …… 107
7.3.1 IaaS 及核心架构安全 …… 107
7.3.2 PaaS 及核心架构安全 …… 114
7.3.3 SaaS 及核心架构安全 …… 120
7.4 本章小结 …… 123
7.5 课堂练习 …… 123
7.6 课后作业 …… 123
7.7 拓展学习 …… 124
第 8 章 大数据及其安全 …… 125
8.1 大数据概述 …… 125
8.1.1 大数据发展史 …… 126
8.1.2 大数据的特征 …… 126
8.1.3 大数据的分类 …… 127

8.2 大数据的价值 …… 128
8.2.1 大数据的社会价值 …… 128
8.2.2 大数据的市场价值 …… 129
8.2.3 大数据促进决策 …… 129
8.2.4 大数据驱动媒体转型 …… 129
8.2.5 大数据推动医疗创新 …… 130
8.2.6 大数据推动教育发展 …… 130
8.3 典型行业大数据应用和安全风险 …… 130
8.3.1 安全大数据 …… 130
8.3.2 电子政务大数据 …… 132
8.3.3 健康医疗大数据 …… 134
8.3.4 电商行业大数据 …… 135
8.3.5 电信行业大数据 …… 136
8.4 大数据应用安全解决思路及实践 …… 138
8.4.1 对数据进行分类标记 …… 138
8.4.2 设置用户权限 …… 138
8.4.3 增强加密系统 …… 138
8.4.4 发现潜在的数据联系 …… 138
8.4.5 大数据应用安全实践案例 …… 138
8.5 本章小结 …… 141
8.6 课堂练习 …… 141
8.7 课后作业 …… 141
8.8 拓展学习 …… 141
第 9 章 隐私保护 …… 142
9.1 隐私的概念 …… 143
9.2 隐私泄露的危害 …… 144
9.2.1 影响个人生活 …… 144
9.2.2 产生恶意广告和诈骗 …… 144
9.2.3 涉及犯罪活动 …… 145
9.2.4 导致黑客攻击 …… 145
9.3 隐私泄露的方式 …… 145
9.3.1 通过用户账号窃取隐私 …… 146
9.3.2 通过诱导输入搜集隐私 …… 147
9.3.3 通过终端设备提取隐私 …… 148
9.3.4 通过黑客攻击获得隐私 …… 148
9.4 隐私保护的措施 …… 149
9.4.1 个人隐私保护措施 …… 149
9.4.2 数据挖掘领域的隐私保护 …… 151
9.4.3 云计算领域的隐私保护 …… 153
9.4.4 物联网领域的隐私保护 …… 156
9.5 本章小结 …… 159
9.6 课堂练习 …… 159
9.7 课后作业 …… 159
9.8 拓展学习 …… 159
参考文献 …… 160

第1章 信息安全概述

随着互联网的不断普及和互联网技术的快速发展，计算机网络逐渐成为当今社会最广泛最重要的基础设施之一，人们生活和工作中的很多时间都离不开计算机网络，但网络的普遍使用也使得信息安全问题日益增多。信息安全与个人安全、社会安全乃至国家安全都密不可分。

1.1 发生在人们身边的信息安全问题

一提到信息安全，很多人就会想到“黑客”，觉得信息安全很神秘，甚至离现实生活很遥远。但实际上，在互联网时代，信息安全与我们的生活和工作是息息相关的，信息安全问题无处不在，在人们身边就发生过以下安全事件和威胁。

1. 支付宝被盗刷

不久前，宋先生发现自己支付宝内余额中的 6 650 元和余额宝中的 5 万元存款相继被转走，与支付宝绑定的工商银行卡也被转走了 7 001 元，另外还有一笔 19 999 元的转账正在进行中，尚未完成。意识到自己的支付宝被盗刷后，宋先生立即打电话通知支付宝客服停止这笔正在进行中的 19 999 元的转账，并向警方报案。

2. QQ 密码被盗

曾经有不法分子在网络上购买了病毒软件和木马程序后，再通过网络上的信息搜集平台或工具，找出或购买财务人员的 QQ 群等信息，并以同行的名义入群，待潜伏一段时间后，大量地群发伪装过的带有病毒或者木马的邮件，等待有人打开该伪装邮件，如有人无意打开，则会被不法分子盗取 QQ 密码。

3. 银行卡被盗刷

吴先生收到了一条陌生号码发来的短信，短信上写着自己的名字，吴先生以为是某个没存号码的朋友发来的，就点击了短信中的图片。一个星期之后，银行突然发来一条消费短信，原本存有 5 万多元人民币的一张银行卡，余额竟然只剩下 300 多元了。

4. 操作系统面临的威胁

目前常用的操作系统是 Windows 和 Linux，这两种系统也面临着信息安全的威胁。例如，2016 年微软在其官网发布的一份公告中表示，目前发现了少量来自俄罗斯黑客组织“Strontium”发起的网络攻击，这些黑客利用了 Windows 操作系统上的一处漏洞，并在其攻击过程中使用了“鱼叉式网络钓鱼”邮件作为工具。

5. 应用程序面临的威胁

我们常用的应用程序也面临着信息安全问题，例如，2015 年网易服务器出现大面积瘫痪，导致多数网易产品和客户端无法连接和刷新，网易旗下部分服务暂时无法正常使用。没过多久，网易邮箱又出了问题，7 月 16 日晚，陆续有网友在微博上反映网易邮箱出现登录故障，网页端显示“繁忙的系统暂时需要停下歇歇，请您稍后再试。”也有网友反馈，126 邮箱突然提示服务器密码更改，通过重输密码、修改密码等方式也无法正常登录。

以上只是曾经发生在人们身边的一部分信息安全事件和威胁，大量的安全问题还在不断地涌现，信息安全问题已经渗透到了我们的日常生活和工作中。

1.2 信息安全的基本认识

通过上面的几个案例可以看出，人们在使用信息设备和网络资源时所引发的信息安全问题越来越多，影响越来越严重。那么到底什么是信息安全？它又是如何发展起来的呢？接下来将对这些内容进行论述。

1.2.1 信息安全的发展历程

20 世纪 40 年代，通信保密正式进入学术界的视野。20 世纪 50 年代，科技文献中开始出现“信息安全”一词，至 20 世纪 90 年代，“信息安全”一词陆续出现在各国和地区的政策文献中，相关的学术研究文献也逐步增加。信息安全的发展历程大体上可以分为“通信安全时代”和“信息安全时代”两个阶段。

1. 通信安全时代

此阶段始于 20 世纪 60 年代，这个阶段一般认为信息安全就是通信安全，研究如何对信息进行编码，然后在通信信道上传输，从而防止攻击者通过窃听通信信道来获取信息。

2. 信息安全时代

此阶段始于 20 世纪 80 年代，这一阶段开始采用信息安全及其属性来描述其内涵，并提出完整性、可用性、机密性、可靠性、不可否认性，其中，机密性、完整性和可用性是信息安全的三个基本目标。这三个基本目标又被称作 CIA 三准则，内容如图 1-1 所示，其作用是为了保障信息“看不到”“改不了”和“用得着”。

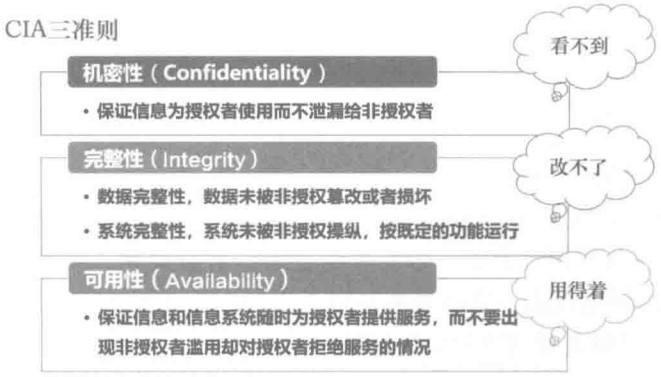


图 1-1 CIA 三准则

进入 21 世纪后，“信息安全”一词出现的范围不断扩大，在各类文献中出现的频次也不断增加，“信息安全”成为各国安全领域聚焦的重点，其既包括理论的研究，也包括国家秘密、商业秘密和个人隐私保护的探讨；既包括国家战略的策划，也包括信息安全内容的管理；既包括信息安全技术标准的制定，也包括国际行为准则的起草。信息安全已成为全球总体安全和综合安全最重要的非传统安全领域之一。

1.2.2 信息安全的含义

所谓信息安全，是指保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受[1]。它是为维护计算机网络的正常秩序，避免信息、言论被滥用，避免对个人隐私、社会稳定、经济发展、国家安全造成恶劣影响而采取的一切措施，也就是为确保网络和信息系统的安全性，所建立和采取的一切技术层面和管理层面的安全防护举措，包括避免联网硬件、网络传输、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露，使系统能够连续、正常运行而采取的技术手段或管理监督的办法，以及对计算机网络中一切可能危害他人或国家利益的行为进行约束、监管及预防和阻止的措施。

以数字化、网络化、智能化、互联化、泛在化为特征的网络社会，为信息安全带来了新技术、新环境和新形态，信息安全开始更多地体现在网络安全领域，反映在跨越时空的网络系统和网络空间之中，反映在全球化的互联互通之中。由于人类开始生存在信息环境当中，人与信息相互作用相互影响，因此信息安全问题更加突出。

目前，一方面是信息技术与产业的空前繁荣，另一方面是危害信息安全的事件不断发生。敌对势力的破坏、黑客的攻击、恶意软件的侵扰、利用计算机进行的犯罪、隐私的泄露等，对信息安全构成了极大威胁。除此之外，科学技术的进步也对信息安全提出了新的挑战。由于量子和 DNA 计算机具有并行性，许多现有公钥密码（RSA、ELGamal、ECC 等）在量子和 DNA 计算机环境下不再安全。可见，信息安全形势越来越严峻。

1.2.3 信息安全的危害

信息安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络乃至生活当中的合法权益面临严峻风险与挑战。

（1）信息渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、信息窃密等活动严重危害国家政治安全。

（2）网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

（3）有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息可能会侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

（4）网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用

网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民的生命财产安全和社会秩序。计算机病毒、木马等在网上传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

1.2.4 信息安全技术体系

信息安全涉及的领域众多，内涵丰富，且信息安全很多相关技术尚在飞速发展中，本书无法将所有内容完整呈现，而是把学术界和产业界对信息安全的阐述做了整合，涵盖了信息安全的主要内容，重点讨论几个核心内容和热点问题，包括操作系统安全、Web 应用安全、网络安全、物联网安全、移动互联网终端安全、云计算及其安全、大数据及其安全和隐私保护。从信息安全的现状和发展来看，这几个层次相互依存、相互交织、相互渗透，而且在一定条件下能够相互转化。

本书的信息安全技术体系架构如图 1-2 所示。

图 1-2 信息安全技术体系

本书的技术体系主要包括以下一些内容。

（1）操作系统安全。本章通过对 PC 和移动终端操作系统常见的安全问题进行讲解，使读者对操作系统安全有更加全面的认识和理解，学会如何更加有效地保护操作系统。

（2）Web 应用安全。本章主要从 Web 应用安全基础、常见的 Web 应用安全漏洞及防护方法等几个方面来阐述 Web 应用系统的安全问题，使读者对 Web 应用安全有更加全面的认识和理解。

（3）网络安全。本章主要介绍部分网络安全协议、网络层所存在的常见攻击方式和网络安全防御手段。

（4）物联网安全。本章将论述物联网的定义和应用领域，物联网的安全特征与架构，以及工业物联网及其安全，使读者能够对什么是物联网、物联网都有哪些安全特性和物联网安全等方面的知识有较为全面的认识和理解。

（5）移动互联网终端安全。本章从手机、PAD 等移动互联网终端行业，来介绍移动终端在新时期互联网时代下面临的安全威胁及防护方法。

（6）云计算及其安全。本章将从云的技术核心、服务类型及发展趋势等方面对当下网络环境中的云做深度剖析。同时针对受到越来越多关注的云安全问题，提出相应的预防和解决方案。

（7）大数据及其安全。从技术上看，大数据与云计算的关系就像一枚硬币的正反面一样密不可分，大数据要依托于云计算基础设施进行大容量数据的存储、挖掘和分析处理。本章将从大数据的价值、一些典型行业的大数据应用和安全风险，以及大数据应用安全解决思路等几个方面来讲解大数据的安全问题。

（8）隐私保护。我们有的时候并不愿意把某些信息告诉给他人，对于个人来说，这些信息被称作隐私，在团队中也有某些信息是不想公布于众的，这些信息大多数被称作保密信息。在本书中，无论是个人的还是团队的信息，统称为隐私，本章将对隐私保护方面的内容进行深入讲解。

1.3 信息安全当前的特点及未来发展趋势

1.3.1 信息安全的当前特点

当前，信息安全问题日益严重，网络渗透的方法越来越隐蔽，形式也越来越多样化，信息安全呈现出以下一些特点。

1. 安全攻击的高级性

在国际互联网的背景下，人们面临的安全攻击级别更高，隐蔽性更强，技术更强大，给信息安全防护带来了前所未有的挑战。信息安全成了政治博弈的主战场，成了窃密与反窃密斗争的前沿阵地，也成了不法分子进行犯罪活动的暗舞台。近年来，有组织的网络犯罪、网络恐怖主义甚至国家层面的高级攻击行为给新形势下的信息安全构成的巨大威胁日益严重。

2. 安全威胁的多元性

安全威胁出现了攻击多元性的特点。在国际互联网条件下，攻击的对象、手段、形式

都层出不穷，呈现出多样化、多类型、特征复杂的态势，安全威胁的多元性，使各类互联网终端都受到影响。

3. 安全危害的倍增性

在国际互联网条件下，各网络相互融合，信息互通和共享性更强，信息安全危害性也更广，一旦出现安全事件，其危害会迅速从区域向广域扩散，由个体向群体蔓延，由一种危害引发多种危害，呈现出非线性激增的态势。

4. 安全对抗的非对称性

根据木桶原理，信息安全体系中出现任何一个薄弱环节，都可能对整体安全体系构成威胁，造成无法估量的严重后果。信息安全防护本身就是一个难守易攻的领域，对于攻击者而言，被攻击目标总是明确的，漏洞总是可以被试探和挖掘的，因此，可以通过搜集、尝试所有可用资源，发动针对目标的攻击；而对于防护者而言，攻击感知、攻击类型分析、密码破译感知等一直以来都是难题，使得安全对抗具有明显的非对称性。

1.3.2 信息安全未来发展趋势

目前，信息安全呈现出安全攻击高级性、多元性、倍增性和非对称性等特点，信息又是继陆、海、空、天以外的第五作战空间和“军事高地”，是人类活动的新领域，已经成为与经济、社会、政治、文化相联系的纽带。未来信息安全的发展趋势可分为以下几个方向。

1. 万物互联

随着新一代移动通信技术、Web 2.0 等网络技术的发展，以及移动互联网、物联网、云计算和大数据等应用的普及，网络已进入“万物互联、智慧互通”的新时代，同时也标志着信息化进入“以数据的深度挖掘与融合应用为特征的智慧化”新阶段，信息的获取和利用即将达到“信息随心行，交互在指间；搜索随意行，推荐在指间”的理想境界。

2. 业务网与工控网互联互通是未来发展趋势

未来各种业务网络互联互通是技术演化的必然结果，大多数场景下，网络之间的物理隔离将不复存在，亟须研究高强度逻辑隔离技术来应对未来广泛互联互通的网络所带来的安全隐患。例如，过去的防护和管控往往分布在不同的设备上，未来需要能够实现防护、管控、感知和处置的综合安全防护设备。

3. 更容易出现重大的信息泄露事件

人类生活越来越依靠现代科技、互联网、移动互联网和物联网，以及随之而来的大数据和云服务，加上黑客行为的组织化和产业化，这些将很有可能造成下一次重大信息泄露事件的发生。云服务的快速普及和应用，使其越来越受到恶意黑客的关注，而且云服务的完全依赖在线服务和一套登录口令对应所有信息存储服务的特性，更有可能使其爆发出大规模的恶性信息泄露事件。

4. 攻防技术的矛与盾，攻击者的技术也在不断进化

随着网络攻防强度、频率、规模，以及影响力的不断升级，未来的安全技术将逐渐朝自动化、智能化、定制化和整体化等方向发展，在单点防护和检测上越来越深，同时在整

体防护上更加系统和智能。不仅能够防范已知的攻击，还能够感知即将发生的威胁，预先采取措施。

总而言之，如今对信息安全的研究已引起世界各国的高度重视，吸收和借鉴国外相关领域的先进理念和科学方法，对推动和促进我国在信息安全领域的发展具有重要意义。长路漫漫，任重道远，我们需要突破以往的发展思路，调动各方科研力量，尝试多种创新实践方法，从根本上解决制约信息安全长远发展的难题，摆脱受制于人的不利局面，占领信息制高点。纵观信息技术发展的历史，就是已有科幻不断成为现实的展现，未来的科幻将不断地涌现，也会持续不断地成为现实。

1.4 本章小结

本章首先描述了曾经发生在人们身边的一些信息安全问题，并对信息安全的发展历程、信息安全的含义及其危害进行了论述。然后对本书所涉及的信息安全技术进行了体系化的整理和说明，最后对信息安全当前的特点和未来发展趋势进行了展望，使读者充分认识到学习信息安全的重要性和紧迫性，为继续学习后面的操作系统安全、Web 应用安全和网络安全等章节打下良好的基础。

1.5 课堂练习

（1）信息安全的发展背景是什么？

（2）信息安全的危害有哪些？

（3）信息安全的当前特点是什么？

1.6 课后作业

（1）什么是信息安全？

（2）信息安全未来的发展前景如何？

（3）列举一些你身边遇到或发现的信息安全问题，尝试分析其中的原因，并说明有哪些防范措施。

1.7 拓展学习

如果读者对信息安全感兴趣，想进一步了解相关技术，可以参阅由清华大学出版社出版，郝玉洁、吴立军、赵洋、刘瑶编著的《信息安全概论》，进行深入学习。

扫一扫在线测