网络空间安全丛书

信息安全原理与实践

(第3版)

[美]马克·斯坦普(Mark Stamp) 著

冯 娟 赵宏伟 姚领田 杜天德 译

清華大學出版社

北 京

北京市版权局著作权合同登记号　图字：01-2022-6221

All Rights Reserved. This translation published under license. Authorized translation from the English language edition, entitled Information Security Principles and Practice, Third Edition, 9781119505907, by Mark Stamp, Published by John Wiley & Sons. Copyright © 2022 by John Wiley & Sons, Inc. No part of this book may be reproduced in any form without the written permission of the original copyrights holder.

Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

本书中文简体字版由 Wiley Publishing, Inc. 授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或传播本书内容。

本书封面贴有 Wiley 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。举报：010-62782989，beiqinquan@tup.tsinghua.edu.cn。

图书在版编目(CIP)数据

信息安全原理与实践：第 3 版/(美)马克·斯坦普(Mark Stamp)著；冯娟等译. —北京：清华大学出版社，2023.10

(网络空间安全丛书)

书名原文：Information Security Principles and Practice，Third Edition

ISBN 978-7-302-64535-1

Ⅰ. ①信…　Ⅱ. ①马…　②冯…　Ⅲ. ①信息系统－安全技术　Ⅳ. ①TP309

中国国家版本馆 CIP 数据核字(2023)第 167125 号

责任编辑：王　军
封面设计：孔祥峰
版式设计：思创景点
责任校对：成凤进
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：010-83470000　　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

印 订 者：涿州汇美亿浓印刷有限公司

经　　销：全国新华书店

开　　本：170mm×240mm　　**印　　张**：24.75　　**字　　数**：457 千字

版　　次：2023 年 10 月第 1 版　　**印　　次**：2023 年 10 月第 1 次印刷

定　　价：99.80 元

产品编号：096094-01

关 于 作 者

我一直活跃在信息安全领域，我在美国国家安全局(National Security Agency，NSA)工作了七年多，随后在硅谷一家初创公司工作了两年。虽然不能透露太多我在国家安全局所做的工作，但可以告诉你，我的职称是密码数学家。在工业界，我帮助设计和开发了一个数字版权管理安全产品。这种现实世界的经历与学术工作相互交叉。在学术界，我的研究涉及各种各样的安全主题，包括机器学习和深度学习的各个方面。

当我在本世纪初回到学术界时，几乎没有什么可用的安全书籍，而且似乎没有一本书与现实世界有紧密联系。我觉得自己可以写一本教科书来填补这一空白，并且该书可以起到双重作用，既是教科书又是 IT 专业人员的有用资源。根据收到的反馈，本书前两个版本似乎在这两个方面都相当成功。

我相信，本书第 3 版将证明其作为教科书和专业人士的资源所起到的双重作用更有价值。可以说，我以前的许多学生现在都在领先的硅谷科技公司工作(有些人已创办了自己的公司)，他们告诉我，他们在该课程中学到的东西特别有用。我当然希望自己在业界工作时，也能有这样一本书，因为我和我的同事们会从中受益匪浅。

在信息安全领域之外，我也有自己的生活。我的家人包括我深爱的妻子 Melody 和两个优秀的儿子，Austin(他的名字首字母是 AES)和 Miles(多亏 Melody，他的名字首字母不是 DES)。除了丰富多彩的其他活动，我们还喜欢户外活动，包括定期的本地徒步旅行。我大部分空闲时间都在蒙特利湾划皮划艇、钓鱼和航行，或者在位于易发生野火和地震的圣克鲁斯山区的老房子里工作。

致　　谢

我从事信息安全领域工作始于读研究生期间。首先，我要感谢我的论文导师 Clyde F. Martin，是他向我介绍了这个令人兴奋的课题。

在国家安全局工作的七年多时间里，我学到的安全知识比在其他任何地方学到的都要多。在职业生涯中，我要感谢 Joe Pasqua 和 Paul Clarke，他们给了我这个机会，让我从事一个迷人而富有挑战性的项目。

对于本书第 1 版，SJSU 的同事 Richard Low 对手稿的早期版本提供了许多有益的反馈。David Blockus(上帝保佑他的灵魂) 特别值得一提，因为他在第 1 版写作的关键时刻对每一章都提供了详细的评论。

对于本书第 2 版，我的许多 SJSU 学生“自愿”担任校对，还有许多人提供了有益的评论和建议。在这里，我还想感谢提出了许多详细评论和问题的 John Trono(圣迈克尔学院)。

对于本书第 3 版，我想感谢的学生太多了，以至于无法一一列举，他们对本书的几乎每个方面都作出了积极的贡献。但是，我想特别感谢 Vanessa Gaeke 和 Sravani Yajamanam，这两位优秀的学生仔细阅读了手稿，并提出了一些深思熟虑和发人深省的问题，这些问题极大地改进了本书的质量。

像任何大型软件项目一样，再多的调试也无法发现如此规模和范围的书中存在的所有不足。当然，任何遗留的瑕疵都是作者一个人的责任。

前　言

拜托，先生或女士，你不看看我的书吗？我花了很多年才写出来的，你不看一下吗？

—Lennon 和 McCartney

我讨厌黑盒。我撰写本书的主要目的在于阐明如今信息安全书籍中流行的一些黑盒。另一方面，我不想用琐碎的细节烦扰你——如果这是你想要的，可以去读 RFC。因此，本书经常会忽略那些我认为与所要表达的观点无关的细节。你可以判断我是否在这两个相互竞争的目标之间取得了适当的平衡。

我一直在努力持续跟进，以便涵盖广泛的主题。本书的目标是深入讨论每一项内容，以便你能够理解安全问题，同时不会在细节上陷入太多的困境。我还试图定期强调和重申要点，这样就不会错过关键信息。

撰写本书的另一个目标是以生动有趣的方式呈现主题。如果有任何计算主题令人兴奋和富有趣味，那就是信息安全。

我也试图在本书中插入一点幽默。人们说幽默源于痛苦，从笑话的质量来看，可以说我的生活绝对是有魔力的。无论如何，大多数糟糕的笑话都会在脚注中出现，所以它们不会太分散你的注意力。

一些安全教科书提供了大量枯燥的理论。阅读它们就像阅读微积分教科书一样令人兴奋。其他书籍提供了一些看似随机的、不相关的事实，给人的印象是安全根本不是一个真正连贯的主题。还有一些书籍把这个主题描述成一堆高级的管理性陈词滥调。最后，一些书侧重于安全中人的因素。虽然所有这些方法都有它们的作用，但我的看法是，首先，安全工程师必须完全理解底层技术的固有优势和弱点。

信息安全是一个巨大的主题，与其他更成熟的领域不同，这类书应该包括什么内容，或者如何以最佳方式组织它，作者并不完全清楚。我选择围绕以下四个主题来组织本书：

- 加密技术

- 访问控制
- 网络安全
- 软件

在上述结构中，这些主题富有弹性。例如，在访问控制主题下，包含了传统的认证和授权主题，以及 CAPTCHA 之类的非传统主题。软件主题非常灵活，包括软件开发、恶意软件和逆向工程等各种话题。

虽然本书关注的是实际问题，但已尽力涵盖了足够多的基本原则，这样就可以为从事该领域的进一步研究做好准备。此外，我已尽可能地将背景要求降到最低。特别是，数学形式主义被保持在最低限度(附录包含几个基本数学主题的回顾)。尽管存在这种自我强加的限制，但我相信这本书比大多数安全书籍包含了更多实质性的加密技术。学习本书，所需的计算机科学背景也很少——一门介绍性的计算机组织课程(或类似的经验)就足够了。假设你有一些编程经验，那么汇编语言的基本知识在几个章节中会有帮助，但不是强制性的。本书涵盖了网络基础知识，因此不需要具备之前在该领域的知识或经验。

如果你是一名信息技术专业人员，正在努力学习更多关于安全的知识，我建议你阅读整本书。本书中大多数话题都是相互关联的，跳过少数不相关的话题也不会节省太多时间。即使你是某个领域的专家，至少浏览一下我的介绍也是值得的，因为在这个领域使用术语时经常会出现不一致的情况，本书可能会提供一个不同于你在其他书中看到的视角。

如果你在教授一门安全课程，本书包含的内容可能会比一学期的课程所能涵盖的知识稍微多一点。我在本科安全课程上通常遵循的时间表如表 1 所示。

表 1 教学大纲建议

章节	时长	建议范围
1. 引言	1	全部
2. 经典加密	3	全部
3. 对称密码	4	全部
4. 公钥加密	4	全部
5. 加密散列函数	4	省略 5.7 节中的攻击细节
6. 认证	4	全部
7. 授权	2	全部
8. 网络安全基础	3	省略 8.5 节
9. 简单认证协议	4	省略 9.4 节
10. 现实世界的安全协议	4	省略 WEP 或 GSM

(续表)

章节	时长	建议范围
11. 软件缺陷与恶意软件	4	全部
12. 软件中的不安全因素	3	全部
总计	40	

安全不是一项观赏性的运动——解答大量的作业习题是学习本书内容的一个重要方面。许多主题在习题中进一步充实，有时会引入额外的主题。底线是你解决的问题越多，你学到的知识就越多。

基于本书的安全课程是个人或团体项目的理想选择。教科书网站(http://www.cs.sjsu.edu/~stamp/infosec/)包括关于密码分析的部分，这是加密项目的一个可能来源。此外，许多作业习题很适合课堂讨论或课堂作业，例如第 10 章中的问题 16 或第 11 章中的问题 17。

在教科书网站上你可以找到 PowerPoint 幻灯片、习题中提到的所有文件、勘误表和许多其他有用的东西。如果第一次教授这门课，我会特别推荐 PowerPoint 幻灯片，这些幻灯片已经过彻底的“实战检验”，并经过多次改进。

附录中提到的数学知识在本书中是如何应用的呢？初等模运算出现在第 3 章和第 5 章的几节中，而数论结果需要在第 4 章和第 9 章的 9.5 节中使用。我发现大多数学生都需要温习模运算基础知识。只需要 20～30 分钟的课堂时间就可以涵盖模运算的内容，在深入研究公钥加密技术之前，花费这些时间是非常值得的。

附录中简要讨论的置换在第 3 章中最为突出，关于离散概率的材料需要在第 6 章的密码破解部分找到。

就像任何大型复杂的软件项目都有缺陷一样，可以形而上学地认为本书也会有不足。我想知道你发现的任何问题——或大或小。我将努力在教科书网站上维护一份最新的勘误表。此外，不要犹豫，请为这本书的未来版本提供任何建议。

第 3 版的新增内容

本书的几部分被重新组织和扩展，而其他部分(和两个完整的章节)被删除。网络安全的主要部分涵盖了更广泛的主题，包括网络简介，这使得基于本书的课程更独立。根据本书的使用者反馈，在加密章节中新增了额外的例子，而协议章节已被修改和扩展。第 1 版和第 2 版包含了一章关于现代密码分析的内容，这一章已从第 3 版中删除了，但仍然可以在教科书网站上找到，其他被删除的主题也是如此。

所有的图形都经过了重新处理，变得更清晰、更好。当然，第 2 版中所有已知的错误都被改正。作业习题也已进行了更新。

信息安全是一个不断发展的领域，自本书于 2005 年首次出版以来，已发生了一些重大变化。然而，第 1 版的基本结构大体上保持不变。我相信这些年来本书主题的组织和列表一直保持得很好。因此，对于第 3 版，本书的结构变化更多的是进化而不是革命。

在此要说明的是，本书的参考文献和第 12 章习题中提到的一些压缩文件读者可通过扫描封底的二维码进行下载。

Mark Stamp
Los Gatos, California
2021 年 6 月

目　录

第III部分 网络安全主题

第 1 章 引 言

"Begin at the beginning," the King said, very gravely,
"and go on till you come to the end: then stop."
—Lewis Carroll, *Alice in Wonderland*

1.1 人物角色

按照传统观念，Alice 和 Bob 是好人(译者注：信息安全类教科书里的两大主角)。分别如图 1.1(a)和(b)所示，Alice 和 Bob 通常会尝试做正确的事情。偶尔，我们也会需要一两个额外的好人，如 Charlie 或 Dave。本书反复强调的一个主题是，固执的人经常犯愚蠢的错误，就像现实生活中的人一样。

图 1.1(c)中的 Trudy 通常是指一个搞破坏的坏家伙，她总是试图以某些方式对系统进行攻击。一些信息安全书籍或文章的作者会组建一个坏小子团队，其中会以不同的人名分别暗示特定的恶意活动，于是在这种情况下，Trudy 就是一个“入侵者”，Eve 则是一个“窃听者”，诸如此类。为简单起见，Trudy 扮演的是一个无

恶不作的坏家伙，而 Eve 只是会暂时客串一下。与经典好莱坞西部片中的坏人一样，本书中的坏人总是戴着一顶黑帽子。

Alice、Bob、Trudy 和其他指代不一定是人。例如，在许多可能的示例中，Alice 可以指笔记本电脑，Bob 可以指服务器，而 Trudy 可以指人。

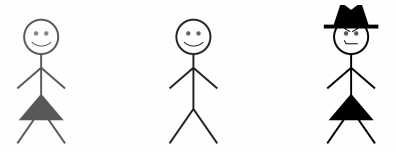

图 1.1　主角

1.2　Alice 的网上银行

假设 Alice 开通了名为 Alice's Online Bank[1](简称 AOB)的网上银行服务，那么 Alice 关注的信息安全问题应该是什么？如果 Bob 是 Alice 的客户，那么 Bob 要关注的信息安全问题是什么？Bob 和 Alice 关注的内容相同吗？如果从 Trudy 的视角来看 AOB，那么能看到哪些安全漏洞？

首先，结合 Alice 的网上银行服务，我们考虑一下 AOB 中传统的机密性、完整性和可用性(Confidentiality、Integrity、Availability，或 CIA[2])三要素。然后，将指出许多其他可能出现的安全问题。

1.2.1　机密性、完整性和可用性

机密性指的是防止未经授权读取信息。AOB 可能不会太在意它所处理的信息的机密性，除非它的客户确实很在意。例如，Bob 不想让 Trudy 知道他的储蓄账户中有多少钱。因此，如果 Alice 的银行未能保护这些信息的机密性，它还将面临相关的法律问题。

完整性指的是防止或至少检测未经授权的“写入”(即对数据的更改)。Alice 的银行必须保护账户信息的完整性，以防止 Trudy 增加其账户中的余额或更改 Bob 账户中的余额。注意，机密性和完整性不是一回事。例如，即使 Trudy 无法读取数据，她也可以修改这些数据，如果她的这种修改行为不被发现，就会破坏数据

1 不要与“Alice 餐厅”混淆[52]。

2 注意不是中情局。

的完整性。在这种情况下，Trudy 可能并不知道她对数据做了哪些更改(因为她不能读取数据)，但她可能不在乎——有时对 Trudy 来说，仅仅制造麻烦就足够了。

拒绝服务(Denial of Service，DoS)攻击是一个相对较新的问题。这类攻击试图阻止用户对信息的访问。由于 DoS 攻击的增多，数据可用性已成为信息安全中的一个重要问题。可用性是 Alice 的银行和 Bob 都关心的问题——如果 AOB 的网站不可用，Alice 就不能从客户交易中赚钱，Bob 也不能做成他的生意。这样，Bob 可能会把他的生意转移到别处。如果 Trudy 对 Alice 怀恨在心，或者只是想恶意攻击，那么她就可能会尝试对 AOB 进行拒绝服务攻击。

1.2.2 CIA 并不是全部

机密性、完整性和可用性只是信息安全这个故事的开始。下面从头开始，考虑 AOB 的客户 Bob 登录到他的计算机时的情景。Bob 的计算机如何确定“Bob”真的是 Bob 而不是 Trudy？当 Bob 登录他在 Alice 网上银行的账户时，AOB 如何知道“Bob”是真实的 Bob，而不是 Trudy 冒充的？虽然这两个认证问题表面上看起来很相似，但实际上其背后的机理几乎完全不同。

在一台独立的计算机上进行认证通常需要验证 Bob 的密码。为了确保安全，需要使用密码学领域的一些巧妙技术。另一方面，网络上的认证容易受到多种攻击，而这些攻击通常与独立的计算机无关。Trudy 可能会看到通过网络发送的消息。更糟糕的是，Trudy 还可能拦截消息、篡改消息，并插入她自己制作的消息。如果是这样，Trudy 就可以简单地重新发送 Bob 的旧信息，以说服 AOB，她真的是 Bob。因此，通过网络进行认证需要特别注意协议，即交换消息的组成和顺序。密码学在安全协议中也扮演着重要的角色。

一旦 Bob 通过了 AOB 的认证，那么 Alice 必须对 Bob 的行为进行限制。例如，Bob 不能查看 Charlie 的账户余额，也不能在 AOB 的系统上安装新的会计软件。但是，AOB 系统管理员 Sam 可以安装新软件。实施这些限制需要经过授权。注意，授权对已认证用户的操作施加了限制。由于认证和授权都涉及对各种计算和网络资源的访问，因此我们将在有关访问控制的章节中讨论它们。

到目前为止讨论的所有信息安全机制都是用软件实现的。如果你仔细想一想，在现代计算系统中，除了硬件，还有什么不是软件呢？如今，软件系统趋向于庞大、复杂并充斥着各种缺陷(bug)。软件缺陷不仅是一种烦恼，它还是一个潜在的安全问题，因为它可能会导致系统行为失常。显然，Trudy 喜欢系统出现错误。

哪些软件缺陷是安全问题，它们是如何被攻击者利用的呢？AOB 如何确保它的软件运行正确？AOB 的软件开发人员如何减少(或者在理想情况下消除)软件中

的安全缺陷？我们将在本书中研究这些与软件开发相关的问题(以及其他更多的内容)。

尽管软件缺陷可能(并且确实)导致安全缺陷，但是这些问题是由善意的开发人员无意中造成的。另一方面，有些软件是带着作恶的意图编写的。这种恶意软件的例子包括当今困扰互联网的众所周知的计算机病毒和蠕虫。这些讨厌的家伙是如何生成的，Alice 的网上银行能做些什么来限制其带来的危害呢？Trudy 又会做些什么来使这种病毒变得更令人讨厌呢？本书将考虑这些问题以及相关的问题。

当然，Bob 也有许多软件上的顾虑。例如，当 Bob 在计算机上输入密码时，他如何知道该密码没有被捕获并发送给 Trudy？如果 Bob 在 Alice 的网上银行进行一笔交易，他如何知道在屏幕上看到的交易与实际去银行柜台办理的交易是同一笔交易呢？也就是说，Bob 如何确信他的软件(更不用说网络)正在按照正常的方式运行，而不是按照 Trudy 希望的方式运行？本书中，我们也会考虑这类问题。

1.3 关于本书

Lampson[69]认为现实世界的安全可以归结为以下几点：

- 规范/策略——系统应该做什么？
- 实现/机制——如何做到的？
- 正确/保证——系统真的可以正常运行吗？

生性谨慎的本书作者在此谨慎地增加了第四点：

- 人的天性——系统能经受住“聪明”用户的考验吗？

本书重点介绍有关实现/机制方面的内容。自信的作者向你保证，对于入门课程来说，这样的安排是合适的，甚至是必要的，因为这些机制的优点、缺点和固有限制会直接影响安全的所有其他方面。换句话说，如果对这些机制没有正确的理解，就不可能对其他相关的安全问题进行讨论。

本书内容分为 4 个主要部分。第 I 部分讨论密码学，第 II 部分讨论访问控制，第III部分将重点转移到网络安全上，重点是安全协议。本书的最后一个主要部分涉及软件这一宽泛而又相对模糊的主题。希望前面对 AOB[1]的讨论已经使你相信这些主题都与现实世界的信息安全相关。

在本章的其余部分，我们将快速预览这 4 个主题。本章以总结结尾，当然，最后还有一些有趣的习题可作为家庭作业。

1 你读过了，对吗？

1.3.1 加密技术

加密技术是信息安全的基本工具。加密技术的用途非常广泛，包括提供机密性和完整性，以及其他重要的信息安全功能。本书将详细讨论加密技术的相关内容，因为对于信息安全领域来说，任何实质性的讨论，都要以此作为基本的背景。

我们将从一些经典的密码系统开始加密技术的学习。除了具有显而易见的历史价值和趣味性，这些经典密码系统均揭示了密码学中的一些基本原则，而这些原则在现代数字加密系统中仍在运用，只是以用户更容易接受的方式呈现出来而已。

有了这个背景，就可以准备学习现代加密技术了。对称密钥密码学(symmetric key cryptography)和公钥密码学(public key cryptography)是加密技术的两个主要分支，在信息安全中发挥着重要作用。本书将用整整一章的篇幅来讨论对称加密，另一章讨论公钥系统。然后，将注意力转向加密散列函数，这是另一种基本的安全工具。散列函数被用在许多不同的环境中，其中一些令人惊讶，甚至近乎违反直觉(如区块链)。

然后，简要考虑几个与加密技术相关的特殊主题。例如，将讨论隐写术，其目标本质上是在众目睽睽之下隐藏信息。

1.3.2 访问控制

如上所述，访问控制解决的是认证和授权的问题。在认证领域，我们将考虑许多与密码相关的问题。密码是当今最常用的认证形式，但这主要是因为密码的成本低廉，而绝对不是因为它们是最安全的选项[1]。

本书将讨论如何安全地存储密码。然后，深入探讨如何选择安全密码以及其他相关的问题。在现实世界的系统中，密码通常是一个主要的安全漏洞。

密码的替代方案包括生物识别技术和各种物理设备，如智能卡。本书将讨论这些认证形式的一些安全优势。特别是，将讨论几种生物认证技术。

回想一下，授权涉及对已认证的用户进行限制。施加这些约束条件有两种经典的方法，即所谓的访问控制列表[2]和访问能力列表(矩阵)。你将了解每种方法的优缺点。

谈到授权，自然会引出一些相对专业的话题。本书还将讨论多级安全性，这

1 如果有人问你，当有更好的选择时，为什么要使用特定的弱安全措施，正确的答案通常是“钱”，或者可能只是因为无法克服惰性。

2 访问控制列表(ACL)是信息安全领域的常见术语之一。

将引导读者了解信息安全领域的深层内容。还讨论了隐蔽信道(covert channel)和推理控制(inference control)，这是一些在实际系统中具有挑战性的问题。

1.3.3 网络安全

第三个主要话题是网络安全，将重点讨论安全协议。首先，概述了网络的相关知识，特别是重点介绍了随之出现的安全问题，包括对防火墙的讨论。

然后，考虑通过网络进行认证时出现的一些问题。下文提供了许多示例，每个示例都说明了一个特定的安全隐患。例如，重放攻击(replay attack)是一个关键问题，因此需要考虑通过有效的方法来防止这种攻击。

密码学是认证协议中的一个基本要素。本书将给出使用对称密码学协议的例子，以及依赖公钥密码学的例子。散列函数在安全协议中也扮演着重要的角色。

对简化的认证协议的研究将说明该领域中可能出现的许多微妙问题——一个看似微不足道的变化可能会完全改变协议的安全性。本书还将重点介绍现实安全协议中常用的各种特定技术。

然后，将继续研究几个现实世界的安全协议。首先，了解所谓的安全外壳协议(Secure Shell，SSH)，这是一个相对简单的例子。接下来，考虑安全套接字层(Secure Sockets Layer，SSL)，它被广泛用于保护互联网上的电子商务。精心设计的 SSL 协议优雅而高效，它具有特定的用途。

我们还讨论了 IPsec，这是另一种互联网安全协议。从概念上讲，SSL 和 IPsec 有许多相似之处，但实现方式却截然不同。与 SSL 相反，IPsec 较为复杂——人们常说它被过度设计了。由于其复杂性，IPsec 中存在一些相当重要的安全问题。SSL 和 IPsec 之间的对比说明了在设计安全协议时所面临的一些固有挑战。

要考虑的另一个现实世界的协议是 Kerberos，它是一个基于对称密码学的认证系统。Kerberos 遵循一种完全不同于 SSL 或 IPsec 的方法。

本书还将讨论两种无线安全协议：WEP 和 GSM。这两种协议都存在许多安全缺陷，包括底层密码学的问题，以及协议本身的问题，这些都将是很有趣的学习案例。

1.3.4 软件

本书的最后一部分，将了解与软件密切相关的某些安全方面。这是一个复杂的话题，但本书的两章内容尽量涵盖了大多数基本问题。首先，我们将讨论上面提到的安全缺陷和恶意软件。此外，还将考虑软件逆向工程，它展示了在无法访问源代码的情况下，一个职业攻击者是如何解构软件的。

1.4 人的问题

用户在无意中对安全系统造成损害的能力令人难以想象。例如，假设 Bob 想从 Amazon 网站上购买一件商品。Bob 可以使用他的 Web 浏览器通过 SSL 协议(在第Ⅲ部分中讨论)安全地接入 Amazon，该协议依赖于各种加密技术(参见第Ⅰ部分)。在这类交易中会出现访问控制问题(参见第II部分)，所有这些安全机制都是在软件中实现的(参见第Ⅳ部分)。到目前为止，一切都很顺利。但你将看到，Trudy 可以对该交易进行实际攻击，这将导致 Bob 的 Web 浏览器发出警告。如果 Bob 听从警告，Trudy 的攻击将被挫败。遗憾的是，Bob 很可能会忽略这个警告，从而否定了这个复杂的安全体系结构。也就是说，即使密码、协议、访问控制和软件都完美无缺地运行，安全性也可能由于用户的疏忽而被破坏。

再举一个有关密码问题的例子。用户希望选择容易记忆的密码，但这也让 Trudy 更容易猜到密码。一个可能的解决方案是为用户分配强密码。然而，这通常是一个坏主意，因为它可能会导致密码被写下来并张贴在显眼位置，与允许用户选择他们自己的(较弱的)密码相比，将密码写下来可能会使系统更不安全。

如上所述，本书旨在理解安全机制——安全的基本要素。然而本书中出现了各种各样的“人的问题”。关于这个主题可以写几本书，但底线是，从安全的角度来看，我们希望尽可能地将人排除在外。

关于人在信息安全中所扮演角色的更多信息，一个很好的来源是阅读 Ross Anderson 的书[3]。Ross Anderson 的这本书中涵盖了安全失效的案例研究，其中(如果不是大部分的话)至少有一个根源与所谓的好人 Alice 和 Bob 的行为有关。虽然我们预计 Trudy 会做坏事，但令人惊讶的是，Alice 和 Bob 的行为往往有助于而不是阻碍 Trudy 做坏事。

1.5 原理和实践

本书不是一本理论著作。虽然理论的重要性毋庸置疑，但笔者坚持认为，信息安全的许多方面还没有成熟到足以开展有意义的理论研究的程度[1]。当然，

1 例如，考虑一下臭名昭著的缓冲区溢出攻击(buffer overflow attack)。它是历史上有史以来最严重的安全缺陷之一。这一特殊现象背后的宏大理论是什么？根本没有——这基本上是由于现代处理器内存布局不当而产生的一个怪癖。

有些主题本质上比其他主题的理论性更强。但即使是理论性更强的安全主题，不需要深入钻研理论也可以学到一些实用知识。例如，加密技术可以(也常常就是这样)从高等数学的角度去教授。不过，除了极少数例外，只需要一些基础的数学知识就足够理解重要的密码技术原理了。

当然，本书也不是攻击者的操作指南。但是，也会为读者理解和体会背后的基本概念提供足够的深度，目的就是要深入到某种恰当的程度，不至于因为烦琐的细节就把读者吓倒。诚然，这需要一种微妙的平衡，毫无疑问的是，许多人并不认同本书已达成了适当的平衡。无论如何，本书涉及了大量与各种基本原理相关的安全主题。这种广度必然以牺牲一些严谨性和细节为代价。

对于那些渴望从理论上探讨本书所涉及的一些主题的人来说，Bishop 的书[10]是首选。有许多优秀的书籍和文章更详细地介绍了本书中讨论的各种安全主题。用你最喜欢的搜索引擎很快就可以搜索到许多这样的资源。

1.6 习题

The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem.

—Theodore I. Rubin

1. 信息安全的基本挑战包括机密性、完整性和可用性，即 CIA。
   a) 定义机密性、完整性和可用性这三个术语。
   b) 请列举一个机密性和完整性都非常重要的具体例子。
   c) 列举一个具体的例子，说明完整性比机密性更重要。
   d) 列举一个可用性是首要考虑的具体例子。

2. 从银行的角度来看，客户数据的完整性和数据的机密性哪个更重要(为什么)?从银行客户的角度来看，哪个更重要(为什么)?

3. 一些作者会区分秘密(secrecy)、隐私(privacy)和保密(confidentiality)。在这种用法中，秘密等同于本书中使用的术语机密性，而隐私是指应用到个人数据的秘密，保密(在这种被误导的意义上)比本书中使用的术语机密性更具限制性，因为它指的是不泄露某些信息的义务。
   a) 讨论一个现实世界中隐私是重要安全问题的情况。
   b) 讨论一个现实世界中保密(在这种受限制的意义上)是关键的安全问题的情况。

4. 加密技术有时被称为是“脆弱的”，因为它可以非常安全，但是当它被破译时，其安全性又会完全丧失[1]。相比之下，一些安全机制可以“让步”但不会完全失效——这种让步可能会导致安全性部分丧失，但是可以保证基本的安全级别。

a) 除了加密技术，给出一个脆弱的安全机制的例子。

b) 提供一个不易被破坏的安全机制的例子，也就是说，安全机制可以让步但不会完全失效。

5. 阅读 Diffie 和 Hellman 的经典论文[30]。

a) 简要总结论文。

b) Diffie 和 Hellman 给出了一个在不安全的信道上分发密钥的系统(参见论文的第 3 节)。这个系统是如何运行的？

c) Diffie 和 Hellman 还推测，“单向编译器”(one way compiler)可能被用来构造公钥密码学。你认为这是一个合理的方法吗？原因是什么？

6. 二战中最著名的密码是德国的 Enigma 密码。盟军破解了这个密码，从 Enigma 密码中获得的情报被证明是无价的。起初，盟军在使用从破解的 Enigma 密码中获得的信息时非常小心——有时盟军并不使用可能给他们带来优势的信息。然而，在战争后期，盟军(尤其是美国)就不那么小心了，因为其倾向于使用几乎所有从破解的 Enigma 密码中获得的信息。

a) 简要讨论一个破解的 Enigma 密码发挥了重要作用的重大二战事件。

b) 盟军对使用从被破解的 Enigma 电文中获得的信息持谨慎态度，担心德国人会意识到他们的密码已泄露。如果德国人意识到这个密码被破解了，他们可能会采取哪些方法，请至少列举两种。

c) 在某种程度上，德国人应该很清楚这个密码被破解了，然而这个密码一直被使用到战争结束。为什么纳粹继续使用 Enigma？

7. 当你想在计算机上验证自己的身份时，最有可能输入你的用户名和密码。用户名被认为是公共信息，因此密码才会验证你的身份。你的密码只有你知道。

a) 也有可能基于“你是什么”来进行认证。这种特征被称为生物特征。列举一个基于生物特征认证的例子。

b) 也可以根据“你拥有的东西”进行认证。列举一个基于你所拥有的东西进行认证的例子。

c) 双因子认证要求使用三种认证方法中的两种(你知道的东西、你拥有的东西、你是什么)。举一个日常生活中使用双因子认证的例子，并说明使用了这三种认证方法中的哪两种？

1 Shadoobie[116]。

8. 验证码(CAPTCHA)[133]通常用于限制人的访问(与自动化过程相反)。
   a) 列举一个真实世界的例子，你需要获得一个验证码来使用某些资源。你必须如何做才能获得验证码？
   b) 讨论可能用来破解你在该问题 a)部分描述的验证码的各种技术方法。
   c) 概述一种可能用于攻击 a)部分验证码的非技术性方法。
   d) a)部分的验证码效果如何？验证码的用户友好程度如何？
   e) 你和本书作者一样讨厌获得验证码吗？

9. 假设一个特定的安全协议设计得很好并且很安全。然而，有一种相当普遍的情况，即没有足够的信息可用来实现安全协议。在这种情况下，协议失效，并且理想情况下，参与者(如 Alice 和 Bob)之间的通信不应该发生。但在现实世界中，协议设计者必须决定如何处理协议失效的情况，并且作为一个实际问题，必须考虑安全性和便利性。讨论以下每种协议失效解决方案的相对优点。一定要提到各自的相对安全性和用户友好性。
   a) 当协议失效时，向 Alice 和 Bob 发出一个简短的警告，但是允许通信继续，就像协议已成功一样，而不需要 Alice 或 Bob 的任何干预。
   b) 当协议失效时，会向 Alice 发出警告，并由她决定(通过单击复选框)是否允许继续通信。
   c) 当协议失效时，向 Alice 和 Bob 发出通知，协议终止。
   d) 当协议失效时，协议终止，没有给 Alice 或 Bob 任何解释。

10. 自动取款机(ATM)是一个有趣的安全案例研究。Anderson[3]声称，当自动取款机首次被开发出来时，大多数注意力都放在了高科技攻击上。然而，大多数现实世界中对自动取款机的攻击显然是低技术含量的。
   a) 对自动取款机的高科技攻击包括破解加密或认证协议。如果可能的话，列举一个真实的案例，在这个案例中，对自动取款机的高科技攻击确实发生了，并提供细节。
   b) 肩窥(shoulder surfing)是低技术攻击的一个例子。在肩窥的场景中，Trudy 站在 Alice 后面排队，看着 Alice 输入PIN 时按下的数字。然后 Trudy 猛击 Alice 的头部，拿走了她的提款卡。请再举一个在现实世界中实际发生的对 ATM 的低技术攻击的例子。

11. 大型且复杂的软件系统总是存在许多缺陷。
   a) 对于诚实的用户，如 Alice 和 Bob，有缺陷的软件当然令人讨厌，但是为什么它是一个安全方面的问题呢？
   b) 为什么 Trudy 喜欢漏洞百出的软件？

12. 恶意软件旨在破坏或伤害系统的安全。恶意软件有许多常见的种类，包括病毒、蠕虫和特洛伊木马。

a) 你的计算机感染过恶意软件吗？如果是，恶意软件做了什么，你是如何解决这个问题的？如果没有，你怎么会这么幸运？

b) 过去，大多数恶意软件都是为了骚扰用户。如今，人们相信(有充分的证据)大多数恶意软件是为了盈利而编写的。恶意软件为什么会有利可图？

13. 在电影 *Office Space* 中，软件开发人员试图修改公司软件，使每一笔金融交易剩余的一分钱都汇入软件开发者的账户中，而不是留在公司账户中。这个想法是，对于任何特定的交易，没有人会注意到少了一分钱，但随着时间的推移，软件开发者将积累一大笔钱。这种类型的攻击有时被称为腊肠攻击(salami attack)。

a) 讨论一个真实的腊肠攻击的例子。

b) 电影中，腊肠攻击失败。这是为什么？

14. 有人说，“复杂性是安全的敌人。”

a) 举一个商业软件的例子，也就是说，找一个大型且复杂的软件示例，它存在严重的安全问题。

b) 找出适用于此语句的安全协议。

15. 假设本书被贪财的作者以 5 美元的价格在网上出售(PDF 格式)，那么作者每卖出一本就能比现在赚更多的钱[1]，并且购买这本书的人也能省下一大笔钱。

a) 网上图书销售的相关安全问题有哪些？

b) 从版权所有者的角度看，如何让网上书籍的销售更安全？

c) b)部分采用的方法有多安全？b)部分的方法对用户的友好程度如何？对所提出的系统有哪些可能的攻击？

16. 参考文献[135]的幻灯片描述了一个安全课程项目，学生们成功入侵了波士顿地铁系统。

a) 总结攻击的种类。导致每次攻击成功的关键漏洞是什么？

b) 学生们计划在这个自称为“黑客大会”的会议上作一场报告。在波士顿交通管理局的要求下，一名法官发布了一项临时限制令，禁止学生谈论他们的工作。根据幻灯片中的材料，你认为这是合理的吗？

c) 什么是拨号攻击(war dialing)和驾驶攻击(war driving)？什么是黑客战车(war carting)？

d) 评论关于“黑客战车”的情节剧视频的制作质量(视频链接可在参考文献[124]中找到)。

1 信不信由你。