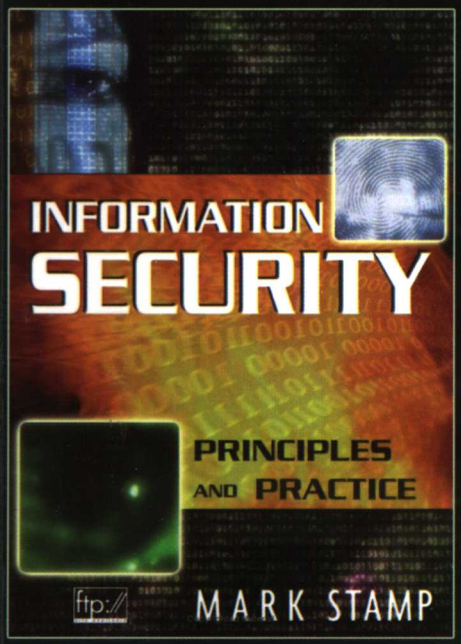
国外计算机科学教材系列

WILEY

信息安全原理与实践

Information Security
Principles and Practice



[美] Mark Stamp 著

杜瑞颖 赵 波 王张宜 彭国军 译

张焕国 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn

国外计算机科学教材系列

信息安全原理与实践

Information Security

Principles and Practice

[美] Mark Stamp 著

杜瑞颖 赵 波 王张宜 彭国军 译

张焕国 审校

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书全面介绍了信息安全的基本原理和应用技术，内容覆盖了信息安全领域的学科分支，包括密码、访问控制、协议安全、软件安全等。作者对信息安全的相关概念与技术进行了深入的探讨，并结合实例，强调了实际应用中所需的信息安全知识。全书叙述简洁、通俗易懂，尽量减少了数学证明与论述，重点放在与实践相结合，并且在每章都给出大量的习题以巩固学习。

本书的概念清楚、逻辑性强、内容新颖，可作为信息安全专业的“信息安全论”课程和计算机、电子通信等专业的“信息安全”课程的教材，也可供工程技术人员参考。

ISBN 0-471-73848-4, Information Security: Principles and Practice by Mark Stamp.

图书在版编目（CIP）数据

信息安全原理与实践 /（美）斯坦普（Stamp, M.）著；杜瑞颖等译.
北京：电子工业出版社，2007.5
（国外计算机科学教材系列）
书名原文：Information Security: Principles and Practice
ISBN 978-7-121-04238-6

Ⅰ.信… Ⅱ.①斯… ②杜… Ⅲ.信息系统－安全技术－教材 Ⅳ. TP309

中国版本图书馆CIP数据核字（2007）第055032号

责任编辑：冯小贝
印　　刷：
装　　订：北京牛山世兴印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
开　　本：787 × 1092　1/16　　印张：20　　字数：512千字
印　　次：2007年5月第1次印刷
定　　价：33.00元

凡所购买电子工业出版社的图书有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

反侵权盗版声明

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

随着计算机和网络技术的迅速发展与广泛应用，社会的信息化程度逐步提高，使用计算机和网络进行信息处理及信息交换，已经成为人们生活和工作中不可缺少的组成部分。如果计算机和网络的信息安全受到危害，将会危及国家安全，引起社会混乱，并造成重大损失。因此，确保计算机和网络的信息安全已经成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。

本书作者 Mark Stamp 是美国 San Jose 州立大学的教授。他在政府和工业界从事信息安全工作已经超过了 12 年。这期间他先在美国国家安全局(NSA)工作了 7 年，之后又在硅谷的信息安全公司从事了 2 年的数字版权管理产品的设计工作。2002 年，作者又回到学术界。Stamp 博士在硅谷的工作期间发现，没有能与实际工作相对应的信息安全方面的教材，于是他撰写了这本书，并且在正式出版之前已用于 3 年的教学。许多读者认为这本书是很成功的，他们从这本书中学到的知识在实际工作中很有用。

信息安全科学技术与产业已经成为我国信息科学技术中的重点发展领域。目前，许多大专院校都开办了信息安全专业或开设了信息安全课程，因此迫切需要适合信息安全专业使用的教材。为此，电子工业出版社与我们合作，翻译出版了《信息安全原理与实践》这本优秀的著作。

本书介绍了信息安全的基本原理和应用技术，内容覆盖了信息安全领域中主要的学科分支，其显著特点是理论联系实际。全书主要包含以下四个部分。第一部分：密码，详细讨论了密码算法及其应用技术，主要包括对称密码、公钥密码、hash 函数和密码分析。第二部分：访问控制，主要介绍了认证和授权技术的原理与应用。第三部分：协议，主要讨论了简单认证协议和现实安全协议。第四部分：软件，主要讨论了软件缺陷与恶意代码、软件的不安全性及操作系统安全。

本书的内容简明扼要，并且讲解深入浅出、生动有趣，尤其适合于课堂教学和自学，的确是一本难得的优秀教材。本书适合作为信息类专业本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的技术人员参考。

本书的第一部分由王张宜翻译，第二部分由赵波翻译，第三部分、前言、第 1 章和附录由杜瑞颖翻译，第四部分由彭国军翻译。全书由张焕国负责统稿和审校。

由于译者的专业知识和外语水平有限，书中的错误在所难免，敬请读者指正，译者在此先致感谢之意。

译者于武汉珞珈山

前　言

作者讨厌黑盒子。作者编写这本书的目的之一就是要解释在今天的信息安全书籍中很流行的一些黑盒子。换句话说，作者不想使读者为了一些琐碎的细节而烦心（如果想要了解这些内容，可以参考一些 RFC 文档），因此忽略了一些与讨论的主题不相关的内容。

作者的另一个目的是以生动有趣的方式来表达主题。如果有一个计算问题是令人兴奋的和有趣的，那它一定就是信息安全方面的问题。信息安全的问题无时无刻不在发生，它们经常成为人们讨论的话题。

现在的一些信息安全教材包含大量枯燥无用的理论。阅读这些书籍就像学一本微积分教材一样。还有一些信息安全书籍，除了收集一些明显不相关的事实以外，什么内容也没有，这让人们觉得信息安全根本不是一系列连贯的主题。这些书籍可能有一定的市场，但如果读者的目的是要设计和构建一个安全系统，那么最好还是了解一些相关的基本技术。另外，还有一类信息安全书籍聚焦于信息安全中的人为因素。虽然理解人在安全领域所扮演的角色非常关键，但作者要说的是，一个信息安全工程师首先必须对安全技术的功能和其弱点有深入的理解。

信息安全是一个巨大的主题，不像其他一些领域已经有一些确定的研究问题与方向。在讨论这个主题的一本书中，我们应该收集哪些素材，并且如何对选择的素材进行最佳的组织？本书的内容主要由以下四个方面组成：

- 密码
- 访问控制
- 协议
- 软件

有关这些问题的概念与知识是相当广泛的，所以作者选择了他认为最有意义的一些材料。例如，作者认为访问控制包含传统的认证和授权，以及非传统的类似防火墙和 CAPTCHA 的一些主题。软件方面的专题极其丰富，比如可以有安全软件开发、计算机病毒、软件逆向工程和操作系统等不同的专题。

本书将由浅入深地介绍很多有意义的内容。作者的目标是通过丰富的内容详细介绍每一个主题，从而让读者能够理解基本的信息安全概念，而不会陷入迷茫之中。同时，本书也会强调一些重要内容，提醒读者掌握一些关键的技术。

尽管本书将重点放在实际问题上，但是也介绍了一些基本的理论，这样便于读者将来继续学习。另外，作者已经尽可能缩小了本书所需的背景知识。特别是对于一些数学公式，已经减到最少（附录中给出了一些必要的数学知识）。尽管进行了一些内容上的限制，但是相对于绝大多数信息安全书籍而言，本书仍然包含了更多的密码学方面的知识。阅读本书并不要求很多的计算机科学的背景知识，简单学习过一些计算机课程（或有相当的经验）就足够了。如果读者具有一些编程经验和熟悉汇编语言的一些基本知识，那么在阅读相关章节的时候会有所帮助（不过这也不是必需的）。有些章节中可能需要基本的网络知识。作为相关的背景资料，附录中已经总结了一些网络知识。

如果读者是一位想学习更多的信息安全知识的相关专业人士，建议完整阅读本书。实际上这是作者对每一位读者的建议。某些章节可能对掌握全书精华不是非常必要，不过可能会影响到读者的阅读速度。如果希望避免这种情况，可以跳过 4.5 节、第 6 章（虽然我强烈推荐阅读 6.3 节）及 8.3 节的内容。

对于一名负责信息安全课程的教师，必须意识到本书的知识点已经远远超过了一个学期课程所能讲授的内容。作者给本科生的授课安排如下表所示，教师可以根据下面的课程安排进行灵活的补充与修改。

章节	课时	说明
1.引言	1	整章
2.密码学基础	3	2.3.6 节及 2.3.8 节可选
3.对称密钥密码	4	3.3.5 节可选
4.公钥密码	4	可略过 4.5 节，4.8 节可选
5.hash 函数及其他密码	3	包括 5.1 节～5.6 节及 5.7.2 节，5.7 节的剩余部分可选
6.高级密码分析	0	可略过整章
7.认证	4	整章
8.授权	2	包括 8.1 节和 8.2 节，8.3 节～8.9 节可选（8.7 节是推荐阅读的）
9.简单认证协议	4	9.4 节和 9.5 节可选（第 13 章将提到 9.5 节的内容）
10.现实安全协议	4	整章
11.软件漏洞与恶意代码	4	整章
12.软件中的不安全因素	4	12.3 节和 12.4 节可选，12.4 节的部分内容是推荐阅读的
13.操作系统及安全	3	整章
总课时	40	

有时可能会对以上安排进行一些改动。例如：

- 为了更加突出网络安全的内容，需要阅读附录及 8.7 节～8.9 节的所有内容。然后将密码学和软件相关话题的内容减到最少。
- 为了更加突出密码学的内容，需要阅读第 2 章～第 6 章。如果时间允许，也可以加入第 9 章～第 10 章（密码学的具体实施）的内容。尽管第 6 章比其他章更强调技术性，但是这一章也对密码分析学的概念进行了详细介绍（在其他书籍中一般很少单独介绍这部分内容）。
- 如果希望更多地讲解一些理论，可以增加 8.3 节～8.6 节的安全模型主题，还可以将文献[212]作为这部分内容的补充。如果课时上有一定限制，可以考虑缩减有关软件的章节。

无论是个人自学还是用于教学，选用本书作为教材的信息安全课程都是非常理想的。文前的目录可以便于读者查找感兴趣的内容；另外，本书的很多习题可以作为课堂讨论的主题或课堂练习（例如，第 10 章的习题 13、第 11 章的习题 11）。

因为作者已经讲过这门课，所以会将相关的 PPT 课件通过本书网站提供给大家。这些 PPT 课件已经实际使用过，并且已经过反复修改。

同样值得注意的是，附录和本书是相辅相成的。A.1 节讲解了网络安全的基础知识，这些内容与本书的第三部分相关。即使读者在网络方面已经有比较扎实的基础，但是这部分内容还是值得回顾一下。因为有时网络术语并不总是一致的，本书更加关注网络的安全方面。

附录 A.2 节中的数学知识对于掌握很多技术都是必需的。初等模运算(A.2.1 节)将会在第 3 章和第 5 章的内容中用到，而一些更深入的概念则会在第 4 章及 9.5 节使用。置换操作(A.2.2 节)在第 3 章是非常有用的，而基础的离散概率(A.2.3 节)在书中多次出现。A.2.4 节的线性代数知识仅在 6.4 节中使用。A.3 节仅是作为第 3 章的一些问题的参考。

正如很多庞大而复杂的软件会存在漏洞一样，本书难以避免地会存在错误。我们将会虚心聆听读者指出的任何一处错误，并且在本书网站上提供一份随时更新的勘误表。同样，也许一些读者为本书的相关章节开发了一些程序，比如描述算法和协议的小应用程序，如果愿意与大家一起分享，作者将非常感激。最后，希望读者能为本书下一版的修订提出更多的建议。本书的网站请参见：

ftp://ftp.wiley.com/public/sci_tech_med/information_security/

目　录

第二部分 访 问 控 制

第三部分 协 议

第四部分 软 件

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

遵循传统,Alice 和 Bob(*Alice in Wonderland* 中的故事人物)是人们认同的好人。有时,我们需要更多的好人,例如 Charlie。

Trudy 是一个试图使用某种方法攻击系统的坏家伙。一些作者使用暗示着特殊邪恶活动的名称来指代一个坏家伙团队。这样,Trudy 指代一个"入侵者",Eve 表示一个"偷听者",等等。

Alice、Bob、Trudy 和其他团伙不一定指的是人,例如,Alice 可能是一个便携机,Bob 可能是一个服务器,而 Trudy 可能是人。

1.2 Alice 的网上银行

假设 Alice 开始进行一个网上银行业务,那么可以给 Alice 的网上银行设定一个恰当的名字:"Alice 的网上银行"(Alice's Online Bank,或简称 AOB)。Alice 在信息安全方面关注的是什么? 如果 Bob 是 Alice 的客户,那么他在信息安全上关注的又是什么? Bob 的关注和 Alice 的关注相同吗? 如果从 Trudy 的角度来考虑,我们可能看到什么样的安全攻击?

首先,我们在 Alice 的银行环境中考虑传统的秘密性、完整性和可用性的情况。然后,我们将指出其他很多与安全相关的问题。

1.2.1 秘密性、完整性、可用性

秘密性的目标是防止未授权者读取信息。AOB 或许并不太关心它所处理的信息的秘密性,除非它的客户要求这样做。Bob 不想让 Trudy 知道他储蓄账户上有多少钱。Alice 的银行也许将面临对这种信息的秘密性保护失败之后的法律问题。

信息的完整性是指禁止未经授权地对信息进行修改。Alice 的银行必须保护账户信息的完整性以防止 Trudy 进行一些未授权的操作,例如增加她自己账户的余额或改变 Bob 账户的余额。

拒绝服务攻击即 DoS 攻击,是近来业界关注的问题。这种攻击设法减少对信息的访问。拒绝服务攻击事件的不断上升,导致数据的可用性成为信息安全中的一个基本问题。可用性与 Alice 的银行和 Bob 都有关。如果 AOB 的站点不可用,那么 Alice 就不能从客户业务获利并

且 Bob 也不能办理他的业务。这样 Bob 就可能到其他银行办理业务。如果 Trudy 对 Alice 有怨恨,或者她仅仅是不怀好意,那么 Trudy 有可能企图对 Alice 的网上银行进行拒绝服务攻击。

1.2.2 CIA 之外

秘密性、完整性和可用性(CIA)仅仅是信息安全故事的开始。当 Bob 登录到他的计算机时,Bob 的计算机怎样才能确定用户"Bob"确实是 Bob 而不是 Trudy 呢? 还有当 Bob 登录他在 Alice 的网上银行的账户时,AOB 怎样才能知道客户"Bob"确实是 Bob 而不是 Trudy 呢? 尽管在表面上看这两个认证问题十分相似,但深入来看,它们却是完全不同的。在单机系统上认证需要核对 Bob 的口令。为了达到这个安全目的,需要使用来自密码领域的一些有效方法。

对于很多种攻击来说,网上认证是开放的。Trudy 能够观察到经过网络发送的消息。更糟糕的是,Trudy 不仅能拦截消息,而且她能按照她自己的意愿随意改变消息和插入消息。为了一些特定的目的,例如为了使 AOB 相信她是真的 Bob,她还能重放旧的消息。在这种情况下,认证需要仔细地关注其所使用的协议的安全性。密码学在协议安全中也扮演了一个重要角色。

一旦 Bob 被 Alice 的银行认证,那么 Alice 必须强行限制 Bob 的行为。例如,Bob 不能查看 Charlie 的账户余额或者在系统上安装新的账目软件。不过系统管理员 Sam 应该能够在 AOB 系统上安装新的账目软件。强行进行这样的限制是授权的职责所在。注意授权对认证用户行为进行了限制。因为认证和授权都涉及了资源访问的问题,所以在最初讨论访问控制的时候,认证和授权的概念是混用的。

迄今为止,所有讨论过的信息安全机制都已用软件实现。现代软件系统的发展趋势是大规模、复杂化和普遍存在缺陷,而这些缺陷经常导致安全漏洞。这些漏洞是什么及它们是怎样被利用的? AOB 怎样确信其软件的行为是正确的? AOB 的软件开发者们在他们开发软件时怎样限制安全漏洞的数目? 当我们讨论软件时,将会审查这些与软件发展相关的问题。

虽然缺陷能(确实)引起安全漏洞,但是这些安全漏洞是无意造成的。另外,还有一些软件是恶意编制的。这种恶意软件(malware)包括如今给 Internet 带来麻烦的、我们所熟知的计算机病毒和蠕虫。这些令人厌恶的东西到底做了什么? Alice 的银行又应该如何对其带来的损害进行限制? 而 Trudy 还能做什么去增加这些恶意程序的危险性? 在研究软件时,我们将考虑这些及相似的问题。

Bob 对软件也有较多顾虑。例如,当 Bob 在计算机上输入他的口令时,如何能够确信他的口令没有被捕获和被发送给 Trudy。如果 Bob 在 www.alicesonlinebank.com 上进行一桩交易,他怎样才能知道在屏幕上看到的交易与软件和银行实际进行的交易是一样的? 总之,Bob 怎样才能确信他的软件的行为是正常的行为,而不是 Trudy 想要的行为? 这些问题我们同样需要考虑。

当讨论软件和安全时,我们必须考虑操作系统(OS)的话题。操作系统本身就很庞大,而且是由很多软件模块组合而成的。在任何系统中,操作系统也实施着很多安全举措。所以,为了更有准备地应对信息安全的挑战,了解一些操作系统的知识是必要的。

1.3 关于本书

Lampson [139]阐述了现实世界的安全需要依靠以下三项:

- 规范/政策：系统要做什么？
- 执行/机制：系统应该如何做？
- 正确性/保证：系统的确那样做了吗？

还应该增加第四个：

- 人类的天性：系统能幸免于“聪明的”用户吗？

这本书的讨论重点主要是执行/机制，因为强度、弱点及内在机制的局限性直接影响安全方面的其他所有关键问题。换而言之，没有对一个机制的充分理解，想对另外三个问题之一展开深入讨论都是不可能的。

我们把这本书包含的主题分为四个主要部分：第一部分涉及密码，接下来的两个部分分别是访问控制和协议，最后一部分是与软件相关的大量主题。

1.3.1 密码

密码或“秘密代码”是一种基本的信息安全工具。密码在很多至关重要的信息安全领域中发挥着关键作用，包括保护秘密性和完整性。我们将详细地讨论密码，因为这是本书其余部分所必需的背景知识。

我们将以古典密码系统作为密码讨论的开始。通过讨论这些古典密码系统，可以阐明现代密码系统中的基本原理，当然我们会采用读者更易理解和接受的方式进行阐述。

在这个背景下，我们将准备研究现代密码。在信息安全中，对称密钥密码和公钥密码都扮演了重要的角色，我们将用一个完整的章节来讨论这个主题。然后，我们将把注意力转移到hash函数，它是另外一个基本安全工具。在信息安全中，hash函数可用在很多不同的信息安全环境里，其中一些用法是十分复杂的且不太直观。我们将讨论hash函数在垃圾邮件抑制和在线投标方面的应用。

我们将简短地讨论和密码有关的少数特殊的主题。例如，我们将讨论信息隐藏，其目的是为了保障Alice和Bob在传输信息时不受Trudy的影响，即使Trudy知道已经传递的任何信息。这和数字水印的概念紧密相关，我们也会对其进行简短的讨论。

密码的最后章节涉及现代密码分析学，即用来破解现代密码系统的方法。尽管这是比较技术化的和专业化的内容，但是为了理解现代密码系统背后的设计原则，了解各种攻击方法是必要的。

1.3.2 访问控制

访问控制涉及认证和授权。在认证范围内，我们将考虑很多与口令相关的问题。口令是目前最常使用的认证形式。但这主要是因为口令是不花钱的而决不是因为它们是安全的。

我们将考虑怎样安全存储口令，然后将围绕安全口令的选择问题展开深入研究。尽管可以选择相对来说容易记忆的、强壮的口令，但是对用户强制执行这些政策是很困难的。事实上，在多数系统中，弱口令是一个主要的安全弱点。

口令的两种代替方案是基于生物的和基于智能卡的认证。我们将考虑这些认证形式的一些安全优势，特别是我们将对几种生物认证方法的细节进行讨论。

授权涉及对合法用户的限制。一旦Alice的银行确信Bob是真实的Bob，它必须强行限制