国外计算机科学经典教材

THOMSON

Principles of Information Security

信息安全原理

(美) Michael E. Whitman 著
Herbert J. Mattord
徐 焱 译

清华大学出版社

国外计算机科学经典教材

信息安全原理

(美) Michael E. Whitman
Herbert J. Mattord 著
徐 焱 译

清华大学出版社
北 京

Michael E. Whitman, Herbert J. Mattord

Principles of Information Security

EISBN: 0-619-06318-1

981-254-452-9

北京市版权局著作权合同登记号　图字：01-2003-2561

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目(CIP)数据

信息安全原理/(美)惠特曼(Whitman,M.E)，(美)马托德(Mattord,H.J.)著；徐焱译.—北京：清华大学出版社，2003

书名原文：Principles of Information Security

(国外计算机科学经典教材)

ISBN 7-302-07678-2

Ⅰ.信… Ⅱ.①惠…②马…③徐… 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(2003)第 106053 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：曹　康

文稿编辑：陈宗斌

封面设计：康　博

版式设计：康　博

印 装 者：北京鑫海金澳胶印有限公司

发 行 者：新华书店总店北京发行所

开　　本：185×260　**印张**：28.25　**字数**：723 千字

版　　次：2004 年 3 月第 1 版　2004 年 3 月第 1 次印刷

书　　号：ISBN 7-302-07678-2/TP·5623

印　　数：1～4000

定　　价：54.00 元

前　言

全球网络使世界的互连变得越来越广泛，通信和计算机系统的安全操作因而也变得更加重要，但诸如病毒和蠕虫攻击以及各种犯罪攻击事件的反复出现，说明了当前信息技术的薄弱，因此需要提高这些系统的安全性。

对保护重要信息资产的机构的迫切需求正不断增长。在当前系统和网络的安全性尝试中，企业必须构建当前信息安全从业人员框架。企业还期望具有丰富经验和技巧的下一代专业人士以开发更加安全的计算环境。为此，需要为技术类的学生准备更高深的内容以及相关的技术材料，同时配合大学教学人员的支持，帮助他们学习设计并开发将来所需的安全系统。

本书是关于信息安全原理的优秀教材。目前有许多面向从业人员的、关于信息安全和保障的优秀出版物，但却缺乏一本针对学生的、平衡地介绍安全管理和安全技术的书籍。我们希望创作一本专门面向信息安全专业学生的书籍来填补此空白。特别是对信息系统、犯罪立法、政治学、会计信息系统以及一些其他学科都需要对信息安全的基础原理有清晰的理解，并基于此原理阐明管理策略并选择技术方案。本书的基本原则为：现代机构内的信息安全是一个要解决的管理问题，而不是仅通过技术就可解答的问题—— 此问题具有重要的经济效益，并对管理效果产生一定的影响。

0.1　方法

本书对信息安全整个领域给出一个广泛的介绍，其中包括许多相关元素的背景以及理解该领域所需的足够细节。本书包含了该领域的术语学、历史，并对如何管理信息安全计划进行了概述。简而言之，阅读本书后可以达到事半功倍的效果。

信息系统安全专业人员资格认证的公共知识体系——因为本书作者是经过认证的信息系统安全专业人员(CISSP)，CISSP 的知识对本书的设计具有一定的影响。虽然在本书的编写过程中已经很谨慎，以避免它成为另一本 CISSP 研究指南类的书，但作者的背景导致了在某种程度上已经将大部分 CISSP 公共知识集成到了本书中。

章首场景——每章的开头都是一个小故事，讲述一个虚拟公司遇到某类信息安全问题。每个场景都会出现一些问题，使学生和老师有机会讨论其根本问题。

“相关资料”和技术细节部分——这部分内容重点讲述一些有趣的主题和详细的技术问题，让学生更深入地了解主题。每章都根据需要，包含了相关资料和技术细节部分。

强化学习——在每章结尾提供了该章的小结、复习题、练习和案例练习。这些内容使学生有机会体验课堂外的信息安全内容。通过练习，学生可以进行研究、分析和记录，以巩固学习目标，并加深对文章的理解。有了案例练习，学生可以运用专业的判断、观察能力和基本研究来为简单信息安全场景创建解决方案。

0.2 作者团队

本书由 Michael Whitman 和 Herbert Mattord 联合创作，结合了学院研究领域内的知识以及商务世界的实际经验。

Michael Whitman 拥有博士学位，是经过认证的信息系统安全专业人员，就任乔治亚州 Kennesaw 州立大学计算机科学和信息系统系的信息系统副教授。他同时还担任该大学信息系统科学的硕士生导师，以及信息安全教育和推广(Information Security Education and Awareness，infosec.Kennesaw.edu）KSU 中心的导师。Whitman 博士也是该系信息安全和保障认证的协调员。此外，Whitman 博士是信息安全、公平可靠使用策略(Fair and Responsible Use Policies)、计算道德准则和信息系统研究方法等领域活跃的研究者。目前他教授信息安全、局域网和数据通信的大学课程和研究生课程。他还在其领域的顶级刊物上发表了一些文章，包括“Information Systems Research”、“Communications of the ACM”、“Information and Management”、“Journal of International Business Studies”和“Journal of Computer Information Systems”。他同时还是 Georgia Electronic Commerce Association 信息安全工作组的活跃分子，Association for Computing Machinery 以及 Association for Information Group 的成员。Whitman 博士目前正在与他人合作编写一本实验手册“The hands-on Information Security lab manual”，这本手册将由 Thomson Learning Custom Publishing 出版。

Herbert Mattord 是工商管理学硕士和 CISSP。他曾经做过应用程序开发人员、数据库管理员、项目经理和信息安全设计人员。最近他结束了 24 年的 IT 职业生涯，进入 Kennesaw 州立大学。在作为 IT 从业者期间，他已经是 Kennesaw 州立大学、乔治亚州玛丽埃塔市 Southern Polytechnic 州立大学、得克萨斯州奥斯丁市 Austin Community 大学以及得克萨斯州圣马科斯市 Southwest Texas 州立大学的副教授。目前他正教授信息安全、局域网、数据通信、数据库技术，项目管理以及系统分析和设计的大学课程。他曾是 Georgia-Pacific 公司 Corporate Information Technology Security 的经理。本书包含了他的诸多实践知识。

0.3 结构

本书的结构遵循一种称为安全系统开发生命周期(或 SecSDLC)的模式。这个结构化方法可用于在那些有很少或只有一些非正式的信息安全措施的企业中实现信息安全，也可以帮助改进已有的信息安全计划。SecSDLC 提供类似于在应用程序开发、软件工程、传统的系统分析和设计以及联网工程中使用的、坚实的基础架构。结构化方法提供了一条支持性(但并不超越主题)的主线，此主线可指导教师和学生对信息安全信息领域的各个方面进行详细研究。为此将本书的结构分为 7 个部分、12 章和一个附录。

第 I 部分——简介

第 1 章——信息安全简介

开篇章节讲述了理解信息安全各领域的基础内容。本部分定义关键术语、解释基本概念，

并概述此领域的起源及其对信息安全理解的影响。

第 II 部分—— 安全调研阶段

第 2 章—— 安全需求

第 2 章介绍安全分析设计过程背后的商业原因。本章介绍了当前机构以及对安全的技术需求，强调并构建了第 1 章介绍的概念。一个原理性概念是：信息安全主要是一个管理问题，而不是技术问题。最佳实践过程是在考虑过商务需求后才应用技术因素。

本章还介绍了企业面临的各种威胁，并给出对这些威胁进行分级的过程，以便在企业开始进行安全计划时提供相应的优先权。本章继续讲解从上述威胁可能导致的各种攻击类型，以及它们对机构的信息和系统产生影响的方式。本章结束部分对信息安全的关键原理进行了进一步讨论，其中一些在第 1 章已经介绍过，如机密性、完整性、可用性、身份验证和标识、授权、可说明性和私密性。

第 3 章——信息安全中的法律、道德以及专业人员问题

SecSDLC 调研过程的基本部分中对国家和国际条款中现有法规和公众道德观念进行了详细介绍，深刻阐述了商业交往中所遵循的规范。本章介绍了信息安全领域的几个重要法律，并对更好地培养实现安全的人员所需的计算机道德教育进行详细的描述。不懂法律不是借口，但疏忽(知道但什么都不做)而引起的错误更危险。本章也介绍了现今机构中经常出现的立法和道德问题，以及可提升道德和法律责任的正规、专业机构。

第 III 部分——安全分析

第 4 章——风险管理：识别和评估风险

在开始设计一个新的安全方案前，安全分析人员必须首先理解机构的当前状况以及它和安全的关系。机构目前有正规的安全机制吗？它们的效率如何？安全管理人员和终端用户发布了什么政策和过程？本章通过描述标识威胁和资产并评定它们优先等级的过程，以及标识当前已有的、保护这些资产免受威胁的控制措施的过程，进而介绍实施基本的安全评估所需的过程。本章还讨论了各种可利用的控制机制类型，并指明准备进行最初风险评估所涉及的步骤。

第 5 章——风险管理：评估和控制风险

作为分析阶段的结论，第 5 章全面介绍了风险管理的过程。风险管理是识别、评估风险并将其降低至可接受的程度、实现有效的控制措施以维持此风险级别的过程。本章开始是对风险分析的讨论，接着介绍各种可行性分析类型。最后介绍定量和定性的评估措施以及对安全控制的评估。

第 IV 部分——逻辑设计

第 6 章——安全蓝本

作为逻辑设计阶段的第一章，本章给出各种被广泛接受的安全模型和基础框架。还介绍了最佳商务实践方案以及 due care and due diligence(合理注意、谨慎处理)标准，并扼要介绍了安全策略的开发。本章详细描述了安全策略每一层次的主要组成内容、范围和目标对象，还解释了军队和私人的数据分类模式以及安全教育培训和意识(SETA)的程序。结尾是有助于有效安全蓝本设计的逻辑技术简介。

第 7 章——持续性计划

第 7 章继续介绍了两个重要领域中的逻辑设计模式。首先介绍支持商务持续性、灾难恢复和事故响应的计划过程，描述机构的角色以及机构需要外部法律执行部门的时机。接着介绍了如何将安全性集成到传统的系统开发生命周期中，以确保自行开发的系统达到所需的安全目标。

第 V 部分——物理设计

第 8 章——安全技术

第 8 章是从逻辑设计到物理设计的一个过渡，概括了机构要提供安全机制时可以选择的特定的安全技术。主题包括防火墙、入侵检测系统、蜜罐(honey pot)、安全协议，虚拟专用网络(VPN)和密码学。

第 8 章的附录——密码学

第 8 章的附录详细介绍了现代密码系统的历史、组成和功能。本附录集中于这些算法的工作原理和使用方式。此外还介绍了依据加密算法在现代数据通信中使用的诸多协议。

第 9 章——物理安全

作为任何信息安全性操作的一个重要环节，物理安全关注的是物理设施的管理，物理访问控制的实现以及环境控制的监督。第 9 章讲解了物理安全威胁中应特别注意的事项，从设计一个安全的数据中心，到警卫和看门狗(watchdog)的相对价值，再到火灾抑制和电力调节的技术问题。

第 VI 部分——实现方案

第 10 章——实现安全

第 10 章介绍了实现前面阶段创建的设计所需的重要元素。本章的关键领域包括实现信息安全的靶心模型以及对机构是否应外购每一安全组件的讨论。此外，还讨论了改动管理，程序改进和商务持续性工作的额外计划等内容。

第 11 章——安全和人员

实现阶段的下一领域解决的是人员问题。第 11 章介绍了人员的两面性：安全人员和人员的安全。具体内容有：人员问题、专业人员安全证书以及雇佣政策和实践的实现。本章还讨论了安全政策与顾问、临时性雇员和外部商务伙伴之间影响和被影响的方式。

第 VII 部分——维护和改动

第 12 章——信息安全维护

最后也是最重要的一部分是对维护和改动操作的讨论。第 12 章介绍了对安全计划实时技术性和管理性评估。本章介绍了实时风险分析、风险评估和度量。这些都是风险管理的一部分。特别考虑了现代机构中所需要的各种弱点分析，涉及到从 Internet 渗透测试到无线网络风险评估等内容。

0.4 教师资源

为支持本书内容我们准备了许多教学工具，它们在多方面增强了课堂教学内容。这些供教

师使用的教学工具需到“汤姆森学习出版集团北京办事处”索取(参见书后的教辅材料申请表)。

Electronic Instructor's Manual(电子教师手册) ——教师手册包括使用本书的建议和策略，如讲述主题的提示。教师手册还包括复习题的答案以及每章结束处练习的建议方案。

图形文件——图形文件允许教师利用本书的图形创建自己的演示文稿。

PowerPoint 演示——本书的每一章都提供有相应的 Microsoft PowerPoint 幻灯片。它们的目的是用作课堂演示，使学生可在网络上回顾每章的内容。教师还需要将那些在课堂上额外介绍的主题加入自己的幻灯片。

Lab Manual(实验室手册) ——Thompson Learning Custom Publishing 正在制作与本书配套的实验室手册“The Hands-On Information Security Lab Manual”(ISBN 0-759-31283-4)。它由本书的一位作者编写，该实验室手册还提供了关于跟踪足迹(footprinting)、枚举和防火墙配置等安全性强化练习，以及诸多作为实验室课件或课堂项目的具体练习和案例，作为本书的补充材料。要了解详细信息，请联系本书的销售代理。

ExamView——ExamView 是基于对象的测试需求的终极工具。它是一个功能强大的基于对象的测试生成器，可使教师创建书面的、LAN 或基于 Web 的测试，这些题目来自专门为 Course Technology 内容而设计的测试题库。教师可以使用非常有效的 QuickTest Wizard 在数分钟内利用 Course Technology 的问题库来创建测试题或重新定制自己的考试。

0.5 致谢

本书作者要感谢他们家人的支持：他们耗费了大量时间来编写本书，从而耽误了很多家务时间，因而非常感谢他们家人对此的谅解。此外还要特别感谢乔治亚州立大学英语系的研究生 Carola Mattord。她负责检查本书的初稿，并建议本书将重点放在学生群体上，这使得本书手稿更易于阅读。

合作伙伴

几位 Kennesaw 州立大学的学生也协助了本书的准备工作，在此对他们的帮助予以感谢。

- Anthony J.Nichols——密码学附录初稿的作者
- Ramona Binder——尾注的研究助理

检查

这里要感谢下列人员，他们分别对最初方案、项目大纲以及各章的复习题提供了宝贵的反馈。

- Snehamay Banerjee(Rutgers 大学)
- Michael L. Casper(Central Piedmont Community 学院)
- Lawrence R. Knupp(DeVry 大学)
- Robert Lipton(Pennsylvania 州立大学)
- Patrick Massaro(Long Island 大学)
- David Ozag(Gettysburg 学院)
- Denise Padavano(Peirce 学院)
- Sara Robben(DeVry 大学)

- JoAnna Burley Shore(Frostburg 州立大学)
- Robert Statica(New Jersey 技术学院)
- Eileen M. Vidrine(Northern Virginia 社区大学)

特别感谢

作者希望感谢 Course Technology 的编辑组和制作组。他们的努力和敬业大大提高了本书最后的质量。

- 产品经理 Barrie Tysko
- 策划编辑 Betsey henkels
- 执行编辑 Jennifer Locke
- 产品助理 Christine Spillett
- 产品助理 Janet Aras
- 图片研究员 Abby Reip

另外，几个专业和商业机构以及个人也对本书的策划作出了贡献，他们提供了信息和创作灵感，这里对他们的贡献表示感谢。

- The Human Firewall Council
- PentaSafe Security Technologies 公司
- Steven Kahan——PentaSafe Security Technologies 公司市场部副主席
- Charles Cresson Wood
- Georgia-Pacific 公司
- Carlos Mena——Georgia-Pacific 公司的 Corporate IT Privacy and Security 部门的高级经理
- Robert D. Hayes——Georgia-Pacific 公司 Corporate Security 部门主管
- Kennesaw 州立大学计算机科学和信息系统系的同事
- Merle King 教授，Kennesaw 州立大学计算机科学和信息系统系的主任

承诺

作者承诺为购买本书的用户和读者提供服务。收到本书及其技术材料的反馈意见，我们将很高兴，也很感荣幸。您可以通过 Course Technology 的电子邮箱 mis@course.com 和我们联系。

目　　录

第Ⅰ部分　简　　介

第II部分　安全调研阶段

第III部分 安 全 分 析

第Ⅳ部分 逻 辑 设 计

第V部分 物 理 设 计