国外计算机科学经典教材(影印版)

THOMSON

Principles of Information Security

信息安全原理

(影印版)

(美) Michael E. Whitman
Herbert J. Mattord 著

清华大学出版社

Principles of Information Security

信息安全原理

(美) Michael E.Whitman
Herbert J. Mattord 著

清华大学出版社
北京

Michael E.Whitman，Herbert J. Mattord
Principles of Information Security
EISBN: 0-619-06318-1

981-243-905-6

北京市版权局著作权合同登记号 图字：01-2003-2561

图书在版编目(CIP)数据

信息安全原理= Principles of Information Security / (美) 惠特曼，(美) 马托德著. —影印本.
—北京：清华大学出版社，2003
ISBN 7-302-06870-4

Ⅰ. 信… Ⅱ ①惠… ②马… Ⅲ.信息系统-安全技术-教材 Ⅳ.[illegible]

中国版本图书馆 CIP 数据核字(2003)第 054031 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：徐燕萍
封面设计：康博
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　印 张：35.25　字　数：902 千字
版　　次：2003 年 7 月第 1 版　2003 年 7 月第 1 次印刷
书　　号：ISBN 7-302-06870-4/TP・5097
印　　数：1~2000
定　　价：58.00 元

Preface

AS GLOBAL NETWORKS EXPAND the interconnection of the world, the smooth operation of communication and computing systems becomes vital. However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need for heightened security of these systems.

The immediate need for organizations to protect critical information assets continues to increase. In an attempt to secure current systems and networks, organizations must draw on the pool of current information security practitioners. These same organizations will count on the next generation of professionals to have the correct mix of skills and experiences to develop more secure computing environments in the future. Improved texts with supporting materials along with the efforts of college and university faculty are needed to prepare students of technology to recognize the threats and vulnerabilities present in existing systems and to learn to design and develop the secure systems needed in the near future.

The purpose of this textbook is to fill the need for a quality academic textbook in the discipline of Information Security. While there are dozens of quality publications on information security and assurance oriented to the practitioner, there is a dramatic lack of textbooks that provide the student with a balance between security management and the technical components of security. By creating a book specifically oriented toward Information Systems students, we hope to close this gap. Specifically, there is a clear need for Information Systems, Criminal Justice, Political Science, Accounting Information Systems, and other disciplines to gain a clear understanding of the foundations of Information Security, the principles on which managerial strategy can be formulated and from which technical solutions can be selected. The fundamental tenet of this textbook is that Information Security in the modern organization is a problem for management to solve and not a problem of that technology alone can answer—a problem that has important economic consequences and for which management will be held accountable.

Approach

The book provides a broad review of the entire field of information security, background on many related elements, and enough detail to facilitate understanding of the field. It covers the terminology of the field, the history of the field, and an overview of how to manage an information security program. In short, it is "an inch deep and a mile wide".

Certified Information Systems Security Professionals Common Body of Knowledge —Because the authors are Certified Information Systems Security Professionals (CISSP), the CISSP

knowledge domains have had an influence in the design of the text. Although care was taken to avoid producing another CISSP study guide, the author's backgrounds have resulted in a treatment that ensures that much of the CISSP Common Body of Knowledge (CBK) has been integrated into the text to some degree.

Chapter-Opening Scenarios— Each chapter opens with a short story that follows the same fictional company as it encounters some of the issues of information security. The discussion questions that accompany each scenario give the student and the instructor the opportunity to discuss the issues that underlay the content.

Off line and Technical Details Boxes— These sections highlight interesting topics and detailed technical issues, giving the student the option of delving into topics more deeply. Chapters include the Offline and Technical Details boxes as needed.

Hands-On Learning— At the end of each chapter, students find a Chapter Summary and Review Questions as well as Exercises and Case Exercises, which give them the opportunity to examine the information security arena outside the classroom. Using the Exercises, the student can research, analyze and write to reinforce learning objectives and deepen their understanding of the text. With the Case Exercises, students use professional judgment, powers of observation, and elementary research, to create solutions for simple information security scenarios.

Author Team

Michael Whitman and Herbert Mattord have jointly developed this text to merge knowledge from the world of academic study with practical experience from the business world.

Michael Whitman, Ph.D., CISSP is an Associate Professor of Information Systems in the Computer Science and Information Systems Department at Kennesaw State University, Kennesaw, Georgia, where he is also the Director of the Masters of Science in Information Systems and the Director of the KSU Center for Information Security Education and Awareness *(infosec.kennesaw.edu)*. Dr. Whitman is also the coordinator for the department's Certificate in Information Security and Assurance. Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, Ethical Computing and Information Systems Research Methods. He currently teaches graduate and undergraduate courses in Information Security, Local Area Networking, and Data Communications. He has published articles in the top journals in his field, including *Information Systems Research, the Communications of the ACM, Information and Management, the Journal of International Business Studies, and the Journal of Computer Information Systems*. He is an active member of the Georgia Electronic Commerce Association's Information Security Working Group, the Association for Computing Machinery and the Association for Information Systems. Dr. Whitman is also currently co-authoring a Lab Manual, "The Hands-On Information Security Lab Manual," to be published by Thomson Learning Custom Publishing.

Herbert Mattord, M.B.A. CISSP recently completed 24 years of IT industry experience as an

application developer, database administrator, project manager, and information security practitioner to join the faculty as Kennesaw State University. During his career as an IT practitioner, he has been an adjunct professor at Kennesaw State University, Southern Polytechnic State University in Marietta, Georgia, Austin Community College in Austin, Texas, and Southwest Texas State University in San Marcos, Texas. He currently teaches undergraduate courses in Information Security, Data Communications, Local Area Networks, Database Technology, Project Management, and Systems Analysis & Design. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this textbook was acquired.

Structure

Principles of Information Security is structured to follow a model called the Security Systems Development Life Cycle (or SecSDLC). This structured methodology can be used to implement information security in an organization that has little or no formal information security measures in place and can also serve as a method to improve established information security programs. The SecSDLC provides a solid framework very similar to that used in application development, software engineering, traditional systems analysis and design, and networking. The use of a structured methodology provides a supportive but not overriding theme that will guide instructors and students through an examination of the various components of the information domains of information security. To serve this end, this textbook is organized into seven sections, twelve chapters and an Appendix.

Section I—Introduction

Chapter 1—Introduction to Information Security

This opening chapter establishes the foundation for understanding the broader field of Information Security. This is accomplished by defining key terms, explaining essential concepts, and providing a review the origins of the field and its impact on the understanding of Information Security.

Section II—Security Investigation Phase

Chapter 2—The Need for Security

Chapter 2 examines the business drivers behind the security analysis design process. It examines current organization and technology needs of security, emphasizing and building on the concepts presented in Chapter 1. One principle concept is that information security is primarily an issue of management, not technology. Best practices apply technology only after considering the business needs.

The chapter also examines the various threats facing organizations and presents the process of ranking these threats to provide relative priority as the organization begins the security planning process. The chapter continues with a detailed examination of the types of attacks that could occur from these threats, and how they could impact the organization's information and systems. The chapter concludes with a further discussion of the key principles of information security, some of which were introduced in Chapter 1: confidentiality, integrity, availability, authentication and identification, authorization, accountability, and privacy.

Chapter 3—Legal, Ethical and Professional Issues in Information Security

As a fundamental part of the SecSDLC investigation process, a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities provides key insights into the regulatory constraints that govern business. This chapter examines several key laws that shape the field of Information Security, and presents a detailed examination of computer ethics necessary to better educate those implementing security. Although ignorance of the law is no excuse, it's considered better than negligence (knowing and doing nothing). This chapter also presents several legal and ethical issues that are commonly found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

Section III—Security Analysis

Chapter 4—Risk Management: Identifying and Assessing Risk

Before the design of a new security solution can begin, the security analysts must first understand the current state of the organization and its relationship to security. Does the organization have any formal security mechanisms in place? How effective are they? What policies and procedures have been published to the security managers and end users? This chapter examines the processes necessary to conduct a fundamental security assessment by describing the procedures for identifying and prioritizing threats and assets, and identifying what controls are in place to protect these assets from threats. The chapter also provides a discussion of the various types of control mechanisms available and identifies the steps involved in preparing for the initial risk assessment.

Chapter 5—Risk Management: Assessing and Controlling Risk

As a conclusion to the analysis phase, Chapter 5 presents a thorough examination of the process of risk management. Risk management is the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. The chapter begins with a discussion of risk analysis and continues through various types of feasibility analyses. Finally the chapter examines quantitative and qualitative assessment measures and evaluation of security controls.

Section IV—Logical Design

Chapter 6—Blueprint for Security

As the first chapter in the logical design phase, Chapter 6 presents a number of widely accepted security models and frameworks. It examines best business practices and standards of due care and due diligence, and offers an overview of the development of security policy. This chapter details the major components, scope, and target audience for each of the levels of security policy. This chapter also explains data classification schemes, both military and private, as well as the security education training and awareness (SETA) program. The chapter concludes with an overview of logical technologies that aid in the design of an effective security blueprint.

Chapter 7—Planning for Continuity

Chapter 7 continues with the logical design scheme in two important areas. First, the chapter examines the planning process that supports business continuity, disaster recovery, and incident response. The chapter describes the organization's role and when the organization should involve outside law enforcement agencies. Second, the chapter examines the integration of security into the traditional systems development life cycle, to ensure that systems developed in-house comply with the desired security profile.

SECTION V—Physical Design

Chapter 8—Security Technology

Supporting the transition from logical to physical design, Chapter 8 outlines the specific security technologies that an organization can select to support security efforts. Topics include firewalls, intrusion detection systems, honey pots, security protocols, virtual private networks (VPNs), and cryptography.

Appendix A—Cryptography

The appendix to Chapter 8 provides additional detail on the history, composition, and function of modern cryptosystems. The appendix focuses on how these algorithms work and how they are used. It also presents a number of protocols used in modern data communications that rely on cryptographic algorithms.

Chapter 9—Physical Security

As a vital part of any information security process, physical security is concerned with the management of the physical facilities, the implementation of physical access control, and the oversight of environmental controls. From designing a secure data center to the relative value of guards and watchdogs to the technical issues of fire suppression and power conditioning, Chapter 9 examines as special considerations for physical security threats.

Section VI—Implementation

Chapter 10—Implementing Security

Chapter 10 examines the elements critical to implementing the design created in the previous stages. Key areas in this chapter include the bull's-eye model for implementing information security and a discussion of whether an organization should outsource each component of security. Change management, program improvement, and additional planning for the business continuity efforts are also discussed.

Chapter 11—Personnel Security

The next area in the implementation stage addresses people issues. Chapter 11 examines both sides of the personnel coin: security personnel and security of personnel. It examines staffing issues, professional security credentials, and the implementation of employment policies and practices. The chapter also discusses how security policy affects, and is affected by, consultants, temporary workers, and outside business partners.

Section VII—Maintenance and Change

Chapter 12—Information Security Maintenance

Last and most important is the discussion on maintenance and change. Chapter 12 presents the ongoing technical and administrative evaluation of the security program. This chapter explores ongoing risk analysis, risk evaluation, and measurement, all of which are part of risk management. The special considerations needed for the varieties of vulnerability analysis needed in the modern organization are explored from Internet penetration testing to wireless network risk assessment.

Instructor Resources

A variety of teaching tools have been prepared to support this textbook and offer many options to enhance the classroom learning experience:

Electronic Instructor's Manual —The Instructor's Manual includes suggestions and strategies for using this text, such as suggestions for lecture topics. The Instructors Manual also includes answers to the review questions and suggested solutions to the exercises at the end of each chapter.

Figure Files — Figure Files allow instructors to create their own presentations using figures taken from the text.

PowerPoint Presentations — This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors can add their own slides for additional topics they introduce to the class.

Lab Manual — Thomson Learning Custom Publishing is producing a lab manual to accompany

this book, which is written by one of the authors: *The Hands-On Information Security Lab Manual* (ISBN 0-759-31283-4). The lab manual provides hands-on security exercises on footprinting, enumeration, and firewall configuration, as well as a number of detailed exercises and cases that supplement the book as a laboratory component or as in-class projects. Contact your Course Technology sales representative for more information.

ExamView —ExamView®, the ultimate tool for objective-based testing needs. ExamView ® is a powerful objective-based test generator that enables instructors to create paper, LAN or Web-based tests from testbanks designed specifically for their Course Technology text. Instructors can utilize the ultra-efficient QuickTest Wizard to create tests in less than five minutes by taking advantage of Course Technology's question banks, or customize their own exams from scratch.

Acknowledgments

The authors would like to thank their families for their support and understanding for the many hours dedicated to this project, hours taken in many cases from family activities. Special thanks to Carola Mattord, graduate student of English at Georgia State University. Her reviews of early drafts and suggestions for keeping the writing focused on the students resulted in a more readable manuscript.

Contributors

Several Kennesaw State University students also assisted in the preparation of the textbook, and we thank them for their contributions:

- Anthony J. Nichols — Author of the first draft of the Appendix on cryptography
- Ramona Binder — Research assistant for endnotes

Reviewers

We are indebted to the following individuals for their respective contributions of perceptive feedback on the initial proposal, the project outline, and the chapter-by-chapter reviews of the text:

- Snehamay Banerjee, Rutgers University
- Michael L. Casper, Central Piedmont Community College
- Lawrence R. Knupp, DeVry University
- Robert Lipton, Pennsylvania State University
- Patrick Massaro, Long Island University
- David Ozag, Gettysburg College
- Denise Padavano, Peirce College
- Sara Robben, DeVry University
- JoAnna Burley Shore, Frostburg State University
- Robert Statica, New Jersey Institute of Technology

- Eileen M. Vidrine, Northern Virginia Community College

Special Thanks

The authors wish to thank the Editorial and Production teams at Course Technology. Their diligent and professional efforts greatly enhanced the final product:

- Barrie Tysko, Product Manager
- Betsey Henkels, Developmental Editor
- Jennifer Locke, Executive Editor
- Christine Spillett, Associate Production Manager
- Janet Aras, Associate Product Manager
- Abby Reip, Photo Researcher

In addition, several professional and commercial organizations and individuals have aided the development of the textbook by providing information and inspiration, and the authors wish to acknowledge their contribution:

- The Human Firewall Council
- PentaSafe Security Technologies, Inc.
- Steven Kahan, Vice President of Marketing, PentaSafe Security Technologies, Inc.
- Charles Cresson Wood
- Georgia-Pacific Corporation
- Carlos Mena, Senior Manager of Corporate IT Privacy and Security, Georgia-Pacific Corporation
- Robert D. Hayes, Director of Corporate Security, Georgia-Pacific Corporation
- Our colleagues in the Department of Computer Science and Information Systems, Kennesaw State University
- Professor Merle King, Chair of the Department of Computer Science and Information Systems, Kennesaw State University

Our Commitment

The authors are committed to serving the needs of the adopters and readers. We would be pleased and honored to receive feedback on the textbook and its supporting materials. You can contact us, through Course Technology, via e-mail at mis@course.com.

Table of Contents