国外计算机科学教材系列

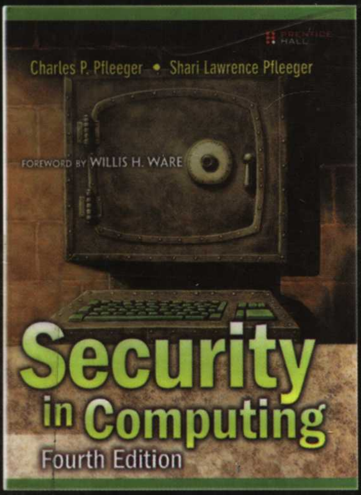
PRENTICE
HALL

信息安全
原理与应用

（第四版）

Security in Computing

Fourth Edition


PRENTICE HALL
Charles P. Pfleeger • Shari Lawrence Pfleeger
FOREWORD BY WILLIS H. WARE
Security
in Computing
Fourth Edition

英文版

［美］ Charles P. Pfleeger
Shari Lawrence Pfleeger 著

PHEI
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

信息安全原理与应用

（第四版）

（英文版）

Security in Computing

Fourth Edition

[美] Charles P. Pfleeger
Shari Lawrence Pfleeger 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是一本信息安全的经典著作和权威指南，内容新颖丰富。全书系统地描述了计算安全的各方面问题，内容涉及计算机安全的概念和术语；密码学基础及应用；程序及软件安全；操作系统安全及可信任操作系统的设计；数据库及数据挖掘的安全；网络安全；安全管理；计算机安全经济学；计算安全中的隐私问题；计算安全中的法律和道德问题，最后对密码学进行了深入研究。

本书既可以作为信息安全或计算机专业本科生、研究生的双语教材，也可以作为相关领域研究人员和专业技术人员的参考用书。

版权贸易合同登记号　图字：01-2007-2895

图书在版编目（CIP）数据

信息安全原理与应用 = Security in Computing：第 4 版：英文 /（美）弗莱格（Pfleeger, C. P.）等著.
北京：电子工业出版社，2007.8
（国外计算机科学教材系列）
ISBN 978-7-121-04744-2

Ⅰ. 信…　Ⅱ. 弗…　Ⅲ. 信息系统－安全技术－教材－英文　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 110652 号

责任编辑：李秦华
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
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 × 980　1/16　　印张：54.75　　字数：1822 千字
印　　次：2007 年 8 月第 1 次印刷
定　　价：79.00 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。

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

Foreword

In the 1950s and 1960s, the prominent conference gathering places for practitioners and users of computer technology were the twice yearly Joint Computer Conferences (JCCs)—initially called the Eastern and Western JCCs, but later renamed the Spring and Fall JCCs and even later, the annual National (AFIPS) Computer Conference. From this milieu, the topic of computer security—later to be called information system security and currently also referred to as "protection of the national information infrastructure"—moved from the world of classified defense interests into public view.

A few people—Robert L. Patrick, John P. Haverty, and I among others—all then at the RAND Corporation—had been talking about the growing dependence of the country and its institutions on computer technology. It concerned us that the installed systems might not be able to protect themselves and their data against intrusive and destructive attacks. We decided that it was time to bring the security aspect of computer systems to the attention of the technology and user communities.

The enabling event was the development within the National Security Agency (NSA) of a remote-access time-sharing system with a full set of security access controls, running on a Univac 494 machine, and serving terminals and users not only within the headquarters building at Fort George G. Meade, Maryland, but also worldwide. Fortuitously, I knew details of the system.

Persuading two others from RAND to help—Dr. Harold Peterson and Dr. Rein Turn—plus Bernard Peters of NSA, I organized a group of papers and presented it to the SJCC conference management as a ready-made additional paper session to be chaired by me. [1] The conference accepted the offer, and the session was presented at the Atlantic City (NJ) Convention Hall in 1967.

Soon thereafter and driven by a request from a defense contractor to include both defense classified and business applications concurrently in a single mainframe machine functioning in a remote-access mode, the Department of Defense, acting through the Advanced Research Projects Agency (ARPA) and later the Defense Science Board (DSB), organized a committee, which I chaired, to study the issue of security controls for computer systems. The intent was to produce a document that could be the basis for formulating a DoD policy position on the matter.

The report of the committee was initially published as a classified document and was formally presented to the sponsor (the DSB) in January 1970. It was later declassified and republished (by the RAND Corporation) in October 1979. [2] It was widely circulated and became nicknamed "the Ware report." The report and a historical introduction are available on the RAND web site. [3]

Subsequently, the United States Air Force (USAF) sponsored another committee chaired by James P. Anderson. [4] Its report, published in 1972, recommended a 6-year R&D security program totaling some $8M. [5] The USAF responded and funded several projects, three of which were to design and implement an operating system with security controls for a specific computer.

Eventually these activities led to the "Criteria and Evaluation" program sponsored by the NSA. It culminated in the "Orange Book" [6] in 1983 and subsequently its supporting array of documents, which were nicknamed "the rainbow series." [7] Later, in the 1980s and on into the 1990s, the subject became an international one leading to the ISO standard known as the "Common Criteria." [8]

It is important to understand the context in which system security was studied in the early decades. The defense establishment had a long history of protecting classified information in document form. It had evolved a very elaborate scheme for compartmenting material into groups, sub-groups and super-groups, each requiring a specific personnel clearance and need-to-know as the basis for access. [9] It also had a centuries-long legacy of encryption technology and experience for protecting classified information in transit. Finally, it understood the personnel problem and the need to establish the trustworthiness of its people. And it certainly understood the physical security matter.

Thus, "the" computer security issue, as it was understood in the 1960s and even later, was how to create in a computer system a group of access controls that would implement or emulate the processes of the prior paper world, plus the associated issues of protecting such software against unauthorized change, subversion, and illicit use, and of embedding the entire system in a secure physical environment with appropriate management oversights and operational doctrine and procedures. The poorly understood aspect of security was primarily the software issue with, however, a collateral hardware aspect; namely, the risk that it might malfunction—or be penetrated—and subvert the proper behavior of software. For the related aspects of communications, personnel, and physical security, there was a plethora of rules, regulations, doctrine, and experience to cover them. It was largely a matter of merging all of it with the hardware/software aspects to yield an overall secure system and operating environment.

However, the world has now changed in essential ways. The desktop computer and workstation have appeared and proliferated widely. The Internet is flourishing and the reality of a World Wide Web is in place. Networking has exploded and communication among computer systems is the rule, not the exception. Many commercial transactions are now web-based; many commercial communities—the financial one in particular—have moved into a web posture. The "user" of any computer system can literally be anyone in the world. Networking among computer systems is ubiquitous; information-system outreach is the goal.

The net effect of all of this has been to expose the computer-based information system—its hardware, its software, its software processes, its databases, its communications—to an environment over which no one—not end-user, not network administrator or system owner, not even government—has control. What must be done is to provide appropriate technical, procedural, operational, and environmental safeguards against threats as they might appear or be imagined, embedded in a societally acceptable legal framework.

And appear threats did—from individuals and organizations, national and international. The motivations to penetrate systems for evil purpose or to create malicious software—generally with an offensive or damaging consequence—vary from personal intellectual satisfaction to espionage, to financial reward, to revenge, to civil disobedience, and to other reasons. Information-system security has moved from a largely self-contained bounded environment interacting with a generally known and disciplined user community to one of worldwide scope with a body of users that may not be known and are not necessarily trusted. Importantly, security controls now must deal with circumstances over which there is largely no control or expectation of avoiding their impact. Computer security, as it has evolved, shares a similarity with liability insurance; they each face a threat environment that is known in a very general way and can generate attacks over a broad spectrum of possibilities; but the exact details or even time or certainty of an attack is unknown until an event has occurred.

On the other hand, the modern world thrives on information and its flows; the contemporary world, society, and institutions cannot function without their computer-communication-based information systems. Hence, these systems must be protected in all dimensions—technical, procedural, operational, environmental. The system owner and its staff have become responsible for protecting the organization's information assets.

Progress has been slow, in large part because the threat has not been perceived as real or as damaging enough; but also in part because the perceived cost of comprehensive information system security is seen as too high compared to the risks—especially the financial consequences—of not doing it. Managements, whose support with appropriate funding is essential, have been slow to be convinced.

This book addresses the broad sweep of issues above: the nature of the threat and system vulnerabilities (Chapter 1); cryptography (Chapters 2 and 12); the Common Criteria (Chapter 5); the World Wide Web and Internet (Chapter 7); managing risk (Chapter 8); software vulnerabilities (Chapter 3); and legal, ethical, and privacy issues (Chapters 10 and 11). The book also describes security controls that are currently available such as encryption protocols, software development practices, firewalls, and intrusion-detection systems. Overall, this book provides a broad and sound foundation for the information-system specialist who is charged with planning and/or organizing and/or managing and/or implementing a comprehensive information-system security program.

Yet to be solved are many technical aspects of information security—R&D for hardware, software, systems, and architecture; and the corresponding products. Notwithstanding, technology per se is not the long pole in the tent of progress. Organizational and management motivation and commitment to get the security job done is. Today, the collective information infrastructure of the country and of the world is slowly moving up the learning curve; every mischievous or malicious event helps to push it along. The terrorism-based events of recent times are helping to drive it. Is it far enough up the curve to have reached an appropriate balance between system safety and threat? Almost certainly, the answer is, "No, not yet; there is a long way to go." [10]

Willis H. Ware
The RAND Corporation
Santa Monica, California

Citations

1. "Security and Privacy in Computer Systems," Willis H. Ware; RAND, Santa Monica, CA; P-3544, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 279 seq, Vol. 30, 1967.

   "Security Considerations in a Multi-Programmed Computer System," Bernard Peters; Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 283 seq, vol 30, 1967.

   "Practical Solutions to the Privacy Problem," Willis H. Ware; RAND, Santa Monica, CA; P-3544, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 301 seq, Vol. 30, 1967.

   "System Implications of Information Privacy," Harold E. Peterson and Rein Turn; RAND, Santa Monica, CA; P-3504, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 305 seq, vol. 30, 1967.

2. "Security Controls for Computer Systems," (Report of the Defense Science Board Task Force on Computer Security), RAND, R-609-1-PR. Initially published in January 1970 as a classified document. Subsequently, declassified and republished October 1979.

3. http://rand.org/publications/R/R609.1/R609.1.html, "Security Controls for Computer Systems"; R-609.1, RAND, 1979

   http://rand.org/publications/R/R609.1/intro.html, Historical setting for R-609.1

4. "Computer Security Technology Planning Study," James P. Anderson; ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA; October 1972.

5. All of these documents are cited in the bibliography of this book. For images of these historical papers on a CDROM, see the "History of Computer Security Project, Early Papers Part 1," Professor Matt Bishop; Department of Computer Science, University of California at Davis. http://seclab.cs.ucdavis.edu/projects/history

6. "DoD Trusted Computer System Evaluation Criteria," DoD Computer Security Center, National Security Agency, Ft George G. Meade, Maryland; CSC-STD-001-83; Aug 15, 1983.

7. So named because the cover of each document in the series had a unique and distinctively colored cover page. For example, the "Red Book" is "Trusted Network Interpretation," National Computer Security Center, National Security Agency, Ft. George G. Meade, Maryland; NCSC-TG-005, July 31, 1987. USGPO Stock number 008-000-00486-2.

8. "A Retrospective on the Criteria Movement," Willis H. Ware; RAND, Santa Monica, CA; P-7949, 1995. http://rand.org/pubs/papers/P7949/

9. This scheme is nowhere, to my knowledge, documented explicitly. However, its complexity can be inferred by a study of Appendices A and B of R-609.1 (item [2] above).

10. "The Cyberposture of the National Information Infrastructure," Willis H. Ware; RAND, Santa Monica, CA; MR-976-OSTP, 1998. Available online at: http://www.rand.org/publications/MR/MR976/mr976.html. Also available as http://rand.org/publications/MR/MR976/mr976.pdf.

Preface

Every day, the news media give more and more visibility to the effects of computer security on our daily lives. For example, on a single day in June 2006, the *Washington Post* included three important articles about security. On the front page, one article discussed the loss of a laptop computer containing personal data on 26.5 million veterans. A second article, on the front page of the business section, described Microsoft's new product suite to combat malicious code, spying, and unsecured vulnerabilities in its operating system. Further back, a third article reported on a major consumer electronics retailer that inadvertently installed software on its customers' computers, making them part of a web of compromised slave computers. The sad fact is that news like this appears almost every day, and has done so for a number of years. There is no end in sight.

Even though the language of computer security—terms such as virus, Trojan horse, phishing, spyware—is common, the application of solutions to computer security problems is uncommon. Moreover, new attacks are clever applications of old problems. The pressure to get a new product or new release to market still in many cases overrides security requirements for careful study of potential vulnerabilities and countermeasures. Finally, many people are in denial, blissfully ignoring the serious harm that insecure computing can cause.

WHY READ THIS BOOK?

Admit it. You know computing entails serious risks to the privacy and integrity of your data, or the operation of your computer. Risk is a fact of life: Crossing the street is risky, perhaps more so in some places than others, but you still cross the street. As a child you learned to stop and look both ways before crossing. As you became older you learned to gauge the speed of oncoming traffic and determine whether you had the time to cross. At some point you developed a sense of whether an oncoming car would slow down or yield. We hope you never had to practice this, but sometimes you have to decide whether darting into the street without looking is the best means of escaping danger. The point is all these matters depend on knowledge and experience. We want to help you develop the same knowledge and experience with respect to the risks of secure computing.

How do you control the risk of computer security?

- Learn about the threats to computer security.
- Understand what causes these threats by studying how vulnerabilities arise in the development and use of computer systems.
- Survey the controls that can reduce or block these threats.
- Develop a computing style—as a user, developer, manager, consumer, and voter—that balances security and risk.

The field of computer security changes rapidly, but the underlying problems remain largely unchanged. In this book you will find a progression that shows you how current complex attacks are often instances of more fundamental concepts.

USERS AND USES OF THIS BOOK

This book is intended for the study of computer security. Many of you want to study this topic: college and university students, computing professionals, managers, and users of all kinds of computer-based systems. All want to know the same thing: how to control the risk of computer security. But you may differ in how much information you need about particular topics: Some want a broad survey, while others want to focus on particular topics, such as networks or program development.

This book should provide the breadth and depth that most readers want. The book is organized by general area of computing, so that readers with particular interests can find information easily. The chapters of this book progress in an orderly manner, from general security concerns to the particular needs of specialized applications, and finally to overarching management and legal issues. Thus, the book covers five key areas of interest:

- *introduction*: threats, vulnerabilities, and controls
- *encryption*: the "Swiss army knife" of security controls
- *code*: security in programs, including applications, operating systems, database management systems, and networks
- *management*: building and administering a computing installation, from one computer to thousands, and understanding the economics of cybersecurity
- *law, privacy, ethics*: non-technical approaches by which society controls computer security risks

These areas are not equal in size; for example, more than half the book is devoted to code because so much of the risk is at least partly caused by program code that executes on computers.

The first chapter introduces the concepts and basic vocabulary of computer security. Studying the second chapter provides an understanding of what encryption is and how it can be used or misused. Just as a driver's manual does not address how to design or build a car, Chapter 2 is not for designers of new encryption schemes, but rather for users of encryption. Chapters 3 through 7 cover successively larger pieces of software: individual programs, operating systems, complex applications like database management systems, and finally networks, which are distributed complex systems. Chapter 8 discusses managing and administering security, and describes how to find an acceptable balance between threats and controls. Chapter 9 addresses an important management issue by exploring the economics of cybersecurity: understanding and communicating the costs and benefits. In Chapter 10 we turn to the personal side of computer security as we consider how security, or its lack, affects personal privacy. Chapter 11 covers the way society at large addresses computer security, through its laws and ethical systems. Finally, Chapter 12 returns to cryptography, this time to look at the details of the encryption algorithms themselves.

Within that organization, you can move about, picking and choosing topics of particular interest. Everyone should read Chapter 1 to build a vocabulary and a foundation. It is wise to read Chapter 2 because cryptography appears in so many different control techniques. Although there is a general progression from small programs to large and complex networks, you can in fact read Chapters 3 through 7 out of sequence or pick topics of greatest interest. Chapters 8 and 9 may be just right for the professional looking for non-technical controls to complement the technical ones of the earlier chapters. These chapters may also be important for the computer science student who wants to look beyond a narrow view of bytes and protocols. We recommend Chapters 10 and 11 for everyone, because those chapters deal with the human aspects of security: privacy, laws, and ethics. All computing is ultimately done to benefit humans, and so we present personal risks and approaches to computing. Chapter 12 is for people who want to understand some of the underlying mathematics and logic of cryptography.

What background should you have to appreciate this book? The only assumption is an understanding of programming and computer systems. Someone who is an advanced undergraduate or graduate student in computer science certainly has that background, as does a professional designer or developer of computer systems. A user who wants to understand more about how programs work can learn from this book, too; we provide the necessary background on concepts of operating systems or networks, for example, before we address the related security concerns.

This book can be used as a textbook in a one- or two-semester course in computer security. The book functions equally well as a reference for a computer professional or as a supplement to an intensive training course. And the index and extensive bibliography make it useful as a handbook to explain significant topics and point to key articles in the literature. The book has been used in classes throughout the world; instructors often design one-semester courses that focus on topics of particular interest to the students or that relate well to the rest of a curriculum.

WHAT IS NEW IN THIS BOOK?

This is the fourth edition of *Security in Computing*, first published in 1989. Since then, the specific threats, vulnerabilities, and controls have changed, even though many of the basic notions have remained the same.

The two changes most obvious to people familiar with the previous editions are the additions of two new chapters, on the economics of cybersecurity and privacy. These two areas are receiving more attention both in the computer security community and in the rest of the user population.

But this revision touched every existing chapter as well. The threats and vulnerabilities of computing system's have not stood still since the previous edition in 2003, and so we present new information on threats and controls of many types. Change include:

- the shift from individual hackers working for personal reasons to organized attacker groups working for financial gain
- programming flaws leading to security failures, highlighting man-in-the-middle, timing, and privilege escalation errors
- recent malicious code attacks, such as false interfaces and keystroke loggers
- approaches to code quality, including software engineering, testing, and liability approaches
- rootkits, including ones from unexpected sources
- web applications' threats and vulnerabilities
- privacy issues in data mining
- WiFi network security
- cryptanalytic attacks on popular algorithms, such as RSA, DES, and SHA, and recommendations for more secure use of these
- bots, botnets, and drones, making up networks of compromised systems
- update to the Advanced Encryption System (AES) with experience from its first several years of its use
- the divide between sound authentication approaches and users' actions
- biometric authentication capabilities and limitations
- the conflict between efficient production and use of digital content (e.g., music and videos) and control of piracy

In addition to these major changes, there are numerous small corrective and clarifying ones, ranging from wording and notational changes for pedagogic reasons to replacement, deletion, rearrangement, and expansion of sections.

ACKNOWLEDGMENTS

It is increasingly difficult to acknowledge all the people who have influenced this book. Colleagues and friends have contributed their knowledge and insight, often without knowing their impact. By arguing a point or sharing explanations of concepts, our associates have forced us to question or rethink what we know.

We thank our associates in at least two ways. First, we have tried to include references to their written works as they have influenced this book. References in the text cite specific papers relating to particular thoughts or concepts, but the bibliography also includes broader works that have played a more subtle role in shaping our approach to security. So, to all the cited authors, many of whom are friends and colleagues, we happily acknowledge your positive influence on this book. In particular, we are grateful to the RAND Corporation for permission to present material about its

Vulnerability, Assessment and Mitigation method and to use its government e-mail analysis as a case study in Chapter 8. Second, rather than name individuals, we thank the organizations in which we have interacted with creative, stimulating, and challenging people from whom we learned a lot. These places include Trusted Information Systems, the Contel Technology Center, the Centre for Software Reliability of the City University of London, Arca Systems, Exodus Communications, the RAND Corporation, and Cable & Wireless. If you worked with us at any of these locations, chances are high that you had some impact on this book. And for all the side conversations, debates, arguments, and light moments, we are grateful. For this fourth edition, Roland Trope and Richard Gida gave us particularly helpful suggestions for Chapters 9 and 10.

Authors are the products of their environments. We write to educate because we had good educations ourselves, and because we think the best response to a good education is to pass it along to others. Our parents, Paul and Emma Pfleeger and Emanuel and Beatrice Lawrence, were critical in supporting us and encouraging us to get the best educations we could. Along the way, certain teachers gave us gifts through their teaching. Robert L. Wilson taught Chuck how to learn about computers, and Libuse L. Reed taught him how to write about them. Florence Rogart, Nicholas Sterling and Mildred Nadler taught Shari how to analyze and probe.

To all these people, we express our sincere thanks.

Charles P. Pfleeger
Shari Lawrence Pfleeger
Washington, D.C.

Contents