

NEXT →



### Security in Computing, Fourth Edition

By Charles P. Pfleeger - Pfleeger Consulting Group, Shari Lawrence Pfleeger - RAND Corporation

.....  
Publisher: **Prentice Hall**

Pub Date: **October 13, 2006**

Print ISBN-10: **0-13-239077-9**

Print ISBN-13: **978-0-13-239077-4**

Pages: **880**

[Table of Contents](#) | [Index](#)

## Overview

The New State-of-the-Art in Information Security: Now Covers the Economics of Cyber Security and the Intersection of Privacy and Information Security

For years, IT and security professionals and students have turned to Security in Computing as the definitive guide to information about computer security attacks and countermeasures. In their new fourth edition, Charles P. Pfleeger and Shari Lawrence Pfleeger have thoroughly updated their classic guide to reflect today's newest technologies, standards, and trends.

The authors first introduce the core concepts and vocabulary of computer security, including attacks and controls. Next, the authors systematically identify and assess threats now facing programs, operating systems, database systems, and networks. For each threat, they offer best-practice responses.

Security in Computing, Fourth Edition, goes beyond technology, covering crucial management issues faced in protecting infrastructure and information. This edition contains an all-new chapter on the economics of cybersecurity, explaining ways to make a business case for security investments. Another new chapter addresses privacy--from data mining and identity theft, to RFID and e-voting.

New coverage also includes

- Programming mistakes that compromise security: man-in-the-middle, timing, and privilege escalation attacks
- Web application threats and vulnerabilities
- Networks of compromised systems: bots, botnets, and drones
- Rootkits--including the notorious Sony XCP
- Wi-Fi network security challenges, standards, and techniques
- New malicious code attacks, including false interfaces and keystroke loggers
- Improving code quality: software engineering, testing, and liability approaches
- Biometric authentication: capabilities and limitations
- Using the Advanced Encryption System (AES) more effectively
- Balancing dissemination with piracy control in music and other digital content
- Countering new cryptanalytic attacks against RSA, DES, and SHA
- Responding to the emergence of organized attacker groups pursuing profit

NEXT →



## Security in Computing, Fourth Edition

By Charles P. Pfleeger - Pfleeger Consulting Group, Shari Lawrence Pfleeger - RAND Corporation

.....  
Publisher: **Prentice Hall**

Pub Date: **October 13, 2006**

Print ISBN-10: **0-13-239077-9**

Print ISBN-13: **978-0-13-239077-4**

Pages: **880**

[Table of Contents](#) | [Index](#)

- [Copyright](#)
- [Foreword](#)
- [Preface](#)
- [Chapter 1. Is There a Security Problem in Computing?](#)
  - [Section 1.1. What Does "Secure" Mean?](#)
  - [Section 1.2. Attacks](#)
  - [Section 1.3. The Meaning of Computer Security](#)
  - [Section 1.4. Computer Criminals](#)
  - [Section 1.5. Methods of Defense](#)
  - [Section 1.6. What's Next](#)
  - [Section 1.7. Summary](#)
  - [Section 1.8. Terms and Concepts](#)
  - [Section 1.9. Where the Field Is Headed](#)
  - [Section 1.10. To Learn More](#)
  - [Section 1.11. Exercises](#)
- [Chapter 2. Elementary Cryptography](#)
  - [Section 2.1. Terminology and Background](#)
  - [Section 2.2. Substitution Ciphers](#)
  - [Section 2.3. Transpositions \(Permutations\)](#)
  - [Section 2.4. Making "Good" Encryption Algorithms](#)
  - [Section 2.5. The Data Encryption Standard](#)
  - [Section 2.6. The AES Encryption Algorithm](#)
  - [Section 2.7. Public Key Encryption](#)
  - [Section 2.8. The Uses of Encryption](#)
  - [Section 2.9. Summary of Encryption](#)
  - [Section 2.10. Terms and Concepts](#)
  - [Section 2.11. Where the Field Is Headed](#)
  - [Section 2.12. To Learn More](#)
  - [Section 2.13. Exercises](#)
- [Chapter 3. Program Security](#)
  - [Section 3.1. Secure Programs](#)
  - [Section 3.2. Nonmalicious Program Errors](#)
  - [Section 3.3. Viruses and Other Malicious Code](#)
  - [Section 3.4. Targeted Malicious Code](#)
  - [Section 3.5. Controls Against Program Threats](#)
  - [Section 3.6. Summary of Program Threats and Controls](#)
  - [Section 3.7. Terms and Concepts](#)
  - [Section 3.8. Where the Field Is Headed](#)
  - [Section 3.9. To Learn More](#)

- [Section 3.10. Exercises](#)
- [Chapter 4. Protection in General-Purpose Operating Systems](#)
  - [Section 4.1. Protected Objects and Methods of Protection](#)
  - [Section 4.2. Memory and Address Protection](#)
  - [Section 4.3. Control of Access to General Objects](#)
  - [Section 4.4. File Protection Mechanisms](#)
  - [Section 4.5. User Authentication](#)
  - [Section 4.6. Summary of Security for Users](#)
  - [Section 4.7. Terms and Concepts](#)
  - [Section 4.8. Where the Field Is Headed](#)
  - [Section 4.9. To Learn More](#)
  - [Section 4.10. Exercises](#)
- [Chapter 5. Designing Trusted Operating Systems](#)
  - [Section 5.1. What Is a Trusted System?](#)
  - [Section 5.2. Security Policies](#)
  - [Section 5.3. Models of Security](#)
  - [Section 5.4. Trusted Operating System Design](#)
  - [Section 5.5. Assurance in Trusted Operating Systems](#)
  - [Section 5.6. Summary of Security in Operating Systems](#)
  - [Section 5.7. Terms and Concepts](#)
  - [Section 5.8. Where the Field Is Headed](#)
  - [Section 5.9. To Learn More](#)
  - [Section 5.10. Exercises](#)
- [Chapter 6. Database and Data Mining Security](#)
  - [Section 6.1. Introduction to Databases](#)
  - [Section 6.2. Security Requirements](#)
  - [Section 6.3. Reliability and Integrity](#)
  - [Section 6.4. Sensitive Data](#)
  - [Section 6.5. Inference](#)
  - [Section 6.6. Multilevel Databases](#)
  - [Section 6.7. Proposals for Multilevel Security](#)
  - [Section 6.8. Data Mining](#)
  - [Section 6.9. Summary of Database Security](#)
  - [Section 6.10. Terms and Concepts](#)
  - [Section 6.11. Where the Field Is Headed](#)
  - [Section 6.12. To Learn More](#)
  - [Section 6.13. Exercises](#)
- [Chapter 7. Security in Networks](#)
  - [Section 7.1. Network Concepts](#)
  - [Section 7.2. Threats in Networks](#)
  - [Section 7.3. Network Security Controls](#)
  - [Section 7.4. Firewalls](#)
  - [Section 7.5. Intrusion Detection Systems](#)
  - [Section 7.6. Secure E-Mail](#)
  - [Section 7.7. Summary of Network Security](#)
  - [Section 7.8. Terms and Concepts](#)
  - [Section 7.9. Where the Field Is Headed](#)
  - [Section 7.10. To Learn More](#)
  - [Section 7.11. Exercises](#)
- [Chapter 8. Administering Security](#)
  - [Section 8.1. Security Planning](#)

- [Section 8.2. Risk Analysis](#)
- [Section 8.3. Organizational Security Policies](#)
- [Section 8.4. Physical Security](#)
- [Section 8.5. Summary](#)
- [Section 8.6. Terms and Concepts](#)
- [Section 8.7. To Learn More](#)
- [Section 8.8. Exercises](#)
- [Chapter 9. The Economics of Cybersecurity](#)
  - [Section 9.1. Making a Business Case](#)
  - [Section 9.2. Quantifying Security](#)
  - [Section 9.3. Modeling Cybersecurity](#)
  - [Section 9.4. Current Research and Future Directions](#)
  - [Section 9.5. Summary](#)
  - [Section 9.6. Terms and Concepts](#)
  - [Section 9.7. To Learn More](#)
  - [Section 9.8. Exercises](#)
- [Chapter 10. Privacy in Computing](#)
  - [Section 10.1. Privacy Concepts](#)
  - [Section 10.2. Privacy Principles and Policies](#)
  - [Section 10.3. Authentication and Privacy](#)
  - [Section 10.4. Data Mining](#)
  - [Section 10.5. Privacy on the Web](#)
  - [Section 10.6. E-Mail Security](#)
  - [Section 10.7. Impacts on Emerging Technologies](#)
  - [Section 10.8. Summary](#)
  - [Section 10.9. Terms and Concepts](#)
  - [Section 10.10. Where the Field Is Headed](#)
  - [Section 10.11. To Learn More](#)
  - [Section 10.12. Exercises](#)
- [Chapter 11. Legal and Ethical Issues in Computer Security](#)
  - [Section 11.1. Protecting Programs and Data](#)
  - [Section 11.2. Information and the Law](#)
  - [Section 11.3. Rights of Employees and Employers](#)
  - [Section 11.4. Redress for Software Failures](#)
  - [Section 11.5. Computer Crime](#)
  - [Section 11.6. Ethical Issues in Computer Security](#)
  - [Section 11.7. Case Studies of Ethics](#)
  - [Section 11.8. Terms and Concepts](#)
  - [Section 11.9. To Learn More](#)
  - [Section 11.10. Exercises](#)
- [Chapter 12. Cryptography Explained](#)
  - [Section 12.1. Mathematics for Cryptography](#)
  - [Section 12.2. Symmetric Encryption](#)
  - [Section 12.3. Public Key Encryption Systems](#)
  - [Section 12.4. Quantum Cryptography](#)
  - [Section 12.5. Summary of Encryption](#)
  - [Section 12.6. Terms and Concepts](#)
  - [Section 12.7. Where the Field Is Headed](#)
  - [Section 12.8. To Learn More](#)
  - [Section 12.9. Exercises](#)

— [Bibliography](#)

— [Index](#)

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.