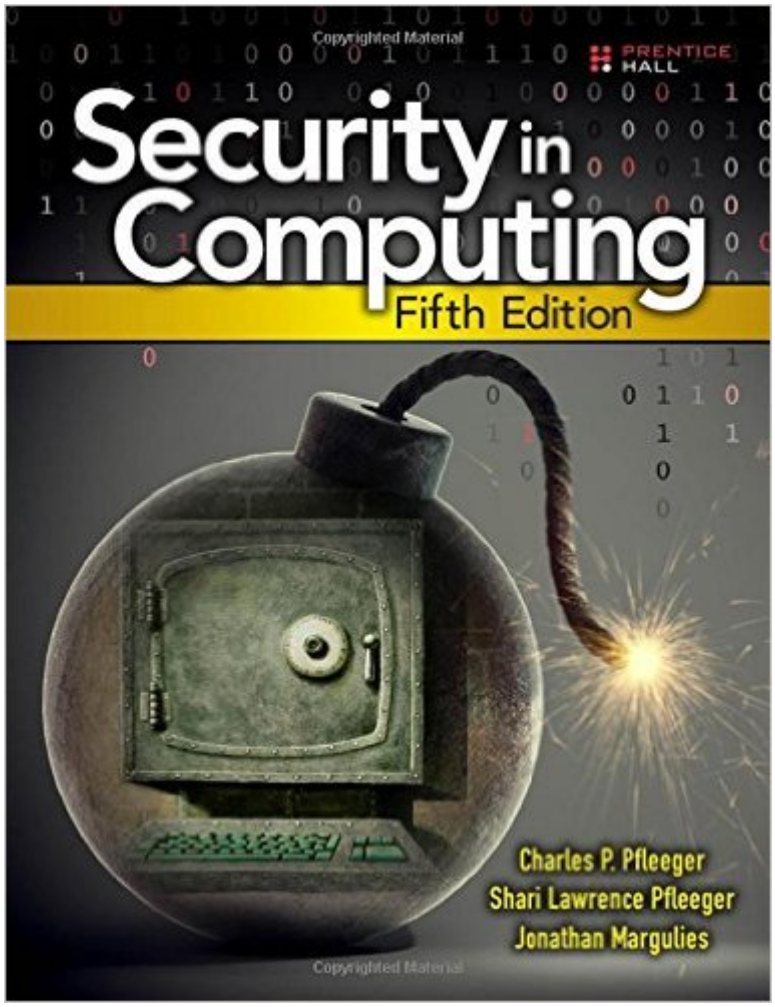
Security In Computing (5th Edition)



Synopsis

The New State of the Art in Information Security: Now Covers Cloud Computing, the Internet of Things, and Cyberwarfare Â Students and IT and security professionals have long relied on Security in Computing as the definitive guide to computer security attacks and countermeasures. Now, the authors have thoroughly updated this classic to reflect todayâ ™s newest technologies, attacks, standards, and trends. Â Security in Computing, Fifth Edition, offers complete, timely coverage of all aspects of computer security, including users, software, devices, operating systems, networks, and data. Reflecting rapidly evolving attacks, countermeasures, and computing environments, this new edition introduces best practices for authenticating users, preventing malicious code execution, using encryption, protecting privacy, implementing firewalls, detecting intrusions, and more. More than two hundred end-of-chapter exercises help the student to solidify lessons learned in each chapter. Â Combining breadth, depth, and exceptional clarity, this comprehensive guide builds carefully from simple to complex topics, so you always understand all you need to know before you move forward. Â Youâ ™ll start by mastering the fieldâ ™s basic terms, principles, and concepts. Next, youâ ™ll apply these basics in diverse situations and environments, learning to â •think like an attackerâ • and identify exploitable weaknesses. Then you will switch to defense, selecting the best available solutions and countermeasures. Finally, youâ ™ll go beyond technology to understand crucial management issues in protecting infrastructure and data. Â New coverage includes A full chapter on securing cloud environments and managing their unique risks Extensive new coverage of security issues associated with userâ ”web interaction New risks and techniques for safeguarding the Internet of Things A new primer on threats to privacy and how to guard it An assessment of computers and cyberwarfareâ “recent attacks and emerging risks Security flaws and risks associated with electronic voting systems Â

Book Information

Hardcover: 944 pages

Publisher: Prentice Hall; 5 edition (February 5, 2015)

Language: English

ISBN-10: 0134085043

ISBN-13: 978-0134085043

Product Dimensions: 7.2 x 1.4 x 9.2 inches

Shipping Weight: 2.8 pounds (View shipping rates and policies)

Average Customer Review: 4.7 out of 5 starsÂ Â See all reviewsÂ (6 customer reviews)

Best Sellers Rank: #37,028 in Books (See Top 100 in Books) #36 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #41 inÂ Books > Textbooks > Computer Science > Networking #122 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

I read and review about 30 books a year on average, plus spend most of my days researching and writing about digital security. I've been doing this routine since 1989 so I have a so-so understanding of cyber security. Security in Computing took me by surprise since it looked like the average security 101 book I read way too often. This book is nothing like any security book I've read before except a few dissertation pieces I've picked up.The 910 page book is filled with heavy research and plenty of great real world examples. One of the first things I noticed was that many of the references were from the 1960s, 70s, 80s and 90s. This tells me that the authors went back to old school style and not just internet searches for content. If you do nothing else, get this book just for the bibliography. It is amazing because it is filled with old ideas that we still haven't learned in security.From a depth standpoint, this book should be mandatory reading for anyone after they obtain their CISSP. The Pfleegers and Margulies do a great job of presenting deeper understandings of security concepts along with pictures and examples from recent security failures. They stick to the basics of confidentiality, integrity and availability (CIA) but build off of those to show the reader how those concepts extend to a much wider field of study.This is not a classroom textbook, this is a manual on digital security with all the juicy stories that didn't make the headlines and all the original papers written before blogs existed. You will find exercises at the end of each chapter that are fairly well written but it's kind of difficult to complete the exercises when your jaw is still on the floor.

This book is a beast!!! It is 100 % textbook, with a lot of exercises at the end of the chapters. If your class uses this book, get ready for a fire hose of information. It covers a ton of topics and covers them in depth.Although it is a text book the authors do there best to keep it interesting. I really enjoyed the sidebars that include true stories of security breaches. I really like the ones that find out what the criminal was thinking. Some of the reasons for doing what they do are nuts.One of the biggest problems with security I see today is the security teams oftentimes don't know what to secure, or how to secure stuff when they do. This book starts out with a really nice introduction to what computer security is. The author discusses Values of Assets, the

Vulnerabilityâ “Threatâ “Control Paradigm, Confidentiality, Integrity, Availability, Types of Threats, Types of Attackers, Risk and Common Sense, Methodâ “Opportunityâ “Motive, Vulnerabilities, and Controls. By the time you are done this chapter you have a high level few of today’s security issues.1. Introduction2. Toolbox: Authentication, Access Control, and Cryptography3. Programs and Programming4. The Webâ ”User Side5. Operating Systems6. Networks7. Databases8. Cloud Computing9. Privacy10. Management and Incidents11. Legal Issues and Ethics12. Details of Cryptography13. Emerging TopicsI was glad to see information on regulations, compliance, and laws. They can wreak havoc on an organization’s productivity when left to an unqualified security team. I usually find that IT organizations that have locked down everything from the Internet to your USBs, have no concept of how to implement security in a managed and efficient way.

Network Auditing: Jay Beale Open Source Security Series (Jay Beale's Open Source Security) Security Strategies In Linux Platforms And Applications (Jones & Bartlett Learning Information Systems Security & Assurance) Laboratory Manual To Accompany Security Strategies In Linux Platforms And Applications (Jones & Bartlett Learning Information Systems Security & Assurance Series)