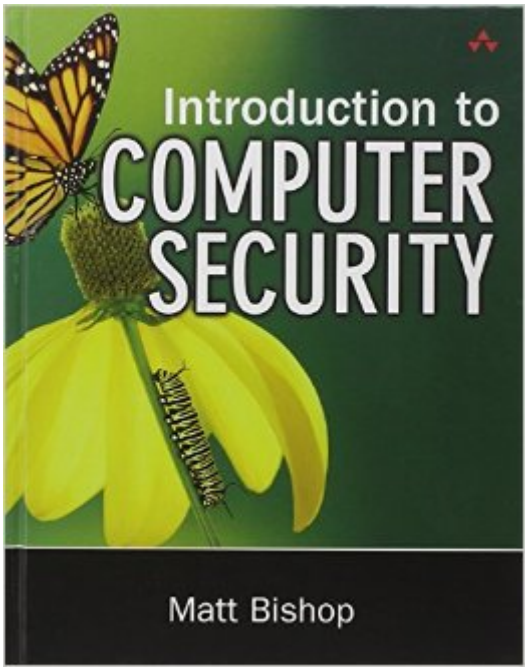
Introduction To Computer Security



Synopsis

In this authoritative book, widely respected practitioner and teacher Matt Bishop presents a clear and useful introduction to the art and science of information security. Bishop's insights and realistic examples will help any practitioner or student understand the crucial links between security theory and the day-to-day security challenges of IT environments. Bishop explains the fundamentals of security: the different types of widely used policies, the mechanisms that implement these policies, the principles underlying both policies and mechanisms, and how attackers can subvert these tools--as well as how to defend against attackers. A practicum demonstrates how to apply these ideas and mechanisms to a realistic company. Coverage includes Confidentiality, integrity, and availability Operational issues, cost-benefit and risk analyses, legal and human factors Planning and implementing effective access control Defining security, confidentiality, and integrity policies Using cryptography and public-key systems, and recognizing their limits Understanding and using authentication: from passwords to biometrics Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more Controlling information flow through systems and networks Assuring security throughout the system lifecycle Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs--and defenses against them Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention Applying security principles to networks, systems, users, and programs Introduction to Computer Security is adapted from Bishop's comprehensive and widely praised book, Computer Security: Art and Science. This shorter version of the original work omits much mathematical formalism, making it more accessible for professionals and students who have a less formal mathematical background, or for readers with a more practical than theoretical interest.

Book Information

Hardcover: 784 pages

Publisher: Addison-Wesley Professional; 1 edition (November 5, 2004)

Language: English

ISBN-10: 0321247442

ISBN-13: 978-0321247445

Product Dimensions: 7.6 x 1.3 x 9.4 inches

Shipping Weight: 3 pounds (View shipping rates and policies)

Average Customer Review: 3.5 out of 5 starsÂ Â See all reviewsÂ (24 customer reviews)

Best Sellers Rank: #436,879 in Books (See Top 100 in Books) #100 inÂ Books > Computers &

Technology > Certification > CompTIA #541 inÂ Books > Textbooks > Computer Science > Networking #1136 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

I recently finished the book Introduction to Computer Security by Matt Bishop (Addison-Wesley). I hope to be fair on this review, but I’m probably going to be a little harsh...Chapter list: Preface; An Overview of Computer Security; Access Control Matrix; Foundational Results; Security Policies; Confidentiality Policies; Integrity Policies; Hybrid Policies; Basic Cryptography; Key Management; Cipher Techniques; Authentication; Design Principles; Representing Identity; Access Control Mechanisms; Information Flow; Confinement Problem; Introduction to Assurance; Evaluating Systems; Malicious Logic; Vulnerability Analysis; Auditing; Intrusion Detection; Network Security; System Security; User Security; Program Security; Lattices; The Extended Euclidean Algorithm; Virtual Machines; Bibliography; IndexOK, for the good stuff. This is probably one of the most complete academic treatments of computer security that I’ve ever seen. According to the preface, this is a "condensed" and updated version of the author’s earlier work, Computer Security: Art and Science. His three goals, which are probably met, are to show the importance of theory to practice/practice to theory, to emphasize that computer security and cryptography are different, and to demonstrate that computer security is a science *and* an art. He also considers this book to omit much of the mathematical formalism. And that’s where I start to have problems. In my opinion, he missed his target entirely.

(NOTE: The title of this book when it was originally published was "Security for the Practical Administrator". Thus, my review reflects what I still firmly believe were an inappropriate title and cover notes. Some time after that, the book was renamed to its current title. So, if you’re confused as to my statements about it not being "practical", that’s why.)I hate to be the fly in the ointment of the other reviews. But as someone who is more concerned with protecting his networks than trying to figure out the math behind the security, I found this book’s title and description on the back cover as well as in the preface to be *highly* misleading.By reading the preface and the back of the book, you gain absolutely no indication that this book is mired in mathematical theory with very little practical application to the everyday, IT environment. The only possible audience for this book comprises computer science students and software engineers who are into encryption, cipher algorithms, and related theories. There is absolutely no indication of that until you actually start getting into the chapters.That is not to belittle Mr. Bishop, what he knows, or what he does. I have

no doubt that as a professor at the University of California at Davis he is well respected and very knowledgeable of his field. I'm equally sure that in a scientific, trivia challenge, his knowledge and experience would beat me into the ground until I was just a thin, red film. I'm only saying that this book is not one that I can recommend to anyone who is looking for practical, security solutions, contrary to what the title might infer.