Synopsis

For one-semester, undergraduate- or graduate-level courses in Cryptography, Computer Security, and Network Security. The book is suitable for self-study and so provides a solid and up-to-date tutorial. The book is also a comprehensive treatment of cryptography and network security and so is suitable as a reference for a system engineer, programmer, system manager, network manager, product marketing personnel, or system support specialist. A practical survey of cryptography and network security with unmatched support for instructors and students. In this age of universal electronic connectivity, viruses and hackers, electronic eavesdropping, and electronic fraud, security is paramount. This text provides a practical survey of both the principles and practice of cryptography and network security. First, the basic issues to be addressed by a network security capability are explored through a tutorial and survey of cryptography and network security technology. Then, the practice of network security is explored via practical applications that have been implemented and are in use today. An unparalleled support package for instructors and students ensures a successful teaching and learning experience.

Book Information

Hardcover: 752 pages
Publisher: Pearson; 6 edition (March 16, 2013)
Language: English
ISBN-10: 0133354695
Product Dimensions: 7.2 x 1.2 x 9.2 inches
Shipping Weight: 2.3 pounds
Average Customer Review: 3.8 out of 5 stars See all reviews (50 customer reviews)

Customer Reviews

This book is intended to serve both as a textbook for an academic course of study, and as a self-study and reference guide for practicing professionals. The material has been extended to emphasize encryption and its central position in network protection. The structure and flow have been reorganized with both classroom use and solo instruction in mind, and additional teaching
material, such as additional problems, have been added. Chapter one is an introduction to the topics to be covered. In a practical way it outlines the concerns involved in the phrase computer security, and the priorities occasioned by the networked nature of modern computing. There is also an outline of the chapters and sequence in the rest of the book. While the text does note that cryptographic techniques underlie most of current security technologies this is only done briefly. Examples in the major categories listed would help explain this primary position. Part one deals with conventional, symmetric, encryption and the various methods of attacking it. Chapter two covers the historical substitution and transposition ciphers. Symmetric block ciphers are discussed in chapter three, illustrated by an explanation of DES (Data Encryption Standard). The additional conventional algorithms of triple DES, IDEA (International Data Encryption Algorithm), and RC5 are reviewed in chapter four. The use of conventional encryption for confidentiality is outlined in chapter five. Part three looks at public-key encryption and hash functions. Chapter six introduces public-key encryption and its uses in confidentiality, authentication, and key management and exchange. Number theory is the basis of these modern algorithms, so some basic mathematical concepts are outlined in chapter seven.

Download to continue reading...


Dmca