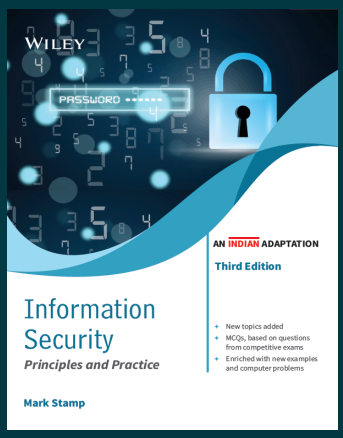
WILEY



Information Security, 3ed: Principles and Practice (An Indian Adaptation)

By Mark Stamp

Paperback 9789354644313 ₹1,099.00

Pages: 552

Description

Information Security: Principles and Practice, third edition, is the perfect textbook for undergraduate and graduate students in all Computer Science programs and remains essential reading for professionals working in industrial or government security. Providing up-to-date coverage of the rapidly evolving field of information security, the book focuses on the four critical components of information security—cryptography, access control, security protocols, and software. In addition, it provides a wealth of real-world examples that clarify complex topics, highlight important security issues, and demonstrate effective methods and strategies for protecting the confidentiality and integrity of data.

About the Author

Mark Stamp

Mark Stamp

(San José State University, San Jose, California

Table of Contents

Preface to the Adapted Edition

Preface to the US Edition

About the Author

Acknowledgments

1 Introduction

1.1 The Cast of Characters

1.2 Alice’s Online Bank

1.3 About This Book

1.4 The People Problem

1.5 Principles and Practice

I Crypto

2 Classic Crypto

2.1 Introduction

2.2 How to Speak Crypto

2.3 Classic Ciphers

2.4 Classic Crypto in History
2.5 Modern Crypto History
2.6 A Taxonomy of Cryptography
2.7 A Taxonomy of Cryptanalysis
3 Symmetric Ciphers
3.1 Introduction
3.2 Stream Ciphers
3.3 Block Ciphers
3.4 Integrity
3.5 Quantum Computers and Symmetric Crypto
4 Public Key Crypto
4.1 Introduction
4.2 Knapsack
4.3 RSA
4.4 Diffie–Hellman
4.5 Elliptic Curve Cryptography
4.6 ElGamal
4.7 Rabin Cryptosystem
4.8 Public Key Notation
4.9 Uses for Public Key Crypto
4.10 Certificates and PKI
4.11 Quantum Computers and Public Key
5 Crypto Hash Functions++
5.1 Introduction
5.2 What Is a Cryptographic Hash Function?
5.3 The Birthday Problem
5.4 A Birthday Attack
5.5 Non-Cryptographic Hashes
5.6 SHA-3
5.7 HMAC
5.8 Additional Cryptographic Hash Functions
5.9 Cryptographic Hash Applications
5.10 Miscellaneous Crypto-Related Topics
II Access Control
6 Authentication
6.1 Introduction
6.2 Authentication Methods
6.3 Passwords

6.4 Biometrics
6.5 Something You Have
6.6 Multi-Factor Authentication
6.7 Single Sign-On and Web Cookies
7 Authorization
7.1 Introduction
7.2 A Brief History of Authorization
7.3 Access Control Matrix
7.4 Multilevel Security Models
7.5 Covert Channels
7.6 Inference Control
7.7 CAPTCHA
III Topics in Network Security
8 Network Security Basics
8.1 Introduction
8.2 Networking Basics
8.3 Cross-Site Scripting Attacks
8.4 Firewalls
8.5 Intrusion Detection Systems
9 Simple Authentication Protocols
9.1 Introduction
9.2 Simple Security Protocols
9.3 Authentication Protocols
9.4 “Authentication” and TCP
9.5 Zero Knowledge Proofs
9.6 Tips for Analyzing Protocols
10 Real-World Security Protocols
10.1 Introduction
10.2 SSH
10.3 SSL
10.4 IPsec
10.5 Kerberos
10.6 WEP
10.7 GSM
IV Software
11 Software Flaws and Malware
11.1 Introduction
11.2 Software Flaws

11.3 Malware
11.4 Miscellaneous Software-Based Attacks
12 Insecurity in Software
12.1 Introduction
12.2 Software Reverse Engineering
12.3 Software Development
12.4 Reproducible Builds
12.5 Secure Coding Practices
Summary
Problems
Computer Problem
Multiple Choice Questions
Appendix
A-1 Modular Arithmetic
A-2 Permutations
A-3 Probability
A-4 DES Permutations
A-5 Substitution–Permutation Networks
A-6 Cyber Laws and Forensics
A-7 Digital Rights Management
Bibliography
Index

To purchase this product, please visit:
https://www.wileyindia.com/information-security-3ed-principles-and-practice-an-indian-adaptation.html

Scan to buy