1. Record Nr. UNINA9910154774103321

Autore	Stallings William
Titolo	Computer security : principles and practice / / William Stallings, Lawrie Brown
Pubbl/distr/stampa	Boston : , : Pearson, , [2015] ©2015
ISBN	1-292-06620-2
Edizione	[Third edition, Global edition.]
Descrizione fisica	1 online resource (840 pages) : illustrations
Collana	Always Learning
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title -- Copyright -- Contents -- Online Resources -- Preface -- Notation -- About the Authors -- Chapter 0 Reader's and Instructor's Guide -- 0.1 Outline of this Book -- 0.2 A Roadmap for Readers and Instructors -- 0.3 Support for Cisp Certification -- 0.4 Support for NSA/DHS Certification -- 0.5 Support for ACM/IEEE Computer Society Computer Science Curricula 2013 -- 0.6 Internet and Web Resources -- 0.7 Standards -- Chapter 1 Overview -- 1.1 Computer Security Concepts -- 1.2 Threats, Attacks, and Assets -- 1.3 Security Functional Requirements -- 1.4 Fundamental Security Design Principles -- 1.5 Attack Surfaces and Attack Trees -- 1.6 Computer Security Strategy -- 1.7 Recommended Reading -- 1.8 Key Terms, Review Questions, and Problems -- Part One Computer Security Technology and Principles -- Chapter 2 Cryptographic Tools -- 2.1 Confidentiality with Symmetric Encryption -- 2.2 Message Authentication and Hash Functions -- 2.3 Public-Key Encryption -- 2.4 Digital Signatures and Key Management -- 2.5 Random and Pseudorandom Numbers -- 2.6 Practical Application: Encryption of Stored Data -- 2.7 Recommended Reading -- 2.8 Key Terms, Review Questions, and Problems -- Chapter 3 User Authentication -- 3.1 Electronic User Authentication Principles -- 3.2 Password-Based Authentication -- 3.3 Token-Based Authentication -- 3.4 Biometric Authentication -- 3.5 Remote User Authentication -- 3.6 Security

Issues for User Authentication -- 3.7 Practical Application: An Iris Biometric System -- 3.8 Case Study: Security Problems for ATM Systems -- 3.9 Recommended Reading -- 3.10 Key Terms, Review Questions, and Problems -- Chapter 4 Access Control -- 4.1 Access Control Principles -- 4.2 Subjects, Objects, and Access Rights -- 4.3 Discretionary Access Control -- 4.4 Example: UNIX File Access Control -- 4.5 Role-Based Access Control.
4.6 Attribute-Based Access Control -- 4.7 Identity, Credential, and Access Management -- 4.8 Trust Frameworks -- 4.9 Case Study: RBAC System for a Bank -- 4.10 Recommended Reading -- 4.11 Key Terms, Review Questions, and Problems -- Chapter 5 Database and Cloud Security -- 5.1 The Need for Database Security -- 5.2 Database Management Systems -- 5.3 Relational Databases -- 5.4 SQL Injection Attacks -- 5.5 Database Access Control -- 5.6 Inference -- 5.7 Database Encryption -- 5.8 Cloud Computing -- 5.9 Cloud Security Risks and Countermeasures -- 5.10 Data Protection in the Cloud -- 5.11 Cloud Security as a Service -- 5.12 Recommended Reading -- 5.13 Key Terms, Review Questions, and Problems -- Chapter 6 Malicious Software -- 6.1 Types of Malicious Software (Malware) -- 6.2 Advanced Persistent Threat -- 6.3 Propagation-Infected Content-Viruses -- 6.4 Propagation-Vulnerability Exploit-Worms -- 6.5 Propagation-Social Engineering-Spam E-Mail, Trojans -- 6.6 Payload-System Corruption -- 6.7 Payload-Attack Agent-Zombie, Bots -- 6.8 Payload-Information Theft-Keyloggers, Phishing, Spyware -- 6.9 Payload-Stealthing-Backdoors, Rootkits -- 6.10 Countermeasures -- 6.11 Recommended Reading -- 6.12 Key Terms, Review Questions, and Problems -- Chapter 7 Denial-of-Service Attacks -- 7.1 Denial-of-Service Attacks -- 7.2 Flooding Attacks -- 7.3 Distributed Denial-of-Service Attacks -- 7.4 Application-Based Bandwidth Attacks -- 7.5 Reflector and Amplifier Attacks -- 7.6 Defenses Against Denial-of-Service Attacks -- 7.7 Responding to a Denial-of-Service Attack -- 7.8 Recommended Reading -- 7.9 Key Terms, Review Questions, and Problems -- Chapter 8 Intrusion Detection -- 8.1 Intruders -- 8.2 Intrusion Detection -- 8.3 Analysis Approaches -- 8.4 Host-Based Intrusion Detection -- 8.5 Network-Based Intrusion Detection -- 8.6 Distributed or Hybrid Intrusion Detection.
8.7 Intrusion Detection Exchange Format -- 8.8 Honeypots -- 8.9 Example System: Snort -- 8.10 Recommended Reading -- 8.11 Key Terms, Review Questions, and Problems -- Chapter 9 Firewalls and Intrusion Prevention Systems -- 9.1 The Need for Firewalls -- 9.2 Firewall Characteristics and Access Policy -- 9.3 Types of Firewalls -- 9.4 Firewall Basing -- 9.5 Firewall Location and Configurations -- 9.6 Intrusion Prevention Systems -- 9.7 Example: Unified Threat Management Products -- 9.8 Recommended Reading -- 9.9 Key Terms, Review Questions, and Problems -- Part Two Software Security and Trusted Systems -- Chapter 10 Buffer Overflow -- 10.1 Stack Overflows -- 10.2 Defending Against Buffer Overflows -- 10.3 Other Forms of Overflow Attacks -- 10.4 Recommended Reading -- 10.5 Key Terms, Review Questions, and Problems -- Chapter 11 Software Security -- 11.1 Software Security Issues -- 11.2 Handling Program Input -- 11.3 Writing Safe Program Code -- 11.4 Interacting with the Operating System and Other Programs -- 11.5 Handling Program Output -- 11.6 Recommended Reading -- 11.7 Key Terms, Review Questions, and Problems -- Chapter 12 Operating System Security -- 12.1 Introduction to Operating System Security -- 12.2 System Security Planning -- 12.3 Operating Systems Hardening -- 12.4 Application Security -- 12.5 Security Maintenance -- 12.6 Linux/Unix Security -- 12.7 Windows Security -- 12.8 Virtualization Security -- 12.9

Recommended Reading -- 12.10 Key Terms, Review Questions, and Problems -- Chapter 13 Trusted Computing and Multilevel Security -- 13.1 The Bell-LaPadula Model for Computer Security -- 13.2 Other Formal Models for Computer Security -- 13.3 The Concept of Trusted Systems -- 13.4 Application of Multilevel Security -- 13.5 Trusted Computing and the Trusted Platform Module -- 13.6 Common Criteria for Information Technology Security Evaluation.
13.7 Assurance and Evaluation -- 13.8 Recommended Reading -- 13.9 Key Terms, Review Questions, and Problems -- Part Three Management Isues -- Chapter 14 IT Security Management and Risk Assessment -- 14.1 IT Security Management -- 14.2 Organizational Context and Security Policy -- 14.3 Security Risk Assessment -- 14.4 Detailed Security Risk Analysis -- 14.5 Case Study: Silver Star Mines -- 14.6 Recommended Reading -- 14.7 Key Terms, Review Questions, and Problems -- Chapter 15 IT Security Controls, Plans, and Procedures -- 15.1 IT Security Management Implementation -- 15.2 Security Controls or Safeguards -- 15.3 IT Security Plan -- 15.4 Implementation of Controls -- 15.5 Monitoring Risks -- 15.6 Case Study: Silver Star Mines -- 15.7 Recommended Reading -- 15.8 Key Terms, Review Questions, and Problems -- Chapter 16 Physical and Infrastructure Security -- 16.1 Overview -- 16.2 Physical Security Threats -- 16.3 Physical Security Prevention and Mitigation Measures -- 16.4 Recovery From Physical Security Breaches -- 16.5 Example: A Corporate Physical Security Policy -- 16.6 Integration of Physical and Logical Security -- 16.7 Recommended Reading -- 16.8 Key Terms, Review Questions, and Problems -- Chapter 17 Human Resources Security -- 17.1 Security Awareness, Training, and Education -- 17.2 Employment Practices and Policies -- 17.3 E-Mail and Internet Use Policies -- 17.4 Computer Security Incident Response Teams -- 17.5 Recommended Reading -- 17.6 Key Terms, Review Questions, and Problems -- Chapter 18 Security Auditing -- 18.1 Security Auditing Architecture -- 18.2 Security Audit Trail -- 18.3 Implementing the Logging Function -- 18.4 Audit Trail Analysis -- 18.5 Example: An Integrated Approach -- 18.6 Recommended Reading -- 18.7 Key Terms, Review Questions, and Problems -- Chapter 19 Legal and Ethical Aspects -- 19.1 Cybercrime and Computer Crime.
19.2 Intellectual Property -- 19.3 Privacy -- 19.4 Ethical Issues -- 19.5 Recommended Reading -- 19.6 Key Terms, Review Questions, and Problems -- Part Four Cryptographic Algorithms -- Chapter 20 Symmetric Encryption and Message Confidentiality -- 20.1 Symmetric Encryption Principles -- 20.2 Data Encryption Standard -- 20.3 Advanced Encryption Standard -- 20.4 Stream Ciphers and RC4 -- 20.5 Cipher Block Modes of Operation -- 20.6 Location of Symmetric Encryption Devices -- 20.7 Key Distribution -- 20.8 Recommended Reading -- 20.9 Key Terms, Review Questions, and Problems -- Chapter 21 Public-Key Cryptography and Message Authentication -- 21.1 Secure Hash Functions -- 21.2 HMAC -- 21.3 The RSA Public-Key Encryption Algorithm -- 21.4 Diffie-Hellman and Other Asymmetric Algorithms -- 21.5 Recommended Reading -- 21.6 Key Terms, Review Questions, and Problems -- Part Five Network Security -- Chapter 22 Internet Security Protocols and Standards -- 22.1 Secure E-Mail and S/MIME -- 22.2 DomainKeys Identified Mail -- 22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) -- 22.4 HTTPS -- 22.5 IPv4 and IPv6 Security -- 22.6 Recommended Reading -- 22.7 Key Terms, Review Questions, and Problems -- Chapter 23 Internet Authentication Applications -- 23.1 Kerberos -- 23.2 X.509 -- 23.3 Public-Key Infrastructure -- 23.4 Recommended Reading -- 23.5 Key Terms, Review Questions, and Problems -- Chapter 24 Wireless

Network Security -- 24.1 Wireless Security -- 24.2 Mobile Device Security -- 24.3 IEEE 802.11 Wireless LAN Overview -- 24.4 IEEE 802.11i Wireless LAN Security -- 24.5 Recommended Reading -- 24.6 Key Terms, Review Questions, and Problems -- Appendix A Projects and Other Student Exercises for Teaching Computer Security -- A.1 Hacking Project -- A.2 Laboratory Exercises -- A.3 Security Education (SEED) Projects -- A.4 Research Projects.
A.5 Programming Projects.

Sommario/riassunto

Computer Security: Principles and Practice, Third Edition, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically-and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. It covers all security topics considered Core in the EEE/ACM Computer Science Curriculum. This textbook can be used to prep for CISSP Certification, and includes in-depth coverage of Computer Security, Technology and Principles, Software Security, Management Issues, Cryptographic Algorithms, Internet Security and more. The Text and Academic Authors Association named Computer Security: Principles and Practice, First Edition, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008. Teaching and Learning Experience This program presents a better teaching and learning experience-for you and your students. It will help: Easily Integrate Projects in your Course: This book provides an unparalleled degree of support for including both research and modeling projects in your course, giving students a broader perspective. Keep Your Course Current with Updated Technical Content: This edition covers the latest trends and developments in computer security. Enhance Learning with Engaging Features: Extensive use of case studies and examples provides real-world context to the text material. Provide Extensive Support Material to Instructors and Students: Student and instructor resources are available to expand on the topics presented in the text.