1. Record Nr. UNINA9910831028903321

Autore	Dube Roger
Titolo	Hardware-based computer security techniques to defeat hackers [[electronic resource]] : from biometrics to quantum cryptography / / Roger Dube
Pubbl/distr/stampa	Hoboken, N.J., : Wiley, c2008
ISBN	1-281-83706-7 9786611837068 0-470-42549-0 0-470-42547-4
Descrizione fisica	1 online resource (254 p.)
Disciplina	005.8
Soggetti	Computer security - Equipment and supplies Computer security - Computer programs Computer input-output equipment Computer crimes - Prevention
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Hardware-Based Computer Security Techniques to Defeat Hackers; CONTENTS; 1 THE ELEMENTS OF COMPUTER SECURITY; Cryptography; Symmetric Key Cryptography; Asymmetric Key Cryptography; Passwords and Keys; Password/Key Strength; Password/Key Storage and Theft; Passwords and Authentication; Something You Know; Something You Have; Something You Are; Random-Number Generators; Pseudo-Random-Number Generators (PRGs); Hardware-Based Random-Number Generators; Hybrid Hardware/Software Random-Number Generators; Key Generation; Security and the Internet; References; 2 CRYPTOGRAPHY APPROACHES AND ATTACKS Symmetric Key CryptographyOne-Time Pad; DES and Triple DES; International Data-Encryption Algorithm; Rivest Cipher 4; Blowfish; Advanced Encryption Standard; Quantum Cryptography; Hash Algorithms; The Birthday Paradox and Hash Algorithms; References; 3 KEY GENERATION AND DISTRIBUTION APPROACHES AND ATTACKS; Key Generation; Software Key Generation; Hardware Key Generation; Noise-

Based Approaches; Noisy Diodes and Resistors; Radio-Frequency Sources; Brownian-Motion Devices; Quantum Devices; Nuclear Decay Devices; Optical Devices; Other Hardware Sources of Randomness; Key Distribution
Key Distribution for Software-Based PRGsKey Distribution; Key Storage; Key Use; Key Distribution for Hardware-Based RNGs; Creation of RNGs; Initialization of RNGs; Distribution of RNGs; Key Storage and Use; Minimizing Hardware Attack Risks; References; 4 THE QUALITIES OF WORKABLE SECURITY SOLUTIONS; Secure Coprocessors; Attack Vectors; Techniques for Creating Strong Coprocessors; Secure Bootstrap Loading; Protection of the Bootstrap Process; Secure Memory Management; Protection of Memory Management; Trusted Platform Module; TPM Attack Vectors; LaGrande (Trusted Execution Technology) Video ProtectionInput Devices; Memory Protection; Trusted Execution Technology Attack Vectors; Field-Programmable Gate Array; Hardware-Based Authentication; Person Authentication Using Biometrics; Fingerprint Scanners; Voiceprints; Iris Scans; Palm Prints; Radio-Frequency IDs; Hardware Based RNGs; Hardware Token Authenticators; References; 5 SECURE COPROCESSORS; The Need for Secure Coprocessors; Physical Security; Initialization; Usability Accessibility and Security; Support and Upgrades; Anticipatory Design; Authentication; References; 6 SECURE BOOTSTRAP LOADING
The Need for Secure Bootstrap LoadingImplementation; Hardware Firmware and Software; The Trusted Computing Base; Concluding Remarks; The Benefits of Secure Bootstrapping; References; 7 SECURE MEMORY MANAGEMENT AND TRUSTED EXECUTION TECHNOLOGY; The Need for Secure Memory Management; Buffer Overflows; Memory Pointer Attacks; The Impact of Memory-Management Attacks; Minimizing Memory-Management Attacks; Platform-Design Considerations; Trusted Execution Technology; Protected Execution; Protected Storage; Protected Input; Protected Graphics; Environment Authentication and Protected Launch
Domain Manager

Sommario/riassunto

Presents primary hardware-based computer security approaches in an easy-to-read toolbox format Protecting valuable personal information against theft is a mission-critical component of today's electronic business community. In an effort to combat this serious and growing problem, the Intelligence and Defense communities have successfully employed the use of hardware-based security devices. This book provides a road map of the hardware-based security devices that can defeat-and prevent-attacks by hackers. Beginning with an overview of the basic elements of computer security, the book covers