Computer and information security handbook [

Vacca, John R.

Morgan Kaufmann Publishers is an imprint of Elsevier, [2013]

Monografía

The second edition of this comprehensive handbook of computer and information security serves as a professional reference and practitioner's guide providing the most complete view computer security and privacy available. It offers in-depth coverage of security theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. The book is organized into ten parts comprised of 70 contributed chapters by leading experts in the areas of networking and systems security; information management; cyber warfare and security; encryption technology; privacy; data storage; physical security; and a host of advanced security topics. New to this edition are chapters on intrusion detection, securing the cloud, securing web apps, ethical hacking, cyber forensics, physical security, disaster recovery, cyber attack deterrence, and more. Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise. Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints.Analysis and problem-solving techniques enhance the reader's grasp of the material and ability to implement practical solutions

Título: Computer and information security handbook Recurso electrónico] edited by John R. Vacca

Edición: 2nd ed

Editorial: Amsterdam Morgan Kaufmann Publishers is an imprint of Elsevier [2013]

Descripción física: 1 recurso electrónico

Mención de serie: EBSCO Academic eBook Collection Complete

Bibliografía: Incluye referencias bibliográficas e índice

What is Cryptography? What is Encryption? -- 2.Famous Cryptographic Devices -- 3.Ciphers -- 4.Modern Cryptography -- 5.The Computer Age -- 6.How AES Works -- 7.Selecting Cryptography: the Process -- 8.Summary -- Chapter Review Questions/Exercises -- Exercise -- 3.Detecting System Intrusions / Almantas Kakareka -- 1. Introduction -- 2.Monitoring Key Files in the System -- 3.Security Objectives -- 4.Oday Attacks -- 5.Good Known State -- 6.Rootkits -- 7.Low Hanging Fruit -- 8.Antivirus Software -- 9.Homegrown Intrusion Detection -- 10.Full-Packet Capture Devices -- 11.Out-of-Band Attack Vectors -- 12.Security Awareness Training -- 13.Data Correlation -- 14.SIEM -- 15.Other Weird Stuff on the System -- 16.Detection -- 17.Network-Based Detection of System Intrusions (DSIs) -- 18.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 4. Preventing System Intrusions / Michael West -- 1.So, What is an Intrusion? -- 2.Sobering Numbers -- 3.Know Your Enemy: Hackers versus Crackers -- 4.Motives -- 5.The Crackers' Tools of the Trade -- 6.Bots -- 7.Symptoms of Intrusions -- 8.What Can You Do? -- 9.Security Policies -- 10.Risk Analysis -- 11.Tools of Your Trade -- 12. Controlling User Access -- 13.Intrusion Prevention Capabilities -- 14.Summary -- Chapter Review Questions /Exercises -- Exercise -- 5.Guarding Against Network Intrusions / Patrick J. Walsh -- 1.Traditional Reconnaissance and Attacks -- 2.Malicious Software -- 3.Defense in Depth -- 4.Preventive Measures -- 5.Intrusion Monitoring and Detection -- 6.Reactive Measures -- 7.Network-Based Intrusion Protection -- 8.Summary -- Chapter Review Questions/Exercises -- Exercise -- 6.Securing Cloud Computing Systems / Cem Gurkok -- 1.Cloud Computing Essentials: Examining the Cloud Layers -- 2.Software as a Service (SaaS): Managing Risks in the Cloud -- 3. Platform as a Service (PaaS): Securing the Platform -- 4.Infrastructure as a Service (laaS) -- 5.Leveraging Provider-Specific Security Options -- 6.Achieving Security in a Private Cloud -- 7.Meeting Compliance Requirements -- 8. Preparing for Disaster Recovery -- 9.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 7.Fault Tolerance and Resilience in Cloud Computing Environments / Vincenzo Piuri -- 1.Introduction -- 2.Cloud Computing Fault Model -- 3.Basic Concepts on Fault Tolerance -- 4.Different Levels of Fault Tolerance in Cloud Computing -- 5.Fault Tolerance against Crash Failures in Cloud Computing -- 6.Fault Tolerance against Byzantine Failures in Cloud Computing -- 7.Fault Tolerance as a Service in Cloud Computing -- 8.Summary -- Chapter Review Questions/Exercises -- Exercise -- Acknowledgments -- References -- 8.Securing Web Applications, Services, and Servers / Gerald Beuchelt -- 1.Setting the Stage -- 2.Basic Security for HTTP Applications and Services -- 3.Basic Security for SOAP Services -- 4.Identity Management and Web Services -- 5.Authorization Patterns -- 6.Security Considerations -- 7.Challenges -- 8.Summary -- Chapter Review Questions/Exercises -- Exercise -- 9.Unix and Linux Security / Gerald Beuchelt -- 1.Unix and Security -- 2.Basic Unix Security Overview -- 3.Achieving Unix Security -- 4.Protecting User Accounts and Strengthening Authentication -- 5.Limiting Superuser Privileges -- 6.Securing Local and Network File Systems -- 7.Network Configuration -- 8.Improving the Security of Linux and Unix Systems -- 9.Additional Resources -- 10.Summary -- Chapter Review Questions /Exercises -- Exercise -- 10.Eliminating the Security Weakness of Linux and Unix Operating Systems / Mario Santana -- 1.Introduction to Linux and Unix -- 2.Hardening Linux and Unix -- 3.Proactive Defense for Linux and Unix -- 4.Summary -- Chapter Review Questions/Exercises -- Exercise -- 11.Internet Security / Jesse Walker -- 1. Internet Protocol Architecture -- 2.An Internet Threat Model -- 3.Defending against Attacks on the internet -- 4. Internet Security Checklist -- 5.Summary -- Chapter Review Questions/Exercises -- Exercise -- 12.The Botnet Problem / Xinyuan Wang -- 1.Introduction -- 2.Botnet Overview -- 3.Typical Bot Life Cycle -- 4.The Botnet Business Model -- 5.Botnet Defense -- 6.Botmaster Traceback -- 7.Preventing Botnets -- 8.Summary -- Chapter Review Questions/Exercises -- Exercise -- 13.Intranet Security / Bill Mansoor -- 1.Smartphones and Tablets in the Intranet -- 2.Security Considerations -- 3.Plugging the Gaps: NAC and Access Control -- 4.Measuring Risk: Audits -- 5.Guardian at the Gate: Authentication and Encryption -- 6.Wireless Network Security -- 7.Shielding the Wire: Network Protection -- 8.Weakest Link in Security: User Training -- 9.Documenting the Network: Change Management -- 10.Rehearse the Inevitable: Disaster Recovery -- 11.Controlling Hazards: Physical and Environmental Protection -- 12.Know Your Users: Personnel Security -- 13.Protecting Data Flow: Information and System Integrity -- 14.Security Assessments -- 15.Risk Assessments -- 16.Intranet Security Implementation Process Checklist -- 17.Summary -- Chapter Review Questions/Exercises -- Exercise -- 14.Local Area Network Security / Dr. Pramod Pandya -- 1.Identify Network Threats -- 2.Establish Network Access Controls -- 3.Risk Assessment -- 4.Listing Network Resources -- 5.Threats -- 6.Security Policies -- 7.The Incident-Handling Process -- 8.Secure Design Through Network Access Controls -- 9.IDS Defined -- 10.NIDs: Scope and Limitations -- 11.A Practical Illustration of NIDS -- 12.Firewalls -- 13.Dynamic NAT Configuration -- 14.The Perimeter -- 15.Access List Details -- 16.Types of Firewalls -- 17.Packet Filtering: IP Filtering Routers -- 18.Application-Layer Firewalls: Proxy Servers -- 19.Stateful Inspection Firewalls -- 20.NIDs Complements Firewalls -- 21.Monitor and Analyze

System Activities -- 22.Signature Analysis -- 23.Statistical Analysis -- 24.Signature Algorithms -- 25.Local Area Network Security Countermeasures Implementation Checklist -- 26.Summary -- Chapter Review Questions /Exercises -- Exercise -- 15.Wireless Network Security / Hongbing Cheng -- 1.Cellular Networks -- 2.Wireless Ad hoc Networks -- 3.Security Protocols -- 4.WEP -- 5.Secure Routing -- 6.ARAN -- 7.SLSP -- 8.Key Establishment -- 9.ING -- 10.Management Countermeasures -- 11.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 16.Wireless Sensor Network Security / Thomas M. Chen -- 1.Introduction to the Wireless Sensor Network (WSN) -- 2.Threats to Privacy -- 3.Security Measures for WSN -- 4.Secure Routing in WSN -- 5.Routing Classifications in WSN -- 6.WSN Security Framework and Standards -- 7.Summary -- Chapter Review Questions /Exercises -- Exercise -- References -- 17.Cellular Network Security / Kameswari Kotapati -- 1.Introduction -- 2. Overview of Cellular Networks -- 3.The State of the Art of Cellular Network Security -- 4.Cellular Network Attack Taxonomy -- 5.Cellular Network Vulnerability Analysis -- 6.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 18.RFID Security / Hongbing Cheng -- 1.RFID Introduction -- 2.RFID Challenges -- 3. RFID Protections -- 4.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 19.Optical Network Security / Lauren Collins -- 1.Optical Networks -- 2.Securing Optical Networks -- 3.Identifying Vulnerabilities -- 4.Corrective Actions -- 5.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 20.Optical Wireless Security / Scott R. Ellis -- 1.Optical Wireless Systems Overview -- 2. Deployment Architectures -- 3.High Bandwidth -- 4.Low Cost -- 5.Implementation -- 6.Surface Area -- 7.Summary -- Chapter Review Questions/Exercises -- Exercise -- pt. II Managing Information Security -- 21.Information Security Essentials for IT Managers: Protecting Mission-Critical Systems / Albert Caballero -- 1.Information Security Essentials for IT Managers, Overview -- 2.Protecting Mission-Critical Systems -- 3.Information Security from the Ground Up -- 4.Security Monitoring and Effectiveness -- 5.Summary -- Chapter Review Questions /Exercises -- Exercise -- 22.Security Management Systems / James T. Harmening -- 1.Security Management System Standards -- 2.Training Requirements -- 3.Principles of Information Security -- 4.Roles and Responsibilities of Personnel -- 5.Security Policies -- 6.Security Controls -- 7.Network Access -- 8.Risk Assessment -- 9.Incident Response -- 10.Summary -- Chapter Review Questions/Exercises -- Exercise -- 23.Policy-driven System Management / Stefano Paraboschi -- 1.Introduction -- 2.Security and Policy-based Management -- 3. Classification and Languages -- 4.Controls for Enforcing Security Policies in Distributed Systems -- 5.Products and Technologies -- 6.Research Projects -- 7.Summary -- Chapter Review Questions/Exercises -- Exercise -- Acknowledgments -- References -- 24.Information Technology Security Management / Bhushan Kapoor -- 1. Information Security Management Standards -- 2.Other Organizations Involved in Standards -- 3.Information Technology Security Aspects -- 4.Summary -- Chapter Review Questions/Exercises -- Exercise -- 25.Online Identity and User Management Services / Jean-Marc Seigneur -- 1.Introduction -- 2.Evolution of Identity Management Requirements -- 3.The Requirements Fulfilled by Identity Management Technologies -- 4.Identity Management 1.0 -- 5.Social Login and User Management -- 6.Identity 2.0 for Mobile Users -- 7.Summary -- Note continued: Chapter Review Questions/Exercises -- Exercise -- pt. VII Physical Security -- 54.Physical Security Essentials / William Stallings -- 1.Overview -- 2.Physical Security Threats -- 3.Physical Security Prevention and Mitigation Measures -- 4.Recovery from Physical Security Breaches -- 5.Threat Assessment, Planning, and Plan Implementation -- 6.Example: A Corporate Physical Security Policy -- 7.Integration of Physical and Logical Security -- 8.Physical Security Checklist -- 9.Summary -- Chapter Review Questions/Exercises -- Exercise -- 55. Disaster Recovery / Lauren Collins -- 1.Introduction -- 2.Measuring Risk and Avoiding Disaster -- 3.The Business Impact Assessment (BIA) -- 4.Summary -- Chapter Review Questions/Exercises -- Exercise -- 56.Biometrics / Luther Martin -- 1.Relevant Standards -- 2.Biometric System Architecture -- 3.Using Biometric Systems -- 4. Security Considerations -- 5.Summary -- Chapter Review Questions/Exercises -- Exercise -- 57.Homeland Security (online chapter) / Bhushan Kapoor -- 58.Cyber Warfare / Marco Slaviero -- 1.Cyber Warfare Model -- 2.Cyber Warfare Defined -- 3.CW: Myth or Reality? -- 4.Cyber Warfare: Making CW Possible -- 5.Legal Aspects of CW -- 6.Holistic View of Cyber Warfare -- 7.Summary -- Chapter Review Questions/Exercises -- Exercise -- pt. VIII Practical Security -- 59.System Security / Lauren Collins -- 1.Foundations of Security -- 2.Basic Countermeasures -- 3.Summary -- Chapter Review Questions/Exercises -- Exercise -- 60.Securing the Infrastructure / Lauren Collins -- 1.Communication Security Goals -- 2.Attacks and Countermeasures -- 3.Summary -- Chapter Review Questions /Exercises -- Exercise -- 61.Access Controls / Lauren Collins -- 1.Infrastructure Weaknesses: DAC, MAC, and RBAC -- 2.Strengthening the Infrastructure: Authentication Systems -- 3.Summary -- Chapter Review Questions /Exercises -- Exercise -- 62.Assessments and Audits / Lauren Collins -- 1.Assessing Vulnerabilities and Risk: Penetration Testing and Vulnerability Assessments -- 2.Risk Management: Quantitative Risk Measurements -- 3.

Summary -- Chapter Review Questions/Exercises -- Exercise -- 63.Fundamentals of Cryptography / Scott R. Ellis -- 1.Assuring Privacy with Encryption -- 2.Summary -- Chapter Review Questions/Exercises -- Exercise -- pt. IX Advanced Security -- 64.Security Through Diversity / Kevin Noble -- 1.Ubiquity -- 2.Example Attacks Against Uniformity -- 3.Attacking Ubiquity with Antivirus Tools -- 4.The Threat of Worms -- 5.Automated Network Defense -- 6.Diversity and the Browser -- 7.Sandboxing and Virtualization -- 8.DNS Example of Diversity Through Security -- 9.Recovery from Disaster is Survival -- 10.Summary -- Chapter Review Questions/Exercises -- Exercise -- 65.Online e-Reputation Management Services / Jean-Marc Seigneur -- 1.Introduction -- 2.The Human Notion of Reputation -- 3.Reputation Applied to the Computing World -- 4.State of the Art of Attack-Resistant Reputation Computation -- 5.Overview of Current Online Reputation Service -- 6.Summary -- Chapter Review Questions /Exercises -- Exercise -- Bibliography -- 66.Content Filtering (online chapter) / Pete Nicoletti -- 67.Data Loss Protection / Ken Perkins -- 1.Precursors of DLP -- 2.What is DLP? -- 3.Where to Begin? -- 4.Data is Like Water -- 5.You Don't Know What You Don't Know -- 6.How Do DLP Applications Work? -- 7.Eat Your Vegetables -- 8. IT's a Family Affair, Not Just IT Security's Problem -- 9.Vendors, Vendors Everywhere! Who do you Believe? -- 10.Summary -- Chapter Review Questions/Exercises -- Exercise -- 68.Satellite Cyber Attack Search and Destroy / Jeffrey Bardin -- 1.Hacks, Interference, and Jamming -- 2.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 69.Verifiable Voting Systems / Zhe Xia -- 1.Introduction -- 2.Security Requirements -- 3. Verifiable Voting Schemes -- 4.Building Blocks -- 5.Survey of Noteworthy Schemes -- 6.Threats to Verifiable Voting Systems -- 7.Summary -- Chapter Review Questions/Exercises -- Exercise -- References -- 70.Advanced Data Encryption / Pramod Pandya -- 1.Mathematical Concepts Reviewed -- 2.The RSA Cryptosystem -- 3. Summary -- Chapter Review Questions/Exercises -- Exercise -- References

Detalles del sistema: Forma de acceso: World Wide Web

ISBN: 9780123946126 0123946123 9780123943972 0123943973 9781784023447 1784023442

Autores: Vacca, John R.

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es