

1. Record Nr.	UNINA9910791090303321
Titolo	Cyber security // edited by John G. Voeller
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, , 2014 ©2014
ISBN	1-118-65168-5 1-118-65173-1
Descrizione fisica	1 online resource (126 p.)
Altri autori (Persone)	VoellerJohn G
Disciplina	005.8
Soggetti	Computer networks - Security measures Cyberspace - Security measures
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	Cover; Title Page; Contents; Preface; Chapter 1 Cyber Security Metrics and Measure; 1.1 Introduction; 1.2 Contrasting Metrics and Measures; 1.3 Selecting Measures to Support Metrics; 1.4 Problems with the Accuracy of Measures; 1.5 Problems with the Selection of Measures; 1.6 Problems with the Use of Measures; 1.7 Common Vulnerability Scoring System (CVSS); 1.8 Research Directions; References; Further Reading; Chapter 2 Multilevel Security; 2.1 Introduction; 2.2 Background; 2.3 Multilevel Security Policies; 2.3.1 Confinement; 2.3.2 Supporting Policies; 2.3.3 Trusted Subjects 2.4 Enforcement of Multilevel Security Policies2.4.1 Design Approaches; 2.4.2 Threats to MLS Systems; 2.4.3 Assurance; 2.4.4 Secure MLS System Development; 2.4.5 Covert Channels; 2.4.6 Object Reuse Considerations; 2.4.7 Target Environment; 2.4.8 Cascade Problem; 2.5 Platforms and Architectures for Multilevel Security; 2.5.1 Use of Applications in MLS Systems; 2.6 Conclusion; References; Chapter 3 Trusted Platforms: The Root of Security; 3.1 Introduction; 3.2 The State of Trusted Computing; 3.2.1 Why Hardware Security?; 3.2.2 Essentials of Trusted Computing; 3.2.3 Extension to Storage 3.2.4 Biometric Devices as Physical Interface3.2.5 Usage Model; 3.3 International Scope; 3.3.1 Integration; 3.3.2 Trusted Software; 3.3.3 Networking Trusted Platforms; 3.4 Expanding the Ring of Trust; 3.5

Remaining Challenges; References; Further Reading; Chapter 4 Cyber Security Technology Usability and Management; 4.1 Introduction; 4.2 Usability and Security: Current Research; 4.2.1 Improving Existing Security Technologies; 4.3 Systems Management; 4.4 Web Security and Phishing; 4.4.1 Designing New Technologies with Usability in Mind; 4.4.2 Design Guidelines for Building Better Systems
4.5 Open Challenges and Take-Aways
4.6 Conclusions; References; Further Reading; Chapter 5 Security of Distributed, Ubiquitous, and Embedded Computing Platforms; 5.1 Introduction; 5.2 Scientific Overview; 5.2.1 Security Properties; 5.2.2 Constraints on the Design Space; 5.2.3 Solution Approaches; 5.2.4 Physical Layer; 5.2.5 Networking Layers; 5.2.6 Middleware and Applications; 5.3 Global Research and Funding; 5.4 Critical Needs Analysis; 5.5 Research Directions; References; Further Reading; Chapter 6 Advanced Attacker Detection and Understanding with Emerging HoneyNet Technologies
6.1 HoneyNet Essentials
6.2 HoneyNet Risk; Legal and Ethical Issues;
6.3 HoneyNet Technologies; 6.3.1 Generation III HoneyNet; 6.3.2 Global Distributed HoneyNet (GDH); 6.3.3 HoneyClients; 6.3.4 Low-Interaction Malware Collectors; References; Chapter 7 Security of Web Application and Services and Service-Oriented Architectures; 7.1 Introduction; 7.2 SOA Security Challenges; 7.3 Secure Web Services for SOA; 7.3.1 Transport-Based Security; 7.3.2 Message-Based Security; 7.4 Web Service Security Directions; 7.4.1 Federation; 7.4.2 Identity; 7.5 Summary; References
Chapter 8 Industrial Process Control System Security

Sommario/riassunto

Cyber Security features articles from the Wiley Handbook of Science and Technology for Homeland Security covering topics related to cyber security metrics and measure and related technologies that meet security needs. Specific applications to web services, the banking and the finance sector, and industrial process control systems are discussed.
