1. Record Nr. UNISA996464504203316

Titolo	Advances in cybersecurity management / / edited by Kevin Daimi and Cathryn Peoples
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-71381-4
Descrizione fisica	1 online resource (494 pages)
Disciplina	005.8
Soggetti	Technical education Computer security - Management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Acknowledgments -- Contents -- About the Editors -- Part I Network and Systems Security Management -- 1 Agent-Based Modeling of Entity Behavior in Cybersecurity -- 1.1 Introduction -- 1.2 Background -- 1.2.1 Modeling of Human Behavior -- 1.2.2 Modeling of System Behavior -- 1.2.3 Agent-Based Modeling (ABM) -- 1.3 Modeling and Simulation -- 1.3.1 Implementation -- 1.3.2 Simulation Results -- 1.3.2.1 Adversary Attack Sophistication -- 1.3.2.2 Trust Level -- 1.3.2.3 Quality or Level of Training -- 1.3.2.4 Quality of Cyber Defense -- 1.3.2.5 Comparison of Slow Growth Rates -- 1.3.2.6 Comparison of Fast Growth Rates -- 1.4 Cybersecurity Management Implications -- 1.5 Limitations of the Study -- 1.6 Conclusions and Future Directions -- References -- 2 A Secure Bio-Hash-Based Multiparty Mutual Authentication Protocol for Remote Health MonitoringApplications -- 2.1 Introduction -- 2.2 Related Work -- 2.3 The Proposed Scheme for Remote Health Monitoring Applications -- 2.3.1 Registration Phase of User -- 2.3.2 Login Phase of User -- 2.3.3 Authentication and Key Agreement Phase of User and MGW -- 2.3.4 Password Change Phase of User -- 2.3.5 System Set Up Phase of Medical Gateway -- 2.3.6 Registration Phase of Sensor with Medical Gateway -- 2.3.7 Registration Phase of Personal Device with Medical Gateway -- 2.3.8 Mutual Authentication Phase of Sensor, Personal Device and Medical Gateway -- 2.4 Security Analysis of Proposed Protocols -- 2.5 Formal

Analysis Using Scyther Tool -- 2.6 Scyther Results and Interpretation -- 2.7 Conclusion -- References -- 3 Cybersecurity Attacks During COVID-19: An Analysis of the Behavior of the Human Factors and a Proposal of Hardening Strategies -- 3.1 Introduction -- 3.2 Cybersecurity Attacks During COVID-19 -- 3.3 Analyzing Human Vulnerabilities for Fake News Using the Diamond Model -- 3.3.1 Adversary.
3.3.2 Capability -- 3.3.3 Infrastructure -- 3.3.4 Victim -- 3.4 Strategies Against Fake News During COVID-19 -- 3.5 Conclusions and Future Work -- References -- 4 Vehicle Network Security Metrics -- 4.1 Introduction -- 4.2 Vehicle Communication -- 4.2.1 Intra-vehicle Communication Protocols -- 4.2.2 Intervehicle Communication Protocols -- 4.3 Automotive Vehicle Network Security -- 4.3.1 Automotive Vehicle Threats and Vulnerabilities -- 4.3.2 Automotive Vehicle Security Attacks -- 4.3.3 Automotive Vehicle Attack Surfaces -- 4.4 Industry and Government Initiatives and Standards -- 4.5 Automotive Vehicle Security Metrics -- 4.5.1 Common Vulnerability Scoring System (CVSS) -- 4.5.2 Common Methodology for IT Security Evaluation (CEM) [49] -- 4.5.3 Security Metrics Visualization -- 4.6 Conclusion and Future Research Directions -- References -- 5 VizAttack: An Extensible Open-Source Visualization Framework for Cyberattacks -- 5.1 Introduction -- 5.2 Cyberattack Visualization Approaches -- 5.2.1 Cyberattack Maps and Graphs -- 5.2.2 Honeypot Data Visualization -- 5.2.3 Attack Visualization Challenges -- 5.3 VizAttack Design Principles -- 5.3.1 Design Objectives -- 5.3.2 High-Level Architectural Design -- 5.3.2.1 User Interface: Temporal Analysis -- 5.3.2.2 User Interface: Predefined Queries -- 5.3.2.3 User Interface: Customized Queries -- 5.3.2.4 User Interface: Profiling Attacks -- 5.4 VizAttack Implementation Details -- 5.4.1 VizAttack Prototype -- 5.4.2 Experimental Findings -- 5.4.3 Attack Postmortem Investigation -- 5.5 Conclusion -- References -- 6 Geographically Dispersed Supply Chains: A Strategy to Manage Cybersecurity in Industrial Networks Integration -- 6.1 Introduction -- 6.2 Challenges of Geographically-Dispersed Supply Chains -- 6.3 Critical Infrastructures -- 6.4 Vulnerabilities in Operational Technology Networks.
6.5 International Cybersecurity Regulations and Standards -- 6.6 Proposed Cybersecurity Strategy for Industrial Networks -- 6.6.1 Perimeter and Security Controls Strategies -- 6.6.1.1 Electronic Security Perimeter -- 6.6.1.2 Data Flow in Segmented Networks -- 6.6.1.3 Network and Perimeter Monitoring -- 6.6.1.4 Network Access and Authentication -- 6.6.1.5 Network Perimeter Ports and Services -- 6.6.2 Host Security Controls Strategies -- 6.6.2.1 Asset Configuration -- 6.6.2.2 Ports and Services -- 6.6.2.3 Anti-Malware -- 6.6.2.4 Authentication -- 6.6.3 Security Monitoring Controls -- 6.6.3.1 Asset Configuration and Documentation -- 6.6.3.2 Monitoring -- 6.6.3.3 Authentication -- 6.7 Discussion -- 6.8 Final Considerations -- References -- 7 The Impact of Blockchain on Cybersecurity Management -- 7.1 Introduction -- 7.2 Anonymity and Privacy -- 7.3 Reputation Management -- 7.4 Identification and Integrity -- 7.5 Availability -- 7.6 Trust Management -- 7.7 Software Development Security -- 7.8 Conclusion -- References -- 8 A Framework for Enterprise Cybersecurity Risk Management -- 8.1 Introduction -- 8.1.1 Contributions of Our Chapter -- 8.1.2 Motivation for Business IT Alignment (BITA) -- 8.2 The Evolution of Cybersecurity RM -- 8.2.1 IT-Centric Approach -- 8.2.2 IS-Centric Approach -- 8.2.3 ERM-Centric Approach -- 8.2.4 Motivation for a New Approach -- 8.3 Evaluation of Existing Frameworks -- 8.3.1 NIST Framework -- 8.3.2 COSO Framework -- 8.3.3 COBIT Framework -- 8.3.4 ISO/IEC 31000

Framework -- 8.4 The Importance of BITA in Cybersecurity RM -- 8.4.1 BITA Capabilities -- 8.5 The CHARM Framework Development -- 8.5.1 The CHARM Framework -- 8.5.2 A Case Study Application of the CHARM Framework -- 8.6 Conclusions -- References -- 9 Biometrics for Enterprise Security Risk Mitigation -- 9.1 Introduction -- 9.2 Overview -- 9.2.1 Biometrics.
9.2.2 The Process of Biometric Authentication and Accuracy Measures -- 9.2.3 Types of Biometrics -- 9.2.3.1 Fingerprints -- 9.2.3.2 Face Recognition -- 9.2.3.3 Iris Recognition -- 9.2.3.4 Other Biometrics -- 9.3 Related Works -- 9.3.1 Biometrics in Business Applications -- 9.3.1.1 Biometrics in Education -- 9.3.1.2 Biometrics for Mobile Device Security -- 9.3.1.3 Biometrics for the Healthcare Sector -- 9.3.1.4 Biometrics for the Financial Sector -- 9.3.2 Our Contribution -- 9.4 Biometrics in Enterprise Cybersecurity Risk Management -- 9.4.1 Biometrics in Multifactor Authentication Systems -- 9.5 The Technical, Financial, and Legal Challenges of Biometrics -- 9.5.1 Technical Challenges -- 9.5.1.1 Storage of Biometric Templates -- 9.5.1.2 Security Threats to a Biometric System -- 9.5.2 Legal Challenges -- 9.5.3 Financial and Usability Challenges -- 9.6 Case Studies of Enterprise Risk Mitigation via Biometrics During the COVID-19 Pandemic -- 9.6.1 The Impact of COVID-19 on Information Technology (IT) -- 9.6.1.1 Health Care -- 9.6.1.2 Academic -- 9.6.1.3 Financial -- 9.6.2 COVID-19 Impact on Information Security (IT) -- 9.6.3 Improving Security via Biometric Authentication -- 9.7 Conclusion -- 9.7.1 Future Research Opportunities -- References -- Part II Vulnerability Management -- 10 SQL Injection Attacks and Mitigation Strategies: The Latest Comprehension -- 10.1 Introduction -- 10.2 Background -- 10.2.1 Web Application Security -- 10.2.1.1 Understanding SQL Injection Attack -- 10.2.1.2 Logical Understanding of SQL Injection Attack -- 10.3 SQL Injection Attack Classification -- 10.3.1 In-Band SQL Injection Attacks -- 10.3.1.1 Union-Based SQL Injection Attack -- 10.3.1.2 Error-Based SQL Injection Attack -- 10.3.2 Inferential SQL Injection Attacks -- 10.3.2.1 Blind Boolean-Based SQL Injection Attack -- 10.3.2.2 Blind Time-Based SQL Injection Attack.
10.3.3 Out-of-Band SQL Injection Attacks -- 10.3.4 Modern SQL Injection Attacks -- 10.4 SQL Injection Mitigation Strategies -- 10.4.1 OWASP [1] Suggested Mitigation Strategies -- 10.4.1.1 Principle of Least Privilege for Web-Application Access -- 10.4.1.2 Prepared Statements with Parameterized Queries -- 10.4.1.3 Stored Procedures -- 10.4.1.4 Query Whitelisting -- 10.4.1.5 Escaping All User-Supplied Input -- 10.4.2 SQL Injection Attack Mitigation Strategies: Research Outcomes -- 10.5 Conclusions -- References -- 11 Managing Cybersecurity Events Using Service-Level Agreements (SLAs) by Profiling the People Who Attack -- 11.1 Introduction -- 11.2 Prior Arts -- 11.2.1 Profiling Attackers from a Personal Perspective for SLA Provisioning and Network Management Objectives -- 11.3 Research Proposal -- 11.3.1 SLA Service Request -- 11.3.2 SLA Management -- 11.3.3 SLA and Data Management Interventions -- 11.4 Conclusions and Further Work -- References -- 12 Recent Techniques Supporting Vulnerabilities Management for Secure Online Apps -- 12.1 Introduction -- 12.2 SQL Injection -- 12.2.1 Introduction -- 12.2.2 Exploitation Techniques -- 12.2.2.1 In-Band SQL Injection -- 12.2.2.2 Inferential SQL Injection -- 12.2.2.3 Out-of-Band SQL Injection -- 12.2.3 Causes of Vulnerability -- 12.2.4 Protection Techniques -- 12.2.4.1 Input Validation -- 12.2.4.2 Data Sanitization -- 12.2.4.3 Use of Prepared Statements -- 12.2.4.4 Limitation of Database Permission -- 12.2.4.5 Using Encryption -- 12.3 Cross-Site Scripting -- 12.3.1 Introduction -- 12.3.2 Exploitation Techniques -- 12.3.2.1 Reflected

Cross-Site Scripting -- 12.3.2.2 Stored Cross-Site Scripting -- 12.3.2.3 DOM-Based Cross-Site Scripting -- 12.3.3 Causes of Vulnerability -- 12.3.4 Protection Techniques -- 12.3.4.1 Data Validation -- 12.3.4.2 Data Sanitization -- 12.3.4.3 Escaping on Output.
12.3.4.4 Use of Content Security Policy.