1. Record Nr. UNINA9910376287303321

Titolo	Proceedings of the 1st ACM SIGSPATIAL Workshop on Prediction of Human Mobility / / Association for Computing Machinery-Digital Library
Pubbl/distr/stampa	New York, NY : , : ACM, , 2017
Descrizione fisica	1 online resource (51 pages) : illustrations
Collana	ACM Conferences
Disciplina	910.285
Soggetti	Geospatial data
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNIORUON00021820

Titolo	National atlas of the Democratic Republic of Afghanistan
Pubbl/distr/stampa	Kabul, : Geokart, 1984
ISBN	83-00-02327-5
Descrizione fisica	xiv, 36 piante ; 36 cm
Classificazione	ATL V
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

3. Record Nr. UNINA9911019501303321

Autore	Shrivastava Gulshan
Titolo	Emerging Threats and Countermeasures in Cybersecurity
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2024 ©2025
ISBN	9781394230587 1394230583 9781394230600 1394230605 9781394230594 1394230591
Edizione	[1st ed.]
Descrizione fisica	1 online resource (533 pages)
Collana	Advances in Antenna, Microwave, and Communication Engineering Series
Altri autori (Persone)	OjhaRudra Pratap AwasthiShashank SharmaKavita BansalHimani
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Series Page -- Title Page -- Copyright Page -- Contents -- Preface -- Chapter 1 Emerging Threats and Trends in Digital Forensics and Cybersecurity -- 1.1 Introduction -- 1.2 Threats Faced by Digital Forensics -- 1.2.1 Technical Challenges -- 1.2.2 Operational Challenges -- 1.2.3 Personnel-Related Challenges -- 1.3 Cybersecurity Threats in 2023 -- 1.3.1 Social Engineering -- 1.3.2 Third-Party Exposure -- 1.3.3 Configuration Mistakes -- 1.3.4 Poor Cyber Hygiene -- 1.3.5 Cloud Vulnerabilities -- 1.3.6 Mobile Device Vulnerabilities -- 1.3.7 Internet of Things (IoT) -- 1.3.8 Ransomware -- 1.3.9 Poor Data Management -- 1.3.10 Inadequate Post-Attack Procedures -- 1.4 New Era of Technology and Their Risks -- 1.4.1 Autonomous Vehicles -- 1.4.2 Artificial Intelligence -- 1.4.3 Robotics and Robotics Process Automation -- 1.4.4 Internet of Things (IoT) -- 1.4.5 5G -- 1.5

Challenges for Digital Forensics -- 1.5.1 High Speed and Volumes -- 1.5.2 Explosion Complexity -- 1.5.3 Development of Standards -- 1.5.4 Privacy-Preserving Investigations -- 1.5.5 Legitimacy -- 1.5.6 Rise of Anti-Forensic Techniques -- 1.6 Impact of Mobile Gadgets on Cybersecurity -- 1.7 The Vulnerabilities in Wireless Mobile Data Exchange -- 1.7.1 Interception of Data -- 1.7.2 Malware Attacks -- 1.7.3 Rogue Access Points -- 1.7.4 Denial of Service Attacks -- 1.7.5 Weak Encryption -- 1.8 Network Segmentation and its Applications -- 1.8.1 Applications -- 1.8.2 Benefits of Network Segmentation -- 1.9 Relationship Between Privacy and Security -- 1.9.1 Security -- 1.9.2 Privacy -- 1.10 Recent Trends in Digital Forensics -- 1.10.1 Cloud Forensics -- 1.10.2 Social Media Forensics -- 1.10.3 IoT Forensics -- 1.11 Opportunities in this Field -- 1.11.1 USB Forensics -- 1.11.2 Intrusion Detection -- 1.11.3 Artificial Intelligence (AI) -- 1.12 Future Enhancements in Digital Forensics.
1.13 Cybersecurity and Cyber Forensics in Smart Cities -- 1.13.1 Smart Cities are Entitled to Cyber-Physical Systems -- 1.13.1.1 Administrative -- 1.13.1.2 Complex CPS in a Glimpse -- 1.13.1.3 IoT Technologies in Smart Cities of the Future -- 1.14 Network Security and Forensics -- 1.15 Software and Social Engineering Attacks on RSA -- 1.16 Cyber Threats and Cybersecurity -- 1.17 Conclusion -- Bibliography -- Chapter 2 Toward Reliable Image Forensics: Deep Learning-Based Forgery Detection -- 2.1 Introduction -- 2.2 Fundamentals of Image Forensics -- 2.2.1 History -- 2.2.2 Image Forgery Types -- 2.2.3 Classical Image Forensics Techniques -- 2.3 Deep Learning in Image Forensics -- 2.3.1 Convolutional Neural Networks (CNNs) -- 2.3.2 Generative Adversarial Networks (GANs) -- 2.4 Datasets of Image Forgery Detection -- 2.5 Feature Extraction and Representation -- 2.6 Model Training and Evaluation -- 2.6.1 Model Training -- 2.6.2 Loss Functions -- 2.6.3 Evaluation Metrics -- 2.7 Challenges and Future Scope -- 2.8 Conclusion -- References -- Chapter 3 Understanding and Mitigating Advanced Persistent Threats in a Dynamic Cyber Landscape -- 3.1 Introduction -- 3.1.1 Advanced -- 3.1.2 Persistent -- 3.1.3 Threat -- 3.1.3.1 Vulnerability -- 3.1.3.2 Risk -- 3.2 APT Lifecycle -- 3.3 Characteristics and Methods of APTs -- 3.4 APT Detection -- 3.5 Mitigation Techniques -- 3.5.1 Application Control/Dynamic Whitelisting -- 3.5.2 Vulnerability Assessment -- 3.5.3 Patch Management -- 3.5.4 Automated Exploit Prevention -- 3.6 Case Study: CozyDuke APT -- Conclusion -- References -- Chapter 4 Class-Imbalanced Problems in Malware Analysis and Detection in Classification Algorithms -- 4.1 Introduction -- 4.2 Background -- 4.2.1 Malware Analysis and Types -- 4.2.2 Class-Imbalanced Problem -- 4.2.3 Imbalanced Techniques -- 4.3 Related Work.
4.4 Detailed Overview of the Methodology -- 4.4.1 Dataset Information -- 4.4.2 Different Evaluation Metrics Used for Class-Imbalanced Study -- 4.4.3 Machine Learning Classifiers -- 4.4.4 Exiting Methods Used for Handling the Class Imbalanced -- 4.5 Discussion and Challenges -- 4.5.1 Research Question -- 4.5.2 Challenges -- 4.6 Conclusion -- References -- Chapter 5 Malware Analysis and Detection: New Approaches and Techniques -- 5.1 Introduction -- 5.2 Malware -- 5.2.1 History of Malware -- 5.2.2 Different Forms of Malware -- 5.2.3 Purpose of Malware Analysis -- 5.3 Case Studies -- 5.4 Future Aspects -- 5.5 Conclusion -- References -- Chapter 6 State-of-the-Art in Ransomware Analysis and Detection -- 6.1 Introduction -- Evolution -- Lifecycle -- Infection Method -- Targets of Ransomware Attacks -- Payment Process and Method -- Ransomware Analysis -- Ransomware Detection -- Ransomware Prevention -- Recovery -- Characteristics -- Difficulties -- Impact of Ransomware Attacks -- Statistics --

Conclusion -- References -- Chapter 7 Cyber-Physical System Security: Challenges and Countermeasures -- 7.1 Introduction -- 7.1.1 Definition and Characteristics of CPS -- 7.1.2 Importance and Applications of CPS -- 7.1.3 Overview of CPS Security Concerns -- 7.2 Challenges in CPS Security -- 7.2.1 Threat Landscape in CPS -- 7.2.2 Vulnerabilities in CPS -- 7.2.2.1 Interconnected System Vulnerabilities -- 7.2.2.2 Lack of Standardized Security Frameworks -- 7.2.2.3 Legacy System Compatibility Issues -- 7.2.2.4 Human Factors and Social Engineering -- 7.3 Security Risks and Consequences -- 7.3.1 Financial Losses and Economic Impact -- 7.3.2 Public Safety and Critical Infrastructure Risks -- 7.3.3 Privacy and Data Breaches -- 7.4 Key Considerations for CPS Security -- 7.4.1 Secure Design and Architecture Principles -- 7.4.1.1 Defense-in-Depth Strategy. 7.4.1.2 Secure Communication Protocols -- 7.4.1.3 Access Control and Authentication Mechanisms -- 7.4.2 Threat Modeling and Risk Assessment -- 7.4.3 Intrusion Detection and Prevention Systems (IDPS) -- 7.4.4 Secure Software Development Practices -- 7.4.4.1 Secure Coding Guidelines -- 7.4.4.2 Code Reviews and Vulnerability Testing -- 7.5 Countermeasures for CPS Security -- 7.5.1 Network Security Measures -- 7.5.1.1 Firewalls and Network Segmentation -- 7.5.1.2 IDPS -- 7.5.2 Physical Security Controls -- 7.5.2.1 Access Controls and Physical Barriers -- 7.5.2.2 Surveillance and Monitoring Systems -- 7.5.3 Incident Response and Recovery Plans -- 7.5.3.1 Incident Handling Procedures -- 7.5.3.2 Backup and Disaster Recovery Strategies -- 7.5.4 Security Awareness and Training Programs -- 7.6 Case Studies and Examples -- 7.6.1 Case Study 1: Industrial Control System (ICS) Security -- 7.6.1.1 Countermeasures -- 7.6.2 Case Study 2: Smart Cities and Infrastructure Protection -- 7.6.2.1 Countermeasures -- 7.6.3 Case Study 3: Autonomous Vehicles and Transportation Systems -- 7.6.3.1 Countermeasures -- 7.7 Future Directions and Emerging Technologies -- 7.7.1 Impact of Emerging Technologies on CPS Security -- 7.7.2 Challenges and Opportunities in Securing CPS in the Future -- 7.8 Conclusion -- References -- Chapter 8 Unraveling the Ethical Conundrum: Privacy Challenges in the Realm of Digital Forensics -- 8.1 Introduction -- 8.2 Fundamental Concepts in Digital Forensics -- 8.3 Privacy Concerns in AI Technology: Security Systems and Cyber Forensics -- 8.4 Maintaining Integrity of Evidence in Forensic Investigations -- 8.5 Ethical Obligations of Forensic Investigators -- 8.6 Conclusion -- References -- Chapter 9 IoT and Smart Device Security: Emerging Threats and Countermeasures -- 9.1 Introduction -- 9.2 The Growth of IoT and Smart Devices. 9.3 Emerging Threat Landscape -- 9.4 Device Vulnerabilities and Exploits -- 9.5 Data Privacy and Leakage -- 9.5.1 Data Privacy Concerns in IoT -- 9.5.2 Data Leakage Concerns in IoT -- 9.6 Network Attacks and Amplification -- 9.6.1 Network Attacks in IoT -- 9.6.2 Amplification Attacks in IoT -- 9.6.3 Preventive Measures and Mitigation -- 9.7 Physical Attacks on Smart Devices -- 9.8 Supply Chain Risks in IoT Ecosystem -- 9.9 Lack of Standardization in IoT Security -- 9.10 Countermeasures and Best Practices -- 9.11 Conclusion and Future Directions -- 9.11.1 Future Directions and Countermeasures -- References -- Chapter 10 Advanced Security for IoT and Smart Devices: Addressing Modern Threats and Solutions -- 10.1 Introduction -- 10.1.1 Overview of IoT and Smart Devices -- 10.1.2 Importance of Security in IoT and Smart Devices -- 10.1.3 Scope of the Chapter -- 10.2 IoT and Smart Device Landscape -- 10.2.1 Growth and Adoption of IoT and Smart Devices -- 10.2.2 Types and Examples of IoT and Smart Devices -- 10.2.3 Challenges in Securing IoT and Smart Devices -- 10.3 Emerging Threats in IoT and Smart

Device Security -- 10.3.1 Malware and Ransomware Attacks -- 10.3.2 Device Exploitation and Hijacking -- 10.3.3 Data Breaches and Privacy Concerns -- 10.3.4 Distributed Denial of Service (DDoS) Attacks -- 10.3.5 Supply Chain Attacks -- 10.3.6 Insider Threats -- 10.3.7 Physical Security Risks -- 10.4 Vulnerabilities in IoT and Smart Devices -- 10.4.1 Insecure Communication Protocols -- 10.4.2 Weak Authentication and Authorization -- 10.4.3 Lack of Security Updates and Patch Management -- 10.4.4 Default or Hardcoded Credentials -- 10.4.5 Lack of Device Integrity Verification -- 10.4.6 Insufficient Encryption -- 10.4.7 Inadequate Access Controls -- 10.5 Countermeasures and Best Practices -- 10.5.1 Secure Device Design and Development.
10.5.2 Robust Authentication and Access Controls.

Sommario/riassunto

This book is an essential resource for anyone seeking to stay ahead in the dynamic field of cybersecurity, providing a comprehensive toolkit for understanding and combating digital threats and offering practical, insightful guidance ideal for cybersecurity professionals, digital forensic investigators, legal practitioners, law enforcement, scholars, and students. In the rapidly evolving domain of digital security, this book emerges as a vital guide for understanding and addressing the sophisticated landscape of cyber threats. This in-depth volume, featuring contributions from renowned experts, provides a thorough examination of the current state and future challenges in digital security and forensic analysis. The book is meticulously organized into seven sections (excluding conclusion), each focusing on a critical aspect of cybersecurity. It begins with a comprehensive overview of the latest trends and threats in the field, setting the stage for deeper explorations in subsequent sections. Readers will gain insights into a range of topics, from the intricacies of advanced persistent threats and malware, to the security nuances of cyber-physical systems and the Internet of Things (IoT). The book covers cutting-edge topics like blockchain, cryptography, social engineering, cloud security, and data privacy, blending theory with practical case studies. It's a practical guide for cybersecurity professionals, forensic investigators, legal practitioners, law enforcement, scholars, and students. Offering a comprehensive toolkit for combating digital threats, it's essential for staying ahead in the fast-evolving field of cybersecurity.