1.

Record Nr.	UNINA9910502594403321
Titolo	Advances in Digital Forensics XVII : 17th IFIP WG 11.9 International Conference, Virtual Event, February 1–2, 2021, Revised Selected Papers / / edited by Gilbert Peterson, Sujeet Shenoi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-88381-7
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (268 pages)
Collana	IFIP Advances in Information and Communication Technology, , 1868-422X ; ; 612
Disciplina	005.8
Soggetti	Data protection Machine learning Computer engineering Computer networks Computers - Law and legislation Information technology - Law and legislation Data and Information Security Machine Learning Computer Engineering and Networks Computer Communication Networks Legal Aspects of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Contents -- Contributing Authors -- Preface -- I THEMES AND ISSUES -- Chapter 1 DIGITAL FORENSIC ACQUISITION KILL CHAIN - ANALYSIS AND DEMONSTRATION -- 1. Introduction -- 2. Related Work -- 3. Digital Forensic Acquisition Kill Chain -- 3.1 Background -- 3.2 Kill Chain Overview -- 3.3 Kill Chain Phases -- 4. Case-Motivated Kill Chain Example -- 5. Conclusions -- Acknowledgement -- References -- Chapter 2 ENHANCING INDUSTRIAL CONTROL SYSTEM FORENSICS USING REPLICATION-BASED DIGITAL TWINS -- 1. Introduction -- 2. Background -- 2.1 Digital Twin -- 2.2 Digital Twin Security -- 2.3 Digital Forensics -- 3. Related Work -- 4. Replication Using Digital

Twins -- 4.1 Replication and Replay Theorems -- 4.2 Conceptual Framework -- 5. Implementation and Evaluation -- 5.1 Implementation and Experimental Setup -- 5.2 Results and Evaluation -- 6. Discussion -- 7. Conclusions -- Acknowledgement -- References -- Chapter 3 COMPARISON OF CYBER ATTACKS ON SERVICES IN THE CLEARNET AND DARKNET -- 1. Introduction -- 2. Background -- 3. Common Targets and Attacks -- 4. Related Work -- 5. Honeypot Deployment -- 5.1 Security Considerations -- 5.2 Deployment Process -- 6. Implementation Details -- 6.1 Virtual Machine Architectures -- 6.2 Honeypot Services -- 7. Experiments and Results -- 7.1 Service Deployments -- 7.2 Announcements -- 7.3 Observed Web Requests -- 7.4 Observed SSH and Telnet Access -- 7.5 Observed SMTP Requests -- 7.6 Observed FTP Requests -- 7.7 Discussion -- 8. Conclusions -- Acknowledgement -- References -- II APPROXIMATE MATCHING TECHNIQUES -- Chapter 4 USING PARALLEL DISTRIBUTED PROCESSING TO REDUCE THE COMPUTATIONAL TIME OF DIGITAL MEDIA SIMILARITY MEASURES -- 1. Introduction -- 2. Previous Work -- 3. Jaccard Indexes of Similarity -- 3.1 Jaccard Index -- 3.2 Jaccard Index with Normalized Frequency -- 4. Jaccard Index with Split Files.

5. Results and Validation -- 6. Conclusions -- References -- Chapter 5 EVALUATION OF NETWORK TRAFFIC ANALYSIS USING APPROXIMATE MATCHING ALGORITHMS -- 1. Introduction -- 2. Foundations and Related Work -- 2.1 Current State of Approximate Matching -- 2.2 Approximate Matching Algorithms -- 3. Controlled Study -- 3.1 All vs. All Evaluation -- 3.2 Evaluation Methodology -- 4. Experimental Results and Optimizations -- 5. Conclusions -- Acknowledgement -- References -- III ADVANCED FORENSIC TECHNIQUES -- Chapter 6 LEVERAGING USB POWER DELIVERY IMPLEMENTATIONS FOR DIGITAL FORENSIC ACQUISITION -- 1. Introduction -- 2. USB Power Delivery Protocol -- 3. Research Methodology -- 4. Results -- 4.1 Information Gathering -- 4.2 Passive Monitoring -- 4.3 Firmware Files -- 4.4 Firmware Reverse Engineering -- 4.5 Apple Vendor-Defined Protocol -- 4.6 Firmware Modification and Rollback -- 5. Conclusions -- Acknowledgements -- References -- Chapter 7 DETECTING MALICIOUS PDF DOCUMENTS USING SEMI-SUPERVISED MACHINE LEARNING -- 1. Introduction -- 2. Background and Related Work -- 2.1 PDF Document Structure -- 2.2 Document Entropy -- 2.3 Malicious PDF Document Detection -- 3. Malicious PDF Document Detection Method -- 3.1 Structural Features -- 3.2 Entropy-Based Statistical Features -- 3.3 Classification -- 4. Experiments and Results. -- 4.1 Dataset Creation and Experimental Setup -- 4.2 Evaluation Metrics -- 4.3 Feature Set Analysis -- 4.4 Classifier Analysis -- 4.5 Detection Method Comparison -- 5. Conclusions -- Acknowledgement -- References -- Chapter 8 MALICIOUS LOGIN DETECTION USING LONG SHORT-TERM MEMORY WITH AN ATTENTION MECHANISM -- 1. Introduction -- 2. Related Work -- 3. Preliminaries -- 3.1 Detection Method Overview -- 3.2 Threat Model -- 4. Proposed Method -- 4.1 Host Vector Learning -- 4.2 Feature Extraction -- 4.3 Attention Mechanism.

4.4 Classification Model Optimization -- 5. Experimental Evaluation -- 5.1 Dataset Description -- 5.2 Experimental Setup -- 5.3 Evaluated Models -- 5.4 Evaluation Results -- 5.5 Optimization and Learning Rate -- 6. Conclusions -- References -- IV NOVEL APPLICATIONS -- Chapter 9 PREDICTING THE LOCATIONS OF UNREST USING SOCIAL MEDIA -- 1. Introduction -- 2. Related Work -- 3. Location Extraction from Web Forum Data -- 3.1 Web Forum Dataset -- 3.2 Dictionary-Based Semi-Supervised Learning -- 3.3 BiLSTM-CRF Model -- 3.4 n-Gram-ARM Algorithm -- 4. Experiments and Results -- 5. Conclusions -- References -- Chapter 10 EXTRACTING THREAT INTELLIGENCE

RELATIONS USING DISTANT SUPERVISION AND NEURAL NETWORKS -- 1. Introduction -- 2. Related Work -- 2.1 Threat Intelligence Datasets -- 2.2 Threat Intelligence Information Extraction -- 3. Proposed Framework -- 3.1 Overview -- 3.2 Problem Specification -- 3.3 Dataset -- 3.4 Neural Network Model -- 4. Experiments and Results -- 4.1 Experiment Details -- 4.2 Comparison with Baseline Models -- 4.3 Extraction Results -- 5. Conclusions -- Acknowledgement -- References -- Chapter 11 SECURITY AUDITING OF INTERNET OF THINGS DEVICES IN A SMART HOME -- 1. Introduction -- 2. Preliminaries -- 2.1 Security Standards and Best Practices -- 2.2 Security Auditing Challenges -- 2.3 Threat Model -- 3. Security Auditing Methodology -- 3.1 Step 1: Build a Knowledge Base -- 3.2 Step 2: Translate to Security Rules -- 3.3 Step 3: Audit IoT Device Security -- 4. Auditing Smart Home Security -- 4.1 Security Rule Definition -- 4.2 Data Collection -- 4.3 Formal Language Translation -- 4.4 Verification -- 4.5 Evidence Extraction -- 5. Security Auditing Framework -- 6. Experiments and Results -- 6.1 Experimental Setup -- 6.2 Experimental Results -- 7. Discussion -- 8. Related Work -- 9. Conclusions -- References -- V IMAGE FORENSICS.
Chapter 12 INDIAN CURRENCY DATABASE FOR FORENSIC RESEARCH -- 1. Introduction -- 2. Related Work -- 3. Indian Currency Security Features -- 4. Indian Currency Database -- 4.1 Sample Collection -- 4.2 Security Feature Identification -- 4.3 Database Creation -- 5. Conclusions -- References -- Chapter 13 SECURITY AND PRIVACY ISSUES RELATED TO QUICK RESPONSE CODES -- 1. Introduction -- 2. QR Code Structure -- 3. QR Code Evolution -- 4. Key Issues -- 4.1 Authentication with QR Codes -- 4.2 Attacks Using QR Codes -- 4.3 Security and Privacy of QR Codes -- 5. Innovative Applications -- 5.1 Self-Authenticating Documents -- 5.2 Color QR Codes -- 5.3 Anti-Counterfeiting QR Codes -- 6. Conclusions -- References.

Sommario/riassunto

ADVANCES IN DIGITAL FORENSICS XVII Edited by: Gilbert Peterson and Sujeet Shenoi Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XVII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: · Themes and Issues · Approximate Matching Techniques · Advanced Forensic Techniques · Novel Applications · Image Forensics This book is the seventeenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of thirteen edited papers from the Seventeenth Annual IFIP WG 11.9 International Conference on Digital Forensics, a fully-remote event held in the winter of 2021. Advances in Digital Forensics XVII is an important resource for researchers, faculty members and graduate students, as well as for

practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.