1. Record Nr. UNINA9910634043903321

Titolo	Network and system security : 16th international conference, NSS 2022, Denarau Island, Fiji, December 9-12, 2022 : proceedings / / edited by Xingliang Yuan, [and three others]
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-23020-5
Descrizione fisica	1 online resource (745 pages)
Collana	Lecture Notes in Computer Science ; ; v.13787
Disciplina	060
Soggetti	Application software
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- AI for Network Security -- Vulnerability Detection Using Deep Learning Based Function Classification -- 1 Introduction -- 2 Background -- 2.1 Vulnerability Categories -- 2.2 Challenges -- 2.3 Perceptions -- 3 Method -- 3.1 Function Processing -- 3.2 Function Classification -- 3.3 Vulnerability Detection -- 4 Experiments and Results -- 4.1 Experiment Setup -- 4.2 RQ 1: Function Classification -- 4.3 RQ2: Vulnerability Detection -- 4.4 RQ 3: Runtime Cost -- 4.5 Case Study -- 4.6 Limitations -- 5 Related Work -- 6 Conclusion and Future Work -- A Additional Vulnerability Cases -- References -- RAIDER: Reinforcement-Aided Spear Phishing Detector -- 1 Introduction -- 2 Background -- 2.1 K Nearest Neighbours (KNN) -- 2.2 Reinforcement Learning (RL) -- 3 Key Insights: Analysis of Spear Phishing Emails -- 4 RAIDER System Design -- 4.1 Threat Model -- 4.2 Overview of RAIDER -- 4.3 RAIDER in Detail -- 5 Evaluation -- 5.1 Experimental Setup -- 5.2 Results of RAIDER -- 6 Discussion and Future Work -- 6.1 Complexity and Time Overhead -- 6.2 Contextual Analysis Limitations -- 6.3 Crafted vs Real Spear Phishing Emails -- 7 Related Work -- 8 Conclusion -- References -- Network Intrusion Detection Adversarial Attacks for LEO Constellation Networks Based on Deep Learning -- 1 Introduction -- 2 Related Work -- 2.1 Low Earth Orbit Satellite Traffic Simulation Platform -- 2.2 Malicious Traffic Collection -- 2.3 Launch Attack -- 2.4 Traffic

Classification Model -- 2.5 Adversarial Examples -- 3 Methods -- 3.1 LEO Traffic Simulation System -- 3.2 Traffic Adversarial Sample Generate Algorithm -- 3.3 Datasets -- 3.4 Traffic Classification Model -- 3.5 Adversarial Sample Defense Algorithm -- 4 Experiment -- 4.1 Defense Model -- 4.2 Experimental Results -- 5 Conclusion -- References.
A Proof of Concept Implementation of Explainable Artificial Intelligence (XAI) in Digital Forensics -- 1 Introduction -- 1.1 Our Contributions -- 1.2 AI in Digital Forensics: The Current State -- 2 Background, Dataset, and Models -- 2.1 What Is XAI? -- 2.2 The Datasets -- 2.3 Data Models -- 3 Forensic Processing -- 3.1 Target Files -- 3.2 Parsing Media Data -- 3.3 File Pre-processing -- 3.4 Implementing AI and Explainability -- 4 Results -- 4.1 Image Classification Results -- 4.2 Video Classification -- 4.3 File Metadata Classification -- 5 Discussion on Results, Limitations, and Future Work -- 5.1 Limitations -- 5.2 Avenues for Further Research -- References -- Graph Intelligence Enhanced Bi-Channel Insider Threat Detection -- 1 Introduction -- 2 Related Works -- 2.1 Insider Threat Detection -- 2.2 Graph-Based Insider Threat Detection -- 3 Methodology -- 4 A Use Case Implementation -- 4.1 Dataset and Pre-processing -- 4.2 Inner-User Channel Feature Extraction -- 4.3 Inter-User Channel Feature Extraction -- 5 Experiments -- 5.1 Comparison Between B-CITD and Inner-User Channel -- 5.2 Comparison Between B-CITD and Inter-user Channel -- 5.3 Discussion -- 6 Conclusion -- References -- Network Security -- Exploiting Redundancy in Network Flow Information for Efficient Security Attack Detection -- 1 Introduction -- 2 Literature Review -- 3 Methodology -- 3.1 Background Techniques -- 3.2 Sampling Based Frameworks -- 4 Experiments -- 4.1 General Experiment Settings -- 4.2 Results and Analysis -- 5 Conclusion -- References -- A Learning Methodology for Line-Rate Ransomware Mitigation with P4 Switches -- 1 Introduction -- 2 Related Work -- 3 Ransomware Threat Model -- 4 Proposed Methodology -- 4.1 Overview and Intuition -- 4.2 Data Processing -- 4.3 RF Implementation -- 5 Evaluation -- 6 Concluding Remarks and Future Directions -- References.
Reducing Intrusion Alert Trees to Aid Visualization -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Paper Outline -- 2 Problem Formalization -- 2.1 Setting and Terminology -- 2.2 Intuitive Problem Statement -- 2.3 Data Structures -- 2.4 Formalizing Intuitive Problems as Research Questions -- 3 Methods -- 3.1 Merging Sibling Leaves -- 3.2 Merging Sibling Branches -- 3.3 Truncating Hypotrees -- 4 Case Study -- 4.1 Evaluation Metrics -- 4.2 Results -- 4.3 Answering Research Questions -- 5 Discussion -- 6 Conclusion -- References -- Attacker Attribution via Characteristics Inference Using Honeypot Data -- 1 Introduction -- 2 Background and Related Work -- 3 Methodology -- 3.1 Data Collection and Processing -- 3.2 Basic Methodology -- 3.3 Generalized Methodology -- 4 Evaluation -- 4.1 Replication of Results -- 4.2 Generalized Results -- 5 Discussion -- 6 Conclusion -- References -- Detecting Contradictions from CoAP RFC Based on Knowledge Graph -- 1 Introduction -- 2 Background and Related Work -- 2.1 Background -- 2.2 Related Work -- 3 Problem Definition -- 3.1 Entity, Rule and Relation -- 3.2 Contradictions -- 4 RFCKG Approach -- 4.1 Rule Statement Extraction -- 4.2 Knowledge Graph Construction -- 4.3 Contradiction Detection -- 5 Evaluation -- 5.1 Knowledge Graph Construction -- 5.2 Contradiction Detection -- 6 Discussion and Future Directions -- 7 Conclusion -- References -- Mobile Security -- A First Look at Android Apps' Third-Party Resources Loading -- 1 Introduction -- 2 Background and Methodology -- 2.1 Third-Party Ecosystem -- 2.2 Collecting App Metadata from Google Play -- 2.3

Extracting Apps' Resource Dependency Chains -- 2.4 Resource Dependency Dataset -- 2.5 Meta-data Collection from VirusTotal -- 3 Analysis of Apps' Resource Dependency Chains -- 3.1 Characterizing Apps' Implicit Trust.
3.2 Characterizing the Types of Resources -- 4 Analyzing Malicious Resource Dependency Chains of Apps -- 4.1 Do Apps Load Suspicious Third-Parties? -- 4.2 Do Apps' Dependency Chains Contain Suspicious Parties? -- 4.3 How Widespread Are Suspicious Parties? -- 4.4 Which Suspicious Third-Parties Are Most Prevalent? -- 4.5 At Which Level Do Suspicious Third-Parties Occur? -- 5 Related Work -- 6 Concluding Remarks -- References -- Comprehensive Mobile Traffic Characterization Based on a Large-Scale Mobile Traffic Dataset -- 1 Introduction -- 2 Related Work -- 3 Mobile Traffic Dataset -- 4 Mobile Traffic Characterization -- 4.1 Basic Information -- 4.2 Domain Name Usage -- 4.3 HTTP/TLS Usage -- 4.4 Traffic Flow -- 5 Discussion -- 5.1 Network Operator -- 5.2 Mobile Traffic Researcher -- 6 Conclusion -- References -- DOT-M: A Dual Offline Transaction Scheme of Central Bank Digital Currency for Trusted Mobile Devices -- 1 Introduction -- 1.1 Design Principles -- 1.2 Related Work -- 1.3 Our Contribution -- 2 System Model and Assumptions -- 2.1 Notation -- 2.2 System Model -- 2.3 Security Assumptions and Threat Model -- 3 DOT-M Scheme for Mobile Devices -- 3.1 Security Solution on Mobile Device -- 3.2 Design of Data Structure -- 3.3 The Details of Dual Offline Transaction Scheme -- 4 Implementation and Evaluation -- 4.1 Implementation -- 4.2 Efficiency and Performance Evaluation -- 5 Conclusion -- References -- A Beyond-5G Authentication and Key Agreement Protocol -- 1 Introduction -- 2 Preliminaries -- 2.1 5G Terms and Acronyms -- 2.2 Key Encapsulation Mechanisms -- 2.3 Post-Quantum Cryptography -- 2.4 Used Symmetric Primitives -- 3 Related Work -- 4 Contributions -- 5 Our Protocol -- 5.1 Phase A: The Identification Phase -- 5.2 Phase B: The Authentication Phase -- 5.3 Remarks on the Enhancements Required by Our Protocol -- 6 The Case of GUTI.
7 Security Analysis -- 7.1 Threat Model -- 7.2 Formal Verification -- 7.3 Further Security Features -- 8 Feasibility of Our Protocol -- 9 Conclusion -- References -- IoT Security -- A Survey on IoT Vulnerability Discovery -- 1 Introduction -- 2 Taxonomy and Research Methodology -- 2.1 Taxonomy -- 2.2 Research Methodology -- 3 IoT Vulnerability Discovery with Code Intelligence -- 3.1 Physical Device -- 3.2 Operation Rule -- 3.3 Communication -- 4 Research Challenges -- 5 Conclusion -- References -- Differentiated Security Architecture for Secure and Efficient Infotainment Data Communication in IoV Networks -- 1 Introduction -- 2 Related Work -- 2.1 Internet-of-Vehicles -- 2.2 Caching with Named Data Networking -- 2.3 Attribute-Based Encryption -- 2.4 Blockchain -- 3 Overview of System Architecture -- 3.1 Data Classification -- 3.2 Design Considerations -- 3.3 Proposed Approach for Infotainment Data Exchange -- 3.4 Subscribed User Revocation -- 4 Time-Sensitive KP-ABE Scheme -- 4.1 Model Evaluation -- 5 Conclusion -- A Summary of Math Notation and Symbols -- References -- An Efficient Authenticated Group Key Agreement Protocol with Dynamic Batch Verification for Secure Distributed Networks -- 1 Introduction -- 1.1 Related Work -- 1.2 Main Contributions -- 1.3 Organization -- 2 Preliminaries -- 2.1 Group Key Agreement Protocol -- 2.2 BLS Multi-Signatures -- 2.3 Protocol Transformation -- 2.4 Notations -- 3 System Model -- 4 The Proposed Protocol -- 4.1 Authenticated Group Key Agreement Protocol -- 4.2 The Proposed Protocol with Precomputation -- 4.3 Dynamic Batch Verification -- 5 Conclusion -- References -- Leveraging Frame Aggregation in Wi-Fi IoT Networks for Low-Rate DDoS Attack Detection