1. Record Nr. UNINA9910634049003321

Titolo	Information systems security : 8th International Conference, ICISS 2022, Tirupati, India, December 16-20, 2022, proceedings / / edited by Venkata Ramana Badarla, Surya Nepal, and Rudrapatna K. Shyamasundar
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-23690-4
Descrizione fisica	1 online resource (297 pages)
Collana	Lecture Notes in Computer Science ; ; v.13784
Disciplina	016.391
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Abstracts of Keynote Addresses -- The Rise of Cyber Physical Security -- Research and Engineering Challenges of Blockchain and Web3 -- Security and Privacy in Federated Learning -- Web3 and the Interoperability of Asset Networks -- Abstracts of Invited Addresses -- Securing Cyber-Physical and IoT Systems in Smart Living Environments -- Advanced Persistent Threats: A Study in Indian Context -- Technology Transfer from Security Research Projects: A Personal Perspective -- Contents -- Ostinato: Cross-host Attack Correlation Through Attack Activity Similarity Detection -- 1 Introduction -- 2 Problem Description -- 3 Approach and Architecture -- 3.1 Tagged Provenance Graphs -- 3.2 Identifying Similar Nodes -- 3.3 Edge Label Similarity -- 3.4 Graph Similarity Detection -- 4 Evaluation -- 4.1 Ostinato Efficacy -- 4.2 Node Similarity Accuracy -- 4.3 Run-Time Performance -- 4.4 Threat Alert Fatigue Mitigation -- 4.5 Comparison with Other Tools -- 5 Related Work -- 6 Conclusion -- References -- DKS-PKI: A Distributed Key Server Architecture for Public Key Infrastructure -- 1 Introduction -- 2 Related Work -- 3 DKS-PKI Architecture -- 3.1 Overview -- 3.2 Node Operations -- 3.3 Authoritative Signing Keys (ASKs) -- 3.4 Certificate Registration/Issuance and Storage -- 3.5 Certificate Distribution -- 3.6 Certificate Revocation -- 3.7 Stored-Data Validation -- 4 Evaluation --

4.1 Security Analysis -- 4.2 Implementation -- 4.3 Experimental Environment -- 4.4 Performance Analysis -- 5 Conclusion -- References -- Generating-Set Evaluation of Bloom Filter Hardening Techniques in Private Record Linkage -- 1 Introduction -- 2 Background and Related Work -- 2.1 Linkage with Bloom Filters -- 2.2 Hardening Bloom Filters -- 2.3 Privacy Measures -- 3 Generating-Sets and Amplification -- 3.1 Generating-Set Amplification Factor.
3.2 Amplification Factor in Deterministic Methods -- 3.3 Amplification Factor in Probabilistic Methods -- 4 Parameter Selection in Probabilistic Methods -- 5 Empirical Evaluation -- 5.1 Setup -- 5.2 Bit Frequency Measures -- 5.3 Generating-Set Amplification Factor -- 5.4 Linkage Quality -- 5.5 Discussion -- 6 Conclusion and Future Work -- References -- .26em plus .1em minus .1emSHIELD: A Multimodal Deep Learning Framework for Android Malware Detection -- 1 Introduction -- 2 Related Work -- 2.1 Static Analysis Based Android Malware Detection Techniques -- 2.2 Dynamic Analysis Based Android Malware Detection Techniques -- 2.3 Hybrid Analysis Based Android Malware Detection Techniques -- 3 SHIELD: The Proposed Framework -- 3.1 Feature Extraction -- 3.2 Markov Image Generation -- 3.3 Network Construction -- 4 Experimental Evaluation -- 4.1 Dataset -- 4.2 Evaluation Environment -- 4.3 Performance Analysis Based Markov Images Separately -- 4.4 Performance Analysis Based on Multimodal Latent Features -- 4.5 Unknown Malware Family Detection -- 4.6 Backdoor Analysis -- 4.7 Comparison with State-of-the-Art Work -- 5 Conclusion and Future Work -- References -- Samyukta: A Unified Access Control Model using Roles, Labels, and Attributes -- 1 Introduction -- 2 Related Work -- 3 Need for a Unified Model -- 4 Preliminaries -- 4.1 Readers-Writers Flow Model -- 5 Samyukta: A Unified Access Control Model -- 5.1 Formal Specification -- 5.2 Request Flow in Samyukta -- 5.3 Authorization Procedure -- 6 Effectiveness of Samyukta -- 6.1 Merits of Samyukta -- 7 Experimental Analysis -- 8 Conclusions -- References -- Efficient and Effective Static Android Malware Detection Using Machine Learning -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Dataset Description -- 3.2 Feature Set -- 3.3 Machine Learning Classifier -- 3.4 Evaluation.
4 Comparison with Existing Approaches -- 5 Discussion -- 6 Conclusion and Future Work -- References -- Attacks on ML Systems: From Security Analysis to Attack Mitigation -- 1 Introduction -- 2 ML Systems and Attacks -- 2.1 ML Systems Have Three Main Perspectives -- 2.2 Adversarial Attacks -- 3 Security Analysis Requirements of ML Systems -- 3.1 ML System Security Analysis Requirements -- 3.2 Limitations of Prior Work on ML Security Analysis -- 4 Proposed Approach -- 4.1 The AI Security Causality Graph -- 4.2 The ML System Dependency Graph -- 4.3 Using the ML-SSA Approach to Analyze the Word Translation Attacks -- 5 AI Security Analysis and Attack Mitigation -- 5.1 Using the Example Word-to-Word Translation ML System to Illustrate Relevant Mitigation Strategies -- 6 Conclusion and Future Directions -- References -- MILSA: Model Interpretation Based Label Sniffing Attack in Federated Learning -- 1 Introduction -- 2 Background and Related Works -- 2.1 Federated Learning -- 2.2 Shapley Value -- 2.3 Inference Attacks -- 3 Threat Model -- 4 MILSA: The Proposed Attack -- 5 Experiments and Results -- 5.1 Experimental Setup -- 5.2 Results -- 6 The Proposed Defense -- 7 Conclusion -- References -- IoTInDet: Detecting Internet of Things Intrusions with Class Scatter Ratio and Hellinger Distance Statistics -- 1 Introduction -- 2 Related Works -- 3 IoTInDet Methodology -- 3.1 Class Scatter Ratio Based Feature Selection -- 3.2 Hellinger Distance Chart Generation -- 3.3 IoT Normal Traffic Description -- 3.4 IoT Traffic

Intrusion Detection -- 4 Experimental Results -- 5 Conclusion -- References -- Detecting Cloud Originated DDoS Attacks at the Source Using Out-Cloud Attack Detection (OCAD) -- 1 Introduction -- 2 Related Work -- 3 Cloud-Based DDoS Attacks -- 4 Out-Cloud Attack Cases in Cloud -- 4.1 An Attacker in the Cloud -- 4.2 A Reflector Server in the Cloud.
5 Out-Cloud Attack Detection (OCAD) -- 5.1 Traffic Directions -- 5.2 Virtual Interfaces vs Real Interfaces -- 5.3 Case 1: An Attacker in the Cloud -- 5.4 Case 2: A Reflector Server in the Cloud -- 5.5 OCAD Modules -- 6 Experimental Evaluation -- 6.1 Experimental Setup -- 6.2 Amplification Attack -- 6.3 Reflection Attack -- 6.4 Experimental Results -- 7 Discussion -- 8 Conclusions -- References -- Mining Attribute-Based Access Control Policies -- 1 Introduction -- 2 Overview of ABAC -- 3 Related Work -- 4 ABAC Policy Extraction -- 4.1 Policy Mining -- 4.2 Policy Extraction Using Machine Learning -- 5 Experimental Evaluation -- 5.1 Performance of Policy Mining Approach -- 5.2 Performance of ABAC Policies with Constraints -- 5.3 Performance of Policy Extraction Using Machine Learning -- 6 Conclusion -- References -- Preventing Privacy-Violating Information Flows in JavaScript Applications Using Dynamic Labelling -- 1 Introduction -- 2 Background -- 2.1 A Brief Introduction to IFC -- 2.2 Dynamic Labelling (DL) Algorithm ch12secrypt18, ch12ghosal2018compile -- 2.3 Readers-Writers Flow Model (RWFM) ch12kumar2017complete -- 3 Security Challenges and Our Approach -- 3.1 Flow Sensitivity -- 3.2 Termination Sensitivity -- 3.3 Eval Statement -- 3.4 Declassification -- 4 Solution for Preventing Privacy-Violating Flows -- 5 Related Work -- 6 Conclusions and Future Work -- References -- On the Impact of Model Tolerance in Power Grid Anomaly Detection Systems -- 1 Introduction -- 2 Background and Related Work -- 2.1 Demand Manipulation Attacks -- 2.2 Anomaly Detection Mechanism -- 2.3 Related Work -- 3 Methodology -- 3.1 Power Consumption Data -- 3.2 Model Training -- 3.3 Anomaly Score -- 3.4 Thresholding Mechanism -- 3.5 Attack Profiles -- 4 Threshold Selection -- 4.1 The Threshold Dilemma -- 5 Model Tolerance and Impact -- 6 Conclusion and Future Work.
References -- WiP: Control Plane Saturation Attack Mitigation in Software Defined Networks -- 1 Introduction -- 2 Literature Review -- 3 Proposed Approach -- 3.1 Saturation Attack Detection -- 3.2 Attack Mitigation -- 4 Experiments and Evaluation -- 5 Conclusion -- References -- WiP: EventTracker-Event Driven Evidence Collection for Digital Forensics -- 1 Introduction -- 2 Literature Review -- 3 Proposed Approach -- 4 Implementation and Evaluation -- 4.1 System Setup -- 4.2 Evaluation -- 4.3 Measurement Study -- 4.4 Comparison with Existing Tools -- 5 Conclusion -- References -- WiP: Characterizing the Impact of Multiplexed DoS Attacks on HTTP and Detection -- 1 Introduction -- 2 Impact Study -- 3 Detecting Attacks -- 4 Experiments and Evaluation -- 5 Conclusion -- References -- Author Index.