1. Record Nr. UNISA996587860003316

Autore	Katsikas Sokratis
Titolo	Computer Security. ESORICS 2023 International Workshops : CyberICS, DPM, CBT, and SECPRE, the Hague, the Netherlands, September 25-29, 2023, Revised Selected Papers, Part I
Pubbl/distr/stampa	Cham : , : Springer, , 2024 ©2024
ISBN	3-031-54204-5
Edizione	[1st ed.]
Descrizione fisica	1 online resource (518 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14398
Altri autori (Persone)	Cuppensédéric Cuppens-BoulahiaNora LambrinoudakisCostas Garcia-AlfaroJoaquin Navarro-ArribasGuillermo NespoliPantaleone KalloniatisChristos MylopoulosJohn AntónAnnie
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents - Part I -- Contents - Part II -- Effects of Organizational Cyber Security Culture Across the Energy Sector Supply Chain -- 1 Introduction -- 2 Related Work -- 2.1 Supply Chain Cyber Security -- 2.2 Cyber Security Culture -- 3 Method -- 3.1 Problem Identification and Literature Review -- 3.2 Data Collection and Analysis -- 3.3 Data Interpretation and Reporting -- 4 Results -- 4.1 Governance -- 4.2 Preparedness and Incident Response -- 4.3 Supply Chain Challenges -- 4.4 Trust -- 4.5 Looking Towards Others and Propagation of Trust -- 4.6 The Impact of Organization Size -- 5 Discussion -- 5.1 Discussion of Main Research Questions -- 5.2 Exploration of Additional Findings -- 6 Conclusion and Future Work -- References -- METRICS: A Methodology for Evaluating and Testing the

Resilience of Industrial Control Systems to Cyberattacks -- 1 Introduction -- 2 Cybersecurity Research for ICSs -- 2.1 Testbeds -- 2.2 Datasets -- 2.3 Related Work -- 2.4 Toward a Cross-Domain ICS Evaluation -- 3 METRICS: A Cybersecurity Evaluation Methodology for ICSs -- 3.1 Exchangeable Evaluation Environment -- 3.2 Adversaries and Responses -- 3.3 Cross-Domain Metrics -- 3.4 Evaluation Control -- 4 Use Case: METRICS for Power Grids -- 4.1 Evaluation Phases -- 4.2 Discussion -- 5 Toward Cross-Domain Resilience -- 6 Conclusion -- A Environment Description File Example -- B Scenario Description File Example -- References -- Threat Analysis in Dairy Farming 4.0 -- 1 Introduction -- 2 Related Work -- 3 CPSs of a Dairy Farm 4.0 -- 4 Threat Modeling and Risk Assessment -- 4.1 Methodology -- 4.2 Threats and Risks in the Dairy Farm 4.0 -- 5 Conclusions -- References -- Overview of Social Engineering Protection and Prevention Methods -- 1 Introduction -- 2 Method Selection Methodology -- 3 Analysis -- 3.1 Overview of Protection Method Categories.
3.2 Criteria for Method Evaluation -- 3.3 Evaluation Results -- 3.4 Analysis of Evaluation Results -- 4 Conclusion -- References -- Skade - A Challenge Management System for Cyber Threat Hunting -- 1 Introduction -- 2 Related Work -- 3 Hypotheses Concerning Threat Hunting Training -- 3.1 Ensuring Constructive Alignment -- 3.2 Supporting Motivating Setting -- 3.3 Providing Feedback and Assessment -- 3.4 Covering Multiple Learning Dimensions -- 4 Realization of the Challenge Manager Skade -- 4.1 Features -- 4.2 Functions -- 4.3 Example Based on the Nordic-US Exercise of 2023 -- 5 Discussion -- 5.1 Skade as a Design Science Effort -- 5.2 Trainees and Requirements on Challenges -- 5.3 Interaction with Emulators -- 5.4 Learning Objectives and Learning Activities -- 5.5 Experiment Plan and Tests of Hypotheses -- 6 Conclusion -- References -- On the Usage of NLP on CVE Descriptions for Calculating Risk -- 1 Introduction -- 2 Cybersecurity Related Background -- 2.1 Common Vulnerabilities and Exposures (CVE) -- 2.2 Common Platform Enumeration (CPE) -- 2.3 Common Weakness Enumeration (CWE) -- 2.4 Common Attack Pattern Enumeration and Classification (CAPEC) -- 2.5 National Vulnerability Database (NVD) -- 2.6 Common Vulnerability Scoring System (CVSS) -- 3 Related Work -- 4 Natural Language Processing Background -- 4.1 Text Classification -- 4.2 spaCy -- 5 Implementation -- 6 Conclusion -- References -- Evaluation of an OPC UA-Based Access Control Enforcement Architecture -- 1 Introduction -- 2 Related Work -- 3 Architecture -- 3.1 Protocol Modeling -- 4 Implementation -- 5 Experiment -- 6 Results -- 6.1 Results on Connection Experiments -- 6.2 Results on Access Resource Experiments -- 6.3 Results on Different Token Expiry Times -- 6.4 Result on Different Token Sizes -- 6.5 Results on Lowering the CPU Clock Frequency of the Resource Server.
7 Suggestions on Optimizations of Session Activation -- 8 Discussion -- 8.1 Recommendations -- 8.2 Limitations and Impact -- 9 Conclusions -- References -- HoneyEVSE: An Honeypot to Emulate Electric Vehicle Supply Equipments -- 1 Introduction -- 2 Background -- 2.1 Internet Exchange Point -- 2.2 Honeypot -- 2.3 Vehicle-to-Grid (V2G) -- 3 Related Work -- 4 HoneyEVSE Honeypot -- 4.1 Architecture -- 4.2 Physical Process -- 4.3 Services and Interaction -- 4.4 Data Logging -- 5 Results -- 5.1 Interactions Analysis -- 5.2 Interactions Origin -- 6 Conclusion -- References -- DPM 2023 -- Foreword from the DPM 2023 Program Chairs -- 18th International Workshop on Data Privacy Management - DPM 2023 -- PC Chairs -- Program Committee -- Steering Committee -- Additional Reviewers -- Not Only Security and Privacy: The Evolving Ethical and Legal Challenges of E-

Commerce -- 1 Introduction -- 2 Background -- 3 Methodology and Research Strategy -- 3.1 Research Questions -- 4 Results -- 4.1 The `old' Ethical Dilemmas of E-Commerce -- 4.2 The `New' Ethical Dilemmas of E-Commerce -- 5 Conclusions -- References -- Synthetic Is All You Need: Removing the Auxiliary Data Assumption for Membership Inference Attacks Against Synthetic Data -- 1 Introduction -- 2 Background and Related Work -- 2.1 Synthetic Data Generation -- 2.2 Membership Inference Attacks Against Synthetic Tabular Data -- 3 Attack Scenarios -- 3.1 (S0) Auxiliary -- 3.2 (S1) Black Box -- 3.3 (S2) Published -- 3.4 (S3) Upper Bound -- 4 Experimental Setup -- 4.1 Synthetic Data Generators -- 4.2 Real World Datasets -- 4.3 Meta-classifier Methods -- 4.4 Parameters of the Attack -- 5 Results -- 5.1 Query Based Attack -- 5.2 Target Attention Attack -- 5.3 Robustness Analysis for Number of Synthetic Records m -- 6 Future Work -- 6.1 Impact of Releasing Less Synthetic Records.
6.2 Differentially Private Synthetic Generation Methods -- 6.3 Bridging the Gap with the Upper Bound -- 7 Conclusion -- References -- Patient-Centric Health Data Sovereignty: An Approach Using Proxy Re-Encryption -- 1 Introduction -- 2 Proxy Re-Encryption -- 2.1 Syntax and Basic Definitions -- 2.2 Umbral's PRE Scheme -- 3 Related Work -- 4 Patient-Centric Health Data Sovereignty -- 4.1 Proposed Solution -- 4.2 Authentication/Authorisation -- 4.3 Access Delegation Scenario -- 4.4 Break-Glass Approach -- 5 Performance Analysis -- 6 Conclusion -- References -- PrivacySmart: Automatic and Transparent Management of Privacy Policies -- 1 Introduction -- 1.1 Related Work -- 1.2 Contribution and Plan of This Paper -- 2 Proposal Description -- 2.1 System Architecture Overview -- 2.2 User Privacy Preferences -- 2.3 Pop-Up Interaction Module -- 2.4 Consent Smart Contract -- 2.5 Workflow -- 3 Discussion -- 3.1 Implementation -- 3.2 Evaluation -- 4 Conclusions and Future Work -- References -- Try On, Spied On?: Privacy Analysis of Virtual Try-On Websites and Android Apps -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Collection of VTO Providers, Websites and Apps -- 3.2 Analyzing the Sharing of Users' Images on VTO Websites/Apps -- 3.3 Analyzing Privacy Policies w.r.t VTO Feature -- 3.4 Measurement of Trackers -- 3.5 Analysing VTO Service Providers -- 4 Results -- 4.1 Sharing of Users' Images on VTO Featuring Websites -- 4.2 Privacy Policy Analysis w.r.t VTO Feature on Websites -- 4.3 Sharing of Users' Images on VTO Featuring Apps -- 4.4 Privacy Policy Analysis w.r.t VTO Feature on Apps -- 4.5 Measurement of Trackers -- 4.6 Analysis of VTO Service Providers -- 5 Conclusion -- References -- Integrally Private Model Selection for Support Vector Machine -- 1 Introduction -- 2 Preliminaries -- 2.1 Support Vector Machine (SVM).
2.2 Model Comparison Attack for SVM and Integral Privacy -- 3 Methodology -- 3.1 Overview -- 3.2 Datasets -- 3.3 Creation of Partitions -- 3.4 Integrally Private SVM (IPSVM) -- 4 Results -- 4.1 Drawbacks -- 5 Conclusion and Future Work -- References -- Differentially Private Traffic Flow Prediction Using Transformers: A Federated Approach -- 1 Introduction -- 2 Preliminaries -- 2.1 Federated Learning -- 2.2 Differential Privacy -- 2.3 Temporal Fusion Transformers -- 3 Related Work -- 4 Differentially Private Federated Traffic Flow Prediction Using Temporal Fusion Transformers -- 4.1 Client-Side Training -- 4.2 Model Perturbation -- 4.3 Aggregation Algorithm -- 5 Dataset and Experimental Settings -- 6 Results and Analysis -- 7 Conclusion and Future Works -- References -- Analyzing Continuous Ks-Anonymization for Smart Meter Data -- 1 Introduction -- 2 Problem Statement and Related Work -- 3 ks-Anonymity and CASTLE -- 4 Evaluation -- 5 Conclusion -- References -- Towards