1.	Record Nr.	UNINA9910842491003321
	Autore	Katsikas Sokratis
	Titolo	Computer Security. ESORICS 2023 International Workshops : CPS4CIP, ADIoT, SecAssure, WASP, TAURIN, PriST-AI, and SECAI, The Hague, The Netherlands, September 25–29, 2023, Revised Selected Papers, Part II / / edited by Sokratis Katsikas, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Rita Ugarelli, Isabel Praça, Wenjuan Li, Weizhi Meng, Steven Furnell, Basel Katt, Sandeep Pirbhulal, Ankur Shukla, Michele Ianni, Mila Dalla Preda, Kim-Kwang Raymond Choo, Miguel Pupo Correia, Abhishta Abhishta, Giovanni Sileno, Mina Alishahi, Harsha Kalutarage, Naoto Yanai
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	3-031-54129-4
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (785 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14399
	Altri autori (Persone)	AbieHabtamu RaniseSilvio VerderameLuca CambiasoEnrico UgarelliRita PraçaIsabel LiWenjuan MengWeizhi FurnellSteven
	Disciplina	005.8
	Soggetti	Computer networks - Security measures Cryptography Data encryption (Computer science) Computers Computer engineering Computer networks Data protection Mobile and Network Security Cryptology Computing Milieux Computer Engineering and Networks Data and Information Security Computer Communication Networks

Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents - Part II -- Contents - Part I -- CPS4CIP 2023 -- CPS4CIP 2023 Preface -- Organization -- General Chairs -- Program Committee Chairs -- Program Committee -- External Reviewer -- An Opportunity-Based Approach to Information Security Risk -- 1 Introduction -- 2 Related Research -- 2.1 Risk Management -- 2.2 Research Questions -- 3 Research Method -- 4 Results -- 4.1 Definition of Risk -- 4.2 Risk Description -- 4.3 Sample Case - Use of Risk Description Strategies -- 4.4 Positive Risk Assessment -- 5 Summary and Conclusion -- References -- A Methodology for Cybersecurity Risk Assessment in Supply Chains -- 1 Introduction -- 2 Related Work -- 3 Security Risk Assessment Methodology -- 3.1 Asset Types -- 3.2 Threat Types -- 3.3 Vulnerability Types -- 3.4 Supply Chain Risk Assessment -- 3.5 Questionnaire -- 4 Preliminary Validation of the Methodology -- 4.1 Security Experts -- 4.2 Fictional Scenario -- 4.3 Result Discussion -- 5 Conclusion -- References -- IM-DISCO: Invariant Mining for Detecting IntrusionS in Critical Operations -- 1 Introduction -- 2 Related Work -- 3 IM-DISCO -- 3.1 Formalization of Concepts -- 3.2 Railway Example -- 3.3 Predicate Generation -- 3.4 Invariant Rule Mining -- 3.5 Summary -- 4 Implementation -- 5 Evaluation -- 5.1 Data Collection and Experiment Setup -- 5.2 Evaluation Metrics -- 5.3 Operational Mode Inference (RQ. 1) -- 5.4 Anomaly Detection (RQ. 2) -- 5.5 Invariant Rules Verification and Validation (RQ. 3) -- 6 Conclusion -- References -- Unravelling Network-Based Intrusion Detection: A Neutrosophic Rule Mining and Optimization Framework -- 1 Introduction -- 2 State-of-The-Art -- 2.1 Accuracy vs Explainability Dichotomy -- 2.2 Classification Rule Mining -- 2.3 Rule Uncertainty -- 3 RUGE Framework -- 3.1 Phase 1: Rule Mining -- 3.2 Phase 2: Rules Selection. 4 Intrusion Detection Case Study: A CICIDS2017 Testbed -- 4.1 Dataset and Data Preprocessing -- 4.2 Scenario and Configuration -- 4.3 Results and Discussion -- 5 Conclusions -- References -- Labeling NIDS Rules with MITRE ATT&amp -- CK Techniques Using ChatGPT -- 1 Introduction -- 2 Background -- 2.1 Cyber Threat Intelligence -- 2.2 Generative Pre-trained Transformers -- 3 Related Work on Language Models for CTI Labeling -- 3.1 Non-networking-based CTI Labeling -- 3.2 Networking-Based CTI Labeling -- 4 Labeling NIDS Rules with MITRE ATT&amp -- CK Techniques -- 4.1 GPT-Based Labeling -- 4.2 Keyword-Based Labeling (KB) -- 4.3 Post-processing -- 5 Evaluation -- 5.1 Evaluation Set -- 5.2 Performance Metrics -- 5.3 Experimental Setup -- 5.4 Results -- 5.5 Discussion -- 6 Conclusions and Future Work -- A Appendix: Chat-GPT Prompt Templates -- References -- User Behavior Analysis for Malware Detection -- 1 Introduction -- 2 Related Work -- 3 Architecture -- 3.1 Enduser Host -- 3.2 Smart Behavior Analysis (SBA) -- 3.3 Metrics -- 4 Machine Learning Model -- 4.1 Autoencoder Model -- 4.2 Kernel Density Estimation Model -- 5 Model Accuracy and Validation -- 5.1 Training Data -- 5.2 Test Data -- 5.3 Metric Relevancy -- 5.4 Models' Comparison -- 5.5 False Positive Reduction -- 6 Conclusion -- References -- Balancing XAI with Privacy and Security Considerations -- 1 Introduction -- 2 Background -- 2.1 XAI Taxonomy Classes -- 2.2 Evaluation Criteria and Methods -- 3 Findings -- 3.1 Privacy Attacks -- 3.2 Privacy Defences -- 3.3 Security

Aspects -- 4 Conclusions -- References -- Utilizing the Ensemble Learning and XAI for Performance Improvements in IoT Network Attack Detection -- 1 Introduction -- 2 Related work -- 3 Methodology -- 3.1 Overview of Approach -- 3.2 Dataset Refinement with XAI -- 3.3 Attack Detection -- 3.4 Attack Identification.

4 Results and Evaluation -- 4.1 Dataset and Experimental Environment -- 4.2 Performance Metrics -- 4.3 Experimental Evaluation on CIC-IDS Dataset -- 5 Conclusions -- References -- Digital Twins in Healthcare: Security, Privacy, Trust and Safety Challenges*-10pt -- 1 Introduction -- 2 Challenges of Digital Twins -- 2.1 Security -- 2.2 Privacy -- 2.3 Trust -- 2.4 Safety -- 3 Digital Twins in Healthcare -- 3.1 Ethical Concerns of Digital Twins in Healthcare -- 3.2 Threat Landscape in Healthcare -- 4 IoT Digital Twins: Challenges and Conflict Analysis -- 4.1 Security vs. Safety -- 4.2 Security vs. Privacy -- 4.3 Security vs. Operational Requirements -- 4.4 Security vs. Trust -- 5 Summary and Conclusion -- References -- ADIoT 2023 -- ADIoT 2023 Preface -- Organization -- General Co-chair -- Program Co-chairs -- Local Chairs -- Technical Program Committee -- Steering Committee -- Subreviewer -- C-TAR: A Compositional Threat Analysis and Risk Assessment Method for Infrastructure-Based Autonomous Driving -- 1 Introduction -- 2 Preliminaries -- 3 Related Work -- 3.1 Threat Modeling -- 3.2 Risk Assessment -- 3.3 Digital Dependability Identities -- 3.4 Automotive Security Surveys -- 3.5 Insights from Literature Review -- 4 C-TAR Method Description -- 4.1 First Phase - C-TAR Input -- 4.2 Second Phase - Compatibility Conditions -- 4.3 Third Phase - Compatibility Statement -- 5 Example -- 5.1 First Phase - C-TAR Input -- 5.2 Second Phase - Compatibility Conditions -- 5.3 Third Phase - Compatibility Statement -- 6 Conclusion -- References -- The VOCODES Kill Chain for Voice Controllable Devices -- 1 Introduction -- 2 Related Work -- 3 The VOCODES Kill Chain -- 3.1 Steps -- 3.2 Discussion -- 4 Applying VOCODES to Alexa vs Alexa -- 4.1 Reconnaissance -- 4.2 Audio Weaponization -- 4.3 Initial Foothold -- 4.4 Exploitation -- 4.5 Persistence -- 4.6 Actions on Objectives.

5 Conclusions -- References -- DETONAR-Light: An IoT Network Intrusion Detection Using DETONAR without a Sniffer Network -- 1 Introduction -- 2 Background on RPL and DETONAR -- 2.1 RPL -- 2.2 DETONAR -- 2.3 RADAR -- 3 DETONAR-Light Design -- 3.1 Running DETONAR Using Data Collected at a Border Router -- 3.2 DETONAR Adaptation to Contiki-NG and Cooja -- 4 Experiments -- 4.1 Attack Implementation in Contiki-NG -- 4.2 Setup -- 4.3 Metrics -- 5 Results -- 5.1 Attack Detection and Classification for Networks Without Packet Loss -- 5.2 Attack Detection and Classification for Networks with Packet Loss -- 6 Discussion and Limitations -- 7 Conclusions -- References -- Firmware-Based DoS Attacks in Wireless Sensor Network -- 1 Introduction -- 2 Background -- 3 Threat Scenario -- 3.1 Assumption -- 3.2 Vulnerable Code -- 4 Attack Simulation -- 5 Defensive Mechanism -- 6 Related Work -- 7 Conclusion -- Appendix -- References -- Single-Server Batch Delegation of Variable-Input Pairings with Unbounded Client Lifetime -- 1 Introduction -- 2 Pairing Definitions -- 3 Our Batch Delegation Protocols -- 3.1 Input Scenario: "017E A Private Online, "017E B Public Online -- 3.2 Input Scenario: "017E A and "017E B Public Online -- 3.3 Input Scenario: "017E A Private Online and "017E B Public Offline -- 3.4 Input Scenario: "017E A Public Online, "017E B Public Offline -- 3.5 Input Scenario: "017E A and "017E B="017E sH Private Online -- 4 Practical Performance Analysis of Our Protocols -- 5 Conclusions -- A Formal Definitions -- References -- SigIL: A Signature-Based Approach of Malware Detection on Intermediate Language -- 1 Introduction -- 2 Background -- 3 Related

Sommario/riassunto

This two-volume set LNCS 14398 and LNCS 14399 constitutes the refereed proceedings of eleven International Workshops which were held in conjunction with the 28th European Symposium on Research in Computer Security, ESORICS 2023, in The Hague, The Netherlands, during September 25-29, 2023. The 22 regular papers included in these proceedings stem from the following workshops: 9th International Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems, CyberICPS 2023, which accepted 8 papers from 18 submissions; 18th International Workshop on Data Privacy Management, DPM 2023, which accepted 11 papers from 18 submissions; 7th International Workshop on Cryptocurrencies and Blockchain Technology, CBT 2023, which accepted 6 papers from 20 submissions; 7th International Workshop on Security and Privacy Requirements Engineering, SECPRE 2023, which accepted 4 papers from 7 submissions. 4th International Workshop onCyber-Physical Security for Critical Infrastructures Protection, CSPS4CIP 2023, which accepted 11 papers from 15 submissions. 6th International Workshop on Attacks and Defenses for Internet-of-Things, ADIoT 2023, which accepted 6 papers from 10 submissions; Second International Workshop on System Security Assurance, SecAssure 2023, which accepted 5 papers from 8 submissions; First International Workshop on Attacks and Software Protection, WASP 2023, which accepted 7 papers from 13 submissions International Workshop on Transparency,

Accountability and User Control for a Responsible Internet, TAURIN 2023, which accepted 3 papers from 4 submissions; International Workshop on Private, Secure, and Trustworthy AI, PriST-AI 2023, which accepted 4 papers from 8 submissions; International Workshop on Security and Artificial Intelligence, SECAI 2023, which accepted 11 papers from 31 submissions. .