1. Record Nr. UNISA996650067803316

Titolo	Computer Security. ESORICS 2024 International Workshops : SECAI, DisA, CPS4CIP, and SecAssure, Bydgoszcz, Poland, September 16–20, 2024, Revised Selected Papers, Part II / / edited by Joaquin Garcia-Alfaro, Harsha Kalutarage, Naoto Yanai, Rafa Kozik, Pawe Ksieniewicz, Micha Woniak, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Rita Ugarelli, Isabel Praça, Basel Katt, Sandeep Pirbhulal, Ankur Shukla, Marek Pawlicki, Micha Chora
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-82362-1
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XVI, 541 p. 113 illus., 94 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15264
Disciplina	005.8
Soggetti	Computer networks - Security measures Computers Cryptography Data encryption (Computer science) Computer engineering Computer networks Data protection Mobile and Network Security Computing Milieux Cryptology Computer Engineering and Networks Computer Communication Networks Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	SECAI PAPERS: Feasibility Study for Supporting Static Malware Analysis Using LLM -- PSY: Posterior Sampling Based Privacy Enhancer in Large Language Models -- Systematic Bug Reproduction with Large Language Model -- BOTracle: A framework for Discriminating Bots and Humans -- Deep Learning for Network Anomaly Detection under Data

Contamination: Evaluating Robustness and Mitigating Performance Degradation -- On Intrinsic Cause and Defense of Adversarial Examples in Deep Neural Networks -- Effects of Poisoning Attacks on Causal Deep Reinforcement Learning -- Generating Traffic-Level Adversarial Examples from Feature-Level Specifications -- PhishCoder: Efficient Extraction of Contextual Information from Phishing Emails -- .On the Robustness of Malware Detectors to Adversarial Samples -- Towards AI-Based Identification of Publicly Known Vulnerabilities -- Machine Learning-Based Secure Malware Detection using Features from Binary Executable Headers -- Improving Adversarial Robustness in Android Malware Detection by Reducing the Impact of Spurious Correlations -- Multi-Objective Evolutionary Algorithm for Automatic Generation of Adversarial Metamorphic Malware -- A RAG-Based Question-Answering Solution for Cyber-Attack Investigation and Attribution. DisA PAPERS: Recognition of Remakes and Fake Facial Images -- A Novel Method of Improving Intrusion Detection Systems Robustness Against Adversarial Attacks, through Feature Omission and a Committee of Classifiers -- Proposition of a Novel Type of Attacks Targeting Explainable AI Algorithms in Cybersecurity -- Data structures towards the recognition of fake news and disinformation written in Polish. CPS4CIP PAPERS: Characterizing Prediction Model Responses to Attack Inputs: A Study with Time-Series Power Consumption Data -- Best Practices - based Training for Improving Cybersecurity in Power Grids -- Proactive Cyber Security Strategies for Securing Critical National Infrastructure -- Weaponizing Disinformation Against Critical Infrastructures. SecAssure PAPERS: Compliance-driven CWE Assessment by Semantic Similarity -- Enabling Android Application Monitoring by Characterizing Security-Critical Code Fragments -- MITRE-Based APT Attack Generation and Prediction -- Assuring Privacy of AI-Powered Community Driven Android Code Vulnerability Detection -- Formalizing Federated Learning and Differential Privacy for GIS systems in IIIf -- AI-Assisted Assurance Profile Creation for System Security Assurance -- Attack to Defend: Gamifying the MITRE ATT&CK for Cyber Security Training using the COFELET Framework -- Canary in the Coal Mine: Identifying Cyber Threat Trends through Topic Mining -- Stack Overflow Case Study.

Sommario/riassunto

This two-volume set LNCS 15263 and LNCS 15264 constitutes the refereed proceedings of eleven International Workshops which were held in conjunction with the 29th European Symposium on Research in Computer Security, ESORICS 2024, held in Bydgoszcz, Poland, during September 16–20, 2024. The papers included in these proceedings stem from the following workshops: 19th International Workshop on Data Privacy Management, DPM 2024, which accepted 7 full papers and 6 short papers out of 24 submissions; 8th International Workshop on Cryptocurrencies and Blockchain Technology, CBT 2024, which accepted 9 full papers out of 17 submissions; 10th Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems, CyberICPS 2024, which accepted 9 full papers out of 17 submissions; International Workshop on Security and Artificial Intelligence, SECAI 2024, which accepted 10 full papers and 5 short papers out of 42 submissions; Workshop on Computational Methods for Emerging Problems in Disinformation Analysis, DisA 2024, which accepted 4 full papers out of 8 submissions; 5th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection, CPS4CIP 2024, which accepted 4 full papers out of 9 submissions; 3rd International Workshop on System Security Assurance, SecAssure 2024, which accepted 8 full papers out of 14 submissions.