1.	Record Nr.	UNISA996691666303316
	Autore	Nicomette Vincent
	Titolo	Computer Security – ESORICS 2025 : 30th European Symposium on Research in Computer Security, Toulouse, France, September 22–24, 2025, Proceedings, Part I / / edited by Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, Jaideep Vaidya
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
	ISBN	3-032-07884-9
	Edizione	[1st ed. 2026.]
	Descrizione fisica	1 online resource (793 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16053
	Altri autori (Persone)	BenzekriAbdelmalek Boulahia-CuppensNora VaidyaJaideep
	Disciplina	005.8
	Soggetti	Data protection Cryptography Data encryption (Computer science) Computer networks - Security measures Computer networks Computer systems Data and Information Security Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer System Implementation
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	-- Time-Distributed Backdoor Attacks on Federated Spiking Learning. -- TATA: Benchmark NIDS Test Sets Assessment and Targeted Augmentation. -- Abuse-Resistant Evaluation of AI-as-a-Service via Function-Hiding Homomorphic Signatures. -- PriSM: A Privacy-friendly Support vector Machine. -- Towards Context-Aware Log Anomaly Detection Using Fine-Tuned Large Language Models. -- PROTEAN: Federated Intrusion Detection in Non-IID Environments through

Prototype-Based Knowledge Sharing. -- KeTS: Kernel-based Trust Segmentation against Model Poisoning Attacks. -- Machine Learning Vulnerabilities in 6G: Adversarial Attacks and Their Impact on Channel Gain Prediction and Resource Allocation in UC-CF-mMIMO. -- FuncVul: An Effective Function Level Vulnerability Detection Model using LLM and Code Chunk. -- LUMIA: Linear probing for Unimodal and MultiModal Membership Inference Attacks leveraging internal LLM states. -- Membership Privacy Evaluation in Deep Spiking Neural Networks. -- DUMB and DUMBer: Is Adversarial Training Worth It in the Real World?. -- Countering Jailbreak Attacks with Two-Axis Pre-Detection and Conditional Warning Wrappers. -- How Dataset Diversity Affects Generalization in ML-based NIDS. -- Llama-based source code vulnerability detection: Prompt engineering vs Finetuning. -- DBBA: Diffusion-based Backdoor Attacks on Open-set Face Recognition Models. -- Evaluation of Autonomous Intrusion Response Agents In Adversarial and Normal Scenarios. -- Trigger-Based Fragile Model Watermarking for Image Transformation Networks. -- Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks. -- On the Adversarial Robustness of Graph Neural Networks with Graph Reduction. -- SecureT2I: No More Unauthorized Manipulation on AI Generated Images from Prompts. -- GANSec: Enhancing Supervised Wireless Anomaly Detection Robustness through Tailored Conditional GAN Augmentation. -- Fine-Grained Data Poisoning Attack to Local Differential Privacy Protocols for Key-Value Data. -- The DCR Delusion: Measuring the Privacy Risk of Synthetic Data. -- StructTransform: A Scalable Attack Surface for Safety-Aligned Large Language Models.

Sommario/riassunto

This four-volume set LNCS 16053-16056 constitutes the refereed proceedings of the 30th European Symposium on Research in Computer Security, ESORICS 2025, held in Toulouse, France, during September 22–24, 2025. The 100 full papers presented in these proceedings were carefully reviewed and selected from 600 submissions. They were organized in topical sections as follows: AI and Data-Centric Security, Systems and Hardware Security, Privacy, Cryptography and Secure Protocol Design, Blockchain and Financial Security, Privacy Policy and Identity Management, Adversarial and Backdoor Defenses. .