1. Record Nr. UNINA9911020426703321

Autore	Dalla Preda Mila
Titolo	Availability, Reliability and Security : 20th International Conference, ARES 2025, Ghent, Belgium, August 11–14, 2025, Proceedings, Part I / / edited by Mila Dalla Preda, Sebastian Schrittwieser, Vincent Naessens, Bjorn De Sutter
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-032-00624-4
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (649 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15992
Altri autori (Persone)	SchrittwieserSebastian NaessensVincent De SutterBjorn
Disciplina	005.8
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Privacy-Enhancing Technologies and Legal Compliance: A Framework for Supporting PET Selection Based on GDPR Principles -- Prink: ks-Anonymization for Streaming Data in Apache Flink -- Stop watching me! Moving from data protection to privacy preservation in crowd monitoring -- Cross-Jurisdictional Compliance with Privacy Laws: How Websites Adapt Consent Notices to Regional Regulations. Network and Communication Security: On the Feasibility of Fingerprinting Collaborative Robot Network Traffic -- Domainator: Detecting and Identifying DNS-Tunneling Malware Using Metadata Sequences -- Mitigation of PFCP Attacks in 5G Networks: Dynamic Defense through Moving Target Defense and Honeynets -- Striking Back At Cobalt: Using Network Traffic Metadata To Detect Cobalt Strike Masquerading Command and Control Channels -- Towards Deterministic DDS Communication for Secure Service-Oriented Software-Defined Vehicles -- TSA-WF: Exploring the Effectiveness of Time Series Analysis for Website Fingerprinting -- Generalized Encrypted Traffic Classification Using Inter-Flow Signals. IoT and Embedded Systems Securit: SHIELD: Scalable and Holistic Evaluation Framework for ML-Based 5G Jamming

Detection -- AARC-FE: Electrical Assembly Authentication with Random Convolution Kernels and Fuzzy Extractors -- In Specs we Trust? Conformance-Analysis of Implementation to Specifications in Node-RED and Associated Security Risks -- Scrambling Compiler: Automated and Unified Countermeasure for Profiled and Non-Profiled Side Channel Attacks -- Leaky Batteries: A Novel Set of Side-Channel Attacks on Electric Vehicles. Machine Learning and Privacy: DP-TLDM: Differentially Private Tabular Latent Diffusion Model -- Share Secrets for Privacy. Confidential Forecasting with Vertical Federated Learning -- Gradient Inversion of Federated Diffusion Models -- Privacy-Preserving Encoding and Scaling of Tabular Data in Horizontal Federated Learning Systems -- BTDT: Membership Inference Attacks against Large Language Models.

Sommario/riassunto

This two-volume set LNCS 15992-15993 constitutes the proceedings of the 20th International Conference on Availability, Reliability and Security, ARES 2025, in Ghent, Belgium, during August 11-14, 2025. The 34 full papers presented in this book together with 8 short papers were carefully reviewed and selected from 186 submissions. They cover topics such as: Privacy-Enhancing Technologies and Legal Compliance; Network and Communication Security; IoT and Embedded Systems Security; Machine Learning and Privacy; Usable Security and Awareness; System Security; Supply Chain Security, Malware and Forensics; and Machine Learning and Security.