1. Record Nr. UNISA996691678803316

Autore	Han Jinguang
Titolo	Information and Communications Security : 27th International Conference, ICICS 2025, Nanjing, China, October 29–31, 2025, Proceedings, Part III / / edited by Jinguang Han, Yang Xiang, Guang Cheng, Willy Susilo, Liquan Chen
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	981-9535-37-9
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (857 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16219
Altri autori (Persone)	XiangYang ChengGuang SusiloWilly ChenLiquan
Disciplina	005.73 003.54
Soggetti	Data structures (Computer science) Information theory Database management Data mining Application software Image processing - Digital techniques Computer vision Cryptography Data encryption (Computer science) Data Structures and Information Theory Database Management Data Mining and Knowledge Discovery Computer and Information Systems Applications Computer Imaging, Vision, Pattern Recognition and Graphics Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Attack and Defense -- Domain Adaptation for Cross-Device Profiled

ML Side-Channel Attacks. -- Find the Clasp of the Chain: Efficiently Locating Cryptographic Procedures in SoC Secure Boot by Semi-automated Side-Channel Analysis. -- Full-phase distributed quantum impossible differential cryptanalysis. -- ProverNG: Efficient Verification of Compositional Masking for Cryptosystem's Side-Channel Security. -- POWERPOLY: Multilingual Program Analysis with the Aid of WebAssembly. -- Not only spatial, but also spectral: Unnoticeable backdoor attack on 3D point clouds. -- Permutation-Based Cryptanalysis of the SCARF Block Cipher and Its Randomness Evaluation. -- Secure and Scalable TLB Partitioning Against Timing Side-Channel Attacks. -- Security Vulnerabilities in AI-Generated Code: A Large-Scale Analysis of Public GitHub Repositories. -- Vulnerability Analysis. -- Towards Efficient C/C++ Vulnerability Impact Assessment in Package Management Systems. -- AugGP-VD: A smart contract vulnerability detection approach based on augmented graph convolutional networks and pooling. -- VULDA: Source Code Vulnerability Detection via Local Dependency Context Aggregation on Vulnerability-aware Code Mapping Graph. -- KVT-Payload: Knowledge Graph-Enhanced Hierarchical Vulnerability Traffic Payload Generation. -- Construction and Application of Vulnerability Intelligence Ontology under Vulnerability Management Perspective. -- Anomaly Detection. -- Speaker Inference Detection Using Only Text. -- DTGAN: Diverse-Task Generative Adversarial Networks for Intrusion Detection Systems Against Adversarial Examples. -- ConComFND: Leveraging Content and Comment Information for Enhanced Fake News Detection. .- Transferable Adversarial Attacks in Object Detection: Leveraging Ensemble Features and Gradient Variance Minimization. -- VAE-BiLSTM: A Hybrid Model for DeFi Anomaly Detection Combining VAE and BiLSTM. -- FluxSketch: A Sketch-based Solution for Long-Term Fluctuating Key Flow Detection. -- RustGuard: Detecting Rust Data Leak Issues with Context-Sensitive Static Taint Analysis. -- Secure Guard: A Semantic-Based Jailbreak Prompt Detection Framework for Protecting Large Language Models. -- Traffic Classification. -- FCAL: An Asynchronous Federated Contrastive Semi-Supervised Learning Approach for Network Traffic Classification. -- TetheGAN: A GAN-Based Synthetic Mobile Tethering Traffic Generating Framework. -- SPTC: Signature-based Cross-protocol Encrypted Proxy Traffic Classification Approach. -- Multi-modal Datagram Representation with Spatial-Temporal State Space Models and Inter-flow Contrastive Learning for Encrypted Traffic Classification. -- FlowGraphNet: Efficient Malicious Traffic Detection via Graph Construction. -- CascadeGen: A Hybrid GAN-Diffusion Framework for Controllable and Protocol-Compliant Synthetic Network Traffic Generation. -- Steganography and Watermarking. -- Towards High-Capacity Provably Secure Steganography via Cascade Sampling. -- When There Is No Decoder: Removing Watermarks from Stable Diffusion Models in a No-box Setting. -- Robust Reversible Watermarking for 3D Models Based on Auto Diffusion Function.

Sommario/riassunto

This three-set volume LNCS 16217-16219 constitutes the refereed proceedings of 27th International Conference on Information and Communications Security, ICICS 2025, held in Nanjing, China, during October 29–31, 2025. The 91 full papers presented in this book were carefully selected and reviewed from 357 submissions. The papers are organized in the following topical sections: Part I: Cryptography; Post-quantum Cryptography; Anonymity and Privacy; Authentication and Authorization. Part II: Blockchain and Cryptocurrencies, System and Network Security, Security and Privacy of AI, Machine Learning for Security. Part III: Attack and Defense; Vulnerability Analysis; Anomaly

Detection; Traffic Classification; Steganography and Watermarking.