

1. Record Nr.	UNISA996466200103316
Titolo	Network and System Security [[electronic resource]] : 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings // edited by Joseph K. Liu, Xinyi Huang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-36938-2
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (xiii, 731 pages) : illustrations
Collana	Security and Cryptology ; ; 11928
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer organization Artificial intelligence Application software Systems and Data Security Cryptology Computer Systems Organization and Communication Networks Artificial Intelligence Information Systems Applications (incl. Internet)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Invited Papers -- Measuring Security of Symmetric Encryption Schemes against On-the-Fly Side-Channel Key-Recovery Attacks -- Unsupervised Insider Detection through Neural Feature Learning and Model Optimisation -- Dynamic Searchable Symmetric Encryption with Forward and Backward Privacy: A Survey -- A Graph Database-based Approach to Analyze Network Log Files -- Full Papers -- A Privacy-Enhancing Framework for Internet of Things Services -- Using Audio Characteristics for Mobile Device Authentication -- Ethereum Analysis via Node Clustering -- Strong Known Related-Key Attacks and the Security of ECDSA -- Threat Assessment of Enterprise Applications via Graphical Modelling -- A Blockchain-based IoT Data Management System for Secure and Scalable Data Sharing -- Towards Secure Open

Banking Architecture: An Evaluation with OWASP -- OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zooms -- OVERSCAN: OAuth 2.0 Scanner for Missing Parameters -- LaT-Voting: Traceable Anonymous E-Voting on Blockchain -- Distributed Secure Storage System Based on Blockchain and TPA -- SSHTDNS: A Secure, Scalable and High-Throughput Domain Name System via Blockchain Technique -- A Practical Dynamic Enhanced BFT protocol -- Pre-adjustment Based Anti-collusion Mechanism for Audio Signals -- Detecting Intruders by User File Access Patterns -- Blockchain-enabled Privacy-preserving Internet of Vehicles: Decentralized and Reputation-based Network Architecture -- Privacy Preserving Machine Learning with Limited Information Leakage -- Blockchain based Owner-Controlled Secure Software Updates for Resource-Constrained -- Sequential Aggregate MACs with Detecting Functionality Revisited -- A Novel Approach for Traffic Anomaly Detection in Power Distributed Control System and Substation System -- EEG-based Authentication with Variational Universal Background Model -- An Efficient Vulnerability Detection Model for Ethereum Smart Contracts -- A Comparative Study on Network Traffic Clustering -- Tell Them From Me: an Encrypted Application Profiler -- Indoor Security Localization Algorithm Based on Location Discrimination Ability of AP -- Gnocchi: Multiplexed Payment Channels for Cryptocurrencies -- Difficulty of decentralized structure due to rational user behavior on Blockchain -- A DNS Tunneling Detection method based on Deep Learning models to prevent Data Exfiltration -- Cryptanalysis of Raindrop and FBC -- Attribute Based Encryption with Publicly Verifiable Outsourced Decryption -- New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defense Cost -- Lattice based verifiably encrypted double authentication preventing Signatures -- Privacy-Preserving Sequential Data Publishing -- A Secure and Efficient Privacy-Preserving Authentication Scheme for Vehicular Networks with Batch Verification Using Cuckoo Filter -- Keyed Non-Parametric Hypothesis Tests: Protecting Machine Learning From Poisoning Attacks -- SparkDA: RDD-Based High Performance Data Anonymization Technique for Spark Platform -- Short Papers -- An Efficient Leakage-Resilient Authenticated Group Key Exchange Protocol -- Traceable and Fully Anonymous Attribute Based Group Signature Scheme with Verifier Local Revocation from Lattices -- Privacy-preserving k-means clustering: an application to driving style Recognition -- Derandomized PACE with Mutual Authentication -- A Multi-attributes-based Trust Model of Internet of Vehicle -- Using Sparse Composite Document Vectors to Classify VBA Macros -- A High-Performance Hybrid Blockchain System for Traceable IoT Applications.

Sommario/riassunto

This book constitutes the proceedings of the 13th International Conference on Network and System Security, NSS 2019, held in Sapporo, Japan, in December 2019. The 36 full papers and 7 short papers presented together with 4 invited papers in this book were carefully reviewed and selected from 89 initial submissions. The papers cover a wide range of topics in the field, including authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability of computer networks and systems.
