1.

Record Nr.	UNISA996466314903316
Titolo	Computer Security – ESORICS 2019 [[electronic resource]] : 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I / / edited by Kazue Sako, Steve Schneider, Peter Y. A. Ryan
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-29959-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XXV, 811 p. 628 illus., 132 illus. in color.)
Collana	Security and Cryptology ; ; 11735
Disciplina	005.8
Soggetti	Computer security Computer organization Computers Artificial intelligence Application software Software engineering Systems and Data Security Computer Systems Organization and Communication Networks Computing Milieux Artificial Intelligence Information Systems Applications (incl. Internet) Software Engineering/Programming and Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes Index.
Nota di contenuto	Machine Learning -- Privacy-Enhanced Machine Learning with Functional Encryption -- Towards Secure and Efficient Outsourcing of Machine Learning Classification -- Confidential Boosting with Random Linear Classifiers for Outsourced User-generated Data -- BDPL: A Boundary Differentially Private Layer Against Machine Learning Model Extraction Attacks -- Information Leakage -- The Leakage-Resilience Dilemma -- A Taxonomy of Attacks using BGP Blackholing -- Local Obfuscation Mechanisms for Hiding Probability Distributions -- A First

Look into Privacy Leakage in 3D Mixed Reality Data -- Signatures and Re-encryption -- Flexible Signatures: Making Authentication Suitable for Real-Time Environments -- A Dynamic & Revocable Group Merkle Signature -- Puncturable Proxy Re-Encryption supporting to Group Messaging Service -- Generic Traceable Proxy Re-Encryption and Accountable Extension in Consensus Network -- Side Channels -- Side-Channel Aware Fuzzing -- NetSpectre: Read Arbitrary Memory over Network -- maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults -- Automated Formal Analysis of Side-Channel Attacks on Probabilistic Systems -- Formal Modelling and Verification -- A Formal Model for Checking Cryptographic API Usage in JavaScript -- Contingent Payments on a Public Ledger: Models and Reductions for Automated Verification -- Symbolic Analysis of Terrorist Fraud Resistance -- Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) vs. QUIC -- Attacks -- Where to Look for What You See Is What You Sign? User Confusion in Transaction Security -- On the Security and Applicability of Fragile Camera Fingerprints -- Attacking Speaker Recognition Systems with Phoneme Morphing -- Practical Bayesian Poisoning Attacks on Challenge-based Collaborative Intrusion Detection Networks -- A Framework for Evaluating Security in the Presence of Signal Injection Attacks -- Secure Protocols -- Formalizing and Proving Privacy Properties of Voting Protocols using Alpha-Beta Privacy -- ProCSA: Protecting Privacy in Crowdsourced Spectrum Allocation -- Breaking Unlinkability of the ICAO 9303 Standard for e-Passports using Bisimilarity -- Symmetric-key Corruption Detection : When XOR-MACs Meet Combinatorial Group Testing -- Useful Tools -- Finding Flaws from Password Authentication Code in Android Apps -- Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution -- iCAT: An Interactive Customizable Anonymization Tool -- Monitoring the GDPR -- Blockchain and Smart Contracts -- Incentives for Harvesting Attack in Proof of Work mining pools -- A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses -- Annotary: A Concolic Execution System for Developing Secure Smart Contracts -- PDFS: Practical Data Feed Service for Smart Contracts -- Towards a Marketplace for Secure Outsourced Computations.

Sommario/riassunto

The two volume set, LNCS 11735 and 11736, constitutes the proceedings of the 24th European Symposium on Research in Computer Security, ESORIC 2019, held in Luxembourg, in September 2019. The total of 67 full papers included in these proceedings was carefully reviewed and selected from 344 submissions. The papers were organized in topical sections named as follows: Part I: machine learning; information leakage; signatures and re-encryption; side channels; formal modelling and verification; attacks; secure protocols; useful tools; blockchain and smart contracts. Part II: software security; cryptographic protocols; security models; searchable encryption; privacy; key exchange protocols; and web security.