1. Record Nr. UNINA9910349298403321

Titolo	Computer Security – ESORICS 2019 : 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II / / edited by Kazue Sako, Steve Schneider, Peter Y. A. Ryan
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-29962-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XXVI, 627 p. 803 illus., 71 illus. in color.)
Collana	Security and Cryptology ; ; 11736
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
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Software Security -- Automatically Identifying Security Checks for Detecting Kernel Semantic Bugs -- Uncovering Information Flow Policy Violations in C Programs -- BinEye: Towards Efficient Binary Authorship Characterization Using Deep Learning -- Static Detection of Uninitialized Stack Variables in Binary Code -- Towards Automated Application-Specific Software Stacks -- Cryptographic Protocols -- Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices -- Forward-Secure

Puncturable Identity-Based Encryption for Securing Cloud Emails -- Feistel Structures for MPC, and More -- Arithmetic Garbling from Bilinear Maps -- Security Models -- SEPD: An Access Control Model for Resource Sharing in an IoT Environment -- Nighthawk: Transparent System Introspection from Ring -3 -- Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement -- Enhancing Security and Dependability of Industrial Networks with Opinion Dynamics -- Searchable Encryption -- Dynamic Searchable Symmetric Encryption with Forward and Stronger Backward Privacy -- Towards Efficient Verifiable Forward Secure Searchable Symmetric Encryption -- Generic Multi-keyword Ranked Search on Encrypted Cloud Data -- An Efficiently Searchable Encrypted Data Structure for Range Queries -- Privacy -- GDPiRated - Stealing Personal Information On- and Offline -- Location Privacy-Preserving Mobile Crowd Sensing with Anonymous Reputation -- OCRAM-assisted Sensitive Data Protection on ARM-based Platform -- Privacy-Preserving Collaborative Medical Time Series Analysis based on Dynamic Time Warping -- Key Exchange Protocols -- IoT-friendly AKE: Forward Secrecy and Session Resumption Meet Symmetric-key Cryptography -- Strongly Secure Identity-Based Key Exchange with Single Pairing Operation -- A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope -- Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids -- Web Security -- The Risks of WebGL: Analysis, Evaluation and Detection -- Mime Artist: Bypassing Whitelisting for the Web with JavaScript Mimicry Attacks -- Fingerprint Surface-Based Detection of Web Bot Detectors -- Testing for Integrity Flaws in Web Sessions.

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.