

|                         |  |
|-------------------------|--|
| 1. Record Nr.           | UNINA9910337565503321  |
| Titolo                  | Innovative Security Solutions for Information Technology and Communications : 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers // edited by Jean-Louis Lanet, Cristian Toma   |
| Pubbl/distr/stampa      | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019  |
| ISBN                    | 3-030-12942-X  |
| Edizione                | [1st ed. 2019.]  |
| Descrizione fisica      | 1 online resource (XIII, 530 p. 248 illus., 91 illus. in color.)   |
| Collana                 | Security and Cryptology, , 2946-1863 ; ; 11359   |
| Disciplina              | 005.8  |
| Soggetti                | Data protection<br>Computer networks<br>Computers - Law and legislation<br>Information technology - Law and legislation<br>Software engineering<br>Application software<br>Artificial intelligence<br>Data and Information Security<br>Computer Communication Networks<br>Legal Aspects of Computing<br>Software Engineering<br>Computer and Information Systems Applications<br>Artificial Intelligence   |
| Lingua di pubblicazione | Inglese  |
| Formato                 | Materiale a stampa   |
| Livello bibliografico   | Monografia   |
| Nota di bibliografia    | Includes bibliographical references and index.   |
| Nota di contenuto       | Ultralightweight Cryptography - Some thoughts on ten years of efforts -- Android Malware Analysis: from technical difficulties to scientific challenges -- Post-Quantum Cryptography and a (Qu)Bit More -- Normalization of Java source codes -- HiddenApp - Securing Linux applications using ARM TrustZone -- Security Knowledge Management in Open Source Software Communities -- Formal Security Analysis of Cloud-connected Industrial Control Systems -- A Hybrid Searchable |

Encryption Scheme for Cloud Computing -- Securing Cloud Storage by Transparent Biometric Cryptography -- Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks -- An Evaluation of OCR Systems against Adversarial Machine Learning -- Intrusion detection and classification with autoencoded deep neural network -- Detecting Malicious Windows Commands Using Natural Language Processing Techniques -- Evolutionary Computation Algorithms for Detecting Known and Unknown Attacks -- Assuring Privacy in Surfing the Internet -- Roaming Interface Signaling Security for LTE Networks -- Limited Proxying for Content Filtering Based on X.509 Proxy Certificate Profile -- Anomaly-based Network Intrusion Detection using Wavelets and Adversarial Autoencoders -- Analysis and Evaluation of Dynamic Feature-based Malware Detection Methods -- Trends in design of ransomware viruses -- Efficient Implementation of the SHA-512 Hash Function for 8-bit AVR Microcontrollers -- Secure IoT Supply Chain Management Solution using Blockchain and Smart Contracts Technology -- ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT using Blockchain Technology -- Development of the unified security requirements of PUFs during the standardization process -- A PUF-based Destructive-private Mutual Authentication RFID Protocol -- Weakened Random Oracle Models with Target Prefix -- An Improved Algorithm for Iterative Matrix-Vector Multiplications over Finite Fields -- On the security of Jhanwar-Barua Identity-Based EncryptionScheme -- Vulnerabilities of the McEliece variants based on Polar codes -- Binary Data Analysis for Source Code Leakage Assessment -- Zero in and TimeFuzz: Detection and Mitigation of Cache Side-Channel Attacks -- A Comparison of the Homomorphic Encryption Libraries HElib, SEAL and FV-NFLlib -- A New DNA-Combining Chaos Scheme for Fast and Secure Image Encryption -- Implementing Searchable Encryption schemes over Multilinear Maps -- A Unified Security Perspective on Legally Fair Contract Signing Protocols -- Relating different Polynomial-LWE problems -- Monoidal encryption over  $(\mathbb{F}_2, \cdot)$  -- Geometric pairwise key-sharing scheme.

---

#### Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the 11th International Conference on Security for Information Technology and Communications, SecITC 2018, held in Bucharest, Romania, in November 2018. The 35 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 70 submissions. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.

---