1.	Record Nr.	UNINA9910595060103321
	Titolo	Applied Cryptography and Network Security Workshops : ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Rome, Italy, June 20–23, 2022, Proceedings / / edited by Jianying Zhou, Sridhar Adepu, Cristina Alcaraz, Lejla Batina, Emiliano Casalicchio, Sudipta Chattopadhyay, Chenglu Jin, Jingqiang Lin, Eleonora Losiouk, Suryadipta Majumdar, Weizhi Meng, Stjepan Picek, Jun Shao, Chunhua Su, Cong Wang, Yury Zhauniarovich, Saman Zonouz
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
	ISBN	9783031168154 3031168151
	Edizione	[1st ed. 2022.]
	Descrizione fisica	1 online resource (630 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13285
	Disciplina	005.8
	Soggetti	Data protection Computer engineering Computer networks Computers Cryptography Data encryption (Computer science) Computer networks - Security measures Data and Information Security Computer Engineering and Networks Computing Milieux Cryptology Mobile and Network Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	AIBlock – Application Intelligence and Blockchain Security -- Universal Physical Adversarial Attack via Background Image -- Efficient Verifiable Boolean Range Query for Light Clients on Blockchain Database -- SuppliedTrust: A Trusted Blockchain Architecture for Supply Chains --

Towards Interpreting Vulnerability of Object Detection Models via Adver [1]sarial Distillation -- Vulnerability Detection for Smart Contract via Backward Bayesian Active Learning -- A Multi-Agent Deep Reinforcement Learning-Based Collaborative -- Hybrid Isolation Model for Device Application Sandboxing Deployment in Zero Trust Architecture -- AIHWS – Artificial Intelligence in Hardware Security -- On the Effect of Clock Frequency on Voltage and Electromagnetic Fault Injection -- S-box Pooling: Towards More Efficient Side-Channel Security Evaluations -- Deep Learning-based Side-channel Analysis against AES Inner Rounds -- A side-channel based disassembler for the ARM-Cortex M0 -- Towards Isolated AI Acceleratorswith OP-TEE on SoC-FPGAs -- Order Vs. Chaos: Multi-trunk classifier for side-channel attack -- AIoTS – Artificial Intelligence and Industrial IoT Security -- Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434 -- Output Prediction Attacks on Block Ciphers using Deep Learning -- HolA: Holistic and Autonomous Attestation for IoT Networks -- CIMSS – Critical Infrastructure and Manufacturing System Security -- The Etiology of Cybersecurity -- Outsider Key Compromise Impersonation Attack on a Multi-Factor Authenticated Key Exchange Protocol -- Toward Safe Integration of Legacy SCADA Systems in the Smart Grid -- Cloud S&P – Cloud Security and Privacy -- RATLS: Integrating Transport Layer Security with Remote Attestation -- DLPFS: The Data Leakage Prevention FileSystem -- Privacy-preserving record linkage using local sensitive hash and private set intersection -- SCI – Secure Cryptographic Implementation -- UniqueChain: Achieving (Near) Optimal Transaction Settlement Time via Single Leader Election -- PEPEC: Precomputed ECC Points Embedded in Certificates and Verified by CT Log Servers -- Efficient Software Implementation of GMT-672 and GMT8-542 PairingFriendly Curves for a 128-bit Security Level -- SecMT – Security in Mobile Technologies -- Leaky Blinders: Information Leakage in Mobile VPNs -- Instrumentation Blueprints: Towards Combining Several Android Instrumentation Tools -- SiMLA – Security in Machine Learning and its Applications -- A Siamese Neural Network for scalable Behavioral Biometrics Authentication -- A methodology for training homomorphic encryption friendly neural networks -- Scalable and Secure HTML5 Canvas-Based User Authentication -- Android Malware Detection Using BERT -- POSTERS -- POSTER: A Transparent Remote Quantum Random Number Generator Over a Quantum-Safe Link -- POSTER: Enabling User-Accountable Mechanisms in Decision Systems -- POSTER: Key Generation Scheme Basedon Physical Layer -- POSTER: ODABE: Outsourced Decentralized CP-ABE in Internet of Things -- POSTER: Ransomware detection mechanism – current state of the project.

Sommario/riassunto

This book constitutes the proceedings of the satellite workshops held around the 20th International Conference on Applied Cryptography and Network Security, ACNS 2022, held in Rome, Italy, in June 2022. Due to the Corona pandemic the workshop was held as a virtual event. The 31 papers presented in this volume were carefully reviewed and selected from 52 submissions. They stem from the following workshops: – AIBlock: 4th ACNS Workshop on Application Intelligence and Blockchain Security – AIHWS: 3rd ACNS Workshop on Artificial Intelligence in Hardware Security – AIoTS: 4th ACNS Workshop on Artificial Intelligence and Industrial IoT Security – CIMSS: 2nd ACNS Workshop on Critical Infrastructure and Manufacturing System Security – Cloud S&P: 4th ACNS Workshop on Cloud Security and Privacy – SCI: 3rd ACNS Workshop on Secure Cryptographic Implementation – SecMT: 3rd ACNS Workshop on Security in Mobile Technologies – SiMLA: 4th ACNS