

1. Record Nr.	UNISA996418208503316
Titolo	Information and Communications Security [[electronic resource]] : 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers // edited by Jianying Zhou, Xiapu Luo, Qingni Shen, Zhen Xu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-41579-1
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XVII, 833 p. 279 illus., 167 illus. in color.)
Collana	Security and Cryptology ; ; 11999
Disciplina	005.8
Soggetti	Data structures (Computer science) Data protection Computer communication systems Application software Computers Computers - Law and legislation Software engineering Data Structures and Information Theory Security Computer Communication Networks Information Systems Applications (incl. Internet) Legal Aspects of Computing Software Engineering/Programming and Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Prototype-based malware traffic classification with novelty detection -- Evading API Call Sequence Based Malware Classifiers -- UBER: Combating Sandbox Evasion via User Behavior Emulators -- AADS: A Noise-Robust Anomaly Detection Framework for Industrial Control Systems -- Maged Abdelaty, Roberto Doriguzzi-Corin and Domenico Siracusa Characterizing Internet-scale ICS Automated Attacks through Long-term Honeypot Data -- Cloning Vulnerability Detection in Driver

Layer of IoT Devices -- Impact of Multiple Reflections on Secrecy
 Capacity of Indoor VLC System -- Road Context-aware Intrusion
 Detection System for Autonomous Cars -- Enterprise Network Security
 -- Automated Cyber Threat Intelligence Reports Classification for Early
 Warning of Cyber Attacks in Next Generation SOC -- HeteroUI: A
 Framework Based on Heterogeneous Information Network Embedding
 for User Identification in Enterprise Networks -- CTLM: Continuous-
 Temporal Lateral Movement Detection Using Graph Embedding --
 VulfHunter: An Automated Vulnerability Detection System based on
 Deep Learning and Bytecode -- Deep Learning-Based Vulnerable
 Function Detection: A Benchmark -- Automatic Demirci-Selcuk Meet-
 in-the-Middle Attack on SKINNY with Key-bridging -- SecFlush: A
 Hardware/Software Collaborative Design for Real-Time Detection and
 Defense against Flush-Based Cache Attacks -- CDAE: Towards
 Empowering Denoising in Side-Channel Analysis -- Practical Evaluation
 Methodology of Higher-order -- Maskings at Different Operating
 Frequencies -- Privacy-Preserving eID Derivation for Self-Sovereign
 Identity Systems -- Provably Secure Group Authentication in the
 Asynchronous Communication Model -- AGE: Authentication Graph
 Embedding for Detecting Anomalous Login Activities -- A Multi-group
 Signature Scheme from Lattices -- Ciphertext Policy Attribute-Based
 Encryption for Circuits from LWE Assumption -- Using Equivalent Class
 to Solve Interval Discrete Logarithm Problem -- Parallel Steepest Ascent
 Hill-Climbing for High Nonlinear Boolean and Vectorial Boolean
 Functions (S-Boxes) -- Accelerating SM2 Digital Signature Algorithm
 using Modern Processor Features -- Improved Differential Attacks on
 GIFT-64 -- Adaptively Secure Puncturable Pseudorandom Functions via
 Puncturable Identity-Based KEMs -- Context-aware IPv6 Address
 Hopping -- Towards Homograph-confusable Domain Name Detection
 using Dual-channel CNN -- FraudJugger: Fraud Detection on Digital
 Payment Platforms with Fewer Labels -- Cloud CoT: A Blockchain-based
 Cloud Service Dependency Attestation Framework -- An Adversarial
 Attack Based on Multi-Objective Optimization in the Neuron Selecting:
 Defending against Adversarial Examples in Deep Neural Networks --
 Capturing the Persistence of Facial Expression Features for Deepfake --
 Video Detection -- Differentially Private Frequent Itemset Mining
 against Incremental Updates -- Privacy-Preserving Distributed Machine
 Learning based on Secret Sharing -- Privacy-preserving Decentralised
 Singular Value Decomposition -- WSLD: Detecting Unknown Webshell
 Using Fuzzy Matching and Deep Learning -- A Character-Level BiGRU-
 Attention For Phishing Classification -- Tear O Your Disguise: Phishing
 Website Detection using Visual and Network Identities --
 Steganography and Steganalysis -- Hierarchical Representation
 Network for Steganalysis of QIM Steganography in Low-Bit-Rate Speech
 Signals -- Convolutional Neural Network based Side-Channel Attacks
 with Customized Filters -- DL chain: a Covert Channel over Blockchain
 based on Dynamic Labels.

Sommario/riassunto

This book constitutes the refereed proceedings of the 21th
 International Conference on Information and Communications Security,
 ICICS 2019, held in Beijing, China, in December 2019. The 47 revised
 full papers were carefully selected from 199 submissions. The papers
 are organized in topics on malware analysis and detection, IoT and CPS
 security enterprise network security, software security, system security,
 authentication, applied cryptograph internet security, machine learning
 security, machine learning privacy, Web security, steganography and
 steganalysis.

2. Record Nr.	UNINA9910894665703321
Titolo	Bemerkungen ... des Landesrechnungshofs Schleswig-Holstein : mit Bericht zur Landeshaushaltsrechnung ... und Stellungnahme ... zur Planung Landesregierung vom ... zum Abbau des strukturellen Finanzdefizits bis .
Pubbl/distr/stampa	Kiel, : Landesrechnungshof Schleswig-Holstein, 1999-
Descrizione fisica	Online-Ressource
Disciplina	340 330
Soggetti	Zeitschrift Haushaltsplan
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Periodico
Note generali	Erscheint jährlich Gesehen am 26.08.2020