| | | |
|---|---|---|
| 1. | Record Nr. | UNISA996635664203316 |
| | Autore | Patil Vishwas T |
| | Titolo | Information Systems Security : 20th International Conference, ICISS 2024, Jaipur, India, December 16–20, 2024, Proceedings / / edited by Vishwas T. Patil, Ram Krishnan, Rudrapatna K. Shyamasundar |
| | Pubbl/distr/stampa | Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025 |
| | ISBN | 9783031800207<br>3031800206 |
| | Edizione | [1st ed. 2025.] |
| | Descrizione fisica | 1 online resource (501 pages) |
| | Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 15416 |
| | Altri autori (Persone) | KrishnanRam<br>ShyamasundarRudrapatna K |
| | Disciplina | 005.8 |
| | Soggetti | Data protection<br>Computer engineering<br>Computer networks<br>Data and Information Security<br>Computer Engineering and Networks<br>Computer Communication Networks |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Nota di contenuto | -- System Security.  -- Microarchitectural Security of Firecracker VMM for Serverless Cloud Platforms.  -- An OS support for Tamper-resistant Software Execution Using Empty Interruptions.  -- S-RFUP: Secure Remote Firmware Update Protocol.  -- Securing Virtual Reality Apps Inter-Process Communication.  -- Network Security.  -- Securing the Web: Analysis of HTTP Security Headers in Popular Global Websites.  -- Countering Subscription Concealed Identifier (SUCI)-Catchers in Cellular Communications.  -- BP-MAP: A Secure and Convenient Mutual Authentication Protocol.  -- Effects of Soft-Domain Transfer and Named Entity Information on Deception Detection.  -- Paving the Way: Advancing V2X Safety Through Innovative Attack Generation and Analysis Framework (V2X-SAF).  -- From Traits to Threats: Learning Risk Indicators of Malicious Insider using Psychometric Data.  -- Identifying Insecure Network Configurations through Attack Modeling and Explainable AI.  -- QIris: Quantum Implementation of Rainbow |

Table Attacks.  -- Malware and Vulnerability Detection.  -- Insights from Running 24 Static Analysis Tools on Open Source Software Repositories.  -- REMEDII: Robust Malware Detection with Iterative and Intelligent Adversarial Training using GANs.  -- Semantics-Based Static Vulnerability Detection of Solidity Using Abstract Interpretation.  -- Privacy & Usability.  -- Web Privacy Perceptions Amongst Indian Users. -- Enabling Privacy in IT Service Operations.  -- Privacy-Preserving Photo Sharing: An SSI Use Case.  -- Zone Recovery Attack on a Secure Privacy-Preserving Ride-Matching Protocol.  -- Making EULA Great Again: A Novel Nudge Mechanism to Improve Readability, User Attention and Awareness.  -- A Decoupling Mechanism for Transaction Privacy.  -- AI Security.  -- Protecting ownership of trained DNN models with Zero-Knowledge Proofs.  -- MALAI: ML-based Attack on Learning With Error problem.  -- Patch based backdoor attack on Deep Neural Networks.  -- Industry Demo/Practice.  -- Integrating Crypto-Based Payment Systems for Data Marketplaces: Enhancing Efficiency, Security, and User Autonomy.  -- Ontologies for WAF configurations: when knowledge-graphs help troubleshooting.  -- IntelliSOAR: Intelligent Alert Enrichment using Security Orchestration Automation and Response (SOAR).  -- InTrust: An Asset Monitoring, Analysis and Vulnerability Assessment system for Zero Trust Network.

| Sommario/riassunto | This book constitutes the refereed proceedings of the 20th International Conference on Information Systems Security, ICISS 2024, held in Jaipur, India, during December 16–20, 2024. The 18 full papers and 6 short papers included in this book were carefully reviewed and selected from 93 submissions. They were organized in topical sections as follows: System Security; Network Security; Attack; Malware and Vulnerability Detection; Privacy & Usability; AI Security; and Industry Demo/Practice. |