1. Record Nr. UNINA9910887888703321

| | |
|---|---|
| Titolo | Advances in Information and Computer Security : 19th International Workshop on Security, IWSEC 2024, Kyoto, Japan, September 17–19, 2024, Proceedings / / edited by Kazuhiko Minematsu, Mamoru Mimura |
| Pubbl/distr/stampa | Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024 |
| ISBN | 981-9777-37-2 |
| Edizione | [1st ed. 2024.] |
| Descrizione fisica | 1 online resource (310 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 14977 |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Application software<br>Computers<br>Computer networks<br>Data and Information Security<br>Computer and Information Systems Applications<br>Computing Milieux<br>Computer Communication Networks |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | -- Authenticated Encryption. -- Bit-wise Analysis for Forgery Attacks on AES-based AEAD Schemes. -- Cryptanalysis of Authenticated Encryption Modes for Wireless and Real-Time Systems. -- Symmetric-key Cryptanalysis. -- Higher-order Mixture Differentials for AES-based Block Ciphers and Applications to TweAES. -- Weak Keys of the Full MISTY1 Recovered in Practical Time. -- Protocols. -- Efficient Card-Based Protocols with a Standard Deck of Playing Cards Using Partial Opening. -- Attribute-Based Inner Product Functional Encryption in Key-Policy Setting from Pairing. -- Analysis of Public-key Cryptosystems. -- Formal Verification of Emulated Floating-Point Arithmetic in Falcon. -- Experimental Analysis of Integer Factorization Methods Using Lattices. -- Sieving Method for SDP with the Zero Window: An Improvement in Low Memory Environments. -- Vulnerability. -- Race condition vulnerabilities in WordPress plug-ins. -- Finding (and exploiting) vulnerabilities on IP Cameras: the Tenda |

CP3 case study. -- Malware Countermeasure. -- File System Shield (FSS): A Pass-Through Strategy Against Unwanted Encryption in Network File Systems. -- Implementation for Malicious Software using ChatGPT-4. -- A Markov Game Model for Evaluating Cybersecurity Attacks on Cloud. -- Network Security and Privacy. -- Few Edges Are Enough: Few-Shot Network Attack Detection with Graph Neural Networks. -- Information Leakage through Packet Lengths in RTC Traffic. -- A Study on Anonymization through Participation in iPWS Cup 2023.

Sommario/riassunto

This book constitutes the proceedings of the 19th International Workshop on Security on Advances in Information and Computer Security, IWSEC 2024, held in Kyoto, Japan, in September 17-19, 2024. The 14 full papers and 3 short papers were carefully reviewed and selected from 47 submissions. These papers were categorized into the following sections: authenticated encryption; symmetric-key cryptanalysis; protocols; analysis of public-key cryptosystems; vulnerability; malware countermeasure; network security and privacy.