| | |
|---|---|
| 1. Record Nr. | UNISA996490353803316 |
| Titolo | Computer security - ESORICS 2022 . Part II : 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26-30, 2022, proceedings / / Vijayalakshmi Atluri [and three others] |
| Pubbl/distr/stampa | Cham, Switzerland : , : Springer, , [2022]<br>©2022 |
| ISBN | 3-031-17146-2 |
| Descrizione fisica | 1 online resource (753 pages) |
| Collana | Lecture Notes in Computer Science |
| Disciplina | 005.8 |
| Soggetti | Computer networks - Security measures<br>Computer security |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Intro -- Preface -- Organization -- Contents - Part II -- Anonymity -- A Machine Learning Approach to Detect Differential Treatment of Anonymous Users -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Collection and Labeling of Training Data -- 3.2 Feature Selection -- 3.3 Classifier Training and Tuning -- 4 Results: Differential Treatment of Tor Users -- 4.1 Data Collection -- 4.2 Block Rates by Visit Type -- 4.3 Block Rates by Characteristics of Tor Exit Nodes -- 4.4 Block Rates by Characteristics of Web Sites -- 4.5 CAPTCHA Rates -- 5 Limitations -- 6 Conclusion -- A Classifier Performance -- B Labeling -- C Block Rates for Subsites and Searches -- References -- Utility-Preserving Biometric Information Anonymization -- 1 Introduction -- 2 Basic Concepts and Problem Statement -- 2.1 Basic Concepts -- 2.2 Problem Statement -- 2.3 Attack Model -- 3 Rationale of Approach -- 4 Methodology -- 4.1 Dynamically Assembled Random Set -- 4.2 Selective Weighted Mean-Based Transformation -- 5 Experimental Evaluation -- 5.1 Experimental Setup -- 5.2 Results -- 6 Related Work -- 7 Conclusions -- References -- Anonymous Traceback for End-to-End Encryption -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Definitions and Security Models -- 2.1 Anonymous Traceback Syntax -- 2.2 Security Model -- 3 Warm-Up: Anonymous Path Traceback -- |

Methodology -- 4 MLBAC Administration Prototype -- 4.1 System for MLBAC Administration Experimentation -- 4.2 Symbolic and Non-symbolic ML Models -- 4.3 Administration Strategies in MLBAC -- 5 Evaluation -- 5.1 Evaluation Methodology -- 5.2 Results -- 6 Conclusion -- A  Additional AAT Generation -- B  Data Generation -- C Dataset Visualization -- D  List of Simulated Task and Criteria -- References.

Real-Time Policy Enforcement with Metric First-Order Temporal Logic -- 1 Introduction -- 2 Related Work -- 3 Policy Enforcement -- 4 Metric First-Order Temporal Logic -- 5 MFOTL Enforceability -- 6 MFOTL Enforcement in the Finite Case -- 6.1 Monitoring MFOTL Formulae -- 6.2 Enforcer -- 6.3 Correctness and Transparency -- 7 Implementation -- 8 Evaluation -- 9 Conclusion -- A  Evaluation Data -- References -- A Tale of Four Gates -- 1 Introduction -- 1.1 Contributions -- 1.2 Responsible Disclosure -- 2 Background -- 3 Related Work -- 4 Analysis of App Components Across User Profiles -- 5 Analysis of Sensor Background Access -- 5.1 Stealthy Background Spyware -- 6 Evaluation -- 6.1 Four Gates Inspector -- 6.2 Real-World Tests -- 6.3 Evaluation and Results -- 6.4 Limitations -- 7 Discussion and Mitigation -- 8 Conclusion -- 9  Appendix -- References -- Authentication -- Sequential Digital Signatures for Cryptographic Software-Update Authentication -- 1 Introduction -- 2 Notation -- 3 Stateless Signatures -- 3.1 Digital Signatures: DS -- 3.2 Strictly One-Time Digital Signatures: SOT-DS -- 4 Sequential Digital Signatures: SDS -- 5 Constructions -- 5.1 Hash Function Based SOT-DS -- 5.2 SDS from SOT-DS -- 6 Implementation and Evaluation -- A  Extractors -- References -- On Committing Authenticated-Encryption -- 1 Introduction -- 2 Preliminaries -- 3 Committing AE -- 4 The CTX Construction -- 5 Commitment Security of GCM and OCB -- 6 Other Committing AE Notions -- References -- Quantum-Resistant Password-Based Threshold Single-Sign-On Authentication with Updatable Server Private Key -- 1 Introduction -- 1.1 Motivation -- 1.2 Contributions -- 2 Preliminaries -- 2.1 Lattices, SIS, and DRLWE -- 2.2 Distributed Key Generation Protocol Over Lattices -- 2.3 Threshold Homomorphic Aggregate Signatures Over Lattices -- 2.4 Oblivious Pseudorandom Function Over Lattices.

3 Basic Scheme Architecture and Security Model -- 3.1 Password-Based Threshold SSO Authentication -- 3.2 Security Model -- 4 Quantum-Resistant Password-Based Threshold Single-Sign-On Authentication with Secret Update -- 5 Security Analysis -- 6 Efficiency Analysis and Protocol Comparison -- 7 Conclusion and Future Work -- A  Security of TOPRF -- B  Proof of Theorem 1 -- References -- The Revenge of Password Crackers: Automated Training of Password Cracking Tools -- 1 Introduction -- 2 Background and Related Work -- 3 Building a Reliable Password Dataset -- 3.1 Dataset Analysis -- 4 Dictionaries with Off-the-Shelf Rules -- 5 Training Masks -- 6 Training Rules -- 7 Conclusion -- References -- Fuzzy Authenticated Key Exchange with Tight Security -- 1 Introduction -- 2 Preliminary -- 3 Fuzzy Authenticated Key Exchange -- 3.1 Definition of Fuzzy Authenticated Key Exchange -- 3.2 Security Model of FAKE -- 4 Our FAKE Scheme -- 5 Security Proof of FAKE -- 6 Instantiation of Our FAKE Construction -- A Figure5: The Security Experiment ExpFAKE,,,A for FAKE -- B Figure6: The Security Games G0-G6 for FAKE -- References -- Continuous Authentication in Secure Messaging -- 1 Introduction -- 1.1 Contributions -- 1.2 Further Related Work -- 2 Continuous Authentication -- 2.1 Messaging Schemes -- 2.2 Security Game -- 3 Introducing Authentication Steps -- 3.1 Recording Ciphertexts -- 3.2 Authentication Steps -- 3.3 Detecting Compromised Long-Term

Secrets -- 4 Security of the Authentication Steps Protocol -- 5 Implementation and Benchmarks -- 6 Observations on the Official Implementation -- 7 Conclusion -- A  Security of the Authentication Steps Protocol -- A.1  Upper Bound for False Negatives -- A.2  Upper Bound for False Positives -- References -- Digital Signatures -- Half-Aggregation of Schnorr Signatures with Tight Reductions -- 1 Introduction -- 1.1 Contributions.
2 Preliminaries.