1. Record Nr. UNINA9910886989703321

Autore	Garcia-Alfaro Joaquin
Titolo	Computer Security – ESORICS 2024 : 29th European Symposium on Research in Computer Security, Bydgoszcz, Poland, September 16–20, 2024, Proceedings, Part IV / / edited by Joaquin Garcia-Alfaro, Rafa Kozik, Micha Chora, Sokratis Katsikas
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-70903-9
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (495 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14985
Altri autori (Persone)	KozikRafa ChorasMicha KatsikasSokratis
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Computer networks - Security measures Computer networks Computer systems Data and Information Security Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer System Implementation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part IV -- Attacks and Defenses -- Cips: The Cache Intrusion Prevention System -- 1 Introduction -- 2 Background -- 3 Cache Attack Detection Overview and Open Challenges -- 4 CIPS in a Nutshell -- 4.1 Attacker Model -- 4.2 Attack Detection -- 4.3 Attack Prevention -- 5 Evaluation -- 5.1 Evaluation Setup -- 5.2 Security Analysis -- 5.3 Performance -- 5.4 Hardware Implementation -- 6 Conclusion -- A Comparison to Related

-- 2 Background and Related Work -- 3 Problem Statement -- 4 Model Definition -- 5 Experimental Setup -- 5.1 Modified CybORG -- 5.2 Experimental Scenarios -- 6 Results -- 7 Conclusion -- A Reduction of Action Space -- B Configuration of Hyperparamters -- C Rewards Definition -- References -- Revoke: Mitigating Ransomware Attacks Against Ethereum Validators -- 1 Introduction -- 2 Background and Motivation -- 3 Revoke Design -- 3.1 Decentralised Key Revocation -- 3.2 Threat Model -- 3.3 Revocation Overview -- 4 Revocation Algorithms -- 4.1 Chain Level -- 4.2 View Level -- 4.3 Ethereum Implementation -- 5 Correctness -- 5.1 Preliminaries -- 5.2 Revoke Definitions -- 5.3 Safety -- 5.4 Liveness -- 6 Revocation Incentives -- 7 Related Work -- 8 Conclusions -- A Appendix -- A.1 Safety -- A.2 Liveness -- References -- Exploiting Layerwise Feature Representation Similarity For Backdoor Defence in Federated Learning -- 1 Introduction -- 2 Background -- 2.1 Centered Kernel Alignment -- 3 FedAvgCKA Design -- 3.1 Design Challenges -- 3.2 Implementation -- 4 Experimental Setup -- 5 Experimental Results -- 6 Related Work -- 7 Conclusion -- A Appendix A: FedAvgCKA Algorithm -- References -- Miscellaneous.
Automatic Verification of Cryptographic Block Function Implementations with Logical Equivalence Checking.

Sommario/riassunto

This four-volume set LNCS 14982-14985 constitutes the refereed proceedings of the 29th European Symposium on Research in Computer Security, ESORICS 2024, held in Bydgoszcz, Poland, during September 16–20, 2024. The 86 full papers presented in these proceedings were carefully reviewed and selected from 535 submissions. They were organized in topical sections as follows: Part I: Security and Machine Learning. Part II: Network, Web, Hardware and Cloud; Privacy and Personal Datat Protection. Part III: Software and Systems Security; Applied Cryptopgraphy. Part IV: Attacks and Defenses; Miscellaneous.