

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

Work -- References -- ReminISCence: Trusted Monitoring Against Privileged Preemption Side-Channel Attacks -- 1 Introduction -- 2 Background -- 2.1 Privileged Side-Channel Attacks -- 2.2 Hardware Performance Monitor -- 2.3 RISC-V Infrastructures -- 3 System Design -- 3.1 Threat Model -- 3.2 ReminISCence Overview -- 4 Implementation -- 4.1 ReminISCing over Side-Channel Vectors on RISC-V -- 4.2 Sampling Facility -- 4.3 Trusted Scheduling -- 5 Evaluation -- 5.1 Monitoring Preemption Attacks -- 5.2 Overhead -- 5.3 Security Discussion -- 6 Related Work -- 7 Conclusion -- References -- A Plug-and-Play Long-Range Defense System for Proof-of-Stake Blockchains -- 1 Introduction -- 2 Preliminaries -- 3 Protocol Description -- 4 Construction of InPoSW -- 4.1 Challenges of Constructing InPoSW -- 4.2 Construction Overview -- 5 Construction of Bootstrap Against Long-Range Attacks -- 5.1 Security -- 6 Performance Estimation with Concrete Parameters -- 7 Related Works -- A Formal Proofs -- References -- Leveraging Hierarchies: HMCAT for Efficiently Mapping CTI to Attack Techniques -- 1 Introduction -- 2 Related Work -- 2.1 Cyber Threat Intelligence -- 2.2 Mapping of Cyber Threat Intelligence -- 3 Method -- 3.1 Processing Step -- 3.2 Hierarchical Mapping of CTI -- 4 Results and Discussion -- 4.1 Main Results -- 4.2 Contribution of Components -- 5 Limitations -- 6 Conclusions and Future Work.

A The Comparison of Dataset Distributions -- B Experimental Setup -- B.1 Datasets and Evaluation Metrics -- B.2 Implementation Details -- References -- Duplication-Based Fault Tolerance for RISC-V Embedded Software -- 1 Introduction -- 2 Related Work -- 3 Protection by Fault Injection Emulation -- 4 Debugger-Driven FI Testing -- 5 Debug Specification Extension -- 6 Code Hardening Tool -- 7 Implementation -- 8 Evaluation -- 9 Conclusion -- References -- Similar Data is Powerful: Enhancing Inference Attacks on SSE with Volume Leakages -- 1 Introduction -- 2 The Proposed Attacks -- 2.1 Intuition -- 2.2 VolScore -- 2.3 RefVolScore -- 2.4 ClusterVolScore -- 3 Experimental Evaluation -- 3.1 Methodology -- 3.2 Results -- 4 Conclusion -- References -- SAEG: Stateful Automatic Exploit Generation -- 1 Introduction -- 1.1 Challenges from Modern Protection Mechanisms -- 1.2 Our Solutions -- 2 Background -- 3 Design -- 3.1 Methodology -- 3.2 Architecture -- 3.3 Example -- 4 Implementation -- 5 Evaluation -- 6 Discussion -- 7 Related Works -- 7.1 AEG -- 7.2 Path Exploration -- 8 Conclusion -- References -- IntentObfuscator: A Jailbreaking Method via Confusing LLM with Prompts -- 1 Introduction -- 1.1 Our Contributions -- 2 Related Work -- 3 Problem Definition -- 3.1 Definition of Successful Prompt Attack -- 3.2 Assumptions on LLM Vulnerability to Query Obfuscation -- 4 Methodology -- 4.1 Obscure Intention -- 4.2 Create Ambiguity -- 5 Experiments and Analysis -- 5.1 Experiment Environment -- 5.2 Datasets Preparation -- 5.3 Evaluation Metrics -- 5.4 Results Analysis of Jailbreak Attack -- 6 Possible Mitigation Strategies for Prompt Injection Attacks -- 7 Conclusion -- References -- Breaking Through the Diversity: Encrypted Video Identification Attack Based on QUIC Features -- 1 Introduction -- 2 Related Work -- 3 Threat Model and Challenges -- 3.1 Threat Model. 3.2 Challenges -- 4 Methodology -- 4.1 Constructing the Key-Value Structured Real Fingerprint Database -- 4.2 Obtaining Accurate Transmission Fingerprints -- 4.3 Implementing Efficient Video Identification -- 5 Evaluation -- 5.1 Dataset -- 5.2 Experimental Setup -- 5.3 Closed-World Analysis -- 5.4 Open-World Analysis -- 5.5 Comparison with Relevant Studies -- 6 Mitigation -- 7 Conclusion -- A Impact of the QUIC-Based Correction -- B Experimental Setup -- B.1 Correction Parameters , , and p -- B.2 HMM Probability Matrix A and B

-- C Open-World Thresholds -- References -- Patronum: In-network Volumetric DDoS Detection and Mitigation with Programmable Switches -- 1 Introduction -- 2 Background and Motivation -- 2.1 Programmable Switches and Count-Min Sketch -- 2.2 Motivating Patronum -- 3 Design of Patronum -- 3.1 Overview -- 3.2 High Frequency Periodic In-Network Measurement -- 3.3 Entropy Difference Based DDoS Detection -- 3.4 In-Network Source-Based Bandwidth Monitor -- 4 Implementation and Evaluation -- 4.1 Methodology -- 4.2 EDM Approximation Accuracy and Micro Benchmarks -- 4.3 Many-to-Few Attacks -- 4.4 Few-to-Few Attacks -- 5 Discussion -- 6 Related Work -- 7 Conclusion -- A Derivation of Entropy Reformulation -- References -- Wherever I May Roam: Stealthy Interception and Injection Attacks Through Roaming Agreements -- 1 Introduction -- 2 Background -- 2.1 Lawful Interception Interfaces and Regulations -- 2.2 Roaming in 5G -- 3 Attacker Model -- 4 Attacks on 5G Roaming -- 4.1 Exploiting the System -- 4.2 Network Name Displayed on UE -- 4.3 Authentication Vector Abuse -- 4.4 Network Traffic Rerouting -- 5 Mitigations -- 5.1 Mitigating the Root Cause -- 5.2 Trust Chain Visibility -- 5.3 Proof of Location -- 5.4 Indicators of Roaming Abuse -- 5.5 Responsible Disclosure -- 6 Related Work -- 7 Conclusion -- A Appendix -- References.

It is Time To Steer: A Scalable Framework for Analysis-Driven Attack Graph Generation -- 1 Introduction -- 2 Preliminaries -- 3 Overview of Our Approach -- 4 StatAG: Statistically Significant Generation -- 4.1 StatAG Validation -- 5 SteerAG: Steered Generation and Analysis -- 5.1 SteerAG Validation -- 6 Case Study Evaluation -- 6.1 Application to Large Real Networks -- 6.2 Coverage of Attack Path Analyses -- 7 Related Work -- 8 Discussion and Concluding Remarks -- A Query Stringency Analysis -- References -- Resilience to Chain-Quality Attacks in Fair Separability -- 1 Introduction -- 2 Related Work -- 3 Model -- 3.1 Processes and Network -- 3.2 Cryptography -- 3.3 Secure Broadcast -- 3.4 Byzantine Agreement -- 3.5 State Machine Replication -- 3.6 Fair Separability -- 3.7 Notations -- 4 Safe Implementation -- 4.1 Overview -- 4.2 Ordering Step -- 4.3 Consensus Step -- 4.4 Delivery Step -- 5 Fixing Liveness -- 5.1 Issue with Previous Protocol -- 5.2 Fixing Liveness -- 6 Protocol Analysis -- 6.1 State Machine Replication -- 6.2 Fair Separability -- 6.3 Discussion -- 7 Conclusion -- References -- Leveraging Transformer Architecture for Effective Trajectory-User Linking (TUL) Attack and Its Mitigation -- 1 Introduction -- 2 Related Work -- 2.1 Trajectory-User Linking (TUL) -- 2.2 Location Privacy-Preserving Mechanisms (LPPM) -- 3 TUL-STEOP and Priv-STEOP -- 3.1 Problem Statement and Adversary Model -- 3.2 Overview of the Approach -- 3.3 Preprocessing Steps -- 3.4 Trajectory Representation Learning -- 3.5 Spatio-Temporal Encoder-Only (STEOP) -- 3.6 Training Procedure -- 4 Experimental Evaluation -- 5 Conclusion and Future Work -- A Multi-resolution Vocabulary Construction -- References -- VFLIP: A Backdoor Defense for Vertical Federated Learning via Identification and Purification -- 1 Introduction -- 2 Preliminaries -- 2.1 Vertical Federated Learning. -- 2.2 Backdoor Attacks in VFL -- 2.3 Threat Model -- 3 Method -- 3.1 MAE Training -- 3.2 VFLIP Mechanism -- 4 Experiments -- 4.1 Experiments Setup -- 4.2 Main Results -- 4.3 Multiple Attackers -- 4.4 Anomaly Score Distribution -- 4.5 Ablation Study -- 5 Adaptive Attack -- 6 Conclusion -- A Appendix -- A.1 VFL Backdoor Attacks -- A.2 Attack Settings -- A.3 Results for Label Inference Attacks -- A.4 Impact of Bottom Model Architecture -- A.5 Impact of the MAE Training Strategies -- References -- How to Better Fit Reinforcement Learning for Pentesting: A New Hierarchical Approach -- 1 Introduction

-- 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 Hyperparameters -- 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 Data Protection. Part III: Software and Systems Security; Applied Cryptography. Part IV: Attacks and Defenses; Miscellaneous.
