1.

Record Nr.	UNINA9910874660003321
Autore	Maggi Federico
Titolo	Detection of Intrusions and Malware, and Vulnerability Assessment : 21st International Conference, DIMVA 2024, Lausanne, Switzerland, July 17–19, 2024, Proceedings / / edited by Federico Maggi, Manuel Egele, Mathias Payer, Michele Carminati
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031641718 9783031641701
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (563 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14828
Altri autori (Persone)	EgeleManuel PayerMathias CarminatiMichele
Disciplina	005.8
Soggetti	Data protection Computer engineering Computer networks Computers Criminology Quantum physics Data and Information Security Computer Engineering and Networks Computing Milieux Crime Control and Security Quantum Physics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Vulnerability Detection and Defense. -- Exceptional Interprocedural Control Flow Graphs for x86-64 Binaries. -- S2malloc: Statistically Secure Allocator for Use-After-Free Protection And More. -- Acoustic Side-Channel Attacks on a Computer Mouse. -- Using Semgrep OSS to Find OWASP Top 10 Weaknesses in PHP Applications: A Case Study. -- Modularized Directed Greybox Fuzzing for Binaries over Multiple CPU Architectures. -- Malware and Threats. -- Constructs of Deceit:

Exploring Nuances in Modern Social Engineering Attacks. -- Tarallo: Evading Behavioral Malware Detectors in the Problem Space. -- Evading Userland API Hooking, Again: Novel Attacks and a Principled Defense Method. -- Extended Abstract: Evading Packing Detection: Breaking Heuristic-Based Static Detectors. -- Listening between the Bits: Privacy Leaks in Audio Fingerprints. -- Mobile and Web Application Security. -- Bringing UFUs Back into the Air With FUEL: A Framework for Evaluating the Effectiveness of Unrestricted File Upload Vulnerability Scanners. -- SandPuppy: Deep-state fuzzing guided by automatic detection of state-representative variables. -- Extended Abstract - Tracking Manifests - Persistent Identifiers in Progressive Web Apps. -- PayRide: Secure Transport e-Ticketing with Untrusted Smartphone Location. -- Knocking on Admin’s Door: Protecting Critical Web Applications with Deception. -- AI for Security. -- Approach for the Optimization of Machine Learning Models for Calculating Binary Function Similarity. -- Inferring Recovery Steps from Cyber Threat Intelligence Reports. -- Pairing Security Advisories with Vulnerable Functions Using Open-Source LLMs. -- Extended Abstract: Assessing Language Models for Semantic Textual Similarity in Cybersecurity. -- Extended Abstract: A Transfer Learning-based Training Approach for DGA Classification. -- Hardware and Firmware Security. -- Seum Spread: Discerning Security Flaws in IoT Firmware Via Call Sequence Semantics. -- Gluezilla: Efficient and Scalable Software to Hardware Binding using Rowhammer. -- SmmPack: Obfuscation for SMM Modules. -- Presshammer: Rowhammer and Rowpress without Physical Address Information. -- Cyber Physical Systems and IoT. -- SecMonS: A Security Monitoring Framework for IEC 61850 Substations Based on Configuration Files and Logs. -- FaultGuard: A Generative Approach to Resilient Fault Prediction in Smart Electrical Grids. -- Wireless Modulation Identification: filling the gap in IoT networks security audit. -- Extended Abstract: Assessing GNSS Vulnerabilities in Smart Grids.

Sommario/riassunto

This book constitutes the proceedings of the 21st International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2024, held in Lausanne, Switzerland, during July 17–19, 2024. The 22 full papers and 6 short paper presented in this volume were carefully reviewed and selected from 110 submissions. The papers are organized in thematical sections named: vulnerability detection and defense; malware and threats; mobile and web application security; AI for security; hardware and firmware security; cyber physical systems and IoT.