1.	Record Nr.	UNISA996279717003316
	Titolo	Conference proceedings : MWSCAS
	Pubbl/distr/stampa	Piscataway, NJ, : IEEE, ©2002-
	ISSN	1558-3899
	Disciplina	621
	Soggetti	Electronics Electronic circuits Electric circuits Electric networks Periodicals. Conference papers and proceedings.
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Periodico
	Note generali	Title from journal fulltext screen (IEL, viewed Jan. 12, 2005).

2.

Record Nr.	UNINA9911015682403321
Titolo	Detection of Intrusions and Malware, and Vulnerability Assessment : 22nd International Conference, DIMVA 2025, Graz, Austria, July 9–11, 2025, Proceedings, Part II / / edited by Manuel Egele, Veelasha Moonsamy, Daniel Gruss, Michele Carminati
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-97623-1
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XVI, 331 p. 104 illus., 92 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15748
Disciplina	004.6
Soggetti	Computer networks Computers Criminology Quantum theory Computer Communication Networks Computing Milieux Crime Control and Security Quantum Physics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- AI/ML & Security. -- Towards Explainable Drift Detection and Early Retrain in ML-based Malware Detection Pipelines. -- InferONNX: Practical and Privacy-preserving Machine Learning Inference using Trusted Execution Environments. -- Hiding in Plain Sight: On the Robustness of AI-generated code detection. -- FlexGE: Towards Secure and Flexible Model Partition for Deep Neural Networks. -- Poster: Exploring the Zero-Shot Potential of Large Language Models for Detecting Algorithmically Generated Domains. -- Poster: Using Machine Learning to Infer Network Structure from Security Metadata. -- Android & Patches. -- More Than You Signed Up For: Exposing Gaps in the Validation of Android’s App Signing. -- An Empirical Study of Multi-Language Security Patches in Open Source Software. -- Red Light for Security: Uncovering Feature Check and Access Control Gaps in AAOS. -- Poster: SPECK: From Google Textual Guidelines to

Automatic Detection of Android Apps Vulnerabilities. -- OS & Network. -- Taming the Linux Memory Allocator for Rapid Prototyping. -- Linux hurt itself in its confusion! Exploiting Out-of-Memory Killer for Confusion Attacks via Heuristic Manipulation. -- Overlapping data in network protocols: bridging OS and NIDS reassembly gap. -- Poster: On the Usage of Kernel Shadow Stacks for User-Level Programs. -- Referencing your Privileges - A Data-Only Exploit Technique for the Windows Kernel. -- Resilient Systems. -- PackHero: A Scalable Graph-based Approach for Efficient Packer Identification. -- A History of Greed: Practical Symbolic Execution for Ethereum Smart Contracts. -- FAULTLESS: Flexible and Transparent Fault Protection for Superscalar RISC-V Processors. -- Poster: Building Confidence in Hardware-based Ransomware Detection through Hardware Performance Counter Event Correlation. -- Poster: FedBlockParadox - A Framework for Simulating and Securing Decentralized Federated Learning.

Sommario/riassunto

The two-volume set LNCS 15747 and 15748 constitutes the refereed conference proceedings of the 12nd International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2025, held in Graz, Austria, during July 9–11, 2025. The 25 revised full papers and 11 posters are presented in these proceedings were carefully reviewed and selected from 103 submissions. The papers are organized in the following topical sections: Part I: Web Security; Vulnerability Detection; Side channels; and Obfuscation. Part II: AI/ML & Security; Android & Patches; OS & Network; and Resilient Systems.