

Difficulty

Artifacts	Why	Difficulty (1-5)
From Attachments to SEO: Click Here to Learn More about Clickbait PDFs!	READ ME explained : +5 Training: -1	2
Triereme: Speeding up hybrid fuzzing through efficient query scheduling	READ ME: +4 RAM: -1 Already tried: -1	4
Lightweight Privacy-Preserving Proximity Discovery for Remotely-Controlled Drones	READ ME: +3	3
Secure Softmax/Sigmoid for Machine-learning Computation	READ ME: +5 STEPS: -1 Already tried: -2	4
Hades: Practical Decentralized Identity with Full Accountability and Fine-grained Sybil-resistance	READ ME: +5 Installation: -1	2
Remote attestation of confidential VMs using ephemeral vTPMs	READ ME: +4 INSTALLATION: -1	3
On the Feasibility of Cross-Language Detection of Malicious Packages in npm and PyPI	READ ME: +4	2
PSP-Mal: Evading Malware Detection via Prioritized Experience-based Reinforcement Learning with Shapley Prior	READ ME: +3 INSTALLATION: -2	5
OAuth 2.0 Redirect URI Validation Falls Short, Literally	READ ME: +4 STEPS: -1	3
Differentially Private Resource Allocation	READ ME: +2	4
Poisoning Network Flow Classifiers	READ ME: +5 INSTALLATION: -3	4
Secure MLaaS with Temper: Trusted and	READ ME: +5 INSTALLATION: -1	2

Efficient Model Partitioning and Enclave Reuse		
Global Analysis with Aggregation-based Beacons Detection across Large Campus Networks	Didn't find it	?
Detection of Anomalies in Electric Vehicle Charging Sessions	READ ME: +5 TIME: -1	2
DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection	READ ME: +1	5
Artemis: Defanging Software Supply Chain Attacks in Multi-repository Update Systems	READ ME: +5 SETUP: -1	2
Can Large Language Models Provide Security & Privacy Advice? Measuring the Ability of LLMs to Refute Misconceptions	READ ME: +4 DOCKER: -1	3
RandCompile: Removing Forensic Gadgets from the Linux Kernel to Combat its Analysis	READ ME: +5 SETUP: -1 STEPS: -1	3
Attack of the Knights:Non Uniform Cache Side Channel Attack	READ ME: +5	1