Categorization of the artifacts

Web Security

- Click Here to Learn More about Clickbait PDFs! : Issues of clickbait and malicious PDFs

- On the Feasibility of Cross-Language Detection of Malicious Packages in npm and PyPI : detection of malicious packages in web-based package managers.

- DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection : Protects privacy against web-based cache attacks.

Critical Infrastructure Security

- Detection of Anomalies in Electric Vehicle Charging Sessions : anomaly detection in critical infrastructure related to electric vehicle charging.

Binary Analysis

- RandCompile: Removing Forensic Gadgets from the Linux Kernel to Combat its Analysis

Data privacy

- Secure MLaaS with Temper: Trusted and Efficient Model Partitioning and Enclave Reuse : data privacy risks as user data must be uploaded to untrusted clouds

- Differentially Private Resource Allocation : privacy to resource allocation

- Hades: Practical Decentralized Identity with Full Accountability and Fine-grained Sybil-resistance : decentralized identity and cryptographic privacy measures.

Malware detection

- PSP-Mal: Evading Malware Detection via Prioritized Experience-based Reinforcement Learning with Shapley Prior EXPIRED LINK

Hardware security

- Attack of the Knights: Non Uniform Cache Side Channel Attack : new distance-based side-channel attack by timing the AES decryption operation

Software security

- Artemis: Defanging Software Supply Chain Attacks in Multi-repository Update Systems : supply chain attacks across multiple repositories

- Triereme: Speeding up hybrid fuzzing through efficient query scheduling : improving fuzzing techniques for security testing.

Machine Learning Security

- Secure Softmax/Sigmoid for Machine-learning Computation : machine learning computations.

- Can Large Language Models Provide Security & Privacy Advice? Measuring the Ability of LLMs to Refute Misconceptions : Evaluates web-based security and privacy advice from LLMs.

Cloud security

- Remote attestation of confidential VMs using ephemeral vTPMs

Network Security

- Poisoning Network Flow Classifiers : attacks on network classifiers

- Global Analysis with Aggregation-based Beaconing Detection across Large Campus Networks : Focuses on network security in large campus environments, often related to web security. EXPIRED LINK

Unmanned Aerial Vehicles security

- Lightweight Privacy-Preserving Proximity Discovery for Remotely-Controlled Drones : Involves privacy in drone operations EXPIRED LINK