NDSS 2023 Accepted Posters

A descriptive security alert through the outlier analysis using multi-sensor data

Abdulkabir Abdulraheem and Im Jung

A Monte Carlo Ensemble Approach to Automatically Identifying Keywords in Binary Message Formats

Jared Chandler

An Early Detection of Android Malware Using System Calls based Machine Learning Model

Xinrun Zhang, Akshay Mathur, Lei Zhao, Safia Rahmat, Quamar Niyaz, Ahmad Javaid and Xiaoli Yang

ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks

Phillip Rieger, Marco Chilese, Reham Mohamed, Markus Miettinen, Hossein Fereidooni and Ahmad-Reza Sadeghi

AUTOLYCUS: Exploiting Explainable AI (XAI) for Model Extraction Attacks against Decision Tree Models

Abdullah Caglar Oksuz, Anisa Halimi and Erman Ayday

Backdoor Attacks to Pre-trained Unified Foundation Models

Zenghui Yuan, Yixin Liu, Kai Zhang, Pan Zhou and Lichao Sun

BadGPT: Exploring Security Vulnerabilities of ChatGPT via Backdoor Attacks to InstructGPT

Jiawen Shi, Yixin Liu, Pan Zhou and Lichao Sun

Client-Side Byzantine Attacks on Raft Algorithm in Blockchain

Donghee Kim and Junbeom Hur

Cybersecurity Chess Manual: A Security Concept Predicting Typical Future Confrontation Scenarios

Xingchen Wu, Jiaqi Li, Yang Yu, Jian Chang, Yang Zhao, Lvyang Zhang and Lidong Zhai

Defending malware detection models against evasion based adversarial attacks

Hemant Rathore, Animesh Sasan, Sanjay K. Sahay and Mohit Sewak

Detecting Anomalous LAN Activities under Differential Privacy

Norrathep Rattanavipanon, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan and Sinchai Kamolphiwong

Diving into Robocall Content with SnorCall

Sathvik Prasad, Trevor Dunlap, Alexander Ross and Bradley Reaves

Facilitating Federated Genomic Data Analysis by Identifying Record Correlations while Ensuring Privacy

Leonard Dervishi, Xinyue Wang, Wentao Li, Anisa Halimi, Jaideep Vaidya, Xiaoqian Jiang and Erman Ayday

Fixing the Foundations: Towards Generalization for Machine Learning Intrusion Detection Systems

Miel Verkerken, Laurens D'hooge, Tim Wauters, Bruno Volckaert and Filip De Turck

Geographically Distributed Management of Enterprise Network Security Policy

Iffat Anjum, Jessica Sokal, Hafiza Ramzah Rehman, Ben Weintraub, Ethan Leba, William Enck, Cristina Nitarotaru and Bradley Reaves

Hades: Practical Partitioning Attack on Cryptocurrencies

Vinay Shetty, Piyush Kumar and Devashish Gosain

He-HTLC: Revisiting Incentives in HTLC

Sarisht Wadhwa, Jannis Stöter, Fan Zhang and Kartik Nayak

Improving Legacy IoT Device Security through Open-Source Intervention

Conner Bradley and David Barrera

Local Differentially-Private Genomic Database Fingerprinting

Tianxi Ji, Erman Ayday, Emre Yilmaz and Pan Li

Looking at the landscape of SMS Phishing

Aleksandr Nahapetyan, Kevin Childs, Sathvik Prasad, Bradley Reaves and Alexandros Kapravelos

Practical Removal Attacks on LiDAR-based Object Detection in Autonomous Driving

Takami Sato, Yuki Hayakawa, Ryo Suzuki, Yohsuke Shiiki, Kentaro Yoshioka and Qi Alfred Chen

Privacy Preserving Collaborative Clustering with Hyper Parameter Recommendation

Maryam Ghasemian and Erman Ayday

Privacy Preserving Population Stratification for Collaborative Genomic Research

Leonard Dervishi, Wenbiao Li, Anisa Halimi, Xiaoqia Jiang, Jaideep Vaidya and Erman Ayday

PrivyTrace: Privacy-Preserving Rapid Traceback of Telephone calls

Dawuda Ahmed and Bradley Reaves

Reproducibility-Oriented and Privacy-Preserving Genomic Dataset Sharing

Yuzhou Jiang, Tianxi Ji and Erman Ayday

Robust Fingerprint of Location Trajectories Under Differential Privacy

Yuzhou Jiang, Emre Yilmaz and Erman Ayday

Securing Biomedical Images from Unauthorized Training with Anti-Learning Perturbation

Yixin Liu, Haohui Ye, Kai Zhang and Lichao Sun

Sleepy Channels: Bi-directional Payment Channels without Watchtowers

Lukas Aumayr, Sri Aravindakrishnan Thyagarajan, Giulio Malavolta, Pedro Moreno-Sanchez and Matteo Maffei

TheHuzz: Instruction Fuzzing of Processors Using Golden-Reference Models for Finding Software-Exploitable Vulnerabilities

Rahul Kande, Addison Crump, Garrett Persyn, Patrick Jauernig, Ahmad-Reza Sadeghi, Dr. Aakash Tyagi and Jeyavijayan Rajendran

Thora: Atomic and Privacy-Preserving Multi-Channel Updates

Lukas Aumayr, Kasra Abbaszadeh and Matteo Maffei

Towards Simultaneous Attacks on Multiple Cellular Networks

Alexander Ross and Bradley Reaves

Unlearnable Graph: Protecting Graphs From Unauthorized Exploitation

Yixin Liu, Chenrui Fan, Pan Zhou and Lichao Sun

UnGANable: Defending Against GAN-based Face Manipulation

Zheng Li, Ning Yu, Ahmed Salem, Michael Backes, Mario Fritz and Yang Zhang

VICEROY: GDPR-/CCPA-compliant Enforcement of Verifiable Accountless Consumer Requests

Scott Jordan, Yoshimichi Nakatsuka, Ercan Ozturk, Andrew Paverd and Gene Tsudik