Accepted papers

Regular Papers

Authors	Title
Jukka Ruohonen, Kalle Hjerppe and Kalle Rindell	A Large-Scale Security-Oriented Static Analysis of Python Packages in PyPI
Pavan Kumar Karkekoppa Narayana Swamy and Marina Gavrilova	User Identification in Online Social Networks using Graph Transformer Networks
Julian Fietkau	The Elephant in the Background:A Quantitative Approach to Empower UsersAgainst Web Browser Fingerprinting
Wei-Yang Chiu, Weizhi Meng and Wenjuan Li	LibBlock - Towards Decentralized Library System based on Blockchain and IPFS
Ayane Sano, Yukiko Sawaya, Akira Yamada, Ayumu Kubota and Takamasa Isohara	Designing Personalized OS Update Message based on Security Behavior Stage Model
Kar Wai Fok and Vrizlynn Thing	Clustering based opcode graph generation for malware variant detection
Arthur Drichel, Mehdi Akbari Gurabi, Tim Amelung and Ulrike Meyer	Towards Privacy-Preserving Classification-as-a-Service for DGA Detection
Andres Rainiero Hernandez Coronado, Wonjun Lee and Wei-Ming Lin	The Race-Timing Prototype
Florian Skopik and Maria Leitner	Preparing for National Cyber Crises Using Non-linear Cyber Exercises
Farzaneh Shoeleh, Masoud Erfani, Saeed Shafiee Hasanabadi, Duc-Phong Le, Arash Habibi Lashkari, Adam Frank and Ali A. Ghorbani	User Profiling on Universal Data Insights tool on IBM Cloud Pak for Security
Kwasi Boakye-Boateng, Ali Ghorbani and Arash Habibi Lashkari	A Novel Trust Model In Detecting Final-Phase Attacks in Substations
Lav Gupta	Securing Critical Infrastructure Through Innovative Use Of Merged Hierarchical Deep Neural Networks
Martin Kodyš, Zhi Lu, Kar Wai Fok and Vrizlynn L. L. Thing	Intrusion Detection in Internet of Things using Convolutional Neural Networks
Andrick Adhikari and Rinku Dewri	Towards Change Detection in Privacy Policies with Natural Language Processing

Matthew Rafuse and Urs Hengartner	PUPy: A Generalized, Optimistic Context Detection Framework for Implicit Authentication
Michele Fontana, Francesca Naretto and Anna Monreale	A new approach for cross-silo federated learning and its privacy risks
Martha Kamkuemah	Reasoning about Authentication and Secrecy in the LoRaWAN Protocol
Ganyu Wang and Miguel Martin	SegmentPerturb: Effective Black-Box Hidden Voice Attack on Commercial ASR Systems via Selective Deletion
Shu Hong, Lingjie Duan and Jianwei Huang	Gaining Location Privacy from Service Flexibility: A Bayesian Game Theoretic Approach
Jonathan Godin and Philippe Lamontagne	Deletion-Compliance in the Absence of Privacy
Fuyuan Song, Zheng Qin, Jinwen Liang, Pulei Xiong and Xiaodong Lin	Traceable and Privacy-Preserving Non-Interactive Data Sharing in Mobile Crowdsensing
Chia-Yi Wu, Tao Ban, Shin-Ming Cheng, Bo Sun and Takeshi Takahashi	IoT Malware Detection Using Function Call Graph Embedding
Jiacheng Jin, Yandong Zheng and Pulei Xiong	EPSim-GS: Efficient and Privacy-Preserving Similarity Range Query over Genomic Sequences
Noreddine Belhadj-Cheikh, Abdessamad Imine and Michael Rusinowitch	FOX: Fooling with Explanations. Privacy Protection with Adversarial Reactions in Social Media
Ehsan Nazari, Paula Branco and Guy-Vincent Jourdan	Using CGAN to Deal with Class Imbalance and Small Sample Size in Cybersecurity Problems
Kathrin Garb, Johannes Obermaier, Elischa Ferres and Martin König	FORTRESS: FORtified Tamper-Resistant Envelope with Embedded Security Sensor
Atthapan Daramas and Vimal Kumar	Searching on Non-Systematic Erasure Codes
Miao He, Xiangman Li, Jianbing Ni and Haomiao Yang	Balancing Efficiency and Security for Network Access Control in Space-Air-Ground Integrated Networks
Sanaz Nakhodchi, Behrouz Zolfaghari, Abbas Yazdinejad and Ali Dehghantanha	SteelEye: An Application-Layer Attack Detection and Attribution Model in Industrial Control Systems using Semi-Deep Learning
Sharmin Afrose, Danfeng Yao and Olivera Kotevska	Measurement of Local Differential Privacy Techniques for IoT-based Streaming Data
Troya Çağıl Köylü, Cezar Rodolfo Wedig Reinbrecht, Said Hamdioui and Mottaqiallah Taouil	Deterministic and Statistical Strategies to Protect ANNs against Fault Injection Attacks

Christian Roth, Ngoc Thanh Dinh, Marc Roßberger and Dogan Kesdogan	DaRoute: Inferring trajectories from zero-permission smartphone sensors
Mordechai Guri	GAIROSCOPE: Leaking Data from Air-Gapped Computers to Nearby Smartphones using Speakers-to-Gyro Communication

Short Papers

Authors	Title
Malte Breuer, Ulrike Meyer and Susanne Wetzel	Introducing a Framework to Enable Anonymous Secure Mulit-Party Computation
Zhao Yongxin, Wanqing Wu and Di Chaofan	A trajectory privacy protection method that satisfies the (s,o,v)-constraint
Tomasz Kosiński, Primal Wijesekera, Morten Fjeld and Riccardo Scandariato	Fool me once: Privacy analysis of companion apps required to get the “smart“ from IoT
Randolph Loh and Vrizlynn Thing	Data Storage in the Multi-Cloud: Data Splitting Leveraging on Existing Data
Kimberly Garcia, Zaira Zihlmann, Simon Mayer, Aurelia Tamò-Larrieux and Johannes Hooss	Towards Privacy-Friendly Smart Products
Yi Xuan Ren, Yi Xin Jie, Qing Tao Wang, Bing Bing Zhang, Chi Zhang and Ling Bo Wei	A Hybrid Approach for Privacy-Preserving Graph Neural Network using SGX
René Helmke, Eugen Winter and Michael Rademacher	EPF: An Evolutionary, Protocol-Aware, and Coverage-Guided Network Fuzzing Framework
Kaja Schmidt, Alexander Mühle, Andreas Grüner and Christoph Meinel	Clear the Fog: Towards a Taxonomy of Self-Sovereign Identity Ecosystem Members
Steffen Enders, Mariia Rybalka and Elmar Padilla	PIdARCI: Using Assembly Instruction Patterns to Identify, Annotate, and Revert Compiler Idioms
Yiran Li, Guiqiang Hu, Xiaoyuan Liu and Zuobin Ying	Cross the Chasm: Scalable Privacy-Preserving Federated Learning against Poisoning Attack
Abdarahmane Wone, Joel Di Manno, Christophe Charrier and Christophe Rosenberger	Impact of environmental conditions on fingerprint system performance
Amir Namavar Jahromi, Hadis Karimipour and Ali Dehghantanha	Deep Federated Learning-Based Cyber-Attack Detection in Industrial Control Systems

Christopher Bonk, Zachary Parish, Julie Thorpe and Amirali Salehi-Abari	Long Passphrases: Potentials and Limits
Nikesh Lalchandani, Jay Jeong, Yevhen Zolotavkin, Frank Jiang and Robin Doss	Evaluating the Current State of ApplicationProgramming Interfaces for Verifiable Credentials
Pranav Kotak, Shweta Bhandari, Akka Zemmari and Jaykrishna Joshi	Unmasking Privacy Leakage through Android Apps Obscured with Hidden Permissions
Wensheng Zhang and Trenton Muhr	TEE-based Selective Testing of Local Workers in Federated Learning Systems
Rahul Dubey and Miguel Vargas Martin	Fool Me Once: A Study of Password Selection Evolution over the Past Decade
Xinyuan Wang	Practical Protection of Binary Applications via Transparent Immunization
Adrian Wood and Mike Johnstone	Detection of Induced False Negatives in Malware Samples
Mansour Aldawood and Arshad Jhumka	Secure Allocation for Graph-Based Virtual Machines in Cloud Environments
Jiao Xubin and Li Jinguo	A Novel Intrusion Detection Model for Class-imbalanced Learning Based on SMOTE and Attention Mechanism
Tasnia Ashrafi Heya, Abdul Serwadda, Isaac Griswold-Steiner and Richard Matovu	Using wrist movements for cyber attacks on examination proctoring
Mini Thomas, Reza Samavi and Thomas Doyle	Trust Quantification for Autonomous Medical Advisory Systems
Srinidhi Madabhushi and Rinku Dewri	Detection of Demand Manipulation Attacks on a Power Grid
Mohammadreza Hazhirpasand, Oscar Nierstrasz and Mohammad Ghafari	Dazed and Confused: What's Wrong with Crypto Libraries?
Farzana Zahid, Matthew Kuo and Roopak Sinha	Light-weight Active Security for Detecting DDoS Attacks in Containerised ICPS
May Almousa, Sai Basavaraju and Mohd Anwar	API-based Ransomware Detection using Machine Learning-based Threat Detection Models
Guiwen Luo, Shihui Fu and Guang Gong	Updatable Linear Map Commitments and Their Applications in Elementary Databases
Mohammad Mehdi Yadollahi, Ali. A Ghorbani and Arash Habibi Lashkari	Towards Query-efficient Black-box Adversarial Attack on Text Classification Models

Wensheng Zhang	A Practical Oblivious Cloud Storage System based on TEE and Client Gateway