

Program

Sunday, December 15, 2019 (Day 1)

08:00 Registration Starts

09:00-09:30 Conference Opening

09:30-10:30 Keynote I (Chair: Jianying Zhou)

Towards Leakage Resilient User Authentication

Prof. Robert Deng

Singapore Management University, Singapore

10:30-11:15 Break

11:15-12:30 Session 1: Malware Analysis and Detection

Prototype-based Malware Traffic Classification with Novelty Detection

Lixin Zhao, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Lijun Cai, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Aimin Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Zhen Xu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Dan Meng, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Evading API Call Sequence based Malware Classifiers

Fenil Fadadu, *C3I Center, Department of CSE, Indian Institute of Technology, Kanpur, India*

Anand Handa, *C3I Center, Department of CSE, Indian Institute of Technology, Kanpur, India*

Nitesh Kumar, *C3I Center, Department of CSE, Indian Institute of Technology, Kanpur, India*

Sandeep K. Shukla, *C3I Center, Department of CSE, Indian Institute of Technology, Kanpur, India*

UBER: Combating Sandbox Evasion via User Behavior Emulators

Pengbin Feng, *George Mason University, United States*

Jianhua Sun, *College of William and Mary, United States*

Songsong Liu, *George Mason University, United States*

Kun Sun, *George Mason University, United States*

12:30-14:00 Lunch

14:00-16:05 Session 2: IoT and CPS Security

AADS: A Noise-Robust Anomaly Detection Framework for Industrial Control Systems

Maged Abdelaty, *Fondazione Bruno Kessler and University of Trento, Italy*

Roberto Doriguzzi-Corin, *Fondazione Bruno Kessler, Italy*

Domenico Siracusa, *Fondazione Bruno Kessler, Italy*

Characterizing Internet-scale ICS Automated Attacks through Long-term Honeypot Data

Jianzhou You, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Shichao Lv, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Yichen Hao, *School of Software Engineering, Chongqing University, China*

Xuan Feng, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Ming Zhou, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Limin Sun, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Cloning Vulnerability Detection in Driver Layer of IoT Devices

Weipeng Jiang, *SKLOIS, Institute of Information Engineering, CAS; School of Cyber Security, University of Chinese Academy of Sciences, China*

Bin Wu, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Zhou Jiang, *School of Computer and Software, Nanjing University of Information Science and Technology Nanjing China, China*

Shaobo Yang, *School of Software, North University of China, Taiyuan, China*

Impact of Multiple Reflections on Secrecy Capacity of Indoor VLC System

Jian Chen, *Auburn University, United States*

Tao Shu, *Auburn University, United States*

Road Context-aware Intrusion Detection System for Autonomous Cars

Jingxuan Jiang, *Shandong University, China*

Chundong Wang, *Singapore University of Technology and Design, Singapore*

Sudipta Chattopadhyay, *Singapore University of Technology and Design, Singapore*

Wei Zhang, *Shandong University, China*

16:05-16:30 Break

16:30-17:45 Session 3: Enterprise Network Security

Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC

Wenzhuo Yang, *Nanyang Technological University, Singapore*

Kwok Yan Lam, *Nanyang Technological University, Singapore*

HeteroUI: A Novel Framework based on Heterogeneous Information Network Embedding for User Identification in Enterprise Networks

Meng Li, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Lijun Cai, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Aimin Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Haibo Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Dan Meng, *Institute of Information Engineering, Chinese Academy of Sciences, China*

CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding

Suya Zhao, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Renzheng Wei, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Lijun Cai, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Aimin Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Dan Meng, *Institute of Information Engineering, Chinese Academy of Sciences, China*

18:30-20:30 Welcome Reception & Best Paper and Best Student Paper Awards

Monday, December 16, 2019 (Day 2)

09:15-10:15 Keynote II (Chair: Xiapu Luo)

Can't You Hear Me Knocking: Novel Security and Privacy Threats to Mobile Users

Prof. Mauro Conti

University of Padua, Italy

10:15-10:45 Break

10:45-12:00 Session 4A: Software Security

VulHunter: An Automated Vulnerability Detection System based on Deep Learning and Bytecode

Ning Guo, *Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, China*

Xiaoyong Li, *Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, China*

Hui Yin, *College of Computer Science and Engineering, Shandong University of Science and Technology, China*

Yali Gao, *Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, China*

Deep Learning-based Vulnerable Function Detection: A Benchmark

Guanjun Lin, *Swinburne University of Technology, Australia*

Wei Xiao, *Changchun University of Technology, China*

Jun Zhang, *Swinburne University of Technology, Australia*

Yang Xiang, *Swinburne University of Technology, Australia*

Automatic Demirci-Selçuk Meet-in-the-Middle Attack on SKINNY with Key-Bridging

Qiu Chen, *State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China*

Danping Shi, *State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China*

Siwei Sun, *State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China*

Lei Hu, *State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China*

10:45-12:00 Session 4B: Authentication

Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems

Andreas Abraham, *Institute of Applied Information Processing and Communications, Austria*

Felix Hörandner, *Institute of Applied Information Processing and Communications, Austria*

Olamide Omolola, *IAIK, TU Graz, Austria*

Sebastian Ramacher, *AIT Austrian Institute of Technology, Austria*

Provably Secure Group Authentication in the Asynchronous Communication Model

Zhe Xia, *Wuhan University of Technology, China*

Lein Harn, *University of Missouri-Kansas City, United States*

Bo Yang, *Shaanxi Normal University, China*

Mingwu Zhang, *Hubei University of Technology, China*

Yi Mu, *Fujian Normal University, China*

Willy Susilo, *University of Wollongong, Australia*

Weizhi Meng, *Technical University of Denmark, Denmark*

AGE: Authentication Graph Embedding for Detecting Anomalous Login Activities

Renzheng Wei, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Lijun Cai, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Aimin Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Dan Meng, *Institute of Information Engineering, Chinese Academy of Sciences, China*

12:00-13:30 **Lunch**

13:30-14:45 **Session 5A: System Security**

SecFlush: A Hardware/Software Collaborative Design for Real-Time Detection and Defense against Flush-based Cache Attacks

Churan Tang, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Zongbin Liu, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Jingquan Ge, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Cunqing Ma, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

CDAE: Towards Empowering Denoising in Side-Channel Analysis

Guang Yang, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Huizhong Li, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Jingdian Ming, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Yongbin Zhou, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Practical Evaluation Methodology of Higher-order Maskings at Different Operating Frequencies

Yuguang Li, *China Academy of Information and Communications Technology, Beijing*

Ming Tang, *School of Cyber Science and Engineering, Wuhan University, China*

Pengbo Wang, *School of Cyber Science and Engineering, Wuhan University, China*

Yanbin Li, *College of Information Science and Technology, Nanjing Agricultural University, China*

Shan Fu, *Beijing University of Posts and Telecommunications, China*

13:30-14:45 **Session 5B: Applied Cryptograph (I)**

A Multi-group Signature Scheme from Lattices

Tian Qiu, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Lin Hou, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Dongdai Lin, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Ciphertext Policy Attribute-Based Encryption for Circuits from LWE Assumption

Geng Wang, *Shanghai Jiao Tong University, China*

Zhen Liu, *Shanghai Jiao Tong University, China*

Dawu Gu, *Shanghai Jiao Tong University, China*

Using Equivalent Class to Solve Interval Discrete Logarithm Problem

Bin Qi, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Jie Ma, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Kewei Lv, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

14:45-16:00 Session 6A: Internet Security (I)

DTGuard: A Lightweight Defence Mechanism against a New DoS Attack on SDN

Jianwei Hou, *Renmin University of China, China*

Ziqi Zhang, *Renmin University of China, China*

Wenchang Shi, *Renmin University of China, China*

Bo Qin, *Renmin University of China, China*

Bin Liang, *Renmin University of China, China*

Towards Comprehensive Security Analysis of Hidden Services Using Binding Guard Relays

Muqian Chen, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Xuebin Wang, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Jinqiao Shi, *Beijing University of Posts and Telecommunications, China*

Yue Gao, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Can Zhao, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Wei Sun, *Beijing Jiaotong University, School of Computer and Information Technology, China*

Context-aware IPv6 Address Hopping

Matthias Marx, *University of Hamburg, Germany*

Monina Schwarz, *University of Hamburg, Germany*

Maximilian Blochberger, *University of Hamburg, Germany*

Frederik Wille, *University of Hamburg, Germany*

Hannes Federrath, *University of Hamburg, Germany*

14:45-16:00 Session 6B: Applied Cryptograph (II)

Parallel Steepest Ascent Hill-Climbing for High Nonlinear Boolean and Vectorial Boolean Functions (S-Boxes)

Athmane Seghier, *Beihang University, China*

Jianxin Li, *Beihang University, China*

Accelerating SM2 Digital Signature Algorithm using Modern Processor Features

Long Mai, *Shanghai Jiao Tong University, China*

Yuan Yan, *Shanghai Jiao Tong University, China*

Songlin Jia, *Shanghai Jiao Tong University, China*

Shuran Wang, *Shanghai Jiao Tong University, China*

Jianqiang Wang, *Shanghai Jiao Tong University, China*

Juanru Li, *Shanghai Jiao Tong University, China*

Siqi Ma, *CSIRO, Australia*

Dawu Gu, *Shanghai Jiao Tong University, China*

Improved Differential Attacks on GIFT-64

Huairfeng Chen, *The 6-th Research Institute of China Electronics Corporation, China*

Rui Zong, *Institute for Advanced Study, Tsinghua University, China*

Xiaoyang Dong, *Institute for Advanced Study, Tsinghua University, China*

16:00-16:30 Break

16:30-17:45 Session 7A: Internet Security (II)

Towards Homograph-Confusable Domain Name Detection Using Dual-Channel CNN

Guangxi Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Xinghua Yang, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Yan Zhang, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Huajun Cui, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Huiran Yang, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Yang Li, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

FraudJuder: Fraud Detection on Digital Payment Platforms with Fewer Labels

Ruoyu Deng, *Shanghai Jiao Tong University, China*

Ruan Na, *Shanghai Jiao Tong University, China*

CloudCoT: A Blockchain-based Cloud Service Dependency Attestation Framework

Zhenyu Zhao, *Peking University, China*

Wu Luo, *Peking University, China*

Qingni Shen, *Peking University, China*

Anbang Ruan, *Octa Innovations Ltd, China*

16:30-17:20 Session 7B: Applied Cryptograph (III)

Adaptively Secure Puncturable Pseudorandom Functions via Puncturable Identity-Based KEMs

Xin Wang, *Chinese Academy of Sciences, China*

Shimin Li, *Chinese Academy of Sciences, China*

Rui Xue, *Institute of Information Engineering, CAS, China*

Towards Blockchain-enabled Searchable Encryption

Qiang Tang, *Luxembourg Institute of Science and Technology, Luxembourg*

18:30-20:30 **Conference Banquet**

Tuesday, December 17, 2019 (Day 3)

09:00-10:15 **Session 8: Machine Learning Security**

An Adversarial Attack based on Multi-Objective Optimization in the Black-box Scenario: MOEA-APGA II

Chunkai Zhang, *Harbin Institute of Technology, China*

Yepeng Deng, *Harbin Institute of Technology, Shenzhen, China*

Xin Guo, *Harbin Institute of Technology, Shenzhen, China*

Xuan Wang, *Harbin Institute of Technology Graduate School, China*

Neuron Selecting: Defending against Adversarial Examples in Deep Neural Networks

Ming Zhang, *National Key Laboratory of Science and Technology on Information System Security, China*

Hu Li, *National Key Laboratory of Science and Technology on Information System Security, China*

Xiaohui Kuang, *National Key Laboratory of Science and Technology on Information System Security, China*

Ling Pang, *National Key Laboratory of Science and Technology on Information System Security, China*

Zhendong Wu, *National Key Laboratory of Science and Technology on Information System Security, China*

Capturing the Persistence of Facial Expression Features for Deep Fake Video Detection

Yiru Zhao, *School of Cyber Science and Engineering, Wuhan University, China*

Wanfeng Ge, *School of Cyber Science and Engineering, Wuhan University, China*

Wenxin Li, *School of Cyber Science and Engineering, Wuhan University, China*

Run Wang, *School of Cyber Science and Engineering, Wuhan University, China*

Lei Zhao, *School of Cyber Science and Engineering, Wuhan University, China*

Jiang Ming, *University of Texas at Arlington, United States*

10:15-10:40 **Break**

10:40-12:20 **Session 9: Machine Learning Privacy**

Differentially Private Frequent Itemset Mining against Incremental Updates

Wenjuan Liang, *Renmin University of China*

Differentially Private Reinforcement Learning

Pingchuan Ma, *Beijing Electronic Science and Technology Institute, China*

Zhiqiang Wang, *Beijing Electronic Science and Technology Institute, China*

Le Zhang, *Beijing Electronic Science and Technology Institute, China*

Ruming Wang, *Hainan University, China*

Privacy-Preserving Machine Learning based on Secret Sharing

Ye Dong, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Xiaojun Chen, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Liyun Shen, *School of Cyber Security, University of Chinese Academy of Sciences, China*

Privacy-Preserving Decentralised Singular Value Decomposition

Qiang Tang, *Luxembourg Institute of Science and Technology, Luxembourg*

Bowen Liu, *Luxembourg Institute of Science and Technology, Luxembourg*

12:20-14:00 Lunch

14:00-15:15 Session 10: Web Security

WSLD: Detecting Unknown Webshell Using Fuzzy Matching and Deep Learning

Zihao Zhao, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Qixu Liu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Tiantian Song, *Tsinghua-Berkeley Shenzhen Institute, Tsinghua University, China*

Zhi Wang, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Xianda Wu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

A Character-Level BiGRU-Attention for Phishing Classification

Lijuan Yuan, *Yunnan University of Finance and Economics, China*

Zhiyong Zeng, *Yunnan University of Finance and Economics, China*

Yikang Lu, *Yunnan University of Finance and Economics, China*

Tao Feng, *Yunnan University of Finance and Economics, China*

Tear Off Your Disguise: Phishing Website Detection using Visual and Network Identities

Zhaoyu Zhou, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China*

Lingjing Yu, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China*

Qingyun Liu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Yang Liu, *Institute of Information Engineering, Chinese Academy of Sciences, China*

Bo Luo, *The University of Kansas, United States*

15:15-16:30 Session 11: Steganography and Steganalysis

Hierarchical Representation Network for Steganalysis of QIM Steganography in Low-Bit-Rate Speech Signals

Hao Yang, *Tsinghua University, China*

Zhongliang Yang, *Tsinghua University, China*

Yongjian Bao, *Tsinghua University, China*

Yongfeng Huang, *Tsinghua University, China*

Convolutional Neural Network based Side-Channel Attacks with Customized Filters

Man Wei, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Danping Shi, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Siwei Sun, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Peng Wang, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

Lei Hu, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*

DLchain: A Covert Channel over Blockchain based on Dynamic Labels

Jing Tian, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Gaopeng Gou, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Chang Liu, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Yige Chen, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Gang Xiong, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

Zhen Li, *Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China*

16:30

Conference Closing
