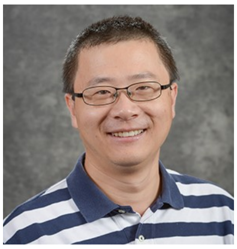
Program

RAID 2023 is going to be held in-person, only. Instructions for traveling to Hong Kong and reaching the venue can be found here. If you need an invitation letter for traveling to Hong Kong, please, contact the Chairs at chairs@raid2023.org .

Monday 16/10/2023

8:30 - 9:00	Registration
9:00 - 9:30	Opening
9:30 - 10:30	Keynote I



Professor Guofei Gu

Revisiting Security in the Age of Software-Defined Everything

Abstract: Software is not only eating the world, but also defining the new world. With the increasing examples such as software-defined compute/storage (aka, cloud), software-defined networking, software-defined radio/5G, and software-defined vehicle, we are now living in a world of software-defined everything (SDx). Infosys estimated that the global SDx market will reach USD 160 billion by 2024 and grow at a compound annual growth rate of 25%. The security of SDx is becoming more interesting and important. On one hand, SDx presents new attack surfaces and security challenges. On the other hand, SDx also provides new opportunities to rethink the design of security. In this talk, we will revisit the security at both sides anddemonstrate with our recentresearch results. In particular, we show that we can well leverage software-defined principles to enhance zero-trust security and design new programmable security frameworks, thus also making this software-defined world more secure.

Bio: Prof. Guofei Gu is a professor and holder of the Eppright Professorship in Engineering in the Department of Computer Science & Engineering at Texas A&M University (TAMU). Before coming to Texas A&M, he received his Ph.D. degree in Computer Science from the College of Computing, Georgia Institute of Technology. His research interests are in network and systems security. Prof. Gu is a recipient of 2010 NSF CAREER Award, 2013 AFOSR Young Investigator Award, 2010 IEEE S&P Best Student Paper Award, 2015 ICDCS Best Paper Award, 2022 ASIACCS Best Paper Award, Texas A&M Dean of Engineering Excellence Award, and Presidential Impact Fellow, among several others. He is an active member of the security research community and has pioneered several new research directions such as botnet detection/defense and SDN security. Prof. Gu has frequently served on the program committees of top-tier security conferences such as IEEE S&P, ACM CCS, USENIX Security, and NDSS. He is an IEEE Fellow and an ACM Distinguished Member. He is currently directing the SUCCESS Lab at TAMU.

10:30 - 11:00	Break	
11:00 - 12:30	Cloud and Network Security	+

Container Orchestration Honeypot: Observing Attacks in the Wild
Noah Spahn, *University of California, Santa Barbara*
Nils Hanke, *Ruhr University Bochum*
Thorsten Holz, *CISPA Helmholtz Center for Information Security*
Christopher Kruegel, *University of California, Santa Barbara*
Giovanni Vigna, *University of California, Santa Barbara*

EnclaveVPN: Toward Optimized Utilization of Enclave Page Cache and Practical Performance of Data Plane for Security-Enhanced Cloud VPN
Jaemin Park, *The Affiliated Institute of ETRI*
Brent Byunghoon Kang, *Korea Advanced Institute of Science and Technology*

EBugDec: Detecting Inconsistency Bugs caused by RFC Evolution in Protocol Implementations
Jingting Chen, *Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences*
Feng Li, *Institute of Information Engineering, Chinese Academy of Sciences*
Qingfang Chen, *Institute of Information Engineering, Chinese Academy of Sciences School of Cyber Security, University of Chinese Academy of Sciences*
Ping Li, *Institute of Information Engineering, Chinese Academy of Sciences School of Cyber Security, University of Chinese Academy of Sciences*
Lili Xu, *Institute of Information Engineering, Chinese Academy of Sciences*
Wei Huo, *Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, China, School of CyberSpace Security at University of Chinese Academy of Sciences*

CoZure: Context Free Grammar Co-Pilot Tool for Finding New Lateral Movements in Azure Active Directory
Abdullahi Chowdhury, *The University of Adelaide*
Hung Nguyen, *The University of Adelaide*

Phantom-CSI Attacks against Wireless Liveness Detection

Qiuye He, *University of Oklahoma*
Song Fang, *University of Oklahoma*

12:30 - 14:00	Lunch	
14:00 - 15:30	Malware and Fuzzing	+

A Method for Summarizing and Classifying Evasive Malware
Haikuo Yin, *University of California, Los Angeles*
Brandon Lou, *University of California, Los Angeles*
Peter Reiher, *University of California, Los Angeles*

Xunpack: Cross-Architecture Unpacking for Linux IoT Malware
Yuhei Kawakoya, *NTT Security (Japan) KK*
Shu Akabane, *Kanagawa Institute of Technology*
Makoto Iwamura, *NTT Security (Japan) KK*
Takeshi Okamoto, *Kanagawa Institute of Technology*

SEnFuzzer: Detecting SGX Memory Corruption via Information Feedback and Tailored Interface Analysis
Donghui Yu, *Shanghai Jiao Tong University*
Jianqiang Wang, *Shanghai Jiao Tong University*
Haoran Fang, *Shanghai Jiao Tong University*
Ya Fang, *Shanghai Jiao Tong University*
Yuanyuan Zhang, *Shanghai Jiao Tong University*

FieldFuzz: In Situ Blackbox Fuzzing of Proprietary Industrial Automation Runtimes via the Network
Andrei Bytes, *Singapore University of Technology and Design*
Prashant Hari Narayan Rajput, *NYU Tandon School of Engineering*
Constantine Doumanidis, *New York University Abu Dhabi*
Michail Maniatakos, *New York University Abu Dhabi*
Jianying Zhou, *Singapore University of Technology and Design*
Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*

Bin there, target that: Analyzing the target selection of IoT vulnerabilities in malware binaries
Arwa Abdulkarim Al Alsadi, *Delft University of Technology*
Kaichi Sameshima, *Yokohama National University*
Katsunari Yoshioka, *Yokohama National University*
Michel Van Eeten, *Delft University of Technology*
Carlos Hernandez Gañán, *Delft University of Technology*

15:30 - 16:00	Break	
16:00 - 18:00	Software Security (I)	+

FineIBT: Fine-grain Control-flow Enforcement with Indirect Branch Tracking
Alexander J. Gaidis, *Brown University*
Joao Moreira, *Intel Corporation*
Ke Sun, *Intel Corporation*
Alyssa Milburn, *Intel Corporation*
Vaggelis Atlidakis, *Brown University*
Vasileios P. Kemerlis, *Brown University*

SCVMON: Data-oriented attack recovery for RVs based on safety-critical variable monitoring
Sangbin Park, *Korea University*
Youngjoon Kim, *Korea University*
Dong Hoon Lee, *Korea University*

Information Flow Tracking for Heterogeneous Compartmentalized Software
Zahra Tarkhani, *Microsoft*
Anil Madhavapeddy, *University of Cambridge*

Renewable Just-In-Time Control-Flow Integrity
Erick Bauman, *The University of Texas at Dallas*
Jun Duan, *The University of Texas at Dallas*
Kevin W. Hamlen, *The University of Texas at Dallas*
Zhiqiang Lin, *The Ohio State University*

Raft: Hardware-assisted Dynamic Information Flow Tracking for Runtime Protection on RISC-V
Yu Wang, *Southern University of Science and Technology*
Jinting Wu, *Southern University of Science and Technology*
Haodong Zheng, *Southern University of Science and Technology*
Zhenyu Ning, *Hunan University, Southern University of Science and Technology*
Boyuan He, *Huawei Technologies Co., Ltd.*
Fengwei Zhang, *Southern University of Science and Technology*

18:00	Welcome Reception

Tuesday 17/10/2023

9:30 - 10:30	Keynote II

Professor Zhiqiang Lin
Unpacking the Threats of All-in-One Mobile Super Apps

Abstract: Mobile apps have evolved. Today, apps like WeChat have transformed from offering just one single service to a unified hub, integrating services ranging from instant messaging and ride-hailing to online shopping. This evolution birthed the term "super apps". To add even more features, these apps let other developers build small miniapps inside them using specific APIs. But as they grow, new security and privacy challenges emerge, particularly given the sheer volume of user data they handle. In this talk, Dr. Lin will walk through these challenges. More specifically, he will highlight the benefits and conveniences of super apps, but more importantly, the potential pitfalls. Some of these problems come from weak spots in how apps connect with each other, not setting clear boundaries for what each mini-app can do, or not vetting these mini-apps properly. Because of these issues, users might face threats like data theft, privacy leaks, or even malicious miniapps. Finally, Dr. Lin will also shed light on how to deal with and prevent these threats when concluding the talk.

Bio: Prof. Zhiqiang Lin is a Distinguished Professor of Engineering, and the Director of Institute for Cybersecurity and Digital Trust at The Ohio State University. His research interests center around systems and software security, with a key focus on developing automated program analysis techniques for vulnerability discovery and malware analysis; hardening the systems and software from binary code rewriting, virtualization, and trusted execution environment; and the applications of these techniques in emerging platforms such as super apps. He has published over 140 papers, many of which appeared in the top venues in cybersecurity. He is an ACM Distinguished Member, a recipient of Harrison

Faculty Award for Excellence in Engineering Education, NSF CAREER award, AFOSR Young Investigator award, and Outstanding Faculty Teaching Award. He received his Ph.D. in Computer Science from Purdue University.

10:30 - 11:00	Break	
11:00 - 12:30	IoT / Firmware / Binaries	+

Black-box Attacks Against Neural Binary Function Detection
Joshua Bundt, *Northeastern University, Army Cyber Institute*
Michael Davinroy, *Northeastern University*
Ioannis Agadakos, *Amazon, Northeastern University*
Alina Oprea, *Northeastern University*
William Robertson, *Northeastern University*

Extracting Threat Intelligence From Cheat Binaries For Anti-Cheating
Md Sakib Anwar, *The Ohio State University*
Chaoshun Zuo, *The Ohio State University*
Carter Yagemann, *The Ohio State University*
Zhiqiang Lin, *The Ohio State University*

Shimware: Toward Practical Security Retrofitting for Monolithic Firmware Images
Eric Gustafson, *UC Santa Barbara*
Paul Grosen, *UC Berkeley*
Nilo Redini, *UC Santa Barbara*
Saagar Jha, *UC Santa Barbara*
Andrea Continella, *University of Twente*
Ruoyu Wang, *Arizona State University*
Kevin Fu, *Northeastern University*
Sara Rampazzi, *University of Florida*
Christopher Kruegel, *UC Santa Barbara*
Giovanni Vigna,*UC Santa Barbara*

MP-Mediator: Detecting and Handling the New Stealthy Delay Attacks on IoT Events and Commands
Xuening Xu, *Stevens Institute of Technology*
Chenglong Fu, *University of North Carolina at Charlotte*
Xiaojiang Du, *Stevens Institute of Technology*

BitDance: Manipulating UART Serial Communication with IEMI
Zhixin Xie, *Zhejiang University*
Chen Yan, *Zhejiang University*
Xiaoyu Ji, *Zhejiang University*
Wenyuan Xu, *Zhejiang University*

12:30 - 14:00	Lunch	
14:00 - 15:30	ML (I): Inference and Toxicity	+

Efficient Membership Inference Attacks against Federated Learning via Bias Differences
Liwei Zhang, *Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing University of Posts and Telecommunications*
Linghui Li, *Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing University of Posts and Telecommunications*
Xiaoyong Li, *Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing University of Posts and Telecommunications*
Binsi Cai, *Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing University of Posts and Telecommunications*
Yali Gao, *Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing University of Posts and Telecommunications*

Ruobin Dou, *China Mobile Group Tianjin Co.,ltd.*
Luying Chen, *HAOHAN Data Technology Co.,ltd*

Exploring Clustered Federated Learning's Vulnerability against Property Inference Attack
Hyunjun Kim, *Seoul National University*
Yungi Cho, *Seoul National University*
Younghan Lee, *Seoul National University*
Ho Bae, *Ewha Womans University*
Yunheung Paek, *Seoul National University*

Witnessing Erosion of Membership Inference Defenses: Understanding Effects of Data Drift in Membership Privacy
Seung Ho Na, *KAIST*
Kwanwoo Kim, *KAIST*
Seungwon Shin, *KAIST*

PrivMon: A Stream-Based System for Real-Time Privacy Attack Detection for Machine Learning Models
Myeongseob Ko, *Virginia Tech*
Xinyu Yang, *Virginia Tech*
Zhengjie Ji, *Virginia Tech*
Hoang Anh Just, *Virginia Tech*
Peng Gao, *Virginia Tech*
Anoop Kumar, *Amazon*
Ruoxi Jia, *Virginia Tech*

Understanding Multi-Turn Toxic Behaviors in Open-Domain Chatbots
Bocheng Chen, *Michigan State University*
Guangjing Wang, *Michigan State University*
Hanqing Guo, *Michigan State University*
Yuanda Wang, *Michigan State University*
Qiben Yan, *Michigan State University*

15:30 - 16:00	Break	
16:00 - 18:00	IDS and Applied Crypto	+

EdgeTorrent: Real-time Temporal Graph Representations for Intrusion Detection
Isaiah J. King, *The George Washington University*
Xiaokui Shu, *IBM Research*
Jiyong Jang, *IBM Research*
Kevin Eykholt, *IBM Research*
Taesung Lee, *IBM Research*
H. Howie Huang, *The George Washington University*

Looking Beyond IoCs: Automatically Extracting Attack Patterns from External CTI
Md Tanvirul Alam, *Rochester Institute of Technology*
Dipkamal Bhusal, *Rochester Institute of Technology*
Youngja Park, *IBM Research*
Nidhi Rastogi, *Rochester Institute of Technology*

Temporary Block Withholding Attacks on Filecoin's Expected Consensus
Tong Cao, *Kunyao Academy*
Xin Li, *Kunyao Academy*

How (Not) to Build Threshold EdDSA
Harry W. H. Wong, *The Chinese University of Hong Kong*
Jack P. K. Ma, *The Chinese University of Hong Kong*
Hoover H. F. Yin, *The Chinese University of Hong Kong*

Sherman S. M. Chow, *The Chinese University of Hong Kong*

Towards Understanding Alerts raised by Unsupervised Network Intrusion Detection Systems
Maxime Lanvin, *CentraleSupélec, Univ. Rennes, IRISA*
Pierre-François Gimenez, *CentraleSupélec, Univ. Rennes, IRISA*
Yufei Han, *Inria, Univ. Rennes, IRISA*
Frédéric Majorczyk, *DGA-MI, Univ. Rennes, IRISA*
Ludovic Mé, *Inria, Univ. Rennes, France*
Eric Totel, *Samovar, Télécom SudParis, Institut Polytechnique de Paris*

18:00	Dinner Banquet

Wednesday 18/10/2023

9:00 - 10:30	Software Security (II)	+

MIFP: Selective Fat-Pointer Bounds Compression for Accurate Bounds Checking
Shengjie Xu, *University of Toronto*
Eric Liu, *University of Toronto*
Wei Huang, *University of Toronto*
David Lie, *University of Toronto*

All Use-After-Free Vulnerabilities Are Not Created Equal: An Empirical Study on Their Characteristics and Detectability
Zeyu Chen, *University of Delaware*
Daiping Liu, *University of Delaware*
Jidong Xiao, *Rensselaer Polytechnic Institute*
Haining Wang, *Virginia Tech*

NatiSand: Native Code Sandboxing for JavaScript Runtimes
Marco Abbadini, *Università degli Studi di Bergamo*
Dario Facchinetti, *Università degli Studi di Bergamo*
Gianluca Oldani, *Università degli Studi di Bergamo*
Matthew Rossi, *Università degli Studi di Bergamo*
Stefano Paraboschi, *Università degli Studi di Bergamo*

DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection
Yizheng Chen, *University of Maryland*
Zhoujie Ding, *University of California, Berkeley*
Lamya Alowain, *King Abdulaziz City for Science and Technology*
Xinyun Chen, *Google Deepmind*
David Wagner, *University of California, Berkeley*

Why Johnny Can't Use Secure Docker Images: Investigating the Usability Challenges in Using Docker Image Vulnerability Scanners through Heuristic Evaluation
Taeyoung Kim, *Sungkyunkwan University*
Seonhye Park, *Sungkyunkwan University*
Hyoungshick Kim, *Sungkyunkwan University*

10:30 - 11:00	Break	
11:00 - 12:30	ML (II): Adversarial, Robust & Explainable AI	+

Flow-MAE: Leveraging Masked AutoEncoder for Accurate, Efficient and Robust Malicious Traffic Classification
Zijun Hang, *National University of Defense Technology*
Yuliang Lu, *National University of Defense Technology*

Yongjie Wang, *National University of Defense Technology*
Yi Xie, *National University of Defense Technology*

Your Attack Is Too DUMB: Formalizing Attacker Scenarios for Adversarial Transferability
Marco Alecci, *University of Luxembourg*
Mauro Conti, *University of Padua*
Francesco Marchiori, *University of Padua*
Luca Martinelli, *University of Padua*
Luca Pajola, *University of Padua*

False Sense of Security: Leveraging XAI to Analyze the Reasoning and True Performance of Context-less DGA Classifiers
Arthur Drichel, *RWTH Aachen University*
Ulrike Meyer, *RWTH Aachen University*

Federated Explainability for Network Anomaly Characterization
Xabier Sáez-de-Cámara, *Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA), Mondragon Unibertsitatea*
Jose Luis Flores, *Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA)*
Cristóbal Arellano, *Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA)*
Aitor Urbieta, *Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA)*
Urko Zurutuza, *Mondragon Unibertsitatea*

PhantomSound: Black-Box, Query-Efficient Audio Adversarial Attack via Split-Second Phoneme Injection
Hanqing Guo, *Michigan State University*
Guangjing Wang, *Michigan State University*
Yuanda Wang, *Michigan State University*
Bocheng Chen, *Michigan State University*
Qiben Yan, *Michigan State University*
Li Xiao, *Michigan State University*

12:30 - 14:00	Lunch	
14:00 - 15:30	Deep into sytems & formats	+

CTPP: A Fast and Stealth Algorithm for Searching Eviction Sets on Intel Processors
Zihan Xue, *Institute of Information Engineering, CAS, University of Chinese Academy of Sciences*
Jinchi Han, *Institute of Information Engineering, CAS, University of Chinese Academy of Sciences*
Wei Song, *Institute of Information Engineering, CAS, University of Chinese Academy of Sciences*

Characterizing and Mitigating Touchtone Eavesdropping in Smartphone Motion Sensors
Connor Bolton, *University of Michigan*
Yan Long, *University of Michigan*
Jun Han, *Yonsei University*
Josiah Hester, *Georgia Institute of Technology*
Kevin Fu, *Northeastern University*

Security Analysis of the 3MF Data Format
Jost Rossel, *Paderborn University*
Vladislav Mladenov, *Ruhr University Bochum*
Juraj Somorovsky, *Paderborn University*

Beware of Pickpockets: A Practical Attack against Blocking Cards
Marco Alecci, *University of Luxembourg*
Luca Attanasio, *University of Padova*
Alessandro Brighente, *University of Padova*
Mauro Conti, *University of Padua*
Eleonora Losiouk, *University of Padova*
Hideki Ochiai, *Yokohama National University*
Federico Turrin, *University of Padua*

Quarantine: Mitigating Transient Execution Attacks with Physical Domain Isolation
Mathé Hertogh, *Vrije Universiteit Amsterdam*
Manuel Wiesinger, *Vrije Universiteit Amsterdam*
Sebastian Österlund, *Intel Corporation*
Marius Muench, *Vrije Universiteit Amsterdam*
Nadav Amit, *VMware Research*
Herbert Bos, *Vrije Universiteit Amsterdam*
Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

15:30 - 16:00	Break	
16:00 - 17:30	Web Sec & Authentication	+

SigA: rPPG-based Authentication for Virtual Reality Head-mounted Display
Lin Li, *Swinburne University of Technology*
Chao Chen, *RMIT University*
Lei Pan, *Deakin University*
Leo Yu Zhang, *Griffith University*
Jun Zhang, *Digital Research & Innovation Capability Platform, Swinburne University of Technology*
Yang Xiang, *Digital Research & Innovation Capability Platform, Swinburne University of Technology*

Boosting Big Brother: Attacking Search Engines with Encodings
Nicholas Boucher, *University of Cambridge*
Luca Pajola, *University of Padua*
Ilia Shumailov, *University of Oxford*
Ross Anderson, *University of Cambridge & University of Edinburgh*
Mauro Conti, *University of Padua*

Honey, I Cached our Security Tokens – Re-usage of Security Tokens in the Wild
Leon Trampert, *CISPA Helmholtz Center for Information Security*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Sebastian Roth, *CISPA Helmholtz Center for Information Security*

Measuring the Leakage and Exploitability of Authentication Secrets in Super-apps: The WeChat Case
Supraja Baskaran, *Concordia University*
Lianying Zhao, *Carleton University*
Mohammad Mannan, *Concordia University*
Amr Youssef, *Concordia University*

Leader: Defense Against Exploit-Based Denial-of-Service Attacks on Web Applications
Rajat Tandon, *University of Southern California Information Sciences Institute, Juniper Networks Inc.*
Haoda Wang, *University of Southern California Information Sciences Institute*
Nicolaas Weideman, *University of Southern California Information Sciences Institute*
Shushan Arakelyan, *University of Southern California Information Sciences Institute*
Genevieve Bartlett, *University of Southern California Information Sciences Institute*

Christophe Hauser, *University of Southern California Information Sciences Institute*
Jelena Mirkovic, *University of Southern California Information Sciences Institute*

17:30	Closure

Sponsors

Diamond

BLOCKSEC

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Supporting Organization

育基金會
ATION FOUNDATION

THE HONG KONG
POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

THE RESE
BLOCKCH