

Mark Huasong MENG

PHONE: +65 8102 8639 / +61 (0)435 730 924
ADDRESS: #COM2 01-09, 15 Computing Dr, Singapore 117418
EMAIL: huasong.meng@u.nus.edu / menghs@i2r.a-star.edu.sg

EDUCATION

- 2019 – PRESENT Doctor of Philosophy in COMPUTER SCIENCE
National University of Singapore, Singapore

Research Area: Cybersecurity & Trustworthy Artificial Intelligence
Supervisors: Prof. Jin Song DONG, Dr. Sin Gee TEO

*A*STAR Computing and Information Science Scholarship (2019 – 2023)*
Dean's Graduate Research Achievement Award (2021 – 2022)
School of Computing's Teaching Fellowship (2023)
Honours List of Student Tutors (2021-2022)
- 2015 – 2016 Master of Computing in INFOCOMM SECURITY
National University of Singapore, Singapore
Graduate with DISTINCTION

Thesis: "Analysing Use of High Privileges in Android Applications"
Keywords: Android Security, Reverse Engineering, Program Analysis
Supervisor: Prof. Jin Song DONG
- 2010 – 2014 Bachelor of Engineering (Hon.) in COMPUTER SCIENCE *with* BUSINESS Minor
Nanyang Technological University, Singapore
Graduate with 2ND UPPER CLASS HONOURS

Thesis: "Chinese Segmentation in User Generated Content"
Keywords: Natural Language Processing
Supervisor: A/Prof. Aixin SUN

SM2 MOE-Industry Joint Scholarship (2008 – 2014)
- 2022 – 2023 Visiting Research Student
The University of Queensland, QLD, Australia
Research Area: Privacy and Security in Android Ecosystem
Supervisors: A/Prof. Guangdong Bai
- 2013 Summer Exchange Programme
University of California, Berkeley, CA, United States

COMPLETE LIST OF PUBLICATIONS

- c1 Duc Phong Le, **Huasong Meng**, Le Su, Sze Ling Yeo and Vrizlynn L. L. Thing, "BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy", *IEEE Region 10 Conference (TENCON)*, 2018
- c2 Li Zhang, **Huasong Meng** and Vrizlynn L. L. Thing, "Progressive Control Flow Obfuscation for Android Applications", *IEEE Region 10 Conference (TENCON)*, 2018
- c3 **Mark Huasong Meng** and Yaou Qian, "A Blockchain Aided Metric for Predictive Delivery Performance in Supply Chain Management," *IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2018
- c4 **Mark Huasong Meng**, Guangdong Bai, Joseph K. Liu, Xiapu Luo and Yu Wang, "Analyzing Use of High Privileges on Android: An Empirical Case Study of Screenshot and Screen Recording Applications", *The 14th International Conference on Information Security and Cryptology (Inscrypt)*, 2018
- c5 Le Su, Yao Cheng, **Huasong Meng**, Vrizlynn Thing, Zhe Wang, Linghe Kong, and Long Cheng, "Securing Intelligent Transportation System: a Blockchain-based Approach with Attack Mitigation," *The 2nd International conference on Smart Block (SmartBlock)*, 2019

- c6 Xinguo Feng, Yanjun Zhang, **Mark Huasong Meng**, and Sin G. Teo. “Detecting Contradictions from CoAP RFC Based on Knowledge Graph”, *International Conference on Network and System Security (NSS)*, 2022
- c7 **Mark Huasong Meng**, Qing Zhang, Guangshuai Xia, Yuwei Zheng, Yanjun Zhang, Guangdong Bai, Zhi Liu, Sin G. Teo, and Jin Song Dong, “Post-GDPR Threat Hunting on Android Phones: Dissecting OS-level Safeguards of User-unresettable Identifiers,” *Network and Distributed System Security Symposium (NDSS)*, 2023
- c8 **Mark Huasong Meng**, Sin G. Teo, Guangdong Bai, Kailong Wang, and Jin Song Dong. “Enhancing Federated Learning Robustness using Data-Agnostic Model Pruning”, *The 26th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)*, 2023
- c9 **Mark Huasong Meng**, Guangdong Bai, Sin G. Teo, and Jin Song Dong. “Supervised Robustness-preserving Data-free Neural Network Pruning”, *The 27th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 2023
- c10 Zhongkui Ma, Xinguo Feng, Zihan Wang, Shuofeng Liu, Mengyao Ma, Hao Guan, and **Mark Huasong Meng**. “Formalizing Robustness against Character-level Perturbations for Neural Network Language Models”, *The 24th International Conference on Formal Engineering Methods (ICFEM)*, 2023.
- c11 Fuman Xie, Chuan Yan, **Mark Huasong Meng**, Shaoming Teng, Yanjun Zhang, and Guangdong Bai, “Are Your Requests Your True Needs? Checking Excessive Data Collection in VPA Apps.” *The 46th International Conference on Software Engineering (ICSE)*, 2024..
- c12 Chuan Yan, Fuman Xie, **Mark Huasong Meng**, Yanjun Zhang, and Guangdong Bai, “On the Quality of Privacy Policy Documents of Virtual Personal Assistant Applications.” *The 24th Privacy Enhancing Technologies Symposium (PETS)*, 2024.
- j1 **Huasong Meng**, Vrizlynn L. L. Thing, Yao Cheng, Zhongmin Dai, and Li Zhang, “A Survey of Android Exploits in the Wild,” *Computers & Security*, vol. 76, pp. 71–91, 2018
- j2 **Mark Huasong Meng**, Guangdong Bai, Sin G. Teo, Zhe Hou, Yan Xiao, Yun Lin, and Jin Song Dong, “Adversarial Robustness of Deep Neural Networks: A Survey from a Formal Verification Perspective,” *IEEE Transactions on Dependable and Secure Computing*, 2022 (Early Access)
- j3 Xinguo Feng, Yanjun Zhang, **Mark Huasong Meng**, Yansong Li, Chegne Eu Joe, Zhe Wang and Guangdong Bai, “Detecting contradictions from IoT protocol specification documents based on neural generated knowledge graph,” *ISA Transactions*, 2023 (In-press,)

RESEARCH PROJECTS

JUL 2020 – PRESENT (ONGOING)	Trustworthy Artificial Intelligence / Deep Learning Conduct a survey of robustness verification for deep neural networks. Perform research on security for deep learning and federated learning.
DEC 2020 – PRESENT (ONGOING)	Privacy and Security in Android Ecosystem Perform research on OS and SDK level safeguard of user unresettable identifiers.
OCT 2016 – FEB 2017	Control Flow Obfuscation for Android Applications Implement the obfuscation theory proposed from previous publications into a comprehensive Android APK transformation solution containing 8 different obfuscation techniques.
DEC 2016 – JAN 2019	EagleEye: Forensic Suite for Android Devices Rewrite the existing laboratory prototype with new functionalities into a web application for demonstration and internal usage.
DEC 2017 – JUL 2018	Blockchain for Digital Assets Tracking Implement an in-house blockchain solution for decentralized digital assets tracking in the industry.
MAY 2018 – OCT 2018	SecSG1: Securing Last-Mile Communication Systems for Smart Grids Implement the algorithm proposed in previous publications and integrate into the smart grid testbed.
JAN 2019 – JUN 2019	Proxy-Assisted Fine-Grained Encryption of Cloud Data Implement the encryption scheme invented in previous publications and integrate it with a file cloud web application for the demonstration.

TEACHING ASSISTANCE

2022 SPRING	CS4221/CS5421 Database Applications Design and Tuning (NUS) Duties include tutorial teaching (152 students in 10 groups, 65 hrs), project consultation, and assignments grading. Teaching feedback score: 4.5/5.0 (CS4221), 4.6/5.0 (CS5221) (CS department average 4.2, school average 4.2).
2022 SPRING	IT5006 Fundamentals of Data Analytics (NUS) Duties include assignments design and grading.
2021 FALL	BT5110 Data Management and Warehousing (NUS) Duties include tutorial teaching (119 students in 8 groups, 45 hrs) and assignments grading. Teaching feedback score: 4.6/5.0 (CS department average 4.3, school average 4.2).
2021 SPRING	CS5232 Formal Specification and Design Techniques (NUS) Duties include project consultation (19 students) and grading.

WORK EXPERIENCE

Oct 2016 to PRESENT (on leave)	AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH (A*STAR), Singapore <i>Research Engineer II</i> Cyber-Security (CS) Department, Institute for Infocomm Research (I ² R) <ul style="list-style-type: none"> • Be involved in researching and developing advanced technologies and algorithms for a wide range of research projects. • Provide scientific work with technical support within the department. • Co-supervise 5 Singapore Polytechnic students' final year projects. • Represent the cluster in the software quality control committee of I²R. • Organize and lead 4 software development training sessions within the institute. • Serve as the treasurer of I²R Recreational Club Management Committee.
Jul 2016 to Sep 2016	NCS PTE LTD, Singapore <i>Software Analyst</i> PaC@Gov Team, Ministry of Finance Project Group <ul style="list-style-type: none"> • Take charge of post penetration testing remediation for the PaC@Gov platform. • Coordinate the development of mobile applications (iOS and Android) with the contractor. • Participate in the pre-release testing of mobile applications for the PaC@Gov platform.
Jun 2014 to Jul 2015	GEMALTO PTE LTD, Singapore ¹ <i>Software Engineer</i> Ezio Mobile SDK Team, R&D Department <ul style="list-style-type: none"> • Serve as a development team member of Gemalto's eBanking product – Ezio Mobile SDK (<i>n.k.a. Mobile Protector</i>). • Focus on stability and security of mobile application development (iOS, Android and Windows Phone). • Work as a Scrum team by applying Agile development methodology. • Test the project by following professional software development process. • Write technical documentation for both internal and external users.
Jul 2012 to Dec 2012	AUTODESK ASIA PTE LTD, Singapore <i>Intern Software Engineer</i> DesignScript Team, R&D Department <ul style="list-style-type: none"> • Contribute in design and development of the new programming language: "DesignScript" (<i>n.k.a. Dynamo BIM</i>). • Study and implement the new parser of DesignScript language. • Be involved in pre-release defects fixing work for the new compiler and IDE.

¹Now known as Thales Technologies Pte Ltd

STUDENT ACTIVITIES

2013	Microsoft Imagine Cup 2013 – Innovation Challenge SOFTWARE DEVELOPER & UI DESIGNER • Represent Nanyang Technological University in Semi-Final Singapore. • Develop an application that enables designers conveniently transfer their ideas into runnable prototypes.
2021 – PRESENT	Graduate Student Association in Computing (NUS) MANAGEMENT COMMITTEE MEMBER
2011 – 2012	NTU Computer Engineering Club PUBLICITY OFFICER, 12TH MANAGEMENT COMMITTEE
2010 – 2012	NTU Cultural Activities Club – Wushu Club HONORARY GENERAL SECRETARY, 8TH MANAGEMENT COMMITTEE PUBLICATION & PUBLICITY OFFICER, 7TH MANAGEMENT COMMITTEE
2011	NTU Students Union – International Undergraduate Committee, China Group BUSINESS MANAGER, SPECIAL PROJECT ORGANIZING COMMITTEE

SERVICES

Reviewer	Transactions on Dependable and Secure Computing (TDSC), Journal of Logical and Algebraic Methods in Programming (JLAMP), Technology in Society (TechSoc) NSS 2022 (Sub-reviewer), AisaCCS 2023 (Poster Track, PC), AAAI 2024 (SRAI Track, PC)
Others	ADMA 2022 (Local Arrangement Team)

SKILLS

Programming	Proficient in JAVA, C/C++ and PYTHON Full Stack Web Development (NODEJS and DJANGO) Mobile Development on Android (<i>since 2014</i>), iOS (<i>since 2014</i>) and Windows Phone (<i>since 2012</i>) Working experience in C, R, JSP and SQL
Software Management	Adobe Software (Photoshop, Lightroom, etc), Microsoft Office SCRUM development methodology

LANGUAGES

Proficient in ENGLISH and CHINESE MANDARIN
Conversational in CANTONESE
Elementary in MALAY

INTERESTS

Photography, Travel, Cooking, Religion and History