

Mark Huasong MENG

Phone: +65 6408 2084 (Office) / +65 8102 8639 (Personal)
 Address: 1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632
 Email: menghs@i2r.a-star.edu.sg / huasong.meng@u.nus.edu
 Website: <https://mark-h-meng.github.io>

Education

-
- | | |
|-------------------------------|---|
| 2019 – 2024
(Viva Pending) | Doctor of Philosophy in Computer Science
National University of Singapore , Singapore

Research Area: Cybersecurity & Trustworthy Artificial Intelligence
Thesis: “Post-GDPR Privacy Preservation in Android Ecosystem”
Supervisors: Prof. Jin Song Dong, Dr. Sin Gee Teo (A*STAR)

<i>A*STAR Computing and Information Science Scholarship (2019 – 2023)</i>
<i>Dean’s Graduate Research Achievement Award (2021 – 2022, 2023-2024)</i>
<i>School of Computing’s Teaching Fellowship (2023)</i>
<i>Honours List of Student Tutors (2021-2022)</i> |
| 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 <i>with</i> Business Minor
Nanyang Technological University , Singapore
Graduate with Second Upper Class Honours

Thesis: “Chinese Segmentation in User Generated Content”
Keywords: Natural Language Processing
Supervisor: A/Prof. Aixin Sun

<i>SM2 MOE-Industry Joint Scholarship (2008 – 2014)</i> |
| 2022 – 2023 | Visiting Research Student
The University of Queensland , QLD, Australia
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 Yanjun Zhang, Ruoxi Sun, Liyue Shen, Guangdong Bai, Jason Xue, **Mark Huasong Meng**, Xue Li, Ryan Ko, and Surya Nepal, “Privacy-Preserving and Fairness-Aware Federated Learning for Critical Infrastructure Protection and Resilience.” *The Web Conference (WWW)*, 2024.
- c13 Liuhuo Wan, Chuan Yan, **Mark Huasong Meng**, Kailong Wang, and Haoyu Wang, “Analyzing Excessive Permission Requests in Google Workspace Add-ons.” *The 28th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 2024.
- c14 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.
- c15 **Mark Huasong Meng**, Hao Guan, Liuhuo Wan, Sin Gee Teo, Guangdong Bai, and Jin Song Dong, “Paoding: A High-fidelity Data-free Pruning Toolkit for Debloating Pre-trained Neural Networks.” *2024 IEEE Conference on Artificial Intelligence (IEEE CAI 2024)*, Short Paper, 2024.
- c16 Chuan Yan, **Mark Huasong Meng**, Fuman Xie, and Guangdong Bai, “Investigating Documented Privacy Changes in Android OS.” *The ACM International Conference on the Foundations of Software Engineering (FSE)*, 2024.
- j1 **Huasong Meng**, Vrizzlynn 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*, vol. 141, pp. 10-19, 2023.

Academic Services

Committee	AAAI 2024 (SRRAI Track, PC), CIKM 2024 (PC), ISACE 2024 (PC), AsiaCCS 2023 (Poster Session, PC), NSS 2022 (Subreviewer)
Reviewer	Transactions on Dependable and Secure Computing (TDSC), Journal of Logical and Algebraic Methods in Programming (JLAMP), Technology in Society (TechSoc)
Others	ADMA 2022 (Local Arrangement Team), ATVA/PRDC 2023 (Session Chair)

Teaching Assistance

2023 Fall	CS4211 Formal Methods for Software Engineering (NUS) Duties include course preparation, logistics, project consultation and grading (92 students enrolled).
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 enrolled) and grading.

Work Experience

Oct 2016 to Present	Agency for Science, Technology and Research (A*STAR), Singapore <i>Research Engineer / Senior Research Engineer (2016 – 2019)</i> <i>Research Scientist (2024 – Present)</i>
Jul 2016 to Sep 2016	NCS Pte Ltd, Singapore <i>Software Analyst</i>
Jun 2014 to Jul 2015	Gemalto Pte Ltd, Singapore ¹ <i>Software Engineer</i>
Jul 2012 to Dec 2012	Autodesk Asia Pte Ltd, Singapore <i>Intern Software Engineer</i>

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	Adobe Software (Photoshop, Lightroom, etc), Microsoft Office
Management	Scrum development methodology

Languages

Proficient in English and Chinese Mandarin
Conversational in Cantonese
Elementary in Malay

Interests

Photography, Travel, Cooking, Religion and History