Updated in November 2024

Mark Huasong MENG

Date of birth:	27 May 1991
Nationality:	Singaporean
Address:	Sichererstraße 18, 74076 Heilbronn, Germany
Email:	mark.meng@tum.de
Website:	https://mark-h-meng.github.io

Education

2019 – 2024 Doctor of Philosophy (Ph.D.) in Computer Science
National University of Singapore, Singapore
Research Area: Cybersecurity & Software Engineering
Thesis: "Privacy Preservation in Android Ecosystem"
Supervisors: Prof. Jin Song Dong, Dr. Sin Gee Teo (A*STAR)
Fully funded by *A*STAR Computing and Information Science Scholarship* (2019 – 2023)

2015 – 2016 Master of Computing (M.Comp.) 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 Second Upper Class Honours
Thesis: "Chinese Segmentation in User Generated Content"
Keywords: Natural Language Processing
Supervisor: Assoc. Prof. Aixin Sun
Fully funded by *SM2 MOE-Industry Joint Scholarship* (2008 – 2014)

2022 – 2023 Visiting Research Student
The University of Queensland, QLD, Australia
Supervisors: Assoc. Prof. Guangdong Bai

2013 Summer Exchange Programme
University of California, Berkeley, CA, United States

Publications

Legend: {c#} for conference and {j#} for journal

c1 Chuan Yan, Ruomai Ren, **Mark Huasong Meng**, Liuhuo Wan, Tian Yang Ooi, and Guangdong Bai, "Exploring ChatGPT App Ecosystem: Distribution, Deployment and Security," *The 39th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2024. (Core Ranking A*, ACM SIGSOFT Distinguished Paper Award (top 2.5%))

c2 Zhibo Zhang, Wuxia Bai, Yuxi Li, **Mark Huasong Meng**, Kailong Wang, Ling Shi, Li Li, Jun Wang, and Haoyu Wang, "GlitchProber: Advancing Effective Detection and Mitigation of Glitch Tokens in Large Language Models," *The 39th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2024. (Core Ranking A*)

c3 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. (Core Ranking A*)

c4 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. (Core Ranking A)

c5 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.

c6 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. (Core Ranking A*)

c7 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. (Core Ranking A*)

c8 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.

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.
(Our tool "`paoding-dl`" is released on PyPI and has received over 17.3k downloads as of Nov 2024)

j1 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. (IF Score 7.3)

c10 **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. (Core Ranking A)

c11 **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. (Core Ranking A*)

c12 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.

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 (TDSC)*, 2022. (IF Score 7.3)

c13 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.

c14 **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.

c15 **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.

c16 Li Zhang, **Huasong Meng** and Vrizlynn L. L. Thing, "Progressive Control Flow Obfuscation for Android Applications", *IEEE Region 10 Conference (TENCON)*, 2018.

c17 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.

j3 **Huasong Meng**, Vrizlynn L. L. Thing, Yao Cheng, Zhongmin Dai, and Li Zhang, "A Survey of Android Exploits in the Wild," *Computers & Security (COSE)*, vol. 76, pp. 71–91, 2018. (IF Score 5.1)

Teaching

2024 Winter	INHN0015/INHN4012 Security of Large Language Models (TUM) Duties include syllabus design, project grading, and teaching delivery (25 students enrolled).
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.

Academic Services

Committee	AAAI 2024 (SRRAI Track, PC, Core Ranking A*), CIKM 2024 (PC, Core Ranking A), ISACE 2024 (PC), ISACE 2025 (Web Chair), AsiaCCS 2023 (Poster Session, PC), NSS 2022 (Subreviewer)
Reviewer	WWW 2025 (Security Track, Core Ranking A*), Transactions on Dependable and Secure Computing (TDSC), Journal of Logical and Algebraic Methods in Programming (JLAMP), Formal Aspects of Computing (FAC), Technology in Society (TechSoc) Frontiers of Computer Science (FCS)
Others	ADMA 2022 (Local Arrangement Team), ATVA/PRDC 2023 (Session Chair)

Work Experience

Sep 2024 to Present	Technische Universität München, Germany School of Computation, Information and Technology (CIT) *Postdoctoral Researcher*
Oct 2016 to Sep 2024	Agency for Science, Technology and Research (A*STAR), Singapore Cybersecurity Department, Institute for Infocomm Research *Research Engineer / Senior Research Engineer* (2016.10 – 2023.12) *Research Scientist* (2024.1 – 2024.9)
Jul 2016 to Sep 2016	NCS Pte Ltd, Singapore *Software Analyst*
Jun 2014 to Jul 2015	Gemalto Pte Ltd, Singapore[1] *Software Engineer*
Jul 2012 to Dec 2012	Autodesk Asia Pte Ltd, Singapore *Intern Software Engineer*

Awards

2024	ACM SIGSOFT Distinguished Paper Award at ASE 2024 *(15 out of the 155 accepted papers were awarded, overall acceptance rate at 2.5%.)*
2022, 2024	Dean's Graduate Research Achievement Award *(Awarded to PhD students who performs well in research during the academic year.)*
2019 – 2023	A*STAR Computing and Information Science Scholarship *(The most prestigious PhD scholarship in Singapore, around 6-8 awardees per year)*
2023	School of Computing's Teaching Fellowship *(Awarded to the top 10 student tutors from the school based on teaching performance.)*
2023	Internet Society NDSS 2024 Travel Grant *(1 out of 13 recipients from both international and US domestic student presenters.)*
2021 – 2022	Honours List of Student Tutors *(Awarded to PhD students who received outstanding teaching feedback.)*

[1] Now known as Thales Technologies Pte Ltd