Pengfei Jing

PhD candidate, Department of Computing (COMP), The Hong Kong Polytechnic University (PolyU)
E-mail:pengfei.jing@connect.polyu.hk — Tel: 852-9311-5348 — Bio Webpage

SHORT BIOGRAPHY

Pengfei Jing is currently a PhD candidate in the department of computing (COMP), The Hong Kong Polytechnic University (PolyU), under the supervision of Prof. Xiapu Luo. His research interests include the security and testing of modern vehicles and autonomous driving systems (ADS), AI-assisted program analysis, LLM implementations, etc. Additionally, Pengfei has been working closely with the Tencent Keen Lab during his PhD career, supervised under Tecent Security Researcher Sen Nie. He is currently exploring new research areas including ADS testing and LLM-assisted program analysis.

EDUCATION

- 09/2019 - Now, Phd Candidate, Department of Computing (COMP), The Hong Kong Polytechnic University (PolyU)
- 09/2015 - 06/2019, Bachelor's degree, Automation, Faculty of Electronic and Information Engineering, Xi'an Jiaotong University (XJTU)

AWARDS

- National Encouragement Scholarship - 2016, 2017, 2018
- Third Prize Scholarship of 2021 Tencent Rhino-Bird Research Elite Program (Top 5%) - 2021

PROJECTS

- **AI Binary Analysis**: Developing a Transformer-based automated binary code analysis tool that can directly recover architectural information, function boundaries, and compiler/optimization option information from the Byte Code level. It achieves over 99% accuracy on more than 50 architectures, significantly outperforming previous traditional ML-based methods.
- **Connected Vehicle Security Testing**: Conducting reverse analysis and penetration testing on the official apps of certain vehicle models. This has helped the team discover and validate numerous security vulnerabilities, including unencrypted critical information in the Bluetooth Low Energy vehicle control protocol within the code, extractable and reversible encryption algorithms, and untimely key updates.
- **LLM Evaluation Framework:** Designing the latest large model security capability evaluation framework, SecBench, in which contributions include the macro design of the evaluation framework, specific evaluation set data collection and cleaning, automated evaluation process development, and related data challenge competition evaluation rules, participant data scoring, and subsequent data cleaning. Compared to existing work, SecBench has the largest number of questions and the most comprehensive evaluation dimensions, and it is also the first framework to directly support numerous security exams and subjective question assessments.

TEACHING ASSISTANT

- COMP3511: Legal Aspects and Ethics of Computing - 2023 Spring
- COMP3438: System Programming - 2022 Fall
- COMP3511: Legal Aspects and Ethics of Computing - 2022 Spring
- COMP3438: System Programming - 2021 Fall
- COMP1011: Programming Fundamentals - 2021 Spring
- COMP3011: Design and Analysis of Algorithms - 2020 Fall
- COMP4531: Emerging Topics in Fintech - 2020 Spring
- COMP5241: Software Engineering and Development -2019 Fall

PUBLICATIONS

1. **Pengfei, Jing**, Zhiqiang Cai, Yingjie Cao, Le Yu, Yuefeng Du, Wenkai Zhang, Chenxiong Qian, Xiapu Luo, Sen Nie, and Shi Wu (2023). "Revisiting Automotive Attack Surfaces: a Practitioners' Perspective". In: 2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, pp. 80–80.
2. **Pengfei, Jing**, Qiyi Tang, Yuefeng Du, Lei Xue, Xiapu Luo, Ting Wang, Sen Nie, and Shi Wu (2021). "Too good to be safe: Tricking lane detection in autonomous driving with crafted perturbations". In: 30th USENIX Security Symposium (USENIX Security 21), pp. 3237–3254.
3. Le Yu, Yangyang Liu, **Pengfei Jing**, Xiapu Luo, Lei Xue, Kaifa Zhao, Yajin Zhou, Ting Wang, Guofei Gu, Sen Nie, Shi Wu (2022). "Towards Automatically Reverse Engineering Vehicle Diagnostic Protocols". 31st USENIX Security Symposium (USENIX Security 22). 2022.