ZHENGJIE JI

Ph.D. Student, Department of Computer Science, Virginia Tech
zhengjie@vt.edu ◇ Homepage ◇ Google Scholar Profile

RESEARCH INTERESTS

My research focuses on eBPF and system security. My current work is to evaluate the effectiveness of BPF versus kernel modules in live patching scenarios. I also work on zero-overhead per-process eBPF tracing by creating per-process kernel views using copy-on-write techniques. My previous work includes system provenance analysis for multi-step attack investigation and constructing comprehensive threat knowledge graphs from open-source cyber threat intelligence (CTI). Furthermore, I am exploring the potential of large language models (LLMs) to enhance cybersecurity practices, such as generating security tests and improving threat detection and response workflows.

EDUCATION

Ph.D. in Computer Science, Virginia Tech	2022 - present
M.S. in Computer Science and Engineering, KTH Royal Institute of Technology	2020 - 2023
B.E. in Electrical and Computer Engineering, Shanghai Jiao Tong University	2017 - 2021

HONORS AND AWARDS

Bitshares Fellowship, Virginia Tech	2023
CCI SWVA Cyber Innovation Scholarship, Virginia Tech	2023
KTH Covid-19 Financial Aid Scholarship, KTH Royal Institute of Technology	2021
Hattrick Award, KTH Royal Institute of Technology	2020

PUBLICATIONS

Conference Papers

1. [eBPF'24] Milo Craun, Khizar Hussain, Uddhav Gautam, Zhengjie Ji, Tanuj Rao, Dan Williams. "Eliminating eBPF Tracing Overhead on Untraced Processes". *Workshop on eBPF and Kernel Extensions*, 2024. [pdf]

2. [arXiv] Ying Zhang, Wenjia Song, Zhengjie Ji, Daphne Yao, Na Meng. "How well does LLM generate security tests?". *CoRR arXiv*, 2023. [pdf]

3. [RAID'23] Myeongseob Ko, Xinyu Yang, Zhengjie Ji, Hoang Anh Just, Peng Gao, Anoop Kumar, Ruoxi Jia. "PrivMon: A Stream-Based System for Real-Time Privacy Attack Detection for Machine Learning Models". *International Symposium on Research in Attacks, Intrusions and Defenses*, 2023. [pdf]

4. [arXiv] Peng Gao, Xiaoyuan Liu, Edward Choi, Sibo Ma, Xinyu Yang, Zhengjie Ji, Zilin Zhang, Dawn Song. "ThreatKG: A System for Automated Open-Source Cyber Threat Knowledge Gathering and Management". *CoRR arXiv*, 2022. [pdf]

5. [arXiv] Haoran Su, Zhengjie Ji, H. Johansson, Li Jin. "A Hybrid Queuing Model for Coordinated Vehicle Platooning on Mixed-Autonomy Highways: Training and Validation". *CoRR arXiv*, 2021. [pdf]

Demo Papers

1. [ICDE'22 Demo] Zhengjie Ji, Edward Choi, Peng Gao. "A Knowledge Base Question Answering System for Cyber Threat Knowledge Acquisition". *IEEE International Conference on Data Engineering*, 2022. [pdf]

Posters

1. [IEEE S&P'23 Poster] Zhengjie Ji*, Xiaoyuan Liu* (* equal contribution), Edward Choi, Sibo Ma, Xinyu Yang, Dawn Song, Peng Gao. "POSTER: ThreatKG - A System for Automated Cyber Threat Knowledge Gathering and Management". *IEEE Symposium on Security and Privacy*, 2023. [pdf]

PROFESSIONAL SERVICES

External Reviewer, *Journal of Complex Networks* 2023
External Reviewer, *IEEE Transactions on Dependable and Secure Computing* 2023
External Reviewer, *ACM Conference on Computer and Communications Security* 2023
Conference Volunteer, *ACM Conference on Computer and Communications Security* 2022

TEACHING EXPERIENCE

Teaching Assistant, CS5560 Fundamentals of Info Security, Virginia Tech 2024
Teaching Assistant, CS5594 Blockchain Technologies, Virginia Tech 2023
Teaching Assistant, VE492 Intro to Artificial Intelligence, Shanghai Jiao Tong University 2021

SKILLS

Languages: English / Mandarin
Programming: C / C++ / Rust / Python / Java / JavaScript / SQL
Technical Experience: eBPF / QEMU / Docker / Kubernetes / PostgreSQL / Neo4j / Elasticsearch / Splunk

ENTRACURRICULAR ACTIVITIES

President, Shanghai Jiao Tong University Small Animal Protection Association (SJTUSAPA) 2018 - 2020