ZHENGJIE JI

Ph.D. Student, Department of Computer Science, Virginia Tech

realruoji@gmail.com ⋄ https://zhengjieji.github.io/ ⋄ Google Scholar Profile

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

PROJECT EXPERIENCE

Empirical Study on Rust Vulnerabilities — 2025/02 - 2025/09

- Developed the first comprehensive, code-level analysis of how security vulnerabilities arise in Rust by classifying vulnerabilities across safe and unsafe code, tracing propagation across the boundary between them, and distilling actionable root-cause patterns (foreign function interface misuse and violated safety invariants in unsafe code; logic and dependency flaws in safe code) to guide analysis tools and secure programming practice.
- Created a reproducible benchmark of real-world Rust vulnerabilities that packages each case with an isolated environment and vendored dependencies for consistent build and execution, and demonstrated its utility by running static analysis, model checking, and fuzzing to standardize evaluation across tools and findings.

Enhancing BPF Safety — 2024/09 - 2025/09

- Built a load-time, policy-driven information flow control system that lets administrators label sensitive sources and trusted sinks per program, tracks dataflow through bytecode, and rejects unsafe flows-enforcing least-privilege access and preventing kernel-to-user leakage without runtime overhead.
- Designed a declarative specification-and-code-generation framework that formally expresses safety for BPF-kernel interfaces (helpers and kernel functions) as pre-conditions, post-conditions, and invariants, then automatically emits verifier and wrapper checks-eliminating ad hoc manual logic, reducing developer error, and improving maintenance as interfaces evolve.

Optimizing BPF Performance — 2024/04 - 2024/08

- Introduced per-process kernel views: a kernel view manager performs copy-on-write on hookpoint pages and remaps traced processes to private pages and state, isolating tracing to targets and achieving zero overhead for untraced processes.

Integrating LLMs for Java Test Generation — 2024/02 - 2024/08

- Established a methodology for prompting LLM to synthesize application-specific security tests from vulnerability descriptions and exemplar library tests, and designed a head-to-head evaluation protocol against state-of-the-art generators (SIEGE and TRANSFER), providing evidence and analysis that LLM-based testing can better operationalize supply-chain vulnerability exploits and informing effective prompt and workflow design.

PROFESSIONAL SERVICES

• Artifact Evaluation Committee, *NDSS*	2026
• Artifact Evaluation Committee, *FAST*	2026
• Program Committee, *LLM4Sec*	2025
• Artifact Evaluation Committee, *CCS*	2025
• Artifact Evaluation Committee, *USENIX*	2025

SELECTED PUBLICATIONS

1. BPFflow - Preventing Information Leaks from eBPF
   Chinecherem Dimobi, Rahul Tiwari, Zhengjie Ji, Dan Williams. *Workshop on eBPF and Kernel Extensions*, 2025.
2. Eliminating eBPF Tracing Overhead on Untraced Processes
   Milo Craun, Khizar Hussain, Uddhav Gautam, Zhengjie Ji, Tanuj Rao, Dan Williams. *Workshop on eBPF and Kernel Extensions*, 2024.
3. How Well Does LLM Generate Security Tests?
   Ying Zhang, Wenjia Song, Zhengjie Ji, Daphne Yao, Na Meng. *CoRR arXiv*, 2023.
4. PrivMon: A Stream-Based System for Real-Time Privacy Attack Detection for Machine Learning Models
   Myeongseob Ko, Xinyu Yang, Zhengjie Ji, Hoang Anh Just, Peng Gao, Anoop Kumar, Ruoxi Jia. *International Symposium on Research in Attacks, Intrusions and Defenses*, 2023.
5. ThreatKG: A System for Automated Open-Source Cyber Threat Knowledge Gathering and Management
   Peng Gao, Xiaoyuan Liu, Edward Choi, Sibo Ma, Xinyu Yang, Zhengjie Ji, Zilin Zhang, Dawn Song. *CoRR arXiv*, 2022.
6. A Knowledge Base Question Answering System for Cyber Threat Knowledge Acquisition
   Zhengjie Ji, Edward Choi, Peng Gao. *IEEE International Conference on Data Engineering*, 2022.

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