Weijie Huang

"Way-Jee(-eh) Hwahng"

✉ Weijie.Huang@rice.edu · ☎ (+1) (346) 504-9503 · @macromogic

Education

Rice University
Houston, TX, United States — Aug. 2022 – Present
Ph.D. Student in Computer Science
Advisor: Dr. Nathan Dautenhahn

Southern University of Science and Technology (SUSTech)
Shenzhen, Guangzhou, China — Sept. 2018 – Jul. 2022
B.Eng. in Computer Science and Engineering
Advisor: Dr. Fengwei Zhang
GPA: 3.70/4.00

Research Experience

High-performance Streaming Query Processor for Semi-structured Data — June 2024 – Present

Supervised by Dr. Konstantinos Mamouras Rice University

Ongoing Project

Efficiently Streaming JSON Documents with Conditional Filters

Abstract. High-performance processing and analytics for JSON documents is crucial for commodity applications. Streaming query mechanisms have been proven significantly outperform parsing-involved ones, especially with the support of the powerful SIMD acceleration techniques. Existing works rely on the popular JSONPath query language for the high-performance streaming queries. However, one important feature – the conditional filter – is ignored. In this work, we propose JsoniQ, an efficient streaming mechanism for JSON queries that supports conditional filters. This mechanism is equipped with a refined query automaton with condition states to select outputs, and experiments shows that it brings little performance degradation compared with the state-of-the-art.

Least-Authority Virtual Architecture for Intra-process Isolation — Aug. 2022 – Present

Supervised by Dr. Nathan Dautenhahn Rice University

Process-level isolation is not sufficient to enforce data security because potentially vulnerable and malicious code/data may reside within one single address space. Existing CVEs like Heartbleed has proven that a memory corruption within a module is just enough to cause information leakage. This project aims to propose Least-Authority Virtual Architecture (LAVA), a general and flexible framework to sandbox, monitor or compartmentalize programs to minimize the privileges of different components.

Publication

- Fangfei Yang, Bumjin Im, Weijie Huang, Kelly Kaoudis, Anjo Vahldiek-Oberwagner, Chia-Che Tsai, and Nathan Dautenhahn. "*Endokernel: A Thread Safe Monitor for Lightweight Subprocess Isolation*". In proceedings of the USENIX Security Symposium (USENIX'24), August, 2024.
- Fangfei Yang, Weijie Huang, Kelly Kaoudis, Anjo Vahldiek-Oberwagner, and Nathan Dautenhahn. "*Endoprocess: Programmable and Extensible Subprocess Isolation*". In proceedings of the New Security Paradigms Workshop (NSPW'23), September, 2023.
- Yudi Yang, Weijie Huang, Kelly Kaoudis, and Nathan Dautenhahn. "*Whole-Program Privilege and Compartmentalization Analysis with the Object-Encapsulation Model*". In proceedings of the Language-Theoretic Security Workshop (LangSec'23), May, 2023.

Ongoing Project

SoftCaps: Software-based Capability Translation and Virtualization Framework for Generic C Programs (first-authored)

Abstract. The concept of program capability exposes a fine-grained notation and semantics to define, describe, analyze and enforce the privilege within a program. Existing mechanisms have realized the capability system to some extent, but none of them interprets the semantics thoroughly and portably to support generic programs, especially those written in C. This work presents SoftCaps, a runtime framework consisting of a capability-based privilege specification, an automated translation mechanism to embed the specification into the binary, and an efficient runtime monitor to enforce the capability semantics. The SoftCaps framework also provides an intuitive insight of generic privilege evaluation for different program sandboxing and/or compartmentalization policies.

Trusted Execution Environment (TEE) on RISC-V — May 2021 – June 2022

Supervised by Dr. Fengwei Zhang SUSTech

This project proposes a flexible, software-based TEE architecture on RISC-V, which supports secure I/O for peripheral devices and novel memory management for enclaves. The architecture is developed on top of OpenSBI v0.9, and tested on QEMU and several development boards.

Publication

- Haonan Li*, Weijie Huang*, Mingde Ren, Hongyi Lu, Zhenyu Ning, Heming Cui, and Fengwei Zhang. "*A Novel Memory Management for RISC-V Enclaves*". In proceedings of Hardware and Architectural Support for Security and Privacy Workshop (HASP'21), October, 2021.
  * Co-first authors

Work Experience

Student Assistant — Feb. 2019 – June 2022

Dept. Computer Science and Engineering, SUSTech, Shenzhen, China

Responsible for creating/grading assignments and exams, and answering questions in the following undergraduate courses:

- *Introduction to Computer Programming A/B (CS102A/B)*
- *Discrete Mathematics (CS201)*
- *C/C++ Programming (CS205)*
- *Computer System Design and Application A (CS209A)*

Teaching Assistant — Aug. 2023 – May 2024

Dept. Computer Science, Rice University, Houston, TX, US

Responsible for creating/grading assignments and exams, and answering questions in the following graduate courses:

- *Advanced Logic in Computer Science (COMP509)*
- *Graduate Design and Analysis of Algorithms (COMP582/ELEC512)*

Summer Intern (Backend) — June 2021 – Aug. 2021

Python Dept. Data, ByteDance Ltd., Shenzhen, China

Responsible for developing and maintaining an automated internal tool that periodically monitors all configuration and runtime statuses across service clusters. This tool is capable of tracking various health and performance indicators of these clusters. If any monitored status reaches an alarm threshold, the tool will automatically alert respective service owners to take timely actions to prevent potential service disruptions or failures.

Honors and Awards

Silver Medal, Award on 2019 International Collegiate Programming Contest (ICPC) Asia Regional (Yinchuan Site) Oct. 2019

Bronze Medal, Award on 2019 International Collegiate Programming Contest (ICPC) Asia Regional (Nanjing Site) Oct. 2019