Yingao (Elaine) Yao

Email: elainedv111@gmail.com
https://elaineyao.github.io/

Education

University of British Columbia, Vancouver, Canada — 09/2021–12/2023 (expected)
MASc student in Electrical & Computer Engineering; Avg. Score: 85.3/100 — Advisor: Karthik Pattabiraman

University of Electronic Science and Technology of China, Sichuan, China — 09/2017–6/2021
B.E. in Electrical & Communication Engineering; GPA: 3.96/4.0

Publications

- **SwarmFuzz: Discovering GPS Spoofing Attacks in Drone Swarms**. Yingao (Elaine) Yao, Pritam Dash, Karthik Pattabiranman.*IEEE/IFIP International Conference on Dependable Systems and Networks, 2023.*
- **Poster: May the Swarm Be With You: Sensor Spoofing Attacks Against Drone Swarms**. Yingao (Elaine) Yao, Pritam Dash, Karthik Pattabiranman. *ACM SIGSAC Conference on Computer and Communications Security, 2023*

Honors and Awards

- **IEEE DSN Student Travel Grant Award (USD 800), IEEE Computer Society** 2023
- **Faculty of Applied Science Graduate Award (CAD 600), University of British Columbia** 2022
- **Outstanding Winner (0.2%), in COMAP Interdisciplinary Contest in Modeling.** 2020
- **Thanksgiving Scholarship for Modern Scientists, CAD 4000, 12 per school per year.** 2020
- **National Scholarship, CAD 1600, for top 1.5% students per school** 2020
- **National Second Prize (3%), in China Undergraduate Mathematical Contest in Modeling.** 2018

Employment Experience

Graduate Research Assistant, University of British Columbia — 2021 – present

Graduate Teaching Assistant, University of British Columbia — 2021 – present

Project Experience

SwarmFuzz: Discovering GPS Spoofing Attacks in Drone Swarms — 04/2022 - 03/2023

– Focused on security implications of swarm control algorithms in drone swarms when under GPS spoofing attacks.
– Developed SwarmFuzz, a fuzzing framework combining **centrality analysis (PageRank)** and **gradient descent algorithm**, to efficiently assess the resilience of drone swarm missions. SwarmFuzz has a $10x$ higher success rate and $3x$ lower runtime than random fuzzing, with the highest success rate of 74%.

Fuzzing CPU by the Assembly Generator — 04/2023 - now

– Implemented **fuzz testing** to identify CPU defects by developing a random generator for x86 assembly instructions. Ensured the generated instructions were both syntactically and semantically correct.
– Conducted a sanity check on the instructions on the CPU emulator (**QEMU**) using the **Centipede** framework.

Is the Synthesized Scene in the Autonomous Driving Realistic? — 02/2022 – 05/2022

– Conducted a feasibility evaluation of the MSF-ADV attack on the camera and **LiDAR** sensors on self-driving cars. Synthesized driving scenarios by integrating adversarial 3D object **point cloud** into environment images.
– Tested the attack on the **YOLOv3** image object detection neural network using the **KITTI dataset**.

Measuring Context Switches in the Serverless Environment — 02/2022 – 05/2022

– Measured the thread and process **context switch** time in serverless computing environments (**Google Cloud Function**). Implemented benchmarks based on ping-pong pipes, conditional variables, and Lmbench in Python.
– Performed **non-parametric analysis** on the measured time for checking its normality.

Encryption in ICS Networks: Is it enough? — 09/2021 – 12/2021

– Identified vulnerabilities of the secure **Modbus protocol** in Industrial Control Systems (**ICS**) by exploiting network side-channel leaks. Leveraged **Wireshark** to monitor ICS activities through packet length and timing.
– Conducted the study on the secure water treatment plant (**SWaT**), successfully inducing ICS malfunctions, including water tank overflow and process delays.

Skills Summary

- **Programming Languages**: Python, C, Bash, Matlab
- **Frameworks& Software**: Linux, Git, AFL, Libfuzzer, Wireshark, Centipede, QEMU