Yibo Wei

y2wei@ucsd.edu | github.com/Microwave-WYB | LinkedIn | 9500 Gilman Drive

I am a PhD student at UC San Diego focusing on IoT security, automotive security, and cybersecurity. I design and build scalable systems from scratch to support real-world security measurement, analysis, and evaluation.

Education

University of California, San Diego Sept. 2023 to Present
Ph.D. in Computer Science and Engineering La Jolla, CA

University of California, San Diego Sept. 2019 to June 2023
B.S. in Computer Science and Engineering La Jolla, CA

Skills

Languages: Python, Rust, C/C++

Systems & Data: Polars, PostgreSQL/PostGIS, Docker, Android Development

Security: Android Reverse Engineering, .NET Reverse Engineering, Ghidra, BLE Protocol Analysis

Professional Experience

Zoox: Software Engineer Intern, Firmware Tools June 2026 to Sept. 2026

- Built data pipelines that transform raw vehicle firmware validation outputs into **Delta Lake** tables on **Amazon S3** and **Databricks**
- Identified a **security vulnerability** in the course of firmware-tools development and coordinated **responsible disclosure** with the Product Security team for investigation and remediation
- Structured validation data to accelerate failure investigation, classification, and root-cause triage
- Established a data foundation for faster build-failure analysis and future automated triage tooling

Publications

BLE Theft Auto: Evaluating the Security of Aftermarket BLE-based Automotive Remote Control Systems
35th USENIX Security Symposium; presented at DEF CON 34 2026

- Co-led the study of pairing, authentication, and encryption in 6 aftermarket BLE vehicle-control systems, identifying critical vulnerabilities in 3 that expose an estimated 2.9 million vehicles
- Developed reverse-engineering and proof-of-concept tooling to analyze custom application-layer security protocols
- Engineered a deterministic, end-to-end source-to-paper build system using **DVC** and **mise**, reproducing the complete paper and its artifacts from versioned inputs; awarded all 3 USENIX artifact badges
- Coordinated responsible disclosure with affected vendors, prompting security improvements to a widely deployed system

Research Projects

VAAS (Victim as a Service): LLM Scam Honeypot Mar. 2026 to Present

- Built an LLM-driven automated honeypot platform for studying social-media scams and collecting scam interaction data
- Implemented the backend entirely in **Rust** with a **Vite** frontend for operating the research platform
- Designed the system to support repeatable analysis of scam strategies and interaction patterns

Cluetooth: BLE Security Research Infrastructure Feb. 2024 to Present

- Architected an end-to-end BLE collection and analysis platform managing more than 10 million advertisements globally and supporting research that led to the discovery of multiple vulnerabilities
- Built an Android scanner with its core data-processing pipeline written entirely in **Rust**, using **Polars** for high-efficiency processing of BLE advertisements
- Implemented a **Rust**-based Lua scripting interface for defining custom BLE central and peripheral behavior, turning the Android app into a programmable universal BLE remote and peripheral
- Designed a scalable storage pipeline using **Firestore** and Parquet datasets hosted on **Google Cloud Storage**
- Developed a standalone **Python** ingest job using **Polars** for high-throughput transformation and loading of collected BLE data

- Defined the separate **PostgreSQL** and **PostGIS** database through version-controlled migrations, enabling reliable schema evolution and geolocation queries with OpenStreetMap data