

# Luke Yamaguchi

Irvine, CA | [yamaluke@g.ucla.edu](mailto:yamaluke@g.ucla.edu) | [yamaluke.com](http://yamaluke.com) | [linkedin.com/in/yamaluke](https://linkedin.com/in/yamaluke) | US Citizen

## EDUCATION

|  |                     |
|--|---------------------|
| <b>University of California, Los Angeles (UCLA)</b>  | Sep 2024 - Jun 2027 |
| <b>M.S. Electrical &amp; Computer Engineering</b> (Exceptional Student Admission Program)  | Expected Jun 2027   |
| <b>B.S. Computer Engineering</b>   | Expected Jun 2026   |
| • <b>GPA:</b> 3.81/4.00  |                     |
| • <b>Relevant Coursework:</b> Operating Systems, Computer Systems Architecture, Computer System Security, Digital Circuits, Algorithms and Complexity, Data Communications and Telecommunication Networks, Communication Systems, Digital Signal Processing, Neural Networks and Deep Learning |                     |

|                                     |                     |
|-------------------------------------|---------------------|
| <b>Irvine Valley College</b>        | Aug 2022 - Aug 2024 |
| <b>AS-T Mathematics, AS Physics</b> |                     |

## SKILLS

|   |
|---|
| <b>Languages:</b> C, C++, Verilog, Python, Bash, MIPS Assembly  |
| <b>Embedded Systems:</b> FPGA (Artix 7), STM32, ARM Cortex-M7, UART / SPI / I2C, Raspberry Pi Pico, Arduino     |
| <b>Wireless &amp; Signal:</b> ADALM-Pluto SDR, GNU Radio, Wireshark, Internet Protocols                         |
| <b>Tools &amp; Lab:</b> Git, Linux, Docker, GDB, MATLAB, Oscilloscopes, Logic Analyzer, DMM, Analog Discovery 2 |
| <b>Language:</b> English, Japanese  |

## EXPERIENCE

|   |                     |
|---|---------------------|
| <b>ASIC/FPGA Security Engineering Grad Intern</b>   | Los Angeles, CA     |
| The Aerospace Corporation   | Jun 2026 - Sep 2026 |
| <b>Undergraduate Researcher</b>   | Los Angeles, CA     |
| Secure Systems and Architectures Lab - UCLA   | Oct 2025 - Present  |
| • Researching BLE security and RF device authentication using physical-layer characteristics as hardware fingerprints       |                     |
| • Built GNU Radio DSP pipeline to extract physical-layer features from BLE signals captured from ADALM-Pluto SDR            |                     |
| • Training ML models for RF device authentication on a Linux remote server  |                     |
| • Implementing adversarial RF spoofing attacks to evaluate authentication robustness under attacker-controlled interference |                     |

## PROJECTS

|  |                     |
|--|---------------------|
| <b>Hardware-Enforced Authentication System (Artix 7 FPGA)</b>  | Feb 2025 - Mar 2025 |
| • Implemented hardware-enforced multi-user authentication system in Verilog on an Artix 7 FPGA                       |                     |
| • Designed role-based access control (RBAC) with admin, user, and guest privilege separation                         |                     |
| • Managed dynamic credential lifecycles, including creation, modification, & deletion                                |                     |
| • Engineered fail-secure features (auto re-locking & brute-force lockout) informed by authentication threat modeling |                     |
| • Validated logic integrity via .vcd waveform analysis and 670+ lines of simulation testbenches                      |                     |
| <b>Project Lead &amp; Software Lead - Mars Rover, 48-hour UCLA Hack Competition</b>                                  | Jul 2024            |
| • Built a Raspberry Pi Pico-based rover with environmental sensors and ESP32 camera managed via React web interface  |                     |
| • Developed Python firmware for motion and data control, optimizing it to reduce MQTT communication latency by 86%   |                     |
| • Led a 4-member team through rapid hardware prototyping and software integration, earning 3rd place overall         |                     |
| <b>Autonomous Embedded Race Car</b>  | Oct 2024 - Dec 2024 |
| • Developed bare-metal C++ firmware to interface with an 8-sensory array, managing PWM, GPIO, and motor drivers      |                     |
| • Implemented sensor fusion algorithms and real-time PID control for precise high-speed line following               |                     |
| • Achieved 2nd fastest overall time  |                     |
| <b>Lead Researcher - Multi-Agent Access Control</b>  | Oct 2025 - Dec 2025 |
| • Designed provenance-based access control framework to prevent Confused Deputy attacks in multi-agent LLM systems   |                     |
| • Implemented instruction-level provenance tainting using information flow control                                   |                     |
| • Built a Python security middleware to intercept tool calls, enforcing least-privilege across multi-hop workflows   |                     |
| • Reduced attack success rates by 65% compared to baseline framework   |                     |