

Luke Yamaguchi

Irvine, CA | yamaluke@g.ucla.edu | yamaluke.com | linkedin.com/in/yamaluke | US Citizen

Embedded Systems • Secure Hardware Architecture • Wireless Systems

EDUCATION

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

Irvine Valley College	Aug 2022 - Aug 2024
AS-T Mathematics, AS Physics	

SKILLS

Languages: C, C++, Verilog, Python, Bash, MIPS Assembly
Embedded Systems: FPGA (Basys 3), STM32, ARM Cortex-M7, UART / SPI / I2C, Raspberry Pi Pico, Arduino
Wireless & Signal: ADALM-Pluto SDR, GNU Radio, Wireshark, Internet Protocols
Tools & Lab: Git, Linux, Docker, GDB, MATLAB, Oscilloscopes, Logic Analyzer, DMM, Analog Discovery 2
Language: English, Japanese

EXPERIENCE

Undergraduate Researcher	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 the robustness of the RF fingerprinting system	

PROJECTS

Hardware-Enforced Digital Lock System - Basys 3 FPGA	Feb 2025 - Mar 2025
• Implemented a hardware-enforced multi-user authentication system in Verilog with role-based access control	
• Managed dynamic credential lifecycle, supporting creation, modification, deletion, and privilege separation for guest, user, and admin roles	
• Added auto re-locking and hardware-enforced brute-force lockout to mitigate unauthorized access attempts	
• Verified fail-secure logic using .vcd waveform analysis and 650+ lines of simulation testbenches covering edge cases	

Project Lead & Software Lead - Mars Rover, 48-hour UCLA Hack Competition	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	

Autonomous Embedded Race Car	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	

Lead Researcher - Multi-Agent Access Control	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	