SECURITY ARCHITECT, PRODUCT AND DEVICE SECURITY

Miguel Jardines

I secure devices and build the tooling that lets a team do it at scale.

Miami, FL · mj@migueljardines.com · LinkedIn

160+	90%+	2×	7
device models secured and cleared for launch	faster threat research, via an LLM triage pipeline I built	threat reporting cadence after automating the research	device OEMs held to our security requirements

Summary

Security Architect with 8+ years in product and device security. I've cleared 160+ device models from seven OEMs for commercial launch, reviewing designs, finding vulnerabilities, and driving OEM fixes. After launch, I lead threat intelligence that identifies exploits in the wild, including zero-days. I also build the automation and AI tooling that lets a team do this at scale. Co-inventor, US Patent 11,985,729.

Experience

Architect IV - Security Architecture

Sep 2026 – Present

U.S. wireless carrier · Miami, FL

- **Review OEM security architecture documents** to identify design flaws before devices reach production.
- **Built an automated OSINT collection and LLM triage pipeline** that cut threat research time by more than 90% and doubled reporting cadence, resulting in continuous monitoring of the threat landscape and double the number of high-severity findings.
- **Brief leadership on emerging device threats** through a recurring threat intelligence report, translating technical findings into business risk and engaging OEMs to fix the issues.
- Led **root cause analysis on high-impact device security issues** with OEM partners through to clear remediation.
- **Identify exploits in the wild, including zero-days**, by monitoring exploit developers, device trafficking networks, and commercial bypass-tool vendors.
- **Own the team's security test automation platform**, with each service isolated in its own Docker container: Jenkins and Gitea for test automation, Jira for test case and issue tracking, and a private RAG assistant (Open WebUI, ChromaDB, Apache Tika) for document search. Run its disaster recovery and the vulnerability and DAST scans required by corporate governance.

Specialist Engineer IV - Security Engineering

Jan 2022 – Sep 2026

U.S. wireless carrier · Miami, FL

- **Cleared 160+ device models, sold in the millions, for commercial launch**, including several first-of-kind products.
- **Found and drove fixes for high-impact vulnerabilities**, ensuring full compliance with FCC and business security requirements.
- **Architected and owned security automation frameworks in CI/CD** that saved thousands of hours of testing over 6 years.
- **Led the migration of critical certification infrastructure into the corporate environment**, following secure-development compliance standards, creating audit-ready evidence, and ensuring zero downtime.

- **Ran a weekly Linux tooling session for the team**, demonstrating tools, reverse engineering techniques, and new ways to improve testing.

Earlier roles

Jul 2018 – Jan 2022

Tracfone Wireless

Product Security Engineer II — Oct 2021 – Jan 2022

Product Security Engineer — Jul 2018 – Oct 2021

Education

B.S., Computer Science

2015 – 2018

Florida International University · Miami, FL

- Member, **Upsilon Pi Epsilon (UPE)**, the honor society for the computing and information disciplines

Patent, Certifications & Languages

Patent US 11,985,729 · SIM card switching system for automated device testing · Co-inventor — 2024

AWS Security Essentials · Amazon Web Services — 2020

Introduction to Large Language Models · LinkedIn Learning — 2024

Languages: Spanish (native or bilingual), English (full professional)

Skills

Device & Platform Security

Android security · iOS device policy · SIM & device lock · eSIM · Activation lock · Unlock compliance · Qualcomm & MediaTek chipsets · Bootloaders

Offensive & Analysis

Firmware reverse engineering · Penetration testing · Root cause analysis · Threat modeling · Threat intelligence · CVE risk analysis · Unlock-fraud tooling analysis

Automation & AI

Python · CI/CD (Jenkins) · Docker · Linux · Git · ADB / Fastboot / AT / Diag · LLM workflows · OSINT collection · Local LLM deployment

Leadership

OEM partnerships · Device certification programs · Executive reporting · Security compliance · Mentoring · JIRA process design