RÉSUMÉ / MURTAZA IZZEE

A technical record, not a one-page abstraction.

Fifteen years across mobile threat signals, payment-terminal hardware, firmware, secure boot, attestation, trusted execution, offensive research, binary analysis, and verification-gated AI systems.

saramena.us · github.com/manizzle

01

Experience

Google

2021–present

- Offensive security for Android's device-attestation stack: hardware-backed attestation and verified boot from secure element and TEE through the OS.
- Hypervisor-assisted runtime kernel integrity measurement across the post-boot trust boundary.

Square

2017–2021

- Four years on Square's POS team across payment-terminal hardware security—firmware integrity, secure boot, and tamper detection—and mobile device trust.
- Owned threat-signal research for iOS and Android: selected signals, implemented collection on both platforms, and built backend threat analysis across millions of devices and hundreds of thousands of transactions a day.

Visa

2017

Mobile security red-team work across Android and iOS.

SourceDNA

2011–2015

Founding security engineer at the YC S15 mobile binary-analysis company, acquired by Apple.

Root Labs

2010–2011

Embedded code auditing, low-level security tooling, and fuzzing research.

02

Selected research

U-Boot NFS client

Independently found a pre-auth buffer overflow in U-Boot's NFS client — pointer hijack, NFS state-machine takeover, shellcode delivery, full chain and public PoC. It collided with a private report filed a month earlier, so the CVE went to the other reporter. Patches are upstream, including a second negative-length bug in `nfs_read_reply()` found on the way.

Exploit chain and PoC ↗

Hardware wallets

Voltage fault injection to bypass RDP2 read-out protection on STM32F2; extracted seeds off bootrom startup. Trezor One and Model T.

Nur security-SDK census

Collected a real, dated census of security and identity SDK code detected in 320 public mobile app binaries using 27 fingerprint signatures. The artifact reports code presence only—not use, configuration, effectiveness, or market share.

Explore the census ↗

Device integrity

Named inventor on a U.S. patent covering device integrity and TEE isolation for payments.

03

Publications & talks

PT_NOTE Disinfector

TmpOut

ELF research using load-segment clustering and code analysis to identify PT_NOTE infection and recover the original entry point.

Read the article ↗

The story of Binary Packers (Cryptors) and Kryptos

2013

Technical report and implementation exploring compiler-assisted, function-by-function binary packing with LLVM and libbfd.

Open the paper ↗

Mach0 and the App Store

Bugcrowd LevelUp 0x03

Public talk on binary formats, application metadata, and the evidence available in public app artifacts.

Watch the talk ↗

AutoQL

2024

An introduction to extending CodeQL with automatic query generation and the ideas behind the experiment.

Read the post ↗

Competitive-security archive

CTF

Challenge solutions, exploit notes, and team research from earlier competitive-security work.

Browse the archive ↗

04

Selected systems

AI SYSTEMS

Orchestrator

Multi-model routing, explicit work queues, checkpointing, bounded execution, and independent criterion-level verification gates.

Repository ↗

NETWORK ANALYSIS

Gridhawk

Distributed packet analysis and automated ThreatCL generation for service and trust-boundary mapping.

Repository ↗

BINARY ANALYSIS

HSVMProc

C++ work in instruction processing and emulation for low-level program analysis.

Repository ↗

AUTOMOTIVE SECURITY

OBD fuzzing

Python tooling and captured traces for analyzing and fuzzing vehicle diagnostic interfaces.

Repository ↗

05

Systems

Platform security

Remote attestation, secure and measured boot, hardware-backed keystores, secure elements, TEEs, hypervisors, Linux internals, and runtime integrity.

Offensive research

Vulnerability research, exploit development, firmware analysis, QEMU and emulation, fuzzing, fault injection, and fix verification.

AI systems

Multi-model routing, checkpointed work queues, bounded parallel work, and independent verification gates for security analysis.

Engineering

Python, C/C++, Go and Rust auditing, security automation, CI-integrated testing, and large-scale binary analysis.

06

Education

NYU Tandon

2020–2023

M.S. Information Security, Cum Laude.

Cal Poly San Luis Obispo

2009–2013

B.S. Computer Engineering.