SHAY MORDECHAI

Product Security Engineer · Security Research · OS Internals & AppSec
Center District, Israel · 052-306-4991 · shay.mordechai@proton.me · linkedin.com/in/shay-mordechai · shay-mordechai.github.io

SUMMARY

Security Researcher focused on reverse engineering, runtime behavior, and security boundary analysis across Android, compilers, and application systems. Published research and responsible disclosures to CERT-IL and MITRE.

TECHNICAL SKILLS

Threat Modeling · Secure Architecture · Code Review · OWASP · SAST/SCA · Android Internals · Linux Internals · Binder IPC · Reverse Engineering · Runtime Analysis · Semantic Fuzzing · AWS · Frida · IDA Pro · JADX · Burp Suite · Checkmarx · C/C++ · Python · Java · Assembly

PROFESSIONAL EXPERIENCE

Independent Security Research | *Aug 2025 – Present (Self-Employed)*

- Researching security boundaries across application frameworks, operating systems, and runtime environments.
- Building PoCs and tooling to analyze unexpected behavior and security assumptions.

Application Security Analyst | Israel Tax Authority | *Aug 2024 – Jul 2025*

- Architecture & Threat Modeling: Served as the Security Lead for a flagship multi-GB file ingestion platform, mapping system architecture alongside R&D and Project Management.
- Designed security requirements for a multi-GB file ingestion pipeline, securing the processing of tens of thousands of files monthly through an external-to-internal CDR sanitization pipeline.
- Led enterprise SAST/SCA operations (Checkmarx/Checkmarx One), significantly reducing false-positive noise and accelerating vulnerability remediation cycles for critical financial systems.

PROJECTS & RESEARCH

Android Internals & Malware Analysis | Published in Digital Whisper

- Reverse engineered Android malware execution flow before UI initialization.
- Analyzed early lifecycle stages (ContentProvider, attachBaseContext, LoadedApk) using Frida.
- Researching Android framework trust boundaries and Binder IPC.

Secure SaaS Architecture (AWS)

- Engineered the security architecture for an AI-generated SaaS platform (Project MyLeads AI) deployed on AWS.
- Implemented secure-by-design principles to mitigate cloud-native and application-level attack vectors.

Envoy Security Tooling

- Designed Rust-based Envoy extension to prevent sensitive data exposure between backend and frontend layers.

AI Security & Isolation Research

- Investigated isolation assumptions in AI-driven environments and interaction boundaries between application layers.

Compiler Security Research | CERT-IL #11265

- Built semantic fuzzing workflow for SBCL compiler internals.
- Identified three compile-time trust boundary issues disclosed to CERT-IL and MITRE.

MILITARY SERVICE

IDF - Combat Intelligence | Reconnaissance Specialist | *2016 – 2018*

- Specialized in data-driven pattern recognition, threat intelligence, and strategic analysis within high-stakes operational environments.

EDUCATION

B.Sc. Computer Science | Jerusalem College of Technology | *2021 – Jul 2025 · GPA: 89*

Hebrew (Native) · English (Professional)