LIAM GOSS

liamjgoss@gmail.com | linkedin.com/in/liamgoss | github.com/liamgoss | Cleveland, TN 37312

EDUCATION

M.S. Cybersecurity and Information Assurance – Western Governors University (Apr, 2025)
B.S. Computer Engineering – California State University, Fresno (May, 2024)

CERTIFICATIONS

- CompTIA PenTest+
- CompTIA CySA+
- (ISC)² Certified in Cybersecurity

EXPERIENCE

NASA Jet Propulsion Laboratory – Mission Control Systems Test, Integration and Deployment Team
Software Engineering Intern *(Oct 2023 – May 2024)*

- Reduced mission-critical configuration errors by 30% for Deep Space Network systems by building schema validation and enforcement tooling for telemetry, tracking, and command (TT&C) data
- Collaborated with cybersecurity engineers to verify secure communication paths and validate data integrity for active mission operations
- Designed telemetry schema validation pipelines preventing malformed inputs from propagating to production systems

NASA Jet Propulsion Laboratory – Mission Control Systems Test, Integration and Deployment Team
Test Automation Engineering Intern *(Jun 2023 – Aug 2023)*

- Developed automated regression test suites (Python/Bash) for DSN subsystems, reducing manual testing by 50% and improving uptime for mission-critical operations
- Built telemetry log parsing and anomaly detection scripts using pattern analysis techniques applicable to intrusion detection & threat hunting
- Integrated test automation into Jenkins CI/CD pipelines for continuous validation across subsystems

PROJECTS

EZRA: Zero-Knowledge Encrypted File Sharing Platform
M.S. Capstone – Zero trust file sharing with cryptographic access control

- Designed and implemented a privacy-preserving file sharing system using ZK-SNARKs (Groth16/bn254, Circom) for anonymous, non-interactive access verification without identity disclosure
- Implemented AES-256-GCM client-side encryption with metadata suppression (timestomping, log disabling) to prevent correlation attacks and forensic recovery
- Conducted OWASP-informed security testing including oracle attack simulations, proof manipulation attempts, and metadata inference vectors; mitigated 100% of identified vulnerabilities
- Built dual deployment architecture: public mode (maximum anonymity, no logging) and enterprise mode (RBAC, configurable audit logging, NIST CSF alignment)

Hardware Cryptographic Attack Research
Undergraduate Research – Side-channel analysis and fault injection on AES

- Recovered full AES-128 keys via Correlation Power Analysis (CPA) using ~1100 electromagnetic traces captured with ChipWhisperer and H-field probe
- Executed Differential Fault Analysis (DFA) attacks using clock glitching to induce round-skipping faults, extracting keys from glitched ciphertexts using phoenixAES
- Implemented AES-128 in Verilog on Intel DE2-115 FPGA as custom IP component, creating attack target with exposed electromagnetic emissions
- Developed Python tooling integrating ChipWhisperer and ChipSHOUTER APIs for automated fault injection campaigns

Embedded Systems Engineering
FPGA Game Console with RTOS

- Designed custom embedded system on Intel Nios II soft processor with Micrium RTOS, demonstrating hardware-software co-design and real-time task scheduling
- Wrote bare-metal C interfacing directly with custom FPGA peripherals

TECHNICAL SKILLS

Security:
Side-Channel Analysis, Reverse Engineering, Zero-Knowledge Proofs, Penetration Testing, Threat Modeling, Vulnerability Assessment
Programming:
Python, C/C++, Bash, Verilog, JavaScript/Node.js, ARM/x86 Assembly
Tools:
Burp Suite, ChipWhisperer, IDA Pro, Ghidra, Wireshark, Docker, Jenkins, Linux