

András Gémes

shadowshell.io | github.com/gemesa | linkedin.com/gemesa | gemesa@protonmail.com

Summary

Compiler engineer and reverse engineer with embedded systems background and 7 years of cybersecurity experience.

Hands-on experience in binary analysis, reverse engineering and malware analysis. Certified in Sec+, CASP+/SecurityX, CEH, PMAT, IMBT and others. Looking to apply my expertise as a security engineer, reverse engineer or malware analyst.

Work experience

Compiler Engineer | Reverse Engineer @ *HighTec EDV-Systeme GmbH - Budapest, Hungary* **Feb 2023 – Present**

- Evaluating security impact of reported LLVM vulnerabilities as a [member of the LLVM security group](#)
- Obfuscating the HighTec Rust toolchain binaries against reverse engineering
- Implementing custom LLVM-based code obfuscator pass plugins

Application Security Engineer @ *Knorr-Bremse - Budapest, Hungary* **May 2018 – Jan 2023**

- Developed and maintained iOS and Android apps for real-time vehicle data visualization
- Implemented and evaluated static application security testing across embedded C codebases
- Resolved embedded systems vulnerabilities discovered through AFL++ fuzzing

Technical skills

Programming languages: C, C++, Rust, Objective-C, Swift, Python 3, Java, Assembly (ARM64, x86-64), Bash

Reverse engineering (static): Ghidra, IDA, otool, llvm-objdump, ipsw, Apktool, jadx, Binwalk, capa, YARA, DiE

Reverse engineering (dynamic): LLDB, GDB, Frida, DTrace, ADB, eBPF, strace, QEMU, Qiling, VirtualBox, x64dbg

Vulnerability research: checksec, ROPgadget, AFL++, ASan, MSan, TSan, UBSan

Network analysis and protocols: Wireshark, Suricata, Zeek, FakeNet-NG, INetSim, TCP, UDP, HTTP, HTTPS, DNS

Platforms and DevOps tools: Linux (Fedora, Ubuntu), macOS, Windows, Git, Docker, GitHub Actions, Jenkins

Embedded systems and protocols: STM32, ESP32, Wi-Fi, CAN, SPI, UART, I2C

Certifications

[CompTIA Security+](#), [CompTIA CASP+/SecurityX](#), [EC-Council CEH](#), [TCM Security PMAT](#), [Invoke RE IMBT](#) and [others](#).

Open source contributions

- [ghidra](#): contributing bug reports and patches to Ghidra, focusing on the BSim, Debugger and FunctionID features
- [phantom-pass](#): implementing custom LLVM-based code obfuscator pass plugins as part of personal research
- [o-mvll](#): improving the LLVM-based iOS code obfuscator passes and diagnostics
- [rust-arm64](#): writing a Rust book about analyzing Rust-to-ARM64 compilation
- [shadow-shell](#): developing a cyber lab for shellcode analysis, using Assembly and C

Education

MSc in Mechatronics Engineering **Feb 2016 – June 2018**

Budapest University of Technology and Economics - Budapest, Hungary

BSc in Mechatronics Engineering **Sept 2012 – Jan 2016**

University of Pannonia - Veszprém, Hungary

Continuous education

Currently I am actively learning on [TryHackMe](#) and reading [Advanced Apple Debugging & Reverse Engineering](#).