

András Gémes

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

Summary

Compiler engineer specializing in reverse engineering with 7 years of cybersecurity experience. [Hands-on experience](#) in binary analysis, reverse engineering and malware analysis (e.g., ransomware and botnets). Certified in [Sec+](#), [CASP+](#)/[SecX](#), [CEH](#), [IMBT](#), [PMAT](#) and [others](#). Looking to apply my expertise as a security engineer, reverse engineer and malware analyst.

Work experience

Compiler Engineer @ HighTec EDV-Systeme GmbH - Budapest, Hungary

Feb 2023 – Present

- Obfuscating the HighTec Rust toolchain binaries against reverse engineering
- Representing HighTec as a [member of the LLVM security group](#)
- Implementing Rust and assembly tests for the HighTec Rust compiler

Application Security Engineer @ Knorr-Bremse - Budapest, Hungary

May 2018 – Jan 2023

- Implemented and evaluated static application security testing across C codebases
- Resolved vulnerabilities discovered through AFL++ fuzzing
- Developed and hardened CAN communication, memory management and RTOS software modules

Technical skills

Programming languages: C, C++, Rust, Go, Python 3, Assembly (ARM64/AArch64, AMD64/x86-64), Bash

Reverse engineering (static): Ghidra, IDA, Binwalk, Joern, capa, YARA, DiE, llvm-readelf, llvm-objdump

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

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), 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](#), [Invoke RE IMBT](#), [TCM Security PMAT](#) and [others](#).

Open source contributions

- [ghidra](#): contributing bug reports and patches to Ghidra, focusing on the BSim, Debugger and FunctionID features
- [ghidra-scripts](#): implementing custom Ghidra scripts to support reverse engineering
- [rust-arm64](#): writing a Rust book (*From Rust to assembly: ARM64 code generation patterns*)
- [joern](#): working on improved binary analysis capabilities through Ghidra integration
- [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](#), reading [Blue Fox: Arm Assembly](#) and managing my [homelab](#).