

András Gémes

shadowshell.io github.com/gemesa [linkedin.com/gemesa](https://www.linkedin.com/company/gemesa) gemesa@protonmail.com

Summary

Embedded software engineer with 7 years of experience and a strong interest in cybersecurity, with [hands-on experience](#) in malware analysis and reverse engineering (e.g., ransomware, loaders and botnets). Certified in [Sec+](#), [CASP+/SecX](#), [CEH](#), [IMBT](#) and [PMAT](#). Looking to apply my technical expertise and security skills in a malware analyst or reverse engineer role.

Work experience

Rust Embedded Software Engineer

Feb 2023 – Present

HighTec EDV-Systeme GmbH - Budapest, Hungary

- Developing Rust compiler tests in Rust and assembly, and creating C and Rust examples for customers
- Hardening the Rust toolchain binaries against reverse engineering
- Representing HighTec as a member of the LLVM security group

Embedded Software Engineer

May 2018 – Jan 2023

Knorr-Bremse - Budapest, Hungary

- Configured, automated and evaluated Static Application Security Testing (SAST) using PC-lint and Clang-Tidy tools
- Configured memory, real-time operating system (RTOS) and Controller Area Network (CAN) software modules
- Integrated Advanced Driver Assistance Systems (ADAS) software across various Electronic Control Units (ECUs)

Skills

Languages: C, Rust, Python 3, Assembly (ARM64/AArch64, AMD64/x86-64), Bash

Malware analysis (static): Ghidra, IDA, capa, YARA, DiE, dnSpy, readelf, objdump

Malware analysis (dynamic): GDB, LLDB, QEMU, strace, eBPF, VirtualBox, Qiling, Frida, x64dbg, Sysinternals, Regshot

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, AURIX, Wi-Fi, CAN, SPI, UART, I2C

Certifications

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

Relevant projects

- [ghidra](#): contributing bug reports and patches to Ghidra, focusing on the BSim, Debugger and FunctionID features
- [ghidra-scripts](#): implementing custom Ghidra scripts to support malware analysis
- [rustbininfo](#): submitting various improvements targeting the compiler version and dependency guesser
- [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

I am actively learning on [Maldev Academy](#) and [TryHackMe](#), reading [Blue Fox: Arm Assembly](#) and managing my [homelab](#).