

# András Gémes

[shadowshell.io](https://shadowshell.io) | [github.com/gemesa](https://github.com/gemesa) | [linkedin.com/gemesa](https://linkedin.com/gemesa) | [gemesa@protonmail.com](mailto: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](#), [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**

- 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 maintained an iOS app for real-time vehicle data visualization

## Technical skills

---

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

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

**Reverse engineering (dynamic):** LLDB, GDB, Frida, QEMU, Qiling, strace, eBPF, 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

## 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 obfuscator pass plugins
- [o-mvll](#): improving the LLVM-based code obfuscator passes and diagnostics (focusing on iOS)
- [rust-arm64](#): writing a Rust book (*Rust to assembly: ARM64 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](#) and reading [Advanced Apple Debugging & Reverse Engineering](#).