

# 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

---

LLVM compiler engineer and malware analyst 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+/SecX](#), [CEH](#) and [others](#). Open to roles in security research, compiler-level obfuscation, reverse engineering or malware analysis.

## Work experience

---

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

- Reverse engineering malware samples to build a knowledge base of obfuscation techniques
- Implementing custom LLVM-based code obfuscator pass plugins
- Evaluating security impact of reported LLVM vulnerabilities as a [member of the LLVM security group](#)

**Software Engineer | 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, Binwalk, capa, otool, ipsw, Apktool, jadx

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

**Detection engineering:** Sigma, YARA, Suricata

**Vulnerability research:** checksec, ROPgadget, AFL++

**Network analysis and protocols:** Wireshark, 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
- [ghidra-scripts/reversing-scripts](#): developing custom scripts to support reverse engineering
- [phantom-pass](#): implementing custom LLVM-based code obfuscator pass plugins
- [o-mvll](#): improving the LLVM-based iOS code obfuscator passes and diagnostics
- [rust-arm64](#): writing a Rust book about analyzing Rust-to-ARM64 compilation

## 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 learning on [Mobile Hacking Lab](#) and reading [Advanced Apple Debugging & Reverse Engineering](#).