

# 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

---

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

## Work experience

---

**Rust Software Engineer @ HighTec EDV-Systeme GmbH - Budapest, Hungary**

**Feb 2023 – Present**

- Implementing Rust and assembly tests for the Rust compiler
- Hardening the Rust toolchain binaries against reverse engineering
- Representing HighTec as a member of the LLVM security group

**Embedded Software Engineer @ Knorr-Bremse - Budapest, Hungary**

**May 2018 – Jan 2023**

- Implemented, automated and evaluated static application security testing (SAST)
- Configured and hardened memory and real-time operating system (RTOS) software modules
- Investigated and debugged critical software issues at the assembly level

## Skills

---

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

**Reverse engineering (static):** Ghidra, IDA, Joern, capa, YARA, DiE, readelf, objdump

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

**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](#) and [TCM Security PMAT](#)

## Open source contributions

---

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

---

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