

Rafi Gana – C.V.

Personal and contact information

Email: mail@rafigana.com

Languages: Hebrew (Native), English (Full professional proficiency)

Professional experience:

Software Security Consultant – Freelance (2023)

- Compiling comprehensive reports on existing vulnerabilities, including risk assessments and detailed remediation plans to guide stakeholders.
- Crafting and implementing a robust secure development process policy to minimize future vulnerabilities and ensure secure coding practices.
- Conducted in-depth reverse engineering and penetration testing projects to uncover, report and/or exploit security weaknesses in software applications, improving their security resilience.

Embedded Systems Security Researcher – CyberToka Ltd. (2020-2022)

- Reverse engineering Automotive embedded systems, with focus on RCE and PE, using different RE and debugging tools including Saleae, IDA, Ghidra, GDB, Frida, ptrace and more.
- Security research from “bare metal” chip off, eMMC OOB data parsing and partition analysis, to patching and Jailbreaking, all the way through vulnerability research on vast attack surfaces, in order to gain full system compromise.
- In-depth knowledge of the Linux kernel including patching the source code and writing LKMs.
- Monitor, analysis and manipulation of traffic throughout the network stack on different protocols including WiFi and Bluetooth while using different tools such as Wireshark, Burp, TCPdump, Ubertooth, Internalblue, Airmo and BlueZ.

Software Engineer and OS Security Researcher – Prime Minister’s Office (2016-2019)

- APKs and ELF reversing for various customer demands using state of the art debugging and decompiling tools.
- Coping with modern OS security mitigations and exploitation countermeasures, including obfuscated code, DEP, ASLR and stack canaries.
- Managing and developing several full-stack projects from planning through execution: design, development, integration, release, full scale deployment and on-site support.

Electronic Warfare R&D and Maintenance Team Leader – Air Force Base 108 (2013-2016)

- Led a team of hardware practical engineers and B.Sc. Graduates, accountable for maintenance and development in the field of RF signal generators and high power transmitters.
- Designing, developing and implementing embedded applications from PCB design through algorithms in C on NIOS CPUs to final user interface in C#.
- Mentored Electronics Practical Engineers during their final project.
- Mastering electronics test equipment e.g. Spectrum Analyzers, Network Analyzers and Scopes

Education:

2016-2020: B.Sc. Computer Science at The Academic College of Tel Aviv-Yafo

2011-2013: Electronics Practical Engineer at “Amal 1 Holtz”, Tel-Aviv-Yafo

2008-2011: High school Graduate at “Amal 1 Holtz”, Tel Aviv-Yafo

Military Service (IAF base 108):

2013-2016:

Position: Electronic Warfare R&D and Maintenance Team Leader