Arash Eslami

Tehran, Iran

+98 9123884101 • 0xarash@duck.com

https://www.linkedin.com/in/arash-eslami-4555b7172/

https://github.com/0xarash

Experience

Mahsan Co.

Senior Software Engineer *2022/10-2024/07*

- Worked with a team on the development of a DLP project, where I primarily contributed to the Windows user-mode service and kernel-mode driver development. Utilized C, modern C++11/14, Google Protobuf, and Boost.

Graph-Inc.

Senior Software Engineer *2022/10-2024/08*

- Architected and led development of Windows EDR agent software, including multi-threaded service and kernel mode driver that aggregated all system events and protected agent. Utilized modern C++11/17, gRPC, Boost, and msgpack.
- Created functionality test framework for EDR software, executing and managing an arbitrary number of tests on virtual machines in parallel. Framework was written in Python, Powershell, and C.
- Developed complete Sandbox monitoring module to analyze malware behavior using C language, enhanced with hypervisor extension, using libclang to generate monotonous hook functions.
- Directed creation of back-end software service for Sandbox project, managing virtual machines and receiving all sandbox logs, using Python and zmq messaging library.
- Designed Hypervisor-based Introspection software to complement Sandbox product, leveraging KVM (Bitdefender branch v7), libvmi and libkvmi open source projects.

Behin Samaneh Farda Co.

Embedded System Engineer *2016/12-2023/11*

- Engineered multi-task CTI (Computer Telephony Integration) software on Texas Instrument C6000 DSP series processor. Analog hardware telephones and DSP-toPC communication accomplished through PCI bus. Utilized Real-Time OS called DSP/BIOS from TI with customized in-house boot-loader.
- Initiated Linux kernel driver based on DAHDI interface to connect analog telephony hardware to Asterisk PBX. Detection of telephony signaling and Voice G.711.

Software Engineer *2016/12-2023/11*

- Built C++11 multi-threaded middle-ware module for communication with CTI hardware, receiving voice and signaling data through PCI bus and processing it for use in DLS2000 server.
- Created Windows kernel driver using Jango WinDriver related to DLS2000. Managed DMA, interrupts, and safe termination of middle-ware software for CTI hardware.
- Enhanced DLS2000 product for Mitel PBXs and IP telephones. Included recording of signaling and voice data and ACD information from Mitel PBXs.
- Managed design of new VoIP license architecture and GUI software to unify configuration of DLS2000 using C++ and Qt.
- Produced new GUI software to unify configuration of DLS2000 with C++ and Qt.

IWIN Co.

Embedded System Engineer *2016/03-2016/06*

- Implemented modular software to evaluate HSM (Hardware Security Module) product device using test cases generated from parsing NIST CAVS (Cryptographic Algorithm Validation Program) files. Executed on both x86 and ARM (Zynq-7000) Linux.
- Customized OpenSSL to communicate with HSM device through IWIN Co APIs.

Amnpardaz Co.

Vulnerability Researcher *2014/05-2014/10*

- Vulnerability analysis of Internet Explorer, reproduced and enhanced known exploits for broader Windows compatibility using Heap Spray and ROP; tools: IDA Pro, IDA Python, Immunity Debugger.

TelecomRose Co.

Software Engineer *2013/06-2013/10*

- Emulated primary functionalities of a reversed-engineered MIPS architecture IPTV device, analyzed HTTP/2-based RPC communication between device and server, extracted authentication and network transmission mechanisms, and developed multi-threaded software accordingly using Python and PySide.

Reverse Engineer *2013/06-2013/10*

- Extracted and examined all binaries and files from the file-system image, analyzed network communication and RPC between the device and server, and reverse-engineered the main software to assess and understand the authentication mechanism.

Amnpardaz Co.

Incident Response Team *2011/01-2013/05*

- Worked with a group of security specialist with the main responsibility of consult to domestic organizations and companies which were affected by cyber attacks

Malware Analyst Team Supervisor *2012/03-2013/05*

- Trained, directed, and managed a small scale team, about 40 personnel.
- The main aim of the team was to monitor and analyze widespread global and domestic malware
- Successful in training most qualified malware analyst who were acquired by top and global security firms.

Malware Analyst *2010/09-2012/02*

- Analyzed top worldwide threats: Duqu, Stuxnet, Flame, Conficker, TDL4 and XPaj.
- Developed specific unpackers for known packers: UPX, FSG, ASPack and MEW.
- Developed an experimental generic unpacker. Using page fault interrupt hook technique in Windows.
- Developed disinfectors for famous viruses: Virut, Sality
- Developed an emulator for PE binaries to detect polymorphic viruses

Education

Islamic Azad University Central Tehran Branch
Associated Degree in Computer Hardware Engineering

Projects

Triangular Arbitrage: This is a simple implementation of triangular arbitrage. The Bellman-Ford algorithm is used to detect tradeable cycles with Go language

x86_64 Bootloader: Implemented a hobby project of a x86_64 boot loader which support ext2 filesystem,

accessing hard disk with ATA interface and tested in QEMU and Thinkpad T410 laptop.

Big Number Library: Developed a hobby project of an arbitrary size big number library. Supports basic arithmetic operation such as addition, subtraction, division, multiplication and other operation such as square root, logarithm and prime test, Implemented in C and recently an attempt to rewrite it in Rust language, digit size (limb) is 232 and 264.

Intel 8086 emulator: A simple hobby project written in C++ language which emulates all 8086 Intel processor instructions.

Open-Source Contribution

KVM: There is a branch which created by Bitdefender company for adding introspection capability to Linux KVM module. I added a patch also to add support for introspection of CPUID instruction, a feature that used in our Hypervisor-Based Project in Graph-Inc. The git commit information can be accessed from this / link: `https://github.com/KVM-VMI/kvm/pull/41/files`

LibVMI: LibVMI is a virtual machine introspection library. I had done couple of small patches while I was working on Graph-Inc hypervisor extension to our Sandbox project. / link: `https://github.com/libvmi/libvmi`

libkvmi (KVM Virtual Machine Introspection Library): This is an internal user-mode library that access to Bitdefender KVM branch. I added user-mode portion of supporting CPUID introspection. / link : `https://github.com/bitdefender/libkvmi`