Emin Ghuliev

E-mail : drmint80@gmail.com
Phone : +994552171929
Website: http://blog.emingh.com

Work experience

Ensign InfoSecurity — Sep 2019 — Nov 2019

Security Engineer

- Perform research to discover vulnerabilities in operating systems, software applications and hardware devices through code audit, black box testing and reverse engineering
- Develop and enhance processes and tools for the discovery and triage of vulnerabilities.
- Research into new vulnerability discovery techniques and processes.

e-Gov Development Center — Sep 2018 — Sep 2019

Senior System Architect

Design architecture of Electronic government of Azerbaijan: :

- Perform research/analysis about technologies (SWOT) for new Data Exchange Layer information system.
- Design high-load architecture for new DXL (Development of Access-list module with XDP to achieve high-performance, new storage functionality, Integration of TPM to protect sensitive credentials for Firecracker, Kubernetes).
- Design architecture of micro-service based system (Container Orchestration, Distributed Tracing System, Continuous Integration etc.)

Freelance — Aug 2018 — Aug 2019

Software Engineer

- Implemented Page-Modification logging, Introspection (MSR, GPRs, Page table tracking) mechanisms to Intel HAXM.
- Write custom Z80 IL/Processor emulator for observable debugging.
- Development of custom OS and Firmware to load linux kernel with VT-x.
- Write own KVM based VMM in spare time (virtio based, PCI, ACPI, Network, VFIO also MSI, MSIx support).
- Contribution open source projects.
- Implement custom features to coreboot (with C/Rust) .
- Development of encryption/storage plugins for Docker.
- Integrate C/Rust based applications to CI/CD environment.
- Development of Linux kernel driver (USB stack, PCIe, IRQ Chip drivers).
- Write win32k/ntoskrnl based hooker in Qemu (https://www.youtube.com/watch?v=W0jNMQhx7HI)

APA Holding — Nov 2017 — Aug 2018

Head Of IT Department

- Manage IT team, periodical appraisals, feedback and coaching.
- Set up IT team and expert groups, define required skill sets and training.
- Maintain IT policy, improve security and data protection methods.
- Outline system development directions and projects define associated processes and
- tasks.
- Responsible for smooth operation of safety solutions and IT system.

APA Holding
Aug 2015 — Nov 2017

System Engineer

- Develop security tools (Web application firewall, Web application security scanner to scan most common vulnerabilities) and monitoring tool to gather system report in production systems (with SNMP protocol)
- Develop high-reliable applications with multithreading and SSE/AVX instruction set to gain performance in high-load systems.
- Setup and configuration of CI/CD environments.
- Develop and deploy APIs in Microservices environment.
- Maintaining software builds, control code submitting at build infrastructure.
- Designing highly available, scalable and durable systems (performance tracing in kernel level with SystemTap, Perf, eBPF etc.).
- Development of Ansible playbooks for the installation of multiplatform agents (Windows, RHEL, Ubuntu).
- Automating infrastructure creation and provisioning using Ansible.
- Experience in containerization and orchestration using Docker and Kubernetes.

I used Golang, C, Python programming languages during this time period to develop most reliable infrastructure.

Azerbaijan Government CERT
Jan 2013 — Jan 2014

Security Researcher

- Penetration testing, vulnerability scanning of government departments networks and web applications.
- Development of Honeypot with PHP/C++.
- Research into advanced exploitation techniques.
- Hunting for vulnerabilities in Open Source (Web servers, Mail platforms etc.).
- PoC Development and testing various concepts.
- Malware and Threat analysis based on Honeypot data.
- Reverse engineering Device Drivers and Firmware for various platforms (IoT researching).
- Malware analysis and research.
- Exploit development for known vulnerabilities

Qualifications

- 1st place in Hackathon Azerbaijan contest (2014)
- 2nd place in Hackathon Azerbaijan contest (2013)

Interests

I have over a decade of experience with security researching, software development, system architecture.
My work area covers Kernel development/researching (NT, Linux), device driver development, virtualization, analysis security implementation in firmware, hardware, operating system. I like research and design CPU with FPGA and discrete components to understand structure and implementation of CPU. Also, I'm interested in optimize high-load systems and measure performance from Micro-architectural state (PMU or develop my custom OS to have minimal noise with few main implementation e.g Memory management, syscall emulator, ABI emulator etc.) to algorithmic state (Time/space complexity).

I did development/research/implement some features in my free time related to virtualization (KVM, Xen), Windows protection mechanisms (ACG, CFG, CFI, HVCI etc.), open source firmware/payload (seabios, coreboot), UEFI (use FT2232h USB UART/SPI module, chipsec, uefitool and develop own scripts), electrical engineering, JS engine researching/development (v8), embedded development. I like Security field that's why I have security related researches and applications. Researching the cutting edge of fuzzing techniques and development hardware-assisted (IntelPT, Qemu) and software-assisted (LLVM SanitizerCoverage) fuzzer. Development of Clang instrumentation for effective feedback-guided/code coverage fuzzing.
Researching UEFI, SMM, Hardware vulnerabilities and Secure Boot/Boot Guard/Flash protection.
I have found the new way of bypass Intel Boot Guard technology (ACM) and PRx protection registers bypass

(SMMLockBox module) mechanism in Lenovo Thinkpad.
https://support.lenovo.com/us/en/product_security/LEN-26332

My Specialties: Software Engineering (C/C++/Rust) Kernel development, FPGA development, Optimization, Reverse Engineering, System/Software Architecture, Compiler (JIT, Interpreter) design/development.

References

Github account:
https://github.com/eminghuliev
Linkedin profile:
https://www.linkedin.com/in/emin-ghuliev-461a22129/
Blog:
http://blog.emingh.com