Petr Zankov

1020 Renens
Switzerland
☎ *+41 78 850-95-57*
✉ *petr.zankov@gmail.com*

Summary

Specialization	Systems software engineer
Software skills	Assembler (x86, x86_64, PowerPC, ARM, SIMD), C, C++, C#, Python, Java, GNU Toolchain (gcc, gdb and others), LLVM, Git, LaTeX, Visual studio, Doxygen, Shell scripts (bash, batch, PowerShell), IDA, GTK, OpenGL, OpenAL, OpenCV, WiX Toolset, Django, Linux kernel drivers, Windows kernel drivers, embedded systems, Symbolic binary execution, Static binary analysis
Hardware skills	FPGA (Verilog, circuit diagrams), microcontrollers (AVR, ARM), PCB layout (Mentor graphics, manual)

Experience

2014–present **Software engineer**, *Dependable Systems Lab, EPFL*, Lausanne, Switzerland.

Improved the document protection endpoint agent:
- developed a userspace-kernel data serialization framework
- improved the labelling of protected applications
- automated builds and testing with Jenkins

Improved the S^{2}E-based malware scanning engine:
- eliminated false positive analysis results
- improved user interface by using the Kibana data visualiser
- extended engine to support Microsoft Office documents
- implemented integration with Microsoft Sharepoint

Integrated the S^{2}E symbolic execution engine with a fuzzer:
- implemented both S^{2}E-to-fuzzer and fuzzer-to-S^{2}E PoV exchange
- allowed to discover 30% more bugs in the same time frame

Automated proof of vulnerability generation with the S^{2}E symbolic execution engine:
- allowed seamless PoV generation for every bug discovered in the binary
- introduced no overhead to the execution process
- successfully used in a CTF security competition

Developed a memory bugs detection technique based on S^{2}E symbolic execution engine:
- utilizes novel metadata propagation approach
- allows dynamic detection of memory violations
- gives zero false positives with a real world applications

2012–2014 **Software engineer**, *LLC "WISE-Technique"*, Zhukovskij, Russia.

Developed a microkernel real time operating system with ARINC 653 and POSIX(partial) layers. Following features were implemented from scratch:
- OS kernel
- multi-arch and multi-core support for PowerPC and IA-32
- drivers for PCI, SATA, Ethernet
- debugging environment (based on KVM and GDB)

Developed kernel drivers and user space software for the helicopter flight recorder:
- implemented an ARINC653 API layer for the common kernel drivers
- deployed RTOS on cutomer's embedded hardware system

2012–2012 **Software engineer**, *FSUE "Flight Research Center"*, Zhukovskij, Russia.
Migrated 3D rendering engine from X11 to Wayland. Also enhanced performance by reimplementing functions using SIMD instructions.

2008–2012 **Software engineer**, *JSC "V.V. Tikhomirov Scientific Research Institute of Instrument Design"*, Zhukovskij, Russia.
Developed software for civil sonar data acquisition and analysis. Full software stack starting from FPGA firmware and up to GUI applications was implemented:

- FPGA firmware for signal synthesis and digitizing
- FPGA device driver for Linux
- user space cross-platform software for sonar control and data processing
- real time data acquisition, processing and layout

Education

2011 **Master of Applied Mathematics and Physics**, *Moscow Institute of Physics and Technology*, Russia.

2009 **Bachelor of Applied Mathematics and Physics**, *Moscow Institute of Physics and Technology*, Russia.

Languages

French	Basic communication skills
English	Upper Intermediate
Russian	Native

Hobbies

Big mountain freeride skiing, freestyle skiing, radio electronics

Last update: December 13, 2016