Name:	Maxim Menshikov
Phone:	+351 91 058 98 54
E-Mail:	`maxim@menshikov.org`
Web site:	`https://menshikov.org`
GitHub:	`https://github.com/maximmenshikov`

I am a white-hat hacker with strong computer science background enjoying breaking boundaries of what's achievable by one person. I prefer jobs where the influence of individuals matters.

Soft skills

- I can **communicate with everyone**, including customers, partners and end-users. Proficient in English and Russian.
- **Strong leadership and planning skills**. Various teams successfully finished projects in time under my leadership.
- **Self-confident**. I don't lose my mind in critical situations and keep developing a solution even when nobody believes it will work. Several saved multi-million USD contracts are good evidence.
- **Self-motivated**. Working towards a solution without any need for micromanagement.

Hard skills

- Writing software and drivers for **Windows**, **Linux**, **Mac**, **Windows Mobile/Windows Phone**.
- Knowledge of **x86**, **ARM** and **MIPS** architectures, recognized expertise in **security** research.
- Proficiency in **C**, **C++**, **C#**, **Assembler**, **Rust**, **Python**. Knowledge of **Java**, **Scala**, **JavaScript**, **TeX**.
- Well aware of toolchains comprising **compilers, analyzers, debuggers and standard libraries**.
- Industrial knowledge of **networking**, **containerization** and **Linux-based environments**.
- Familiarity with DevOps and infrastructure building.

Education

Saint Petersburg State University

2018-2022	Finished PhD studies (Researcher, teacher-researcher) Department of software engineering — "Informatics" (Computer Science) Thesis **"Hybrid language-independent static analysis as an element of complex programming technology"**.
2016-2018	Master of Science — **with honors**. "Fundamental informatics and information technologies" (Computer Science) Thesis **"Hybrid system for static analysis with proof-based verification of invariants"**.
2012-2016	Bachelor of Science. "Fundamental informatics and information technologies" — "Programming and Information Technologies" (Computer Science) Thesis **"Detecting race conditions in C code by static analysis"**.

Professional work experience

Interpretica, Unipessoal Lda 2023-present	**Chief Executive Officer** • Starting up development tools business. • Managed the corporate infrastructure. • Managed to get approval of **Portuguese IAPMEI - the agency for competitiveness and innovation**.

Interpretica, Unipessoal Lda
2023-present

Chief Executive Officer
- Starting up development tools business.
- Managed the corporate infrastructure.
- Managed to get approval of **Portuguese IAPMEI - the agency for competitiveness and innovation**.

Unnamed startup
2020-2023

Founder
- Prepared a static analyzer tool for commercial use.
- Managed administrative work, reports, taxes, trademarks, patents.
- Managed the infrastructure.

Softcom, Ltd
2020-2023

Principal developer / Team Leader
- Leading a team developing static analysis tools: technical requirements, plans, official documentation, task assignment, code reviews, release preparation.
  - **Released static analysis core with customer-requested features**.
  - Helped shape IDE integrations.
- Help planning and developing features for various teams, judging technical solutions.
  - **Participated in a novel secure programming language project**, judging technical solutions, preparing integration with a static analyzer.
  - Prepared a set of infrastructural tools used throughout the company: Wireguard user management, automatic documentation builder, release server maintenance, etc.
- Led a team developing firmware for a wristband firmware (9 developers of various levels, from junior to senior). ARM architecture.
  - Technical requirements, plans and documentation.
  - Task assignment, code reviews.
  - Architected a wristband firmware solution, negotiated architecture with a customer, did hardware design negotiations.
  - Coded firmware solutions for wristband project.

OKTET Labs, Ltd
2014-2023

Senior Software Engineer / Team Leader
- Worked on software for Linux-based routers for Tilgin/Seliro/Iopsys (Sweden). ARM/MIPS/MIPSEL architectures.
  - Main domains: internal management system, WiFi drivers, uBoot, SoC, networking and storage subsystems, Linux.
  - **Did router-related security research. Successfully deactivated several country-wide attacks on routers. Was gradually improving security on devices.**
  - Created infrastructure for storing and processing security certificates used for over 9 years without production issues.

- Developed a package manager for internal needs promoted as a part of OpenHGA SDK.

- Implemented a container-based virtualization system for the Internet-Of-Things devices, which was marketed at the Internet Service Provider gateway market. **Ported Docker to MIPS during initial feasibility investigation**.

- Maintained SMB/FTP/TFTP protocol support, coded a complete OverlayFS-based solution for overlaying squashfs.

- Added support for IPSec (KLIPS and XFRM) and OpenVPN tunnels with partial hardware traffic acceleration.

- Did a big rewrite of unstable USB Host Controller driver shipped with SoC, that **helped save multi-million contract as recognized by management team**.

- Debugged a memory leak in WiFi Mesh daemons, **saving multi-million contracts for the customer**.

- Backported SECCOMP, AppArmor mechanisms to an older kernel.

- Coded numerous Linux kernel drivers and fixed issues in various third-party drivers.

- Worked around numerous issues in packet processing accelerator drivers.

- Consulted clients about network protocols, operating system architecture, security.

- Managed a team performing testing and detailed analysis of UndoDB (Undo Software, UK) for native and managed code.

  - Coded a complete Test Suite for reproducible verification of stability and performance of the reversible debugger for C++ and Java. Based on Docker, multi-agent test environment in C and Python scripting.

  - Reported thousands of defects in the debugger.

- Integrated my own static analyzer to company's projects.

NowSecure (formerly viaForensics LLC)
2013-2014

Security analyst, Windows Phone 8 lead, consultant.
- Worked on porting the company's data extraction projects to Windows Phone 8.
- Investigated Windows Phone 8 security and found several exploits in it.
- Prepared multiple Proof Of Concepts for future *Jailbreak*.
- Participated in making strategic decisions about the company's product line.

Enthusiastic projects - highlights

The complete list is available at: `https://menshikov.org/projects`

2014-... **Visao - static analyzer for industrial applications**
Lead developer.
- Developed language-agnostic analysis architecture from scratch.
- Implemented "Semantic Virtual Machine" for fast distributed analysis.
- Created an internal programming language **Midair** for a semantic virtual machine.
- Designed a method for combining Abstract Interpretation and Model Checking.
- Prepared client-server APIs for accessing static analysis features.
- The project is tested at OKTET Labs, Ltd and used in Softcom, Ltd.
- Managed a full cycle of development.
- Developed the hypervisor server and web interface for it (in Rust).

2013-2014 **Windows Phone 8 projects**
- **OSBuilder for Windows Phone 8**.
  Started the project. Implemented full build cycle for all OS partitions, wrote a tool to install images to unlocked devices, designed a policy file and registry compiler.

- **Jailbreak for Windows Phone 8**.
  Actively participated in a security research project, primarily aimed at Nokia Lumia devices. Consulted project members on various aspects of security.
  In particular, explored UEFI implementation, TrustZone code of Lumia phones, made my deobfuscator for their code and prepared implementation of security algorithms.

2011-2013 **Windows Phone 7 projects**
- **Full Unlock** – Jailbreak for Windows Phone 7.
  Lead developer.
  Designed and implemented jailbreak used in more than 100.000 devices around the world. Reverse-engineered OS binaries related to platform security.

- **OSBuilder for Windows Phone 7** – unpacking of OS images, image generation for various devices.
  Co-author.
  Wrote a module for D000FF format developed by Microsoft. Added support for modules with Z relocation flag (first used in Windows Phone 7), prepared tools for relocating such modules. OSBuilder is the only unofficial tool to build Windows Phone 7 images.

- **Dynamics7 ROM** – *the reference custom ROM in Windows Phone 7 community used by nearly all developers.*
  Lead developer and visionary.
  Planned features, created modules, ported features from different devices, managed releases. Used in more than 100.000 devices around the world.

2009-2011   **Windows Mobile 6 projects**

- **OSBuilder for Windows Mobile – unpacking of OS images, image generation for various devices.**
  Co-developer.
  Created a robust tool for building OS images. After thorough investigation of OS internals I created a set of functions improving stability and performance of Windows Mobile 6.x devices.

- **Dynamics ROM**
  Developed a custom ROM for Windows Mobile devices with various low-level improvements.

- **uTask – soft key reassignment for Windows Mobile 6.5.3.**
  Created a set of libraries injecting to the system and changing Close key behaviour globally.

2007-2009   **Non-commercial ELFPack for Sony Ericsson**

- **ELFPack** – Executable and Linkable Format support on SE. Wrote a set of native applications using undocumented features of Sony Ericsson phone platform; actively participated in developing ELF loader and had big influence on a project.

Selected scientific publications

The full list is available at `https://menshikov.org/papers`.

- Menshikov M. **Review of Static Analyzer Service Models**. (SYRCoSE-2021)
- Menshikov M. **Midair: An Intermediate Representation for Multi-purpose Program Analysis**. International Conference on Computational Science and Its Applications (ICCSA-2020).
- Menshikov M. **Static analyzer debugging and quality assurance approaches**. (SYRCoSE-2020)
- Menshikov M. **Towards a Resident Static Analysis**. International Conference on Computational Science and Its Applications (ICCSA-2019).
- Menshikov M. **Equid — A Static Analysis Framework for Industrial Applications**. International Conference on Computational Science and Its Applications (ICCSA-2019).
- Menshchikov M.A. **Hybrid system of static analysis with proof-based verification of invariants**. Master's thesis. 2018.
- Menshchikov M.A. **Design and testing of LXC-based virtualization system for resource-constrained MIPS devices**. Third Conference on Software Engineering and Information Management (SEIM-2018).
- Menshchikov M.A., Lepikhin T.A. **5W+1H Static Analysis Report Quality Measure**. Tools and Methods of Program Analysis 2017 (TMPA-2017).
- Menshchikov M.A., Lepikhin T.A. **Applying MapReduce to static analysis**. Control Processes and Stability 2017 (CPS-2017).

- Menshchikov M.A. **Detecting race conditions in C-code by static analysis**. Bachelor's thesis. 2016.

Patents & registered software packages

- **Virtual machine for static analysis**. RU 2021612228. Issued Feb 15, 2021.
  Registered software package.
- **Equid - a static analyzer for program code**. RU 2021612141. Issued Feb 12, 2021.
  Registered software package.
- **Multi-layer program analysis module**. RU 2021612145. Issued Feb 12, 2021.
  Registered software package.
- **libasp — a library for client-server communication with static analysis servers**. RU 2021611950.
  Issued Feb 9, 2021.
  Registered software package.

Certificates and awards

- Certificate of **Cambridge Advanced English (CAE) — C1**.
- **Stipend for mathematicians-researchers** for research excellence issued by biotechnology company
  BIOCAD. 2016–2018.
- **Presidential stipend for PhD students of priority directions of economical development**.
  2019–2020, 2020-2021.
- Winner of "Petropolitan Science (Re)Search" (St. Petersburg State University) student competition in
  Computational Technologies subject. 2017, 2018.
- Winner of the annual award on 4PDA forum in the nomination "Best Author (Windows Phone 7)". 2011.
- Winner of Sony Ericsson competition on making X-Panels for Sony Ericsson XPERIA X1. Mobile-
  Review.com. 2009.
- Coursera certificate on "PC Architecture" from Saint Petersburg State University.
- Coursera certificate on "Quantum Computing" from Saint Petersburg State University.
- Coursera certificate on "Databases" from Saint Petersburg State University.