

Michael Rofel  
Phone: 058-7782290  
roflogin@gmail.com  
ID: 336454962

## Personal details:

**Date of Birth:** 11/21/1990

**Country of Origin:** Russia

**Year of Repatriation:** 2014

**Address:** Haifa (prepared to move in accordance with the work)

**Marital status:** Single

## Education:

**2008-2013** Master's degree in engineering of computer hardware and networks, Technical State University, Penza, Russia

Final Project: Automated knowledge testing system for schools and universities.

Project details: PHP code running on Denver server provides an interface that allows logged in user to pass several tests recently prepared by the administrator or the teachers that are sorted in specific user group with corresponding rights. Results of passed tests are being stored in MySQL database and are being retrieved with according language of requests.

## Courses and Certifications:

**2013-2014** Course of information security within program of "MASA," the Technion, Haifa, MCSA certificate.

## Work Experience:

**2015-2016** Mobile phone repair technician in company "Ivritech".

Position: Diagnostic and repairs of various cellular devices, including repairs of various electronic circuitry malfunctions like short-circuited board components or BGA chips contact issues, damaged software restoration through debug interfaces such as JTAG(Medusa kit) and Apple DCSD. Resolution of corporate network problems (Active Directory maintenance, DHCP, NAT, RDP, Port forwarding) as needed.

**2015** Military Service(Haifa). Naval shipyard, Computers and networks technician (shortening the service due to age of Repatriation).

Position: Resolution of network problems at OSI levels 1-3.

**2012-2011** Technician in service laboratory of customer electronic devices "Aksioma".

Position: diagnostics and repair of electronic hardware, integration of the Xilinx (CPLD) hardware, Xilinx hardware timing debug, JTAG testing, maintenance and setup of Ethernet networks, Wi-Fi 802.11, security checks of wireless networks (WEP, WPA2-PSK, WPS By Linux Aircrack-ng set and Wireshark, security checks of Windows apps (IDA, Net reflector, Ollydbg).

**2011** Internship at “Penza research institute of electronics and electrics”, development of electronic communication devices’ nodes.

Position: Description and following debugging of electronic crypto device memory management nodes via VHDL (IDE Xilinx ISE).

**2009-2010** Engineer in computer hardware repair laboratory at computer hardware store "Ruscomp", Russia.

Position: Computer hardware diagnostics and repair technician (SMD, BGA).

## **Personal projects:**

**2015-2016** Touchscreen based wall-mountable unified electrical light switching device with wireless networking capabilities.

Summary: According to the description of this project it performs control of any household 220v electric device by the means of electromagnetic relay, it is able to provide simple touch button interface on 240x320 LCD touchscreen panel, or by means of running HTML server in home network environment.

Realization: LCD and touch panel are being driven by Arduino-UNO Development board with Atmel 328P family controller, using SPI interface and analog data to read touch points. Relay is being controlled by a ESP-8266-12 WIFI-SoC which provides wireless network functions as well, synchronization of switch status change on different control devices is performed by sending pre-described value on i2c interface.

Completion status: Development in progress. Although project development prototype is functioning according to its description, the goal is to have a device that will function in open circuit, but the current that will flow through the device will sometimes trigger controlled device to power on. Further AC part of the device development needed.

**2016** Automated cellphone repair status monitoring system.

Summary: The system allows logged in user to view the table of completed cellphone repairs, he also can add new completed repair to the database(mongodb), when the new completed repair is added, the system will send an SMS message(Twilio) to the laboratory administrator to minimize the amount of communication between technicians and other staff.

Realization: System is based on Spring Boot framework, so, literally, this is its main component. Spring Boot has built in RESTful servlet class to manage http requests, that are being made from the HTML page, the front part of system is based on AngularJS framework to optimize it for single page operation. Data is being stored and retrieved through mongodb, custom repository also presents. The system supports migration from the Google Sheets to fill all the data that was gathered before start of the system’s usage.

Completion status: Development in progress. Although the basic CRUD functionality is present, there is need to add and improve some parts of business logic, such as automatic number incrementation, grouping repairs by date, counting income for described period of time, etc.

**2016** USB fake keyboard pincode bruteforce attack tool.

Summary: Various devices have very bulwark and obsolete protection methods such as 4-6 digits pincode that can be triggered through internet by mistake or by evil intention of somebody on the side. Even if the customer is able to provide the proof of property there is no guarantee that authorised service center will be able to help him. So the idea was to recreate the device that acts like keyboard with random keystroke delays to prevent lockdown.

Realization: This device is using simple Arduino UNO board with Adafruit lcd shield. The Atmega 16U2 USB controller’s alternative firmware is written using LUFA to make device

recognizable as USB-HID device(Usage 0X07), Arduino IDE libraries have static class Serial that is responsible for handling RS232 debug interface, normally Atmega 16U2 acts as USB2SERIAL transceiver, but altered firmware allows it to forward arguments of function Serial.write to PC's USB port as keyboard keystroke buffer. The attempt to perform such bruteforce sequences from android phone that can also be mounted with keyboard usage after patching the kernel was made, but it only works well on fully UEFI supporting systems. The LCD module displays current PIN try.

Completion status: Development complete, the device has proved itself working and functioning as needed. Although there are some improvements to be made to make the device more comfortable to use. It is possible to access USB functionality through general data input-output ports of Atmel 328P, but it requires adding some circuitry to the ports, but it will make possible to read the USB bus state to, for example, catch the remount moment to save the pincode that triggered it to microsd card(microsd card support presents, but without a way to decide which pin was successful it is useless).

**Languages:** Hebrew - raised, English – excellent, Russian (native language).

### **Computer knowledge:**

Excellent (technical background in computers, infrastructure, programming).

### **Experience in operating systems:**

#### **Linux**

Basic bash maintenance commands, kernel function calls.

#### **Windows**

### **Programming experience:**

C++(console, MFC), ASM, C# in Visual Studio IDE.

IntelliJ Idea – Java SE 1.8. Core library, Spring(boot), Maven, OAuth 2.0 implementation(Google, VK), Junit. JavaScript - AngularJS.

Arduino IDE – C++, LUA. Different hardware library implementations in hardware design(Adafruit\_LCD, ESP8266, Arduino.Wire etc.), serial port terminal debug.

Xilinx ISE – VHDL, Block Diagram device entity description, simulation results analysis, following upload of compiled firmware to the device via Xilinx JTAG download cable, configured device debug(Lab Tools), timing analysis and debug (XC2C64A, XC3S250E).

Altera Quartus II – VHDL, Block Diagram device entity description, simulation results analysis.

MATLAB – writing asm code for PIC controller entities. Following port simulation debug.

### **Known Applications:**

Wireshark – TCP/UDP traffic analysis.

Cisco Packet Tracer – Cisco endpoint hardware administration.

Ollydbg – attaching to win32 process, text constants retrieval, callback address changing to acquire various results, asm cpu code analysis.

.Net Reflector – various .Net applications disassembly, analysis of source code (C++, C#).

Isolation of used methods from parent class.

IDA – win32 application disassembly. Attempt to analyze output IL code, traced calls diagram analysis.

### **MacOS X**

Slight experience in Xcode programming (cocos2dx, C++)

**Other known software**

Sprint Layout, PCAD, x86 TurboAssembler/Debugger, putty.

**Personal skills:** Creative, responsible, collaboration and work in group, effectiveness under pressure and multitasking.