Dennis Yurichev

(Curriculum vitæ)

dennis(a)yurichev.com

December 27, 2022

What I want to do

- Decompilation to pure C or C++ (AKA reverse engineering).
- Penetration testing. I can crack your software protection to test its strength.
- Technical writing.
- Programming.

Professional Experience

2013–present Author

I wrote the “Reverse Engineering for Beginners” book:
http://beginners.re

Published by Acorn publishing company (www.acornpub.co.kr)
in January 2015 and in 2021: https://www.facebook.com/acornpub/posts/4722763351083996.

Published by Pendare Pars Iranian publisher in 2016: https://beginners.re/#farsi.

Published by PTPress Chinese publisher in April 2017: https://beginners.re/#chinese.

Also translated by many contributors to many languages,
including French, German, Japanese, Italian, Polish.

Used in many universities as a textbook: https://beginners.re/#uni.

The English version can be accessed here:
https://beginners.re/pvt875194/RE4B-EN.pdf.
Russian, German, French, Japanese, Polish, Chinese: vol1, vol2.

The “SAT/SMT by Example” book:
https://sat-smt.codes/

Also used in many universities: https://sat-smt.codes/#uni.

The less known book: “Mathematical recipes”:
https://math.recipes/

2015–2017 Freelancer, reverse engineer

I rewrote complex piece of software (100KiB executable file) to pure C using decompiler and various hand-made tools.

2008–present Freelancer, freelance teacher

I made two FPGA brute-force crackers.
First was related to specific dongle crypto algorithm. Using Altera EP2S60 FPGA device, I made a hardware system which able to find crypto key extremely fast compared to modern Wintel systems.
Second project was a cracker of Oracle RDBMS passwords (pre-11g, based on DES algorithm). While most fast software brute-force attacker running on Intel Core Duo 2 able to check 1.5 million passwords per second, a hardware system built by me is able to check about Oracle RDBMS 110 million passwords per second: it was built on Altera EP2SGX90 FPGA chip. It is now easy to check all possible 8-symbol passwords spending only 9 hours.
It was connected to the Internet on 24h basis.
Short article about it: http://conus.info/ops/ops.html
I have 3 Altera FPGA boards for experiments (two on Stratix II and one on Cyclone III).

I also worked as reverse engineer.
Some of examples are in my “Reverse Engineering for Beginners” book:
http://beginners.re

Occasionally I also do software dongle protection dongle replacements or emulators:
https://dongle-emulator.net/
https://yurichev.com/dongles.html

I discovered several previously unknown vulnerabilities in Oracle RDBMS and IBM DB2 and was credited for:
https://yurichev.com/vuln.html

2010–2012 Reverse engineer and programmer

Digital Syphon

2005–2008 Reverse engineer and security researcher

"Blue Lane" (http://www.bluelane.com):

My duty was to compare original and patched binary versions of some well-known software products, investigate differences, understand the nature of security vulnerability, finding a way how malicious (for these specific vulnerabilities) packets can be blocked at the network level.

My specialization was primarily Oracle RDBMS, so I collected a lot of information related to Oracle RDBMS internals.

I developed my own x86 code tracer for navigating in such large software as Oracle RDBMS.
It was partially evolved into my own x86 tracer:
https://yurichev.com/tracer-en.html

1999 - 2005 Freelancer in areas of reverse engineering, web-scripting and programming

1998 - 1999 Linux system administrator, C/C++/CGI-scripts programmer

"Beckets-Service" (Kiev, Ukraine):
Last project I made at, was company-specific Voicemail system working with cheap voice modems.

1996 - 1998 Various computers maintenance and repairing

"Tandem-Plus" (Enakievo, Donetsk region, Ukraine)

Skills

My perfect skills:
Technical writer (software manuals, help pages, etc.)
Optimization of time-critical code parts.
Reverse engineering, restoration of code into various
high-level languages: C, C++, C#, Python, Java.
Reverse engineering various proprietary network protocols.

My very good skills:
C/C++/C#/Java/Python/x86 assembler programming for Windows/Linux.
Verilog coding (for FPGAs)
I'm familiar with SAT, SMT, CUDA, SIMD, OpenMP.

Just skills: drivers creation for any version of Windows, MS-DOS, OS/2, Linux programming.

I have knowledge of cryptography, major internet protocols, digital electronics,
computer security, Oracle RDBMS.

Other contacts

My blog about reverse engineering, programming, SAT/SMT, etc: https://yurichev.com/news/

Other information

Languages: Russian, English, Ukrainian.