Dennis Yurichev

(Curriculum vitæ)

dennis(a)yurichev.com

May 16, 2017

P.O. box 10, Kyiv, Ukraine, 04071 Skype: dennis.yurichev

Professional Experience

2013–present	**Author** Wrote “Reverse Engineering for Beginners” book: http://beginners.re Published by Acorn publishing company (www.acornpub.co.kr) in January 2015: http://www.acornpub.co.kr/book/reversing-for-beginners. Published by Pendare Pars Iranian publisher in 2016: https://beginners.re/#farsi. Published by PTPress Chinese publisher in April 2017: https://beginners.re/#chinese.
2015–present	**Freelancer, reverse engineer** I rewrote complex piece of software (100KiB executable file) to C/C++.
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:
http://yurichev.com/dongles.html.

I discovered several previously unknown vulnerabilities in Oracle RDBMS and IBM DB2 and was credited for.

Two DoS vulnerabilities in IBM DB2 9.5 (CVE-2009-0172, CVE-2009-0173)
http://www-01.ibm.com/support/docview.wss?uid=swg1IZ36534
http://www-01.ibm.com/support/docview.wss?uid=swg1IZ39373
http://blog.yurichev.com/node/17

CVE-2009-0991 in CPUapr2009 (CVSS 5.0):
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html
http://blog.yurichev.com/node/18

Four vulnerabilities patched in CPUjul2009:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html
CVE-2009-1970 (CVSS 5.0):
http://blog.yurichev.com/node/26

CVE-2009-1963 (CVSS 7.5)
http://blog.yurichev.com/node/25

CVE-2009-1019 (CVSS 7.5)
http://blog.yurichev.com/node/24

CVE-2009-1020 (CVSS 9.0)
http://blog.yurichev.com/node/23

CVE-2009-1979 in CPUoct2009 (CVSS 10.0)
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
http://blog.yurichev.com/node/28

CVE-2010-0071 in CPUjan2010 (CVSS 10.0)
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html
(also listed among security-in-depth contributors)
http://blog.yurichev.com/node/38

CVE-2010-0911 in CPUjul2010 (CVSS 7.8):
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html

Mentioned in CPUapr2011:
http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

CVE-2011-2242 in CPUjul2011:
http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html

CVE-2012-0072 in CPUjan2012:
http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

I discovered one DoS vulnerability in binkd FidoNet mailer:
http://binkd2.grumbler.org/viewcvs/HISTORY?root=binkd&view=co

2010–2012 **Reverse engineer and programmer**

Digital Syphon (http://www.digitalsyphon.com/)

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:
http://conus.info/gt/
http://blog.yurichev.com/taxonomy/term/7

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:
Optimization of time-critical code parts.
Reverse engineering, restoration of code into various high-level languages: C, C++, C#, Java, Pascal/Delphi.
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 CUDA, OpenCL, 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, Oracle RDBMS, etc: http://blog.yurichev.com/

Date of birth: 11-October-1979.
Citizenship: Ukrainian.
Gender: male.
Marital status: separated.
Children: 1.
Languages: Russian, English, Ukrainian.

Education

Donetsk National Technical University (never finished).