Volodymyr Kuznetsov

Co-founder and CEO at Cyberhaven

Phone: +1 (617) 818-0311
E-mail: vova@cyberhaven.io
URL: http://volodymyrkuznetsov.info

Cyberhaven, Inc.
25 First Street, Suite 303
Cambridge, MA 02141, United States

Education

Ph.D. in Computer Science — May 2016
École Polytechnique Fédérale de Lausanne (EPFL)

M.S. in Applied Physics and Mathematics — June 2009
Moscow Institute of Physics and Technology

B.S. in Applied Physics and Mathematics — June 2007
Moscow Institute of Physics and Technology

Work Experience

Chief Executive Officer, Cyberhaven, Switzerland — 7/2016 – Present

- Bringing the world's simplest solution for complete cyber security to the market.

Chief Technology Officer, Cyberhaven, Switzerland — 10/2014 – 6/2016

- Building the world's simplest solution for complete cyber security.

Research Assistant, EPFL, Switzerland (Supervisor: Prof. George Candea) — 5/2010 – 5/2016

- Designed and implemented Code-Pointer Integrity (CPI), a technique that prevents all control-flow hijack attacks on programs written in C/C++. Parts of CPI are now integrated into Clang/LLVM and are being integrated into Chrome and Android.
- Designed and implemented efficient state merging algorithm, which improves the performance of symbolic execution program analysis technique by several orders of magnitude, while preserving its compatibility with efficient state search heuristics.
- Refined the formulation of the execution consistency models that improve the scalability of symbolic execution while controlling its precision through automated over- and under-approximation.
- Co-designed and built the S2E platform for in-vivo multi-path analysis of software systems. The S2E platform is released open-source and is being used by hundreds of researchers and security experts around the world.

Visiting Researcher, UC Berkeley, USA (Supervisor: Prof. Dawn Song) — 4/2013 – 7/2013

- Built a fast and precise control flow integrity enforcement system (FP-CFI), which prevents arbitrary code execution attacks on non-memory-safe programs.

Research Intern, EPFL, Switzerland (Supervisor: Prof. George Candea) — 11/2009 – 4/2010

- Built a system for automated testing of closed-source binary device drivers based on selective symbolic execution and a novel concept of symbolic hardware and interrupts.

Lead Developer, EPFL, Switzerland (Remote, Supervisor: Dr. Alexey Boyarsky) — 3/2009 – 11/2009

- Designed and implemented scientific ontology, automated paper annotation and semantic bookmarking application ScienceWISE.info.

Software Developer, RAPAS, Moscow, Russia — 2004 – 2009

- Designed and implemented cycle-accurate models of various embedded platforms (including SPARC32 and MicroBlazer CPUs) that run unmodified Linux kernel.
- Developed device drivers for embedded Linux, created embeded Linux distribution.

Freelance Software Developer, Moscow, Russia — 2003 – 2005

- Designed and implemented a high performance software stack for real-time DSP-accelerated signal processing, network communication and data visualisation.
- Ported the Linux kernel to a new embedded platform and wrote device drivers for it.

Refereed Publications

Improving Systems Software Security Through Program Analysis and Instrumentation
Volodymyr Kuznetsov
EPFL PhD Thesis, May 2016

High System-Code Security with Low Overhead
Jonas Wagner, Volodymyr Kuznetsov, George Candea, and Johannes Kinder
36th IEEE Symposium on Security and Privacy (IEEE S&P), San Jose, CA, USA, May 2015

Code Pointer Integrity
Volodymyr Kuznetsov, Laszlo Szekeres, Mathias Payer, George Candea, R. Sekar, and Dawn Song
11th USENIX Symposium on Operating Systems Design and Implementation (OSDI),
Broomfield, CO, October 2014

-OVERIFY: Optimizing Programs for Fast Verification
Jonas Wagner, Volodymyr Kuznetsov, and George Candea
14th Workshop on Hot Topics in Operating Systems (HotOS XIV),
Santa Ana Pueblo, NM, May 2013

Efficient State Merging in Symbolic Execution
Volodymyr Kuznetsov, Johannes Kinder, Stefan Bucur, and George Candea
33rd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI),
Beijing, China, June 2012

The S2E Platform: Design, Implementation, and Applications
Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea
ACM Transactions on Computer Systems (TOCS), Volume 30 Issue 1, February 2012

S2E: A Platform for In-Vivo Multi-Path Analysis of Software Systems
Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea
16th International Conference on Architectural Support for Programming Languages
and Operating Systems (ASPLOS), Newport Beach, CA, March 2011
[Best Paper Award]

Testing Closed-Source Binary Device Drivers with DDT
Volodymyr Kuznetsov, Vitaly Chipounov, and George Candea
USENIX Annual Technical Conference, Boston, MA, June 2010

Invited Talks

Fast and Precise Control-Flow Hijack Protection, Dagstuhl invite-only seminar "The Continuing Arms Race: Code-Reuse Attacks and Defenses", Dagstuhl, 2015
Protecting Systems Software Against Control-Flow Hijack Attacks, Cisco, Rolle, Switzerland, 2015
Fast and Precise Control-Flow Hijack Protection, Google, Mountain View, CA, 2015
Code-Pointer Integrity, MIT, Cambridge, MA, 2014
Code-Pointer Integrity, Columbia University, New York, NY, 2014
Code-Pointer Integrity, Stanford, CA, 2014
Practical Protection Against Control-Flow Hijack Attacks, Dropbox, San Francisco, CA, 2014
Pracical Analysis of Large Sofware Systems Using Symbolic Execuion, UC Berkeley, CA, 2013
Teaching physics with free software, Edu-day on the Gran Canaria Desktop Summit, Las Palmas, Spain, 2009
Step: interactive physical simulator for KDE, Akademy, Sint-Katelijne-Waver, Belgium, 2008

Open Source Projects

SafeStack: stack-based buffer overflows protection mechanism (integrated in Clang/LLVM)
CPI: guaranteed protection against control-flow hijack attacks for C/C++ (to be included in FreeBSD)
StateMerging: a technique that improves performance of symbolic execution by several orders of magnitude
S^2E: a platform for in-vivo multi-path analysis of software systems (used by hundreds of researchers)
Step: interactive physical simulator for education (included in most Linux distributions today)
ScienceWISE.info: scientific ontology and automated paper annotation engine (partly open-source)
TeXpp: TeX language interpreter and document parsing library

Awards

The Open Source Software World Challenge Award, silver prize, 2012
ASPLOS Best Paper Award, 2011
Microsoft Research PhD Scholarship, 2010
International Group Physics Contest, Moscow, Russia, 1st prize, 2002
Complex Olympiad in Physics, Math and Computer Science, Ukraine, 1st prize, 2002
National Physics Olympiad, Ukraine: 3rd prize in 2002, 1st prize in 2001, 2nd prize in 2000

Patents

Advantageous State Merging During Symbolic Analysis
Volodymyr Kuznetsov, Johannes Kinder, Stefan Bucur, George Candea (US Patent Nr. 9,141,354)

System and method for in-vivo multi-path analysis of binary software
George Candea, Vitaly Chipounov, Volodymyr Kuznetsov (US Patent Nr. 8,776,026)

Program Committee Member

EuroSec (The 9th European Workshop on Systems Security): 2016
EuroSys Shadow PC (ACM SIGOPS/EuroSys European Conference on Computer Systems, Shadow PC): 2013

External Reviewer

OSDI (Symposium on Operating Systems Design and Implementation): 2014
SOSP (Symposium on Operating Systems Principles): 2013, 2011
ASPLOS (ACM Conf. on Architectural Support for Programming Langs. and OSes): 2010
EuroSys (ACM SIGOPS/EuroSys European Conference on Computer Systems): 2011, 2012
USENIX (USENIX Annual Technical Conference): 2011
HotOS (Workshop on Hot Topics in Operating Systems): 2013
SOCC (ACM Symposium on Cloud Computing): 2012
CIDR (Biennial Conference on Innovative Data Systems Research): 2013
DSN (Annual IEEE/IFIP International Conference on Dependable Systems and Networks): 2011
SPIN (International Workshop on Model Checking of Software): 2011

Teaching Experience

Supervised M.S. thesis, EPFL
- "Efficient String Solving for Symbolic Execution", Fall 2014

Supervised master semester projects, EPFL
- "Applications and improvements to software hardening techniques", Fall 2014
- "Unmerging in a symbolic execution engine", Spring 2015

Supervised bachelor semester projects, EPFL
- "SafeStack implementation in FreeBSD", Fall 2015

Teaching Assistant for Principles of Computer Systems (5th year master course), EPFL, Fall 2012, Fall 2013
- Led in-class discussions and recitation sessions
- Prepared and graded homework assignments and exams

Teaching Assistant for Software Engineering (3rd year undergraduate course), EPFL, Fall 2011
- Prepared and graded homework assignments and exams

Google Summer of Code, Summer 2008 and 2009
- Mentored three students during three months software development project

Teacher at the Federal Distance Education Physics and Mathematics School at MIPT, Moscow, 2002 – 2003
- Remotely supervised a class of 15 high school students

Google Summer of Code Program

Fast Gas and Water Simulation, mentor, 2009
StepGame: educational game based on Step, co-mentor, 2008
Step: interactive physical simulator for education, student, 2007

Languages

English: fluent, Russian: native, Ukrainian: native