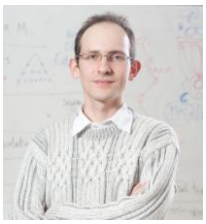
VITALY CHIPOUNOV

BUILDING TOOLS FOR AUTOMATED ANALYSIS OF PROPRIETARY SOFTWARE SYSTEMS



School of Computer and Communication Sciences
EPFL – IC – DSLAB, Station 14
Building INN, Room 319
1015 Lausanne, Switzerland
vitaly.chipounov@epfl.ch
http://people.epfl.ch/vitaly.chipounov
Tel. +41 (0) 21 693 8189

CURRENT RESEARCH

I am building S2E, a platform for multi-path in-vivo analysis of complex software systems, at the Dependable Systems Laboratory, led by Prof. George Candea. S2E empowers developers to build practical analysis tools such as comprehensive performance profilers, tools for reverse engineering of proprietary software, and bug finders for both kernel-mode and user-mode binaries. The S2E platform is automated, scalable, and allows for flexible precision depending on the analysis. This is achieved by two new techniques: *selective symbolic execution*, a way to automatically minimize the amount of code that has to be executed symbolically given a target analysis, and *relaxed execution consistency models*, a way to make principled performance/precision trade-offs in complex analyses.

S2E is a virtual machine augmented with symbolic execution. The user installs and run any unmodified x86 software stack in S2E, including programs, libraries, the OS kernel, and drivers. Symbolic execution then automatically explores hundreds of thousands paths through the system, allowing users to check desired properties even in corner-case situations. Unlike existing analysis tools, S2E does not require to write code in special languages or model the environment.

With this platform, I developed a tool – RevNIC – that reverse-engineers proprietary closed-source device drivers to synthesize new, safer, and portable device drivers for different operating systems and architectures. RevNIC takes a binary device driver, explores it automatically across multiple paths to witness all the ways in which the driver communicates with the hardware, and synthesizes an equivalent driver that captures this interaction.

We also successfully used S2E to implement a novel bug finder – DDT – that uncovered many bugs in various Microsoft-certified drivers that have been shipping for years. S2E combines our novel selective symbolic execution approach with state-of-the-art virtualization techniques to scale multi-path exploration to systems composed of millions of lines of code.

S2E is publicly available[1] and has an active community of more than 150 users, including several research institutions.

EDUCATION

2008-now	**Ph.D. Student in Computer Science** *EPFL, Switzerland*
2008	**M.S. in Computer Science** *EPFL, Switzerland*
2008	**Minor in Management of Technology and Entrepreneurship** *EPFL, Switzerland*
2006	**B.S. in Computer Science** *EPFL, Switzerland*
2005	**Exchange year as Erasmus student** *Karlsruhe Institute of Technology (KIT), Germany*
2003	**Baccalauréat National (highest honors)** *Lycée International de Ferney-Voltaire, France*

[1] http://s2e.epfl.ch

PEER-REVIEWED PUBLICATIONS

JOURNAL PAPER

The S2E Platform: Design, Implementation, and Applications
Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea
In ACM Transactions on Computer Systems (TOCS), vol. 30, num. 1, 2012.

PEER-REVIEWED CONFERENCE PAPERS

S2E: A Platform for In-Vivo Multi-Path Analysis of Software Systems
Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea
In Proceedings of the 16th ASPLOS Conference, 2011 **BEST PAPER AWARD**

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

Reverse Engineering of Binary Device Drivers with RevNIC
Vitaly Chipounov and George Candea
In Proceedings of the 5th ACM SIGOPS/EuroSys European Conference, 2010

PEER-REVIEWED WORKSHOP PAPERS

The Case for System-level Backtracking
Edouard Bugnion, Vitaly Chipounov, and George Candea
In Workshop on Hot Topics in Operating Systems, May 2013

Enabling Sophisticated Analysis of x86 Binaries with RevGen
Vitaly Chipounov, Vlad Georgescu, Cristian Zamfir, and George Candea
In Proceedings of the 7th Workshop on Hot Topics in System Dependability, 2011

Selective Symbolic Execution
Vitaly Chipounov, Vlad Georgescu, Cristian Zamfir, and George Candea
In Proceedings of the 5th Workshop on Hot Topics in System Dependability, 2009

Reverse-Engineering Drivers for Safety and Portability
Vitaly Chipounov and George Candea
In Proceedings of the 4th Workshop on Hot Topics in System Dependability, 2008

PATENT

System and method for in-vivo multi-path analysis of software systems
George Candea, Vitaly Chipounov, and Volodymyr Kuznetsov (US# 61/405,224 – pending)

AWARDS

Silver Prize at the World Open Source Challenge 2012[2] for
DDT, the automated device driver testing tool

Best paper award at *ASPLOS 2011* for the paper titled
S2E: A Platform for In-Vivo Multi-Path Analysis of Software Systems

[2] http://ossaward.org

MEDIA COVERAGE

The Achilles' Heel of Your Computer
In MIT Technology Review, June 30, 2010

Software spürt schlechte Gerätetreiber auf
In Pressetext, July 1, 2010

WORK EXPERIENCE

TEACHING

Software Engineering, 2009-2013
In charge of the Android/Eclipse tool chain setup on the computer labs, preparing and grading assignments, and giving lectures.

System-oriented Programming, 2008-2009-2010
Assisting undergraduate students in the learning of the Unix environment, shell scripting and C programming. Responsible for organizing exams and supervising pools of teaching assistants.

Real-Time Embedded Systems, 2008
Responsible for the design, implementation, and integration in Altera Quartus/NIOS IDE of hardware and software components used during the course (MMC/SD Card reader, FAT driver, VGA controller)

Computer Architecture, 2007
Responsible for assisting the students in the implementation of a NIOS-compatible soft-core processor for the FPGA4U development board and the grading of a large number of exams.

Information Technology Project, 2007
Managing and evaluating student groups for the implementation of a peer-to-peer file sharing project.

EXTERNAL REVIEWER FOR SYSTEMS CONFERENCES

SOSP (Symposium on Operating Systems Principles): 2011, 2013
DSN (Annual IEEE/IFIP International Conference on Dependable Systems and Networks): 2011
EuroSys (ACM SIGOPS/EuroSys European Conference on Computer Systems): 2008, 2011
ASPLOS (ACM Conf. on Architectural Support for Programming Langs. and OSes)**:** 2010
HotOS (Workshop on Hot Topics in Operating Systems): 2009, 2011, 2013
USENIX (USENIX Annual Technical Conference): 2009, 2011

MISCELLANEOUS

CONTESTS

Finalist of the French National Informatics Contest[3] (2003, 2004, 2005)

LANGUAGE SKILLS

French: native
Russian: native
English: fluent (Cambridge Certificate in Advanced English)
German: working technical knowledge
Spanish: basic knowledge

[3] http://www.prologin.org