Dmitrii Kuvaiskii

7079 NE Ronler Way
97124 Hillsboro
OR, USA

Mobile: +1 (503) 724 6684
Email: dmitrii.kuvaiskii@gmail.com
Homepage: https://dimakuv.github.io/
GitHub: https://github.com/dimakuv

Research Interests

My research interests lie in the field of dependability in software systems, with a particular focus on fault tolerance and security. Within these fields, I investigate the applicability of modern hardware extensions to increase reliability of real-world applications while imposing low overheads. My current research at Intel Labs concentrates on Intel SGX and future security extensions.

Education

Ph.D. in Computer Science (Dec 2013 - Jan 2018)
TU Dresden, Germany
Thesis: Hardware-Assisted Dependable Systems, **Summa cum laude**
Advisors: Prof. Dr. Christof Fetzer and Prof. Dr. Pramod Bhatotia

M.Sc. in Computer Science (Oct 2011 - Nov 2013)
TU Dresden, Germany

Diplom in Electrical Engineering (Sep 2004 - Jul 2010)
Bauman University, Moscow, Russia

Employment

Intel Labs, Hillsboro, OR, USA, May 2018 - present
Datacenter Security Research Scientist
Responsibilities: hardware/software co-design of security solutions.

Intel Labs, Hillsboro, OR, USA, July 2017 - Sep 2017
Datacenter Security Intern
Responsibilities: developing applications with Intel SGX (C/C++).

Auriga Inc, Moscow, Russia, Sep 2010 - Aug 2011
Certification engineer, Software developer
Responsibilities:

– documenting and testing code of the PikeOS embedded operating system (C);

– writing medical special-purpose programs (C++ and C#).

Diasoft, Moscow, Russia, Sep 2007 - Aug 2010
Software developer
Responsibilities: programming insurance subsystems using Transact SQL and Delphi.

Honors and Awards

Summa cum laude for PhD thesis, 2018

Best paper award at EuroSys'17

Carter Award (best student paper) at DSN'15

Best paper award at SRDS'14

Erasmus Mundus Action 2 MULTIC scholarship, 2011-2013

Ph.D. Dissertation

Topic: Hardware-Assisted Dependable Systems
Supervisors: Prof. Dr. Christof Fetzer and Prof. Dr. Pramod Bhatotia

In the context of my Ph.D. dissertation, I investigated and built systems to increase software dependability leveraging recent sets of extensions in Intel processors, with the focus on software-based fault tolerance and security for legacy C/C++ programs.

Research projects:

Detailed evaluation of Intel MPX and discussion of its applicability in comparison to other bounds-checking approaches **[ACM SIGMETRICS'18]**;

SGXBounds: LLVM-based bounds checker to detect and tolerate security bugs in multithreaded legacy C/C++ programs inside Intel SGX enclaves **[EuroSys'17]**;

Elzar: LLVM compiler pass to detect and mask transient CPU faults in multithreaded legacy C/C++ programs using Intel AVX **[DSN'16] [code]**;

HAFT: LLVM compiler pass to detect and tolerate transient CPU faults in multithreaded legacy C/C++ programs using Intel TSX **[EuroSys'16] [code]**;

Δ-*Encoding*: Source-to-source compiler to detect transient and permanent CPU faults in legacy C programs utilizing unused IPC resources of modern CPUs **[DSN'15]**.

Publications

Conference publications:

Intel MPX Explained
Oleksii Oleksenko, Dmitrii Kuvaiskii, Pramod Bhatotia, Pascal Felber, and Christof Fetzer
ACM SIGMETRICS 2018.

Fex: A software systems evaluator
Oleksii Oleksenko, Dmitrii Kuvaiskii, Pramod Bhatotia, and Christof Fetzer
DSN 2017.

SGXBounds: Memory Safety for Shielded Execution
Dmitrii Kuvaiskii, Oleksii Oleksenko, Sergei Arnautov, Bohdan Trach, Pramod Bhatotia, Pascal Felber, and Christof Fetzer
EuroSys 2017. Best paper award.

Elzar: Triple Modular Redundancy using Intel Advanced Vector Extensions
Dmitrii Kuvaiskii, Oleksii Oleksenko, Pramod Bhatotia, Pascal Felber, and Christof Fetzer
DSN 2016.

HAFT: Hardware-Assisted Fault Tolerance
Dmitrii Kuvaiskii, Rasha Faqeh, Pramod Bhatotia, Pascal Felber, and Christof Fetzer
EuroSys 2016.

Δ-Encoding: Practical Encoded Processing
Dmitrii Kuvaiskii and Christof Fetzer
DSN 2015. Carter Award (best student paper).

Needles in the Haystack—Tackling Bit Flips in Lightweight Compressed Data
Till Kolditz, Dirk Habich, Dmitrii Kuvaiskii, Wolfgang Lehner, and Christof Fetzer
DATA 2015.

HardPaxos: Replication hardened against hardware errors
Diogo Behrens, Dmitrii Kuvaiskii, and Christof Fetzer
SRDS 2014. Best paper award.

Other Publications:

Snort Intrusion Detection System with Intel Software Guard Extension (Intel SGX)
Dmitrii Kuvaiskii, Somnath Chakrabarti, and Mona Vij
ArXiv.org 2018.

Open Source Projects

Intel MPX Explained
https://intel-mpx.github.io

SGXBounds
https://github.com/tudinfse/sgxbounds

Elzar
https://github.com/tudinfse/elzar

HAFT
https://github.com/tudinfse/haft

SEC-IDS aka Snort-SGX
https://github.com/cloud-security-research/sgx-ids

Graphene-SGX (contributor)
https://github.com/oscarlab/graphene

Talks

ACM EuroSys'17, Belgrade, April 2017
SGXBounds: Memory Safety for Shielded Execution

ACM EuroSys'16, London, April 2016
HAFT: Hardware-Assisted Fault Tolerance

IEEE DSN'16, Toulouse, June 2016
Elzar: Triple Modular Redundancy using Intel Advanced Vector Extensions

IEEE DSN'15, Rio de Janeiro, June 2015
Δ-Encoding: Practical Encoded Processing

Teaching experience

Teaching assistant: Distributed Systems Engineering courses, TU Dresden, Dec 2013 - Jan 2018.

— Concurrent and Distributed Systems lab, Summer Semesters 2014 - 2016
— Principles of Dependable Systems exercises, Winter Semesters 2014 - 2018
— Software Fault Tolerance exercises, Summer Semesters 2014 - 2018

Professional activities

Shadow PC member: **EuroSys 2016**.

Skills

Languages: C, C++, Assembly (expert), Unix shell, Python, R (competent);

Frameworks: LLVM, gdb, Intel Pin, Intel SDE;

Technologies: Intel SSE/AVX, Intel TSX, Intel MPX, Intel SGX.

References

Prof. Dr. Christof Fetzer
TU Dresden, Germany
Email: `christof.fetzer@tu-dresden.de`

Prof. Dr. Pramod Bhatotia
University of Edinburgh, UK
Email: `pramod.bhatotia@ed.ac.uk`

Prof. Dr. Pascal Felber
University of Neuchatel
Email: `pascal.felber@unine.ch`

Mona Vij
Intel Labs, USA
Email: `mona.vij@intel.com`