Qemu-based tools

V. Makarov, NovSU

03 may 2018

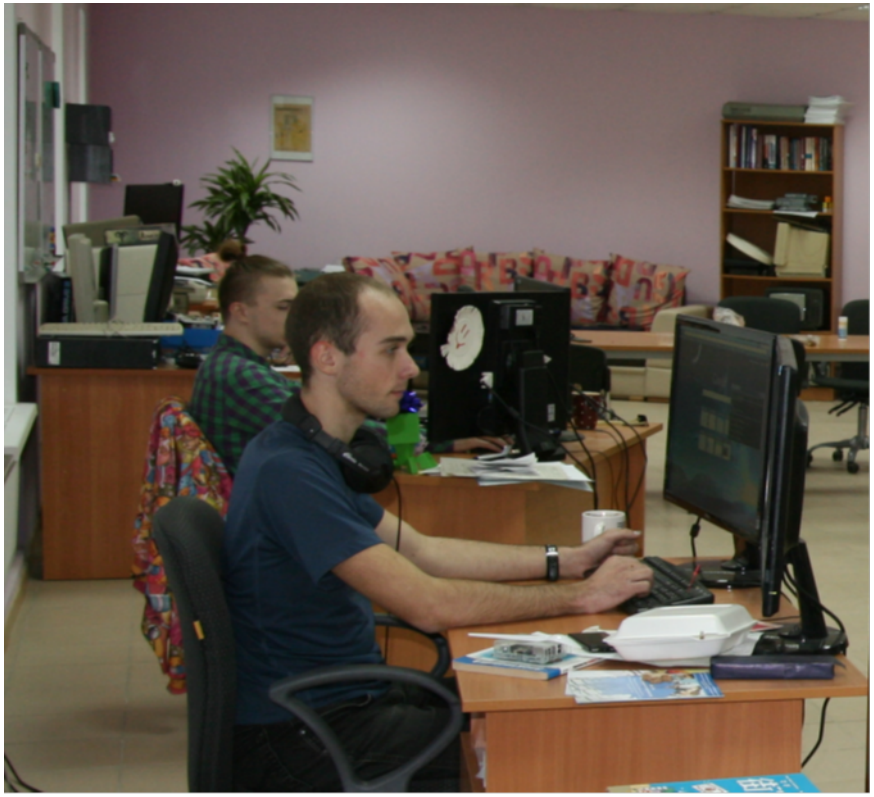
On June 28-29, 2004 in Veliky Novgorod was held a seminar called "Compilation technologies"

October 25, 2007 Pavel Dovgalyuk defended his thesis for the degree for a candidate of technical sciences on the topic: "*The study of a sparse model of basic blocks for optimizing the flow of commands of a computational pipeline*"

Lead organization:
Institute for System Programming of the RAS

On February 26, 2010, a cooperation agreement was signed between ISP RAS and NovSU

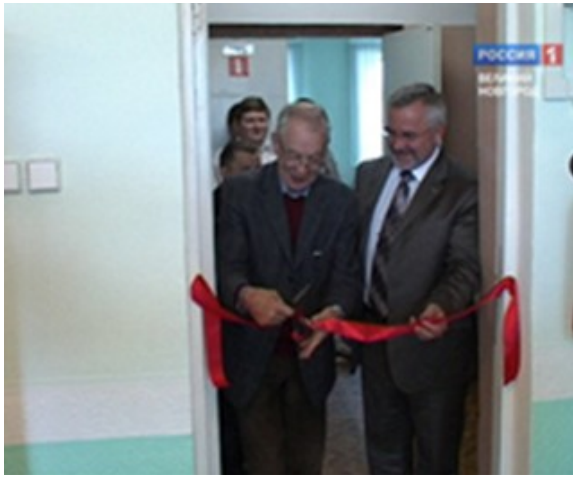
On March 30, 2010 the new laboratory for system programming was created in cooperation with ISP RAS



The laboratory was created with the purpose of cooperation in the field of scientific, educational and innovative practices and for the implementation of cooperative projects

Scientific adviser of the laboratory – Academician of the Russian Academy of Sciences **Ivannikov Victor Petrovich**

May 27, 2010 in NovSU the festive opening of the laboratory for system programming was held



Academician V.P. Ivannikov proposed to establish a scholarship of ISP RAS for the best students of NovSU

September 22, 2010 in NovSU laureates of nominal scholarship of ISP RAS were granted with certificates

The first scholarship winners were four students from NovSU: *Natalya Fursova*, Sergey Kurdov, Vasily Zubov and Denis Pavlov

«Academician V.P. Ivannikov hopes that the university will develop a group that would be interested in the problems of compiler technologies, and which, on the one hand, will conduct researches, and on the other - will prepare a new teaching staff.

The purpose of the ISP RAS laboratory is to train not only high-level specialists, but those who are able to solve complex problems by themselves.

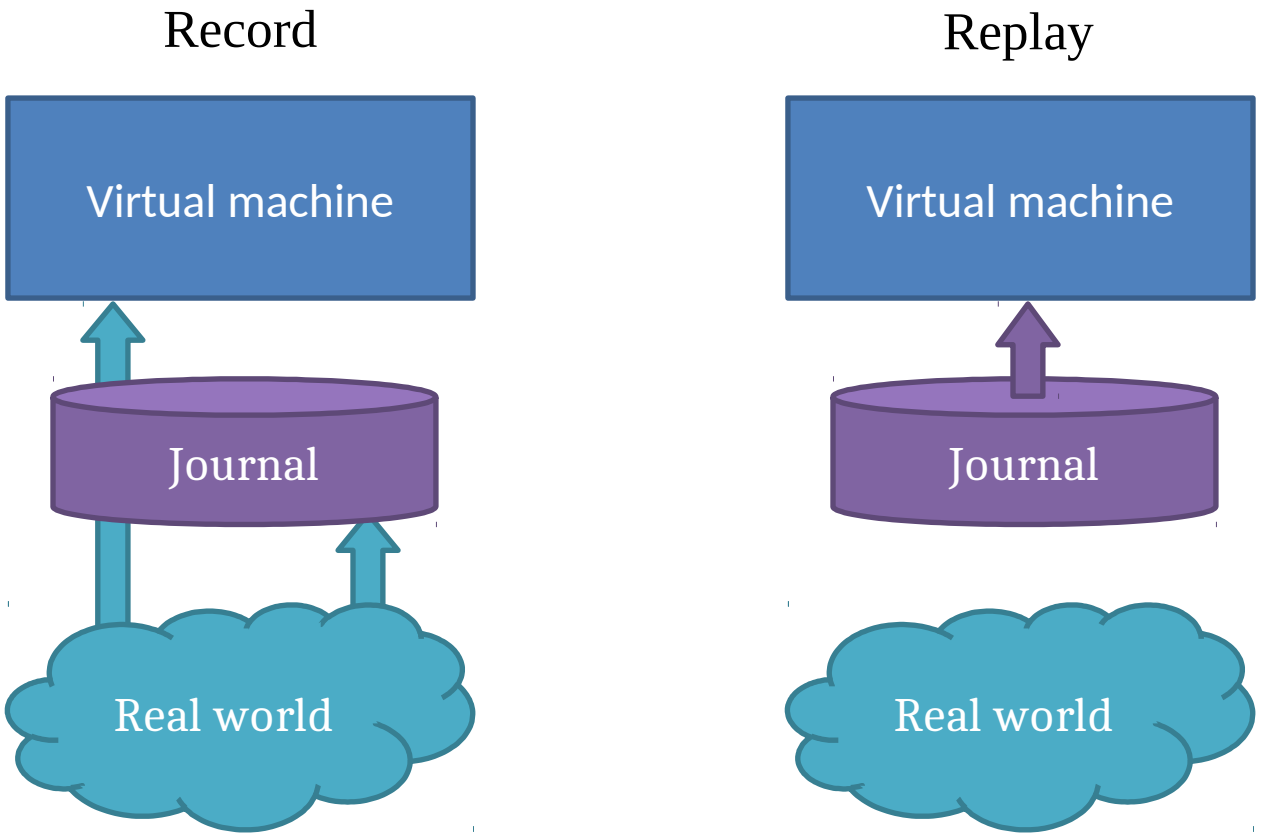
As noted by Viktor Petrovich, preparation of such specialists is not an easy task, and it usually takes from 5 to 7 years»

Newspaper «Novgorodskie Vedomosti» 05/27/2010

QEMU

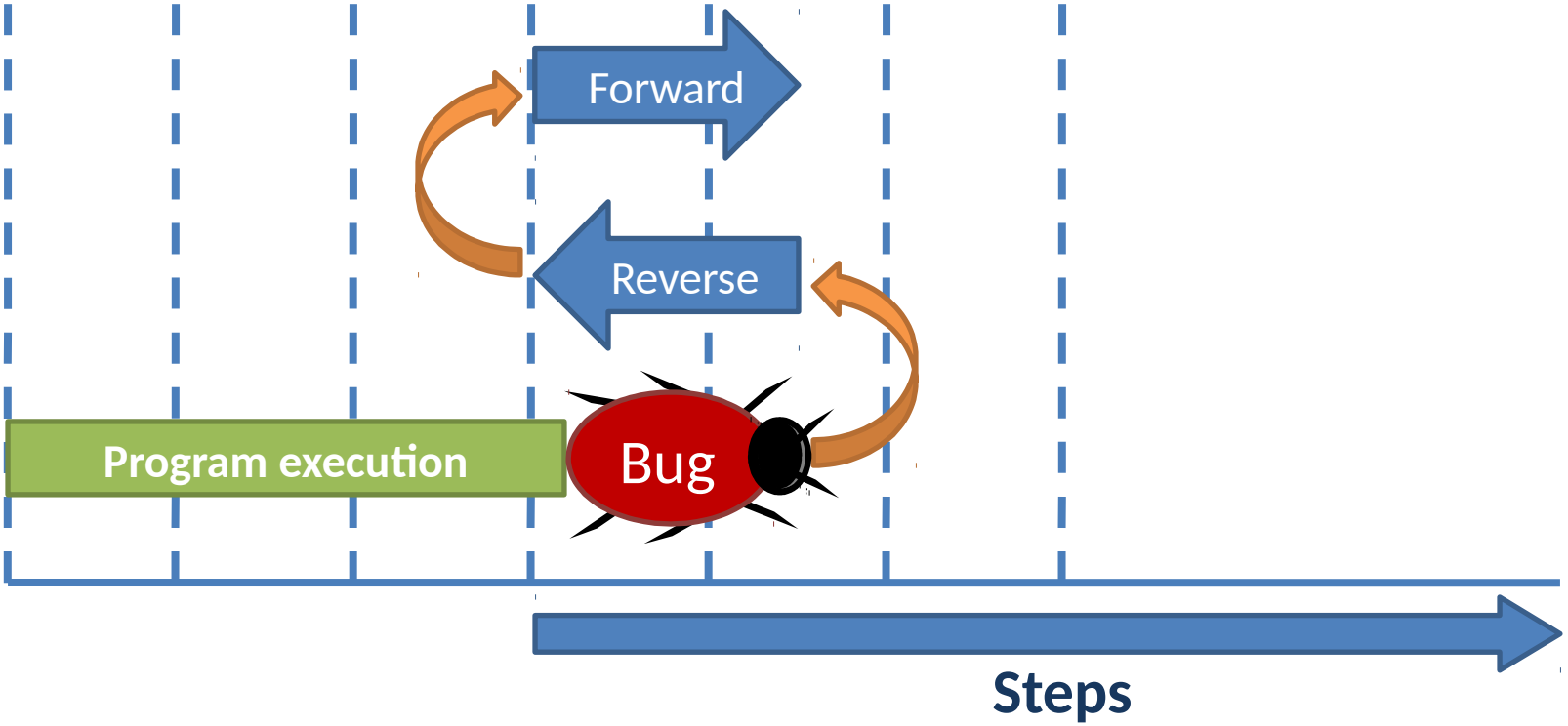
Is an open-source program that is being actively used by developers of mobile platforms, such as Android, Tizen and Symbian

- Capable of full system simulation
- Support for common platforms – x86, ARM, PowerPC, Sparc
- Easily expandable list of supported peripherals



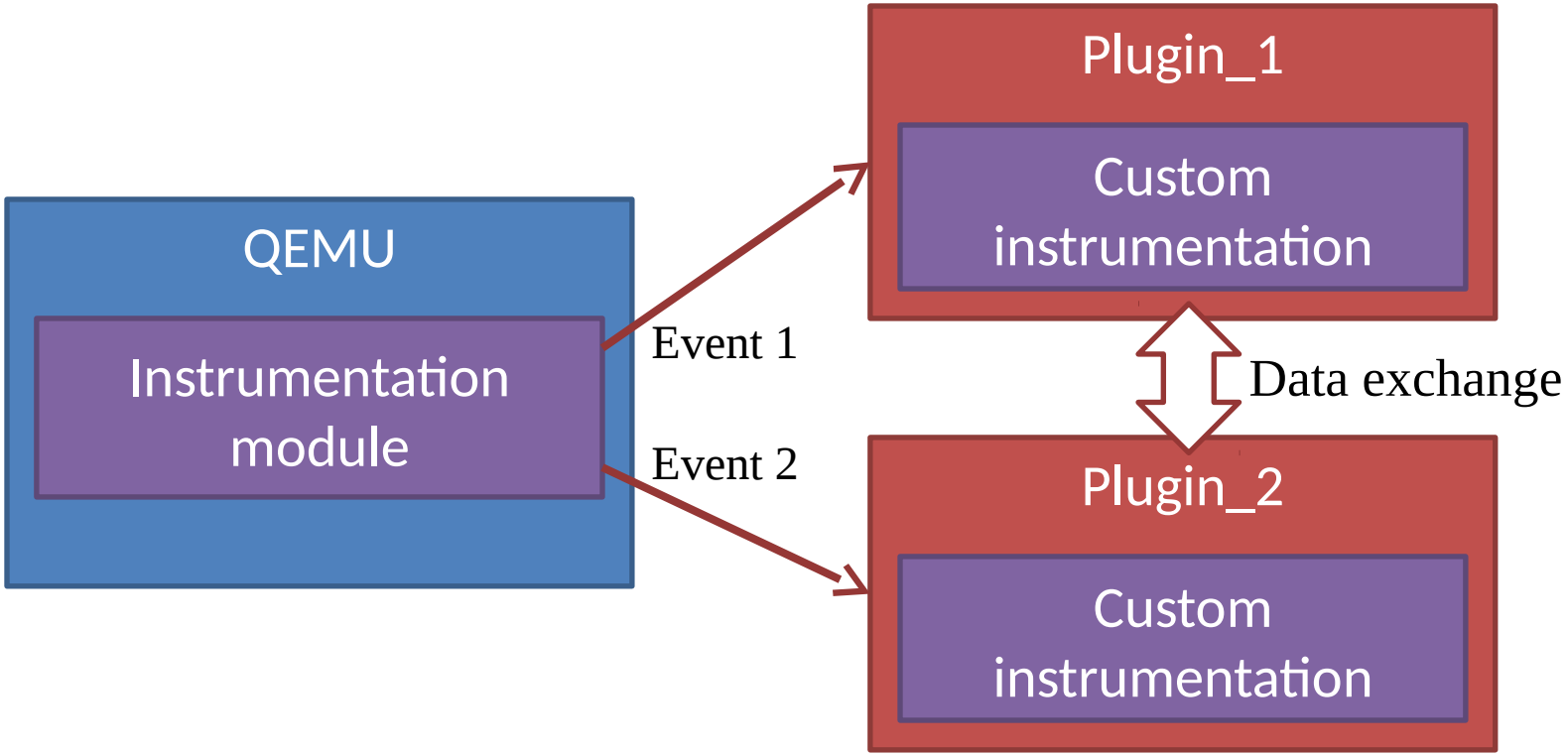
The technology of deterministic replay was developed; mechanisms for recording and replaying a log of nondeterministic events in the QEMU simulator was also developed

Reverse debugging



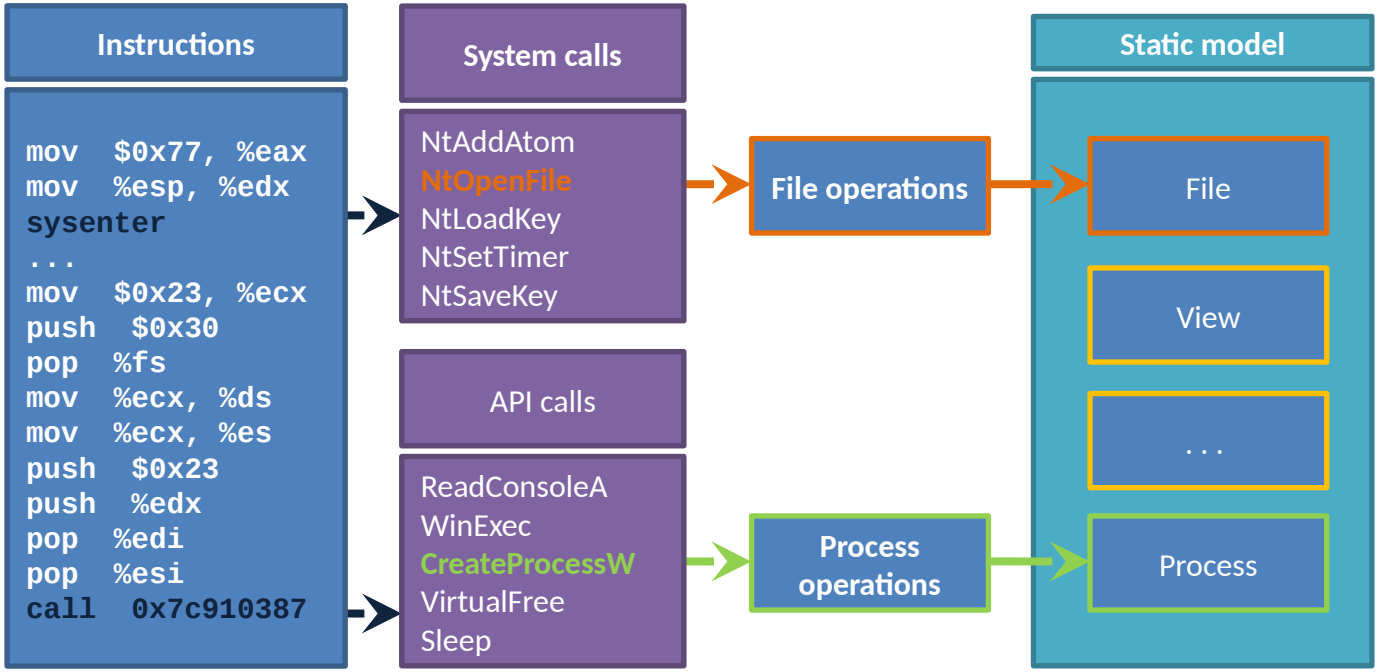
Instruments of reverse debugging allow to return from the place where the error shown itself to the place where it actually occurred

The mechanism of dynamic instrumentation



Scheme of interaction between QEMU and plugins, and between plugins themselves

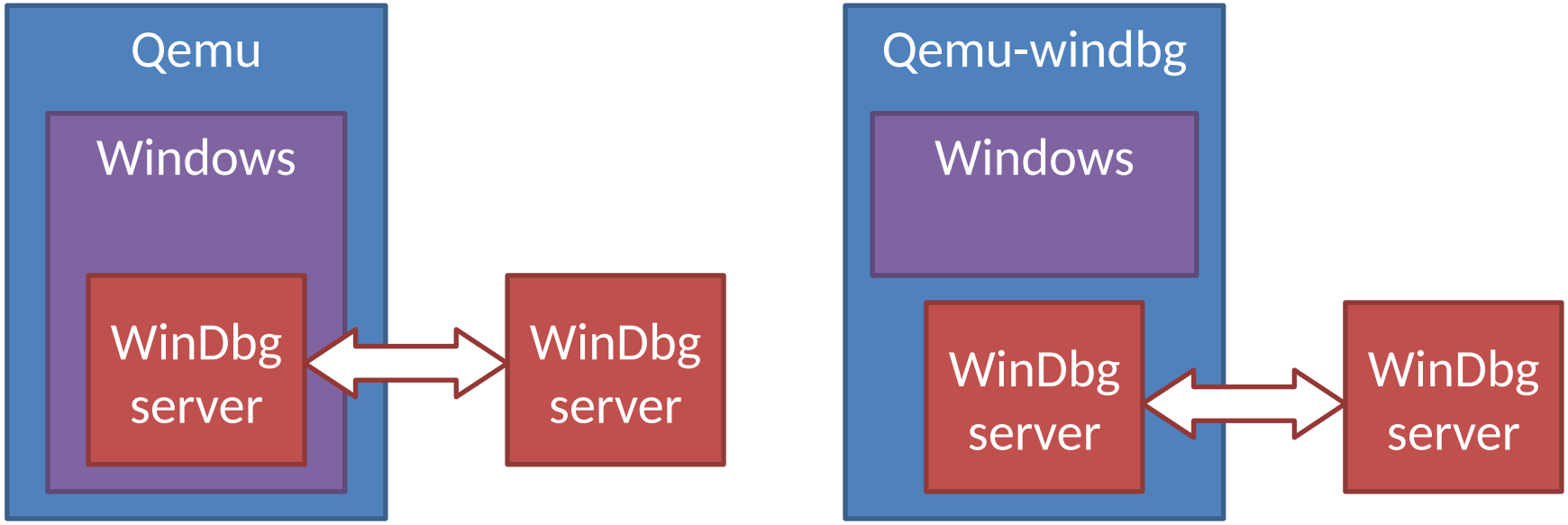
Introspection



Analysis of parameters and return values of system calls and API calls allows obtaining of high-level information about OS objects (such as processes, files, threads, etc.)

- The lightness of the method is due to the minimization of knowledge about the system
- The method achieves high performance
- Based on QEMU 2.8

WinDbg module for QEMU



- The debugging process is undetectable by programs under analysis
- Works with common WinDbg commands
- High-level features of WinDbg are available

Other important results

- The mechanisms of taint-analysis based on the QEMU with plugins and deterministic replay were implemented
- Deterministic replay was implemented for QEMU-Android
- Research was made on problem of implementation of VMX instructions in QEMU
- The use of technique of symbolic execution with the purpose of determining values of variables for the analyzed branch of the algorithm was studied
- Fixed many bugs in the mainline version of QEMU

Cooperation with the Qemu community

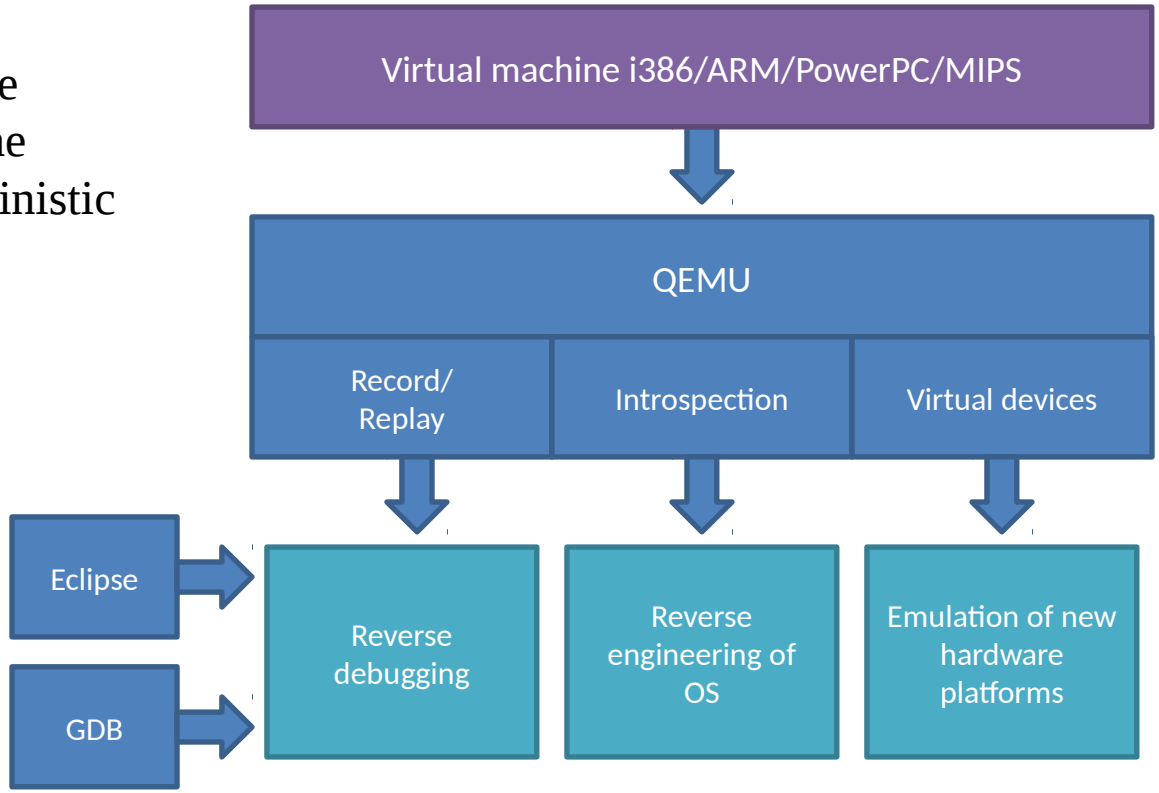
- July 2014 (Qemu 2.2) – the first patches for execution recording and replaying were suggested to the Qemu community
- September 2014 – the community accepted the first patches
- November 2015 (Qemu 2.5) – the kernel of recording/replaying is accepted
- December 2016 (Qemu 2.8) – more patches accepted
- April 2018 (Qemu 2.12) – record/replay is available in Qemu

Now the plugin engine for Qemu and WinDbg module are available in the separate Qemu repository

System of vulnerability analysis and reverse debugging of software

Purpose:
Detection of vulnerabilities in the absence of the source code for the program by the means of deterministic replay

Advantages:
- Works with a wide range of target platforms;
- Has an ability to debug software for devices that are at the development stage;
- The ability to identify difficult-to-reproduce errors



ISP RAS is the main sponsor of the summer computer camp

On October 2016 NovSU was granted with the diploma from Russian Ministry of Education and Science for implementing creative practices in school “Algorithms and Data Structures” and the “System Programming” club .

21 students from NovSU passed the internship in our laboratory.


МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДИПЛОМ

НАГРАЖДАЕТСЯ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НОВГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ЯРОСЛАВА МУДРОГО»

за создание лучших практик в сфере деятельности практико-ориентированных научно-технических клубов творческого развития студентов и школьников
«Школа «Алгоритмы и структуры данных»
«Клуб «Системное программирование»

Заместитель Министра образования и науки Российской Федерации
В.Ш. Каганов