BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Supervisor's Opinion on the PhD Thesis of

Viktor Malík

The PhD thesis of Viktor Malík concentrates on static analysis and verification of low-level C code. The subject of automated analysis and verification of software belongs to those that, despite having been studied for a long time, still offer a number of challenges and attract a lot of interest both in academia as well as in the industry. That is why, I find the subject area of the thesis of Viktor Malík highly up to date and important.

More concretely, the work of Viktor Malík has led to original contributions in two different areas:

1. *Formal verification of low-level code in the 2LS framework.* The 2LS framework combines in a unique way multiple approaches to formal analysis and verification—namely, encoding of programs using first order formulae, *k*-induction, bounded model checking, SMT solving, invariant templates, and abstract domains. The original contribution of Viktor in this area concerns extensions of the framework to support verification of dynamic linked data structures (with a stress on linked lists) and arrays. The extensions allowed 2LS to handle programs combining the use of dynamic data structures and other data values that no other known verifier could handle in a sound way.

2. *Static checking of semantic equivalence of different versions of large refactored system code.* This line of works was done in collaboration with the Red Hat company. It was motivated by a need of Red Hat to check that the semantics of the kernel binary interface (KABI) of the Red Hat Enterprise Linux (RHEL) is preserved during refactoring of the code. The original contribution of Viktor in this area lies in a proposal of a light-weight approach that can correctly handle most refactoring changes[1] in code as large as different versions of the Linux kernel or of the C language standard library. The approach has been implemented in the DiffKemp tool.

The research of Viktor Malík was conducted within the VeriFIT research group at the Faculty of Information Technology of Brno University of Technology (FIT BUT). In the research direction concerning the 2LS framework, Viktor collaborated in an intense way with Dr. Peter Schrammel from DiffBlue, Ltd., and University of Sussex, UK (at the beginning of the collaboration, University of Oxford). Moreover, as already said above, the research direction concerning semantic equivalence involved a close collaboration with Red Hat. Due this collaboration, Viktor has finally become one of the coordinators of research between Red Hat and FIT BUT from the side of Red Hat, and he actively helped to get involved into common research with Red Hat and get a financial support of Red Hat for multiple FIT BUT students (not only on the DiffKemp tool).

The research conducted by Viktor Malík was and still is an important part of various research projects, including the projects ROBUST, SNAPPY, and AIDE of the Czech Science Foundation,

[1] It is hard to imagine that some approach would handle everything in this case.