Title: Analysis of a File System Using the Verifying C Compiler

Author: Bc. David Škorvaga

Department: Department of Distributed and Dependable Systems

Supervisor: RNDr. Jan Kofroň, Ph.D.

Abstract: Formal verification is a way to improve reliability of software systems. One approach of formal verification is focused on proving correctness of annotated source code of an established programming language. Verifying C Compiler (VCC) is a verifier for concurrent C that accepts an annotated code in C language and automatically verifies its correctness with respect to the given annotation. There have been successful attempts to verify some critical systems, including the operating system kernel. Another critical part of operating system is its file system. In the thesis, we choose FatFs file system, a simple device-independent implementation of the FAT file system. We specify a part of it using the VCC annotation and successfully verify its correctness.

Keywords: Formal Verification, File System, VCC