

Název práce: Analýza souborového systému pomocí Verifying C Compiler

Autor: Bc. David Škorvaga

Katedra: Katedra distribuovaných a spolehlivých systémů

Vedoucí diplomové práce: RNDr. Jan Kofroň, Ph.D.

Abstrakt: Formální verifikace je jeden ze způsobů, jak zlepšit spolehlivost softwarových systémů. Jeden z přístupů formální verifikace se zaměřuje na dokazování správnosti anotovaného zdrojového kódu v široce používaném programovacím jazyce. Verifier C Compiler (VCC) je verifikátor pro concurrent C, který přijímá anotovaný kód v jazyce C a automaticky ověřuje jeho správnost s ohledem na tuto anotaci. Už se objevily úspěšné pokusy o ověření některých kritických systémů, včetně jádra operačního systému. Další důležitou součástí operačního systému je jeho systém souborů. V diplomové práci jsme si vybrali souborový systém FatFs, odlehčenou implementaci souborového systému FAT, nezávislou na zařízení. V této práci vytvoříme specifikaci jeho části pomocí anotace VCC a úspěšně ověříme jeho korektnost.

Klíčová slova: Formal Verification, File System, VCC