Rozšíření DiOSu, interního operačního systému verifikačního nástroje DIVINE

Petr Ročkai Jan Mrázek Zuzana Baranová

Masaryk University

Brno, Czech Republic

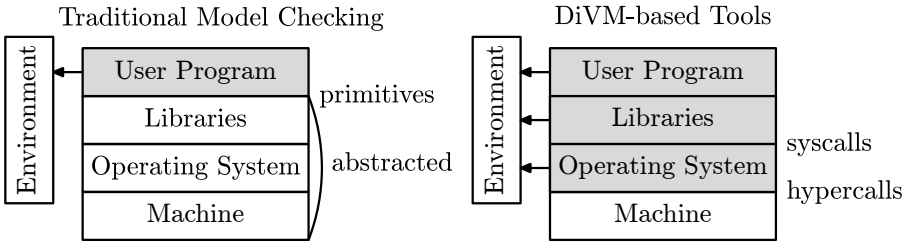
26. listopadu 2018

DIVINE 4

- explicitní model-checker pro C/C++
- vyvíjen v laboratoři ParaDiSe
- cílí na verifikaci paralelního a reálného kódu

`https://divine.fi.muni.cz`

Architektura DIVINE 4



Klasický model-checker vs. DIVINE 4

- “modelový” operační systém
  - není bootovatelný
  - běží nad rozhraním DiVM
  - simuluje vstupně-výstupní operace
- POSIXové rozhraní
  - libc & libstdc++
  - pthread
  - filesystem

Cíl projektu

Rozšířit DiOS a k němu příslušné nástroje.

- modularizace a konfigurovatelnost systému
- implementace podpory pro procesy
- implementace podpory pro synchronní systémy
- implementace fairness pro scheduler
- integrace DiOSu s DIVINE simulátorem

Modularizace, konfigurovatelnost, schedulery

- DiOS rozdělen na téměř nezávislé komponenty
  - scheduler, process manager, fault handler, virtual file system, ...
  - lze vypustit nepotřebné komponenty (např. procesy)
  - lze vyměnit komponenty za specializované (fair nebo synchronní scheduler)
- konfigurace skrze vrstvení šablon

Modularizace, konfigurovatelnost, schedulery

- DiOS rozdělen na téměř nezávislé komponenty
  - scheduler, process manager, fault handler, virtual file system, ...
  - lze vypustit nepotřebné komponenty (např. procesy)
  - lze vyměnit komponenty za specializované (fair nebo synchronní scheduler)
- konfigurace skrze vrstvení šablon
- konfigurovatelností nebyl zaznamenán žádný propad výkonu

Modularizace, konfigurovatelnost, schedulery

- DiOS rozdělen na téměř nezávislé komponenty
  - scheduler, process manager, fault handler, virtual file system, ...
  - lze vypustit nepotřebné komponenty (např. procesy)
  - lze vyměnit komponenty za specializované (fair nebo synchronní scheduler)
- konfigurace skrze vrstvení šablon
- konfigurovatelností nebyl zaznamenán žádný propad výkonu
- implementován fair scheduler (verifikace vlastností LTL)
- implementován synchronní scheduler (verifikace Simulinkových diagramů)

Implementace podpory pro procesy

- DiOS umí imitovat chování programů na bázi POSIXu
- přibyla nová systémová komponenta

Implementace podpory pro procesy

- DiOS umí imitovat chování programů na bázi POSIXu
- přibyla nová systémová komponenta

- výzvy během implementace:
  - ochrana paměti při forku
  - implementace `kill` (volání na sebe sama a zajištění volání uživatelských handlerů)

Integrace DiOSu se simulátorem

DIVINE simulátor byl vylepšen o:

- demanglování jmen funkcí
- skrytí implementace DiOSu v simulátoru:
  - DiOS byl pro simulátor nerozeznatelný od uživatelského kódu
  - výpisy zahlcovaly uživatele
  - zavedeny jmenné aliasy, skákání po funkčních rámcích
- implementovány lepivé příkazy
  - užitečné např. pro vypsání útržku kódu, rámce apod.
  - připodobňuje práci se simulátorem práci s GDB
- uživatelský manuál byl rozšířen o sekci práce s DiOSem a simulátorem

Závěr

- v rámci projektu jsme úspěšně:
  - udělali DiOS konfigurovatelným
  - implementovali fair scheduler
  - přidali do DiOSu podporu pro synchronní systémy
  - přidali podporu pro POSIXové procesy
  - zpříjemnili uživatelský zážitek
- nad rámec projektu jsme:
  - téměř zdvojnásobili sadu regresních testů pro DIVINE 4 (na 1200)
- výstupy začleněny do hlavní vývojové větve DIVINE

Projekt k nalezení na `https://divine.fi.muni.cz`.