Souhrnná výzkumná zpráva k projektu *Zlepšování kvality software* za rok 2018

Objednatel: Red Hat Czech, s.r.o.
Zhotovitel: Fakulta informačních technologií, Vysoké učení technické v Brně
Koordinátor projektu na FIT VUT: prof. Ing. Tomáš Vojnar, Ph.D.

1. Úvod

Projekt *Zlepšování kvality software* zahrnuje výzkumné, vývojové a experimentální práce v několika vzájemně komplementárních oblastech týkajících se různých aspektů kvality software. V roce 2018 byly zahrnuty různé aspekty zajištění spolehlivosti, výkonnosti i bezpečnosti software a také další podpora pro efektivní vývoj kvalitního software. Předmětem projektu byly mimo jiné následující oblasti:

- Pokračování vývoje technik a nástrojů pro automatizovanou statickou i dynamickou analýzu výkonnosti programů, respektive analýzu spotřeby výpočetních zdrojů programy.
- Vývoj nástrojů pro automatizovanou analýzu tvaru dynamických datových struktur na hromadě.
- Vývoj metod a nástrojů pro automatizované rozpoznávání rozdílů v různých verzích jádra, případně dalších utilit.
- Vývoj nástroje pro automatizované generování bezpečnostních politik pro volání systémových služeb založeného na analýze záznamů systémových volání.
- Testování nástroje Red Hat Satellite pro správu systémů.
- Vývoj nástroje pro automatickou detekci selhání služeb poskytovaných zákazníkům a jejich notifikaci.
- Vývoj nástroje pro měření výkonnosti plánovače v Linuxu, ukládání naměřených skutečností, jejich vhodnou grafickou presentaci pro následnou analýzu člověkem a pro automatickou detekci degradace výkonu.
- Vývoj virtualizační knihovny a nástroje pro správu virtualizací v prostředí Cockpit.
- Vývoj doporučovacího systému, založeného na technikách strojového učení, pro personalizované doporučování webového obsahu vhodného pro vývojáře.

- Vývoj komponenty pro automatickou detekci chyb v rámci prostředí Red Hat Insights, jež je určeno pro prediktivní analýzu možných rizik v rozsáhlých IT systémech.
- Testování základních síťových komponent Red Hat Enterprise Linux.
- Vývoj webové komponenty pro zobrazení hierarchické struktury ve tvaru stromu. pro prostředí ManageIQ, které je vyvíjeno společností Red Hat.
- Vývoj zásuvného modulu pro GCC, který ověřuje vybraná pravidla pro bezpečnou obsluhu signálů v C/C++ kódu.

Níže jsou blíže zmíněny tři nejvýznamnější oblasti, které byly v roce 2018 rozvíjeny.

2. Statická a dynamická analýza výkonnosti programů

Statická a dynamická analýza výkonnosti programů patří v rámci projektu k dlouhodobě rozvíjeným oblastem. V roce 2018 byla pozornost věnována primárně dynamické analýze v nástroji Perun. Tento nástroj umožňuje sběr různých informací o běhu programu z hlediska výkonnosti (spotřeba času, paměti apod.) buď pomoci předdefinovaných sond, nebo pomoci sond definovaných uživatelem. Nástroj Perun poskytuje pro tvorbu takových sond patřičnou podporu. Údaje naměřené sondami se ukládají do speciálního repositáře paralelně k jednotlivým verzím programu a umožňují analyzovat vývoj výkonnosti v čase. V roce 2018 se pozornost zaměřila jednak na vývoj nové infrastruktury pro implementaci sond a jednak na vývoj nových statistických způsobů analýzy získaných dat. Cílem je zejména automatické odvození odhadu asymptotické složitosti daného kódu a jednak automatická detekce degradace výkonu (a to nejen absolutní, ale také na úrovni změny asymptotické složitosti, např. změna ze složitosti lineární na kvadratickou, která může indikovat nežádoucí zanoření cyklů, apod.).

V oblasti statické analýzy výkonnosti začal nově vývoj statického analyzátoru složitosti v otevřeném prostředí Facebook Infer. Jedná se o reimplementaci analýz navržených původně v nástroji Loopus, jehož aktivní vývoj byl již ukončen. Implementace v prostředí Facebook Infer umožní přenést myšlenky z nástroje Loopus do intenzivně se rozvíjejícího nástroje s řadou uživatelů a perspektivně také další rozvoj těchto analýz k vyšší efektivitě s využitím přístupů běžných v prostředí Facebook Infer.

3. Vývoj metod a nástrojů pro automatizované porovnání verzí jádra

V roce 2018 byla dále významná pozornost věnována vývoji nového nástroje DiffKemp určeného pro automatické porovnávání verzí jádra a potenciálně i dalších programů. V případě jádra se jedná o porovnávání efektů jednotlivých systémových volání (za jejichž stabilitu Red Hat ručí svým zákazníkům) a také způsobu práce s parametry jádra. Za daným účelem se používá originální kombinace technik z oblasti formální analýzy, jako jsou vyřezávání relevantních částí kódu a symbolické provádění.

4. Statická analýza v nástroji 2LS

Statický analyzátor 2LS vznikl původně na Oxford University a nyní je rozvíjen jako experimentální platforma zejména firmou DiffBlue z Velké Británie, nicméně s plně

otevřenými zdrojovými kódy. V rámci projektu probíhaly v roce 2018 práce zaměřené na doplnění nástroje 2LS o první verzi podpory práce s dynamickými datovými strukturami, zejména seznamy, a to s důrazem na možnost kombinovat analýzu zaměřenou na tvar dynamických datových struktur s dalšími analýzami zaměřenými na data uložená v těchto datových strukturách. Další práce v dané oblasti pak byla zaměřena na vytvoření generického rozhraní pro práci s abstraktními doménami a na nástroj usnadňující analýzu vygenerovaných invariantů a zjištění, které jejich části jsou problematické z hlediska selhání analýzy na určitém programu.

5. Závěr

Výstupy projektu dosažené v roce 2018 byly objednateli předány v jím požadované podobě zahrnující (dle konkrétních témat) zdrojové kódy, zprávy, či experimentálně získaná data. V řadě z uvedených oblastí přitom probíhá a bude probíhat další výzkum i v roce 2019.