Souhrnná výzkumná zpráva k projektu *Zlepšování kvality software* za rok 2015

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* zahrnul výzkumné a vývojové práce v několika vzájemně komplementárních oblastech týkajících se různých aspektů kvality software. Byly přitom zahrnuty jak aspekty spolehlivosti, efektivity, tak také bezpečnosti software. Předmětem projektu byly mimo jiné následující oblasti:

- vývoj technik a nástrojů pro automatizovanou statickou formální analýzu programů pracujících s dynamickými datovými strukturami,
- vývoj nástrojů pro shromažďování výsledků průběžných testů software,
- výzkum v oblasti využití technik dolování z dat pro posouzení kvality změn prováděných v komponentách vyvíjených třetími stranami,
- podporu automatizace testování,
- výzkum v oblasti automatického generování dokumentace testů,
- testování výkonnosti síťové vrstvy linuxového jádra,
- práce v oblasti zlepšování zabezpečení OS Linux (SE Linux, Free IPA atd.).

Níže jsou blíže zmíněny nejvýznamnější výsledky, které byly v rámci projektu dosaženy.

2. Statická analýza programů s dynamickými datovými strukturami

V rámci tohoto dílčího zaměření projektu byl nejprve optimalizován nástroj *Predator Hunting Party* kombinující nad-aproximující a pod-aproximující analýzu programů s dynamickými datovými strukturami v rámci několika paralelně probíhajících procesů. Všechny uvedené analýzy jsou založeny na využití *symbolických paměťových grafů* (SMG) implementovaných již dříve v nástroji Predator. Jeden z procesů spouštěných v rámci Predator Hunting Party pak používá konzervativní nad-aproximující analýzu založenou na abstrakci konkrétních počtů konkrétních paměťových uzlů reprezentovaných jednotlivými souhrnnými uzly SMG. Zbývající procesy nepoužívají abstrakci a pod-aproximovávají

množinu dosažitelných stavů, kterou prohledávají do šířky nebo do hloubky. Cílem je co nejrychleji dosáhnout buď nalezení chyby nebo ukázání, že program pracuje s pamětí korektně, a to při minimu hlášení neexistujících chyb.

Optimalizovaný nástroj Predator Hunting Party se zúčastnil mezinárodní soutěže ve verifikaci software SV-COMP'16 (kde vlastní soutěž proběhla již na podzim roku 2015), která je součástí prestižní konference TACAS'16, kde získal zlatou medaili v kategorii verifikace programů s dynamickou pamětí. Výsledný nástroj Predator Hunting Party je volně dostupný zde: http://www.fit.vutbr.cz/research/groups/verifit/tools/predator-hp/.

V další části práce na uvedeném dílčím zaměření pak byla navržena a částečně implementována architektura nového nástroje pro automatizovanou analýzu programů s dynamickými datovými strukturami, který by měl v budoucnu nahradit nástroj Predator.

3. Shromažďování výsledků testů

Mnoho softwarových projektů prochází dlouhým vývojem, proto vyžadují rozsáhlé testovací sady pro automatizaci testování. Tyto testovací sady často neuspějí celé a je potřeba jejich výsledky v čase shromažďovat a následně analyzovat, jak se daná testovací sada chovala dříve. Za tím účelem byl v rámci spolupráce mezi FIT VUT a Red Hat Czech, s.r.o. implementován již v roce 2014 nástroj *ResultCloud*, který umožňuje zpracování výsledků testovacích sad, zařazuje je do kontextu vývoje a umožňuje jejich analýzu. Díky své modularitě není závislý na konkrétním formátu výsledků. ResultCloud využívá moderní nástroje pro tvorbu uživatelského rozhraní, a to AngularJS a Foundation, pomocí kterých bylo docíleno rychlejší odezvy systému a schopnosti přizpůsobit se obrazovkám mobilních zařízení.

V roce 2015 se nástroj ResultCloud dále výrazně posunul vpřed. Byla např. přidána podpora pro vyjádření odezvy uživatelů na použití nástroje, byl optimalizována efektivita nástroje při zpracování velkých sad výsledků testů a byla přidána podpora pro automatické testy samotného nástroje ResultCloud. V roce 2015 se také rozběhl výzkum zaměřený na využití výsledků získaných pomocí nástroje ResultCloud pro řízení kvality software, čemuž se věnuje následující sekce.

4. Dolování z dat pro posouzení kvality software

Výzkum v oblasti využití technik dolování z dat pro posouzení kvality změn prováděných v komponentách vyvíjených třetími stranami je předmětem dlouhodobější spolupráce mezi FIT VUT a Red Hat Czech, s.r.o. V roce 2015 tento výzkum dospěl do fáze, kdy jsou pomocí nástroje ResultCloud vytvářeny sady historií výsledků testů několika vybraných softwarových produktů. Současně je vyvíjen prediktor, který pomocí dolování z dat a strojového učení dokáže predikovat riziko a relevanci testovacích případů pro vstupní navrženou změnu software. Dokončení uvedeného prediktoru, jeho implementace a experimentální ověření se očekává v průběhu roku 2016.

5. Automatické generování dokumentace testů

V rámci tohoto dílčího zaměření projektu byl navržen, implementován a ověřen generátor dokumentace pro testy používající knihovnu *BeakerLib*. Vyvinutý generátor je schopen automaticky generovat dokumentaci z neokomentovaných BeakerLib testů. V prvním kroce generátor extrahuje data z BeakerLib příkazů. Následně jsou data přetvořena do informací v přirozeném jazyce. Na závěr jsou tyto informace vloženy do šablony dokumentace. Při tvorbě generátoru dokumentace byl použit modul argparse pro hledání

dat z BeakerLib příkazů. Ve srovnání s existujícími nástroji navržený generátor přináší nový způsob vytváření dokumentací bez použití dokumentačních komentářů. Díky této vlastnosti lze generovat dokumentace, které jsou vytvořeny na základě automatizovaného porozumění zdrojového kódu testu.

6. Nástroj pro analýzu bezpečnostních politik SELinux

V rámci tohoto dílčího zaměření projektu je vyvíjen nový nástroj pro analýzu bezpečnostních politik SELinux. Jako první krok při vývoje tohoto nástroje byla v roce 2015 navržena grafová reprezentace bezpečnostních politik SELinuxu vhodná pro jejich následnou automatizovanou analýzu s ohledem na shodu s požadovanými integritními omezeními. V dalším kroku je nyní aktuálně vyvíjen nástroj, který využívá uvedenou grafovou reprezentaci pro detekci porušení příslušných integritních omezení a poskytnutí diagnostické informace usnadňující opravu nalezených problémů.

7. Rozšíření FreeIPA o správa přístupu dle URI

V rámci tohoto dílčího zaměření projektu je rozvíjena technologie FreeIPA pro centrální správu identit, a to konkrétně v oblasti autorizace pro potřeby webových aplikací. Konkrétně je vyvíjen rozšířený mechanismus řízení přístupu založený na využití URI, ke kterému uživatel přistupuje. V roce 2015 byl navržen základní koncept uvedeného přístupu. Jeho implementace a ověření se očekává v roce 2016.

8. Závěr

Ve výše uvedeném textu byl prezentován přehled některých z oblastí řešených pro společnost Red Hat Czech, s.r.o. na Fakultě informačních technologií Vysokého učení technického v Brně v roce 2015 v rámci projektu *Zlepšování kvality software*. Mimo uvedené oblasti byla řešena celá řada dalších témat, jako např. refaktorizace a verifikace kódu mkfs xfs, verifikace vybraných vlastností protokolu AMQP 1.0, vylepšení nástrojů pro práci se soubory deltarpm, rozšíření modulů OpenStack pro platformu Ansible či testování aplikací s využitím Linuxových kontejnerů.

Výstupy projektu dosažené v roce 2015 byly objednateli předány v jím požadované podobě zahrnující (dle konkrétních témat) zdrojové kódy, zprávy, či experimentálně získaná data. Ve většině z uvedených oblastí přitom probíhá další výzkum i v roce 2016.