Oponentský posudek dizertační práce

Název práce: Retargetable Analysis of Machine Code

Autor: Ing. Jakub Křoustek

Školitel: Doc. Dr. Dušan Kolář

Posudek

Shrnutí výsledků

Předkládaná dizertační práce Ing. Jakuba Křoustka je prací z oblasti překladačů, analýzy cílového spustitelného kódu a zpětného inženýrství (dekompilace kódu), s využitím i nově zavedených formalismů teorie formálních jazyků, gramatik a automatů. Nejedná se o analýzu zdrojového programu nebo bytekódu. Téma práce odpovídá oboru disertace a je aktuální z hlediska současného stavu vědy.

Práce obsahuje úvod do problému dynamické a statické analýzy kódu, souhrn použitých základních pojmů, popis používaných formátů spustitelných souborů a podrobnou rešeršní část. V rešešní části je výborným a podrobným způsobem popsán současný stav v oblasti disasemblerů, debugerů a dekompilátorů.

Část práce popisující nové výsledky studenta je rozdělena na dvě části: popis nových výsledků v oblasti dynamické analýzy kódu a popis nových výsledků v oblasti statické analýzy kódu. Jedná se o několik nových technik, které byly na dostatečné úrovni prezentovány na řadě odborných konferencích a publikovány v časopisech a jsou začleněny do projektu Lissom vyvíjeného na FIT VUT Brno, tj. byly implementovány a experimentálně prověřeny. Důraz v nástrojích je kladen na rekonfigurovatelnost cílové architektury. Z formalismů z teorie formálních jazyků jsou vhodně použity tzv. two-way coupled finite automata v nástroji dynamické analýzy kódu a nově zavedené tzv. scattered context grammars with priority v nástroji pro statickou analýzu kódu. Předposlední kapitola práce obsahuje experimentální výsledky z měření a srovnání s hlavními existujícími podobnými nástroji. Tyto výsledky ukazují, že nové výsledky jsou srovnatelné nebo dokonce lepší ve výkonu s existujícími nástroji pro analýzu. Práce jednoznačně obsahuje původní přínosné části studenta.

Formální úroveň práce

Po formální stránce je práce napsána velice pečlivě a na výborné úrovni: práce téměř neobsahuje formální ani věcné chyby, po jazykové stránce je psaná srozumitelnou angličtinou bez chyb. Z textu práce je poznat, že práce je založena na řadě již publikovaných článků, které byly nejednou čteny mnoha recenzenty. Vytkl bych pouze to, že v Kapitole 2 je Definice 5 kontextové gramatiky chybná a

dále, že definice 16 až 21 nejsou klasickými definicemi, kdy je pojem od začátku jednoznačně definován pomocí sérií známých definic, ale jsou spíš popisy pojmů, jako jsou základní blok, graf volání atd…

Budoucí práce

Práce má řadu možných témat pro budoucí práci, která jsou vhodně shrnuta v sekci 8.1.

Výhrady k práci

K práci nemám žádné vážnější výhrady.

Dotazy k obhajobě:

Co vedlo autora práce k výběru a použití výše zmíněných formalismů z teorie automatů a gramatik? O jakých dalších vhodných formalismech autor při své práci uvažoval?

Celkové hodnocení

Celkově konstatuji na základě předložené práce, že Ing. Jakub Křoustek jednoznačně prokázal své znalosti a schopnosti potřebné pro úspěšnou vědeckou práci, což take vyplývá ze seznamu vědecké činnosti uchazeče. Množství výsledků a jejich kvalita bez pochyb splňují kritéria kladená na získání titulu Ph.D., a proto práci **doporučuji k obhájení.**

V Praze 3.4.2015,

doc. Ing. Jan Janoušek, Ph.D.

vedoucí katedry teoretické informatiky,

Fakulta informačních technologií,

České vysoké učení technické v Praze