FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jan Brož
Oponent práce:	Ing. Jiří Buček, Ph.D.
Název práce:	Hledaní zranitelností nad LLVM mezikódem
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 6. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Zadání bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Písemná část práce je sice poněkud stručná, obsahuje však všechny důležité kapitoly. Přehlednost a logické členění práce by potřebovalo zlepšit, např. kapitola Implementace má pouhé 4 strany. Poněkud chybí přehledný diagram návrhu studentova programu. Po formální stránce je práce uspokojivá, obsahuje chyby v typografii (přetékající řádky) i v pravopisu. V seznamu literatury chybí odkaz na testovací sady (Juliet Test Suite, ...).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*75 (C)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Práce je dodána ve formě zdrojových kódů, které jsou řídce, ale ještě přiměřeně komentovány. V příloze chybí instalační příručka a uživatelská příručka. Student na vyžádání dodal návod k instalaci a použití mailem, bylo by vhodné aktualizovat i přiložené CD. Student nepřiložil zdrojové kódy ani přeložený tvar použité knihovny LLVM nebo překladače clang, a příloha neobsahuje ani testovací sady, ani skripty na jejich otestování. Pokud by to licence umožňovaly, bylo by lepší do přílohy začlenit vše, co je nutné k otestování práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*80 (B)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Vzhledem k použití staré verze LLVM je překlad a otestování programu na moderním systému pracnější, než by muselo být. Výsledný program jsem vyzkoušel na jednoduchém vlastním příkladu, a zde program fungoval podle očekávání. Výstup programu je poněkud nepřehledný, nalezené zranitelnosti by měly být více zvýrazněny. Program označí nalezenou zranitelnost jmény funkcí, ale už nevypíše číslo řádku ve zdrojovém kódu (je otázka, zda je tento údaj k dispozici). Program je funkční a je využitelný zejména k dalšímu studiu zranitelností a metod jejich odhalování.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Proč jste zvolil jako základ Vaší práce LLVM verze 3.8.1, a ne některou z novějších verzí? Liší se aktuální verze vnitřní formy programu v LLVM podstatně od verze, kterou jste použil Vy?

Dal by se Váš program vylepšit o označení čísla řádku ve zdrojovém kódu s nalezenou zranitelností?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení

78 (C)

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Studentova práce je zdařilá, a výsledný program je funkční. Hodnocení snižuje zejména formální úroveň textu práce a chybějící návody. Je však vidět, že student do práce vložil nemalé úsilí a prokázal schopnost samostatné tvůrčí práce. Práci doporučuji k obhajobě.

Podpis oponenta práce: