FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jan Brož
Vedoucí: práce:	Ing. Josef Kokeš
Název práce:	Hledaní zranitelností nad LLVM mezikódem
Obor:	Počítačová bezpečnost

Datum vytvoření: 19. 5. 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:

Cílem práce bylo navrhnout a implementovat algoritmus, který by dokázal v programech v LLVM mezikódu hledat běžné bezpečnostní chyby. Jde o poměrně náročnou a rozsáhlou problematiku s velkými dopady na bezpečnost. V rámci mezí daných časovou dotací a požadovaným rozsahem diplomové práce byly požadované cíle na teoretickou práci splněny, praktická implementace však vykazuje vážné nedostatky uvedené v dalších bodech posudku.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*80 (B)*

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:

Práce přehledně a srozumitelně vysvětluje jak teoretická východiska pro předmětnou oblast, tak návrh algoritmu pro její řešení i jeho vyhodnocení. Textová část mohla být o něco rozsáhlejší, formálně jen těsně naplňuje požadované minimum, a to ještě s pomocí řady ukázek kódu (které však považuji za vhodné a užitečné), ale potřebné informace přináší a těžiště práce bylo v návrhu algoritmu a jeho implementaci, takže nemám výhrady. Slabiny nacházím ve formální stránce práce, jazyk není vždy stoprocentní (např. čárky) a technická stránka také vykazuje chyby (např. seznam ukázek kódu je nesprávně uveden v obsahu jako první významová strana).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*60 (D)*

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:

Vytvořený algoritmus se zdá být funkční a vytvořený program ho realizuje. Bohužel až po odevzdání práce se projevil vážný nedostatek z pohledu použitelnosti: chybí detailní dokumentace toho, jak vlastně program použít. Ukazuje se, že to není tak přímočaré, jak se zdálo, protože je nutné použít konkrétní verzi LLVM i kompilátoru jak pro kompilaci programu, tak i pro kompilaci programů, které mají být vyhodnoceny na zranitelnosti. To v práci není psáno a bohužel se mi nepodařilo zreplikovat prostředí, na které jsem byl později upozorněn (LLVM verze 3.8.1 pro všechny činnosti). V důsledku toho se mi sice podařilo zkompilovat některé jednoduché testovací prográmky, které však nejsou vyhodnoceny dobře, jeden program doběhl do konce bez varování (měl nahlásit přetečení bufferu ve funkci gets), druhý předčasně spadl. Důvod je nejasný, může to být chyba v programu i chyba v sestavovacím prostředí. Na složitější programy jsem si každopádně netroufl. Otevřená tak zůstává otázka výkonu algoritmu, která patrně bude dalším problémovým místem.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*60 (D)*

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:

Využitelnost výsledků je nejistá. Koncept analýzy nad LLVM mezikódem, se kterým student přišel, je podle mě výborný. Algoritmus se zdá být v pořádku a věřím, že by mohl být velmi užitečnou součástí statického analyzátoru. Program, který ho realizuje, však v současné době nefunguje správně a i když některé nedostatky jsou snadno napravitelné, jiná jeho omezení (nutná shoda verzí analyzátoru a analyzovaného programu) bude obtížné překonat.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* *3=průměrná aktivita,* ***4=slabší, ale ještě dostatečná aktivita,*** *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student pracoval velmi samostatně. Konzultace byly jen občasné, ale vždy byly k věci a týkaly se podstatných částí problematiky. Chyby v programu však ukazují, že konzultací mělo být více a že by měly probíhat i nad programem, ne pouze nad teoretickou částí práce a nad textem.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*60 (D)*

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:

Samotná myšlenka analyzátoru zranitelností nad LLVM mezikódem je podle mě výborná a vytvořený algoritmus se zdá být funkční. Praktická realizace však pokulhává, některé problémy ani studenta ani mě nenapadlo detailně řešit, dokud se neprojevily v praxi (bohužel až po odevzdání). Z toho důvodu nemůže být práce hodnocena lepší známkou. Na druhou stranu nemám pochyby o tom, že student je schopen inženýrské práce. Proto práci doporučuji k obhajobě, i když jen se známkou D - uspokojivě.

Podpis vedoucího práce: