



Posudek oponenta závěrečné práce

Oponent práce: Ing. Filip Kodýtek, Ph.D.
Student: Dmytro Khimchenko
Název práce: Detektory zranitelností Ethereum projektů
Obor / specializace: Informační bezpečnost 2021
Vytvořeno dne: 30. května 2024

Hodnotící kritéria

1. Splnění zadání

- [1] zadání splněno
- ▶ [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Zadání bylo splněno, měl bych však drobnou výhradu. V zadání je zmíněna analýza a vyhodnocení existujících detektorů v nástroji Wake a implementace nových dle domluvy s vedoucím. V práci je analyzována jen vybraná podmnožina detektorů (3) a implementován byl 1 nový detektor. Rozsah splnění je tedy v tomto případě spíše otázka na vedoucího práce, zda to takto bylo myšleno, nebo ne.

2. Písemná část práce

80/100 (B)

Rozsah práce je adekvátní, vyskytuje se zde však řada překlepů nebo vět, které nedávají smysl. Chyběl zde silnější důraz na motivaci, k čemu celá práce směřovala a proč byl implementován zrovna detektor na odhalení write-after-write operací s celkovým uvedením do kontextu v problematice hledání chyb a zranitelností ve smart kontraktech. Také bych zde očekával větší uvedení do problematiky statické analýzy kódu, vzhledem k tématu práce.

3. Nepísemná část, přílohy

70/100 (C)

Práce se zabývá statickou analýzou kódu, očekával bych zde řešerši v této oblasti. Přestože jde o statickou analýzu kódu pro smart kontrakty, tak by mohlo být užitečné se problematikou statické analýzy zabývat obecně a aplikovat obecně známé postupy a metody z jiných oblastí následně na smart kontrakty. Toto v práci chybí a ani není zmíněno, proč to nebylo provedeno.

4. Hodnocení výsledků, jejich využitelnost

95 /100 (A)

Zjištění z práce a výsledky byly využity pro vylepšení Wake a rozšíření množiny existujících detektorů.

Celkové hodnocení

80 /100 (B)

Celkově práci hodnotím kladně i přes výše zmíněné nedostatky, kde jako zásadní nedostatek bych vytknul právě chybějící rešerši v oblasti statické analýzy kódu. Proto hodnotím práci na pomezí stupně B a C.

Otázky k obhajobě

V kapitole 5 je provedeno vyhodnocení kvality detektoru implementovaného v této práci. Pro vyhodnocení byla použita množina kontraktů zkontrolovaných Slitherem. Neexistuje nějaká větší množina manuálně zkontrolovaných/klasifikovaných smart kontraktů, které by šlo pro přesnější porovnání využít?

Instrukce

Splnění zadání

Posudte, 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, posudte 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.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.