



Posudek oponenta závěrečné práce

Oponent práce: Ing. Filip Kodýtek, Ph.D.
Student: Bc. Ihor Salov
Název práce: Detekce malwaru pomocí vizualizačních technik
Obor / specializace: Počítačová bezpečnost
Vytvořeno dne: 31. 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

Práce celkově působí neupraveně, je zde řada formálních nedostatků. Co se splnění zadání týče, tak body 2 a 4 ze zadání se sice dají do určité míry považovat za splněné, ale velmi minimalisticky. Spíše bych se přikláněl až k nesplněnému zadání.

2. Písemná část práce

60/100 (D)

Je zde řada jazykových chyb, a to dokonce hned ve velmi krátkém abstraktu.

Také je zde mnoho formálních nedostatků, mimo jiné:

- nevysvětlení používaných zkratk při jejich prvním výskytu (ale jsou v seznamu zkratk, přesto to působí rušivě při čtení práce)
- nestandardně vytvořené odkazy na tabulky a obrázky
- na některé obrázky/tabulky není v textu odkazováno
- nejednotně vypadající reference (někde celá jména, někde iniciály)

Práce se celkově i velmi špatně čte kvůli nedostatečné strukturovanosti textu, např. rešerše v sekci 1.1 je nedostatečně členěná textová posloupnost s hromadou faktů, ve které se velmi těžko orientuje. Chybí zde nějaký přehled a případné srovnání mezi rozdílnými přístupy. Student používá nepřesná vyjádření. Kapitola 5 (Implementace), která by měla být pro práci stěžejní, je velmi krátká a vlastně téměř nic neobsahuje. Také je otázka, jestli se vůbec jedná o kapitolu o implementaci, vzhledem k tomu, že implementace zde není popsána. Je v ní zahrnut i závěr, který by měl být v samostatné kapitole.

3. Nepísemná část, přílohy

30/100 (F)

Zdrojové kódy jsem nedostal k dispozici, tudíž nemohu hodnotit. Z prezentovaných výsledků práce však působí implementační a experimentální část práce nedokončeně. Také není jasné, co vlastně student sám naimplementoval a co převzal jinde.

4. Hodnocení výsledků, jejich využitelnost

30/100 (F)

Vzhledem k nedostatečnému zpracování implementační a experimentální práce není využití výsledků práce valné.

Celkové hodnocení

49/100 (F)

Vzhledem k výše zmíněným nedostatkům a především nedokončení práce nedoporučuji tuto práci k obhajobě.

Otázky k obhajobě

Jak byly vytvořeny obrázky pro dataset SORRY?

Dle zadání mělo být provedeno srovnání Vaší detekce malware pomocí vizualizačních technik s jinými technikami. V kapitole 5 je popsáno pouze použití datasetu MaleVis a jednoho konkrétního modelu z již existující knihovny. Co konkrétně tedy bylo nebo mělo být přínosem této práce? Vzhledem k názvu kapitoly - Implementace - co zde bylo vlastního implementováno?

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.