FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Pavla Louthánová
Název práce:	Porovnání adversariálních učících technik pro detekci malwaru
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. června 2023

Hodnotící kritéria

1. Splnění zadání

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

Všetky body zo zadania práce považujem za splnené.

2. Písemná část práce 98 /100 (A)

Práca je dobre členená a má odpovedajúci rozsah. Text je starostlivo pripravený a obsahuje len malý počet drobných nedostatkov, ktoré nebránia v pochopení textu. Práca obsahuje pomerne široko spracovanú časť o súvisiach článkoch. Taktiež obsahuje nové výsledky, ktoré porovnávajú tri rôzne techniky generovania adversariálnych vzorkov, pričom študentka výsledky získané z týchto techník ďalej zlepšila pomocou kombinácie jednotlivých generátorov.

3. Nepísemná část, přílohy 100 /100 (A)

Zdrojové kódy sú dôkladne spracované, pričom bol kladený dôraz na to, aby ich budúci študenti mohli bez väčších problémov použiť v naväzujúcich diplomových prácach. Experimentálne výsledky je možné zreprodukovať.

4. Hodnocení výsledků, jejich využitelnost 98 /100 (A)

Výsledky práce poukazujú na to, ako jednoduché je vygenerovať malware, ktorý nie je detekovaný žiadnym z top antivírových produktov. Na základe tejto práce by sa mohli vytvoriť obranné techniky proti generátorom adversariálnych vzorkov, čo by mohlo mať vysoké uplatnenie v antivírovom priemysle.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

V priebehu celého obdobia práce študentka pracovala aktívne a konzultovala s vedúcim najnovšie výsledky a smerovanie práce.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Študentka si samostatne naštudovala teóriu a dokázala ju aplikovať na daný problém generovania adversariálnych vzorkov škodlivého kódu.

Celkové hodnocení 99 /100 (A)

Táto práca je pokračovaním projektu, na ktorom študentka pracovala v rámci VýLeTu. Práca prispieva novými poznatkami k danej výskumnej oblasti a má potenciál k publikácii vo vedeckom časopise. Celkovo hodnotím prácu známkou A.

Instrukce

Splnění zadání

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.

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 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. 52/2021, 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.

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.