FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Jakub Ács
Vedoucí: práce: Mgr. Martin Jureček
Název práce: Static detection of malicious PE files
Obor: Bezpečnost a informační technologie

Datum vytvoření: 7. 6. 2018

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:

Hlavným cieľom práce bolo zoznámiť sa s problematikou statickej detekcie malware a naimplementovať program založený na strojovom učení, ktorý by oddelil malware od legitímneho software. Program obsahuje dve netriviálne časti: výber optimálnych príznakov a samotný klasifikačný algoritmus. Obe tieto časti sú taktiež v texte podložené teóriou. Namerané výsledky boli v práci vyhodnotené štandardnými metrikami. Porovnanie nameraných výsledkov s predošlými prácami by mohlo byť obsiahlejšie. Všetky časti zadania považujem za splnené.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*91 (A)*

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:

Práca obsahuje relevantné informácie týkajúce sa statickej detekcii malware, ktoré sú logicky rozdelené do jednotlivých kapitôl. Po formálnej stránke je práca na dobrej úrovni a obsahuje minimálne množstvo typografických a gramatických chýb. Prácu s literatúrou hodnotím taktiež kladne a všade v texte je jasné, ktoré časti sú prevzaté a ktoré patria autorovi tejto práce. Štruktúra odkazov na citované zdroje by mohla byť jednotnejšia. Použité datasety aj Python knižnice sú voľne dostupné a preto nedošlo k žiadnemu porušeniu práv.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (A)*

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:

Študent za programovací jazyk vhodne zvolil Python, ktorý obsahuje knižnicu na parsovanie PE súborov a taktiež knižnicu obsahujúcu algoritmy strojového učenia. Študent naprogramoval nemalé množstvo vlastných nástrojov, výsledkom čoho je program, ktorý predspracuje dáta, klasifikuje ich a vyhodnotí.
Malware sadu a sadu legitimného software tvorili reálne súbory a preto dosiahnuté výsledky sú relevantné. Vykonané experimenty je jednoduché opakovať a vykonať i na iných datasetoch.

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

4. Hodnocení výsledků, jejich využitelnost	*92 (A)*

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:

Výsledkom práce je funkčný program určený na detekciu malware, ktorý by mohol mať uplatnenie v antivírovom priemysle.

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:

Aktivitu a samostatnosť študenta hodnotím veľmi pozitívne. Študent začal pracovať na BP už počas druhého ročníku a až do odovzdania práce sa nevyskytlo väčšie časové okno, počas ktorého by práca stála.
Študent si sám získal a pripravil datasety pre strojové učenie, čo nebola jednoduchá úloha. Okrem vedúcim zadanej literatúry si študent sám vyhľadal a preštudoval ďalšiu relevantnú literatúru, ktorú použil pri práci.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*93 (A)*

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:

Študent sa zoznámil s problematikou automatickej detekcie malwaru, samostatne si naštudoval vybrané postupy a niektoré z nich modifikoval a naimplementoval. Všetky body zo zadania boli splnené a preto doporučujem jeho prácu k obhajobe.

Podpis vedoucího práce: