FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Jakub Kaloč
Název práce:	Analýza krypterů a jejich detekování
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	January 27, 2022

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 popísané v pokynoch pre vypracovanie považujem za splnené.

2. Písemná část práce 85 /100 (B)

Rozsah predloženej DP je v súlade s požadovaným rozsahom podľa príslušnej fakultnej smernice. Práca študenta je dobre čitateľná, gramatické chyby sa vyskytujú v minimálnej miere a je dobre členená. Zoznam použitej literatúry práce obsahuje pomerne veľké množstvo relevantných odkazov, celkom 45. Práca obsahuje nasledujúce okrajové chyby:
- odkazy na literatúru by mali byť oddelené od predchádzajúceho slova. Niekedy sú súčasťou vety a niekedy sú uvedené až za vetou alebo celým odsekom
- niektoré obrázky (napr. obr. 2.1, 3.3, 3.4, 3.5) a tabuľka 2.1 nie je spomenutá v texte
- objavuje sa nepresné vyjadrovanie, napr. "matematický odolná" šifra versus "odolná" šifra
- nástroj dnSpy spomenutý na str. 26 je predstavený až na str. 30
- text obsahuje pár nejasností, viď otázky k obhajobe

3. Nepísemná část, přílohy 90 /100 (A)

Nepísomná časť je pomerne rozsiahla a všetky použité technológie ako napr. Cuckoo Sandbox, YARA, ConfuserEx 2 a ďalšie, sú adekvátne k téme DP. Analyzované vzorky sú priložené, takže výsledky je možné overiť.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Študentove výsledky môžu byť a pravdepodobne už sú využité v antivírovom priemysle. Dosiahnuté výsledky sú však obmedzené na vybrané kryptery a je otázne, do akej miery by sa použité techniky dali aplikovať aj na iné kryptery.

Celkové hodnocení 89 /100 (B)

Daná problematika spolu s experimentami bola spracovaná pomerne obšírne. Základné pojmy a techniky považujem za pekne spracované, avšak študentom vykonané analýzy sa z môjho pohľadu nezdajú byť náročné. Ale je potrebné poznamenať, že neovládam reverzné inžinierstvo a neviem, koľko práce bolo za dosiahnutím daných výsledkov. Vzhľadom k vyššie uvedeným chybám v texte prácu hodnotím známkou na hranici medzi A a B.

Otázky k obhajobě

1. Ako je definovaná malwarová rodina a aký je jej vzťah k pojmu strain?
2. Akými ďalšími postupami, ktoré nie sú uvedené v práci, je možné znížiť počet chýb typu false-positive pre súbory, ktoré sú chránené kryptermi, packermi alebo protektormi?
3. Na str. 35 sa píše "Po otvorení programu chráneného touto funkcionalitou nie je možné v dekompilátore vidieť žiadny pôvodný kód, teda statická analýza je nemožná." Statická analýza pracuje s mnohými typmi príznakov. Je skutočne pravda, že keď nie je vidieť žiadny pôvodný kód, tak statická analýza je nemožná?

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.

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.