FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Bc. Jakub Kaloč
Název práce:	Analýza krypterů a jejich detekování
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	January 15, 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadání práce bylo splněno v odpovídající kvalitě.

2. Písemná část práce 90 /100 (A)

Práce je logicky strukturovaná, srozumitelná a dobře pokrývá zvolenou problematiku. Po věcné stránce je v pořádku, pokud obsahuje nějaké faktické chyby, mají vesměs charakter překlepů (např. "32" iterací s posuny "0..32" na straně 49). Zvláštní pochvalu si zaslouží analýza protektorů v kapitolách 4 a 6, délka textu možná nepůsobí ohromujícím dojmem, ale je za ním veliké množství práce nad analýzou kódu a dosažená zjištění jsou výborná. Naopak problematiku false-positive detekcí považuji za podstatně důležitější než jak ji vnímá student, zasloužila by si podle mě podrobnější rozbor (ale toto nelze příliš kritizovat, protože F.P. detekce dosud neumí uspokojivě vyřešit nikdo).
Co se týče jazykové stránky, necítím se být kvalifikován hodnotit detailně slovenskou gramatiku, ale až na čárky mezi větami nenarážím na nic, co by mě připadalo podezřelé. Formální stránka práce odpovídá běžným standardům.

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

Nepísemná část práce je tvořena několika navazujícími, ale přesto spíše oddělenými částmi.
V první řadě jde o jednotlivé vzorky, které student analyzoval. Právě tato analýza reprezentuje nejrozsáhlejší a nejnáročnější část celé diplomové práce a je možná škoda, že výsledky nejsou dostupné v jiné podobě než jako popisy v textu práce - sice zachycují hlavní zjištění a způsob jejich dosažení, ale bylo by přínosné mít k tomu i úplnou verzi

např. v podobě dekompilovaného zdrojového kódu s komentáři v klíčových místech. Bez toho je pro čtenáře obtížné analýzu zopakovat (ověřit) nebo se blíže podívat na nějaký konkrétní detail, který ho zajímá. Navíc se tím student připravuje o uznání, protože před čtenářem skrývá, kolik práce tato analýza obnášela. Právě toto je důvod vysokého bodového hodnocení tohoto kritéria.
Druhou částí je pak vlastní kód studenta, který rozšiřuje možnosti nástroje YARA o lepší spolupráci s monitorem Cuckoo. Toto rozšíření je velice důležité pro praktickou použitelnost zjištěných informací. Rozsahem je velice krátké, což je ale v pořádku vzhledem k rozsahu předchozí části. Přidaný kód je označen, bylo by ale vhodné vyznačit i verzi programu, pro kterou je určen - nyní to není problém, protože rozdíly proti aktuální verzi jsou pouze ve studentových úpravách, za rok nebo za dva už ale může být situace jiná. Ideální by bylo mít na CD naklonovaný repozitář s větví obsahující studentovy úpravy.
Třetí částí práce jsou vytvořené signatury pro nástroj Cuckoo, které umožňují detekovat analyzované techniky. Zde jsem na rozpacích, protože signatury jsou typicky velice jednoduché, takže za prvé zcela jistě povedou na falešné detekce, i když jich použijeme více současně, a za druhé v nich nemá čtenář dostatek podkladů pro to, aby je mohl upravit na komplexnější detekci. Byl bych také opatrnější s pojmenováním, od toho, co dělá signatura "detect_analysis_process", je ještě dlouhá cesta ke kategorickému prohlášení, že "Sample probably looks for a process related to a sandbox or an analysis tool".

4. Hodnocení výsledků, jejich využitelnost

75 /100 (C)

Praktickou použitelnost výsledků vnímám jako rozporuplnou. Student analyzoval několik protektorů a navrhl kritéria, podle kterých je možné je spolehlivě detekovat - to ale stávající antimalware umí také. Připravil pro tyto detekce YARA pravidla - ale možná ještě užitečnější by bylo využít zjištěné slabiny v obfuskacích pro implementaci obecného unpackeru. (Toto nicméně nelze hodnotit jako chybu, zadání práce chtělo detekční pravidla.) Student rozšířil možnosti spolupráce YARA a Cuckoo a implementoval několik signatur pro Cuckoo, což může mimo jiné posloužit jako alternativní dokumentace jinak poměrně špatně oficiálně popsaného rozhraní - ale ty signatury jsou natolik jednoduché, že je obtížné z nich usuzovat, jak je rozšířit pro komplexnější případy.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení

90 /100 (A)

Celkově práci hodnotím jako zdařilou, nedostatky uvedené výše jsou více než převýšeny přínosy. Chtěl bych zejména zdůraznit, že problematika reverzní analýzy je velice náročná, zvlášť v případech, kdy analyzujeme malware nebo software s malwarem související - zde konkrétně software zaměřený na to, aby analýzu ztížil až znemožnil. Bylo by naprosto vyhovující, kdyby student v rámci diplomové práce analyzoval i jen jeden protektor - on jich analyzoval pět. Považuji za nepochybné, že student prokázal zvládnutí relevantní teorie i praxe na inženýrské úrovni, a proto jeho práci doporučuji k obhajobě a hodnotím známkou A-výborně.

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.