FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Bc. Daniel Uhříček
Název práce:	Detekce IoT malware v počítačových sítích
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	19. května 2021

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno v plném rozsahu. Z práce je viditelná značná pečlivost studenta, která se projevuje na perfektně zpracované analýze současného IoT malware, která obohatí jistě nejen mé znalosti v této oblasti. Z této podrobné analýzy následně vychází koncept návrhu detekčního algoritmu, který využívá slabé (weak) klasifikátory. To se projevilo nejen na přesnosti detekce, ale také na pracnosti, která značným způsobem překonala plánovanou náročnost. Dále, nad rámec zadání práce, student implementoval knihovnu FET sloužící k usnadnění hledání užitečných charakteristik síťového provozu pro klasifikaci. Tato knihovna se stala velice oblíbenou v rámci týmu kolem Laboratoře monitorování síťového provozu a zařadila se mezi nepostradatelné nástroje.

2. Písemná část práce

100 / 100 (A)

Práce je psaná v angličtině, je logicky členěná a text i úroveň jazyka jsou na špičkové úrovni. Během jejího čtení jsem nezaznamenal žádný překlep ani typografickou chybu. Perfektně dokumentuje uvažování studenta, popisuje důvody jeho návrhových rozhodnutí i vyhodnocování a testování vytvořeného algoritmu.

3. Nepísemná část, přílohy

100 / 100 (A)

V příloze práce jsou zdrojové kódy detektoru, které jsou poměrně obsáhle a skládají se z několika klasifikátorů. Dále přílohy obsahují nové datové sady z reálného malware, analytické jupyter notebooky a knihovnu FET usnadňující vyhodnocování užitečnosti charakteristik ze síťového provozu. I nepísemná část je v rámci této práce mimořádně kvalitní a nenašel jsem na ní žádné nedostatky. Zdrojové kódy jsou perfektně

dokumentované pomocí automatického nástroje sfinx. Oceňuji i rozdělení a čitelnost analytických jupyter notebooků.

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

Vytvořený algoritmus používá poměrně inovativní řešení v podobě slabých klasifikátorů zaměřujících se na specifické signatury jednotlivých malwarových rodin. Aplikace tohoto řešení není triviální a není možné jej dohledat v literatuře, a proto předpokládáme konferenční publikaci prezentující výsledky této práce. Mimo vědeckou využitelnost výsledků je možné tento nástroj nasadit na detektorech v síti CESNET2, či na libovolné domácí síti monitorované pomocí systému NEMEA. Nedílnou součástí je také knihovna FET, která už je v tomto roce využívána řadou studentů během řešení jejich závěrečných prací.

5. Aktivita studenta

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

Student se účastnil pravidelných konzultací na které chodil vždy perfektně připraven.

6. Samostatnost studenta

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

Student samostatně vyhledával informace na pravidelné konzultace přicházel s množstvím nápadů.

Celkové hodnocení 100 /100 (A)

Jedná se o perfektně zpracovanou práci, které dle mého názoru nic nechybí. Práce prezentuje inovativní prototyp detekce IoT malware, který je založený na hlubokých znalostech studenta v této oblasti. Celkový systém se skládá z pěti různých detektorů, jejiž návrh a implementace nebyla triviální. Tento prototyp je poměrně pečlivě testován na několika datových sadách z naprosto odlišných sítí a dosahuje velice přesných výsledků. Vzhledem ke kvalitě textu, kvalitě nepísemné části a inovativnosti daného řešení považuji práci za excelentní, a proto bych rád komisi doporučil její nominování na cenu děkana.

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. 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.

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.