Posudek oponenta bakalářské práce

Student: Štěpánek Martin
Téma: Vylepšení generování vzorů pro detekci škodlivého kódu (id 21872)
Oponent: Regéciová Dominika, Ing., UIFS FIT VUT

1. **Náročnost zadání** — **obtížnější zadání**
   Zadání se řadí mezi obtížnější z důvodu nutnosti nastudování hned několika pokročilých nástrojů a pro navržení vylepšení bylo potřeba dobré porozumění rozsáhlé problematiky detekce škodlivého kódu.
2. **Splnění požadavků zadání** — **zadání splněno**
   Zadání bylo splněno ve všech bodech.
3. **Rozsah technické zprávy** — **splňuje pouze minimální požadavky**
   Rozsah technické zprávy splňuje minimální rozsah.
4. **Prezentační úroveň předložené práce** — **80 b. (B)**
   Členění práce je dobré, jednotlivé kapitoly na sebe logicky navazují. Zpráva je však místy poněkud stručnější, zvláště vyhodnocení výsledků mohlo být rozebráno více do detailů.
5. **Formální úprava technické zprávy** — **85 b. (B)**
   Typografická stránka práce je na dobré úrovni, v textu je pouze pár drobných chyb. Některé věty mají trochu krkolomný slovosled, stejně tak skloňování nebylo vždy v pořádku. Není jasné, zda je prázdná strana 41 záměrem, nebo přehlédnutým detailem, na straně 17 je to však jistě nechtěné. Student až nadbytečně používá anglických terminů i u slov, které mají ustálený český výraz.
6. **Práce s literaturou** — **90 b. (A)**
   Práce s literaturou je velmi dobrá. Na bakalářskou práci je seznam literatury nadstandardně dlouhý, všechny zdroje se ale zdají relevantní. Odkazování v textu je také v pořádku, zajímavé je také využití průzkumů, kterým student zdůvodňuje například zaměření na systémy Microsoft Windows.
7. **Realizační výstup** — **95 b. (A)**
   Realizační výstup vypadá velmi dobře navržen i implementován, s citem při doplňování původní verze nástroje. Samotný kód je dobře rozčleněn a je pečlivě okomentován. Uspokojivý je u počet jednotkových a integračních testů vytvořených studentem. Autorství kódu je ošetřeno seznamem vytvořených a upravených souborů v rámci projektu.
8. **Využitelnost výsledků**
   Práce byla od začátku zaměřena na využití v praxi. Student vypracoval vylepšení nástroje YaraGen, který je v současné době využíván firmou Avast Software.
9. **Otázky k obhajobě**
   1. Jak nástroj YaraGen rozhoduje o zařazení generovaného pravidla do jednotlivých kategorií?
   2. Proč je žádoucí, aby byl binární soubor detekován pouze jedním pravidlem?
   3. V tabulce 5.3 je vidět značný pokles pokrytí u kategorie know_sequences, je to způsobeno pouze přidáním dalších dvou kategorii, nebo ještě díky jiným vlivům?
10. **Souhrnné hodnocení** — **87 b. velmi dobře (B)**
    Obě části, implementační i technická, jsou velmi dobře vypracovány, vytknout mohu pouze drobnější věci a trochu strohé shrnutí výsledků.
    Celkově proto navrhuji hodnotit práci stupněm B (87 bodů).

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 29. května 2019

.....
podpis