Posudek oponenta bakalářské práce

Student: Kender Tomáš
Téma: Rozšiřování jazyka YARA (id 23242)
Oponent: Zobal Lukáš, Ing., UIFS FIT VUT

1. **Náročnost zadání** — **průměrně obtížné zadání**
   Zadání hodnotím jako průměrné až lehce obtížnější. Student měl nastudovat požadovaný jazyk a navrhnout a implementovat jeho vylepšení. Přesto, že kvantitativně nebylo technologií mnoho, bylo třeba seznámit se s jazykem YARA ve velkém detailu, společně s jeho moduly.
2. **Splnění požadavků zadání** — **zadání splněno**
   Zadání bylo splněno. Student navrhl, implementoval a vyhodnotil množství vylepšení, jak bylo požadováno.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
   Technická zpráva je obvyklého rozsahu. Práce neobsahuje redundantní text, naopak, text Návrhu by mohl detailněji popisovat jednotlivé navrhované změny.
4. **Prezentační úroveň předložené práce** — **65 b. (D)**
   Na nejvyšší úrovni je dělení do kapitol vhodné a odpovídá zadání. Kapitoly ale nemají úvod a není zcela jasná korelace mezi sekcemi návrhu a implementace. Kapitola Návrh je v některých částech až příliš stručná. Tabulky ani obrázky se v textu vůbec neodkazují a často ani nejsou vysvětleny. Jejich hodnota pro čtenáře je tedy nízká.
5. **Formální úprava technické zprávy** — **95 b. (A)**
   Formální úprava je bez problému. Kladně hodnotím vizuální podobnost prezentovaných schémat a využití přehledných pseudokódů a ukázek YARA pravidel.
6. **Práce s literaturou** — **60 b. (D)**
   Literature je velmi stručná. Z devíti záznamů jsou pouze dva odborné články (z toho pouze jeden relevantní k tématu), zbytek jsou články a dokumentace na internetu. Toto mohlo být dle mého názoru rozšířeno. Student nevyužil ani vedoucím doporučovanou literaturu.
   V samotném vysázeném seznamu literatury se pak míchají anglické a slovenské měsíce.
7. **Realizační výstup** — **90 b. (A)**
   Student v práci navrhl dostatek nových rozšíření jazyka YARA, které navíc mají okamžité praktické využití. Implementované funkcionality vhodně vyhodnotil, odpovídajícím způsobem zhodnotil i špatné výsledky. Student následoval licenční podmínky open-source nástroje YARA i využívaných modulů.
8. **Využitelnost výsledků**
   Implementované vylepšení bylo ihned aplikováno do praxe. Vedlo k ulehčení práce uživatelů jazyka YARA a ve výsledku tak k efektivnější ochraně uživatelů před kybernetickými hrozbami.
9. **Otázky k obhajobě**
   - Zhodnoťte prosím hlavní důvody špatných výsedků použití knihovny Hyperscan, s přihlédnutím k původnímu očekávání od tohoto vylepšení.
10. **Souhrnné hodnocení** — **80 b. velmi dobře (B)**
    Student úspěšně navrhl a implementoval vylepšení požadovaná zadáním. Přes ne vždy srozumitelnou formu popisu v práci odvedl dobrou implementační práci včetně zhodnocení výsledků, a vybraná vylepšení byla ihned aplikována do praxe. Z těchto důvodů navrhuji hodnocení B.

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

V Brně dne: 25. května 2021

Zobal Lukáš, Ing.
oponent