Posudek oponenta diplomové práce

Student: Kočí Jan, Bc.
Téma: Monitorování mobilních aplikací pomocí otisků TLS (id 24834)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání

průměrně obtížné zadání

2. Splnění požadavků zadání

zadání splněno pouze částečně s vážnými výhradami

Práce má za cíl monitorovat mobilní aplikace pomocí otisků TLS. V rámci práce mám výhrady ke splnění některých bodů zadání - zejména body, 4., 5., které jsou v práci sice zmíněny, ale považuji jejich popis za neúplný. Chybí mi zejména diskuze k výsledkům - proč vyšly hodnoty některých detekčních metod tak nízko, popis jednotlivých datasetů, aj. Také mi chybí podrobnější demonstrace monitorování nad reálným provozem. V práci je zde pouze ukázka nad komunikací 4 uživatelů, což nepovažuji za dostatečné.

3. Rozsah technické zprávy

je v obvyklém rozmezí

4. Prezentační úroveň předložené práce

60 b. (D)

Práce je logicky strukturována a jednotlivé části na sebe navazují. Text práce je srozumitelný, některé části by ale měly být diskutovány podrobněji - zejména získání a vyhodnocení datasetů, výběr detekčních metod, aj.

5. Formální úprava technické zprávy

80 b. (B)

K typografické stránce práce nemám výhrady. Práce využívá LateX šablonu a je kvalitně zpracována. Práce je psaná anglicky. K jazykové stránce práce nemám vážnější výhrady. Angličtina je na slušné úrovni, čitelná, bez větších chyb.

6. Práce s literaturou

80 b. (B)

V práci je využito celkem 39 zdrojů. Řada z nich jsou články zabývající se různými přístupy k danému problému, které jsou shrnuty v related works. Práce cituje dle zvyklostí. Nezaznamenal jsem porušení citační etiky.

7. Realizační výstup

50 b. (E)

Realizační výstup představuje nástroj v jazyce Python. Nástroj je vcelku jednoduchý, čitelně napsaný. Z pcap souborů dokáže vytvořit JA3 hash, po zpracování informace z TLS hlavičky. Nástroj primárně zpracovává csv data exportované ze sondy Flowmon, které klasifikuje na základě jednotlivých algoritmů pro výpočet skóre. Z hlediska detekce je pak použito primárně SNI.

Výstup práce nepovažuji za příliš použitelný. Pro provoz a monitorování aplikací v reálném provozu (viz 5. bod zadání), by musel být nástroj navržen pravděpodobně zcela jinak. Takto je určen jako jednoúčelový skript pro výpočet hodnot, dle jednotlivých algoritmů.

8. Využitelnost výsledků

Vytvořený dataset JA3 otisků pro aplikace by teoreticky šlo využít v navazujících pracích, zabývajících se danou problematikou. Vytvořený způsob detekce a zpracování dat je ale obtížně dále využitelný.

9. Otázky k obhajobě

- Výsledné skóre klasifikace (7.10) je suma všech ostatních klasifikátorů. Jak může dané skóre fungovat? Nemůže dojít při součtu klasifikací k překročení 100%?
- Z popisu klasifikace mi vyplývá, že dojde vždy k identifikaci flow k nějaké aplikaci (výpočet skóre bude vždy nějaká hodnota). Podle čeho určíte, že je identifikace správná?

10. Souhrnné hodnocení

50 b. dostatečně (E)

Práce má za cíl monitorovat mobilní aplikace na základě otisků TLS. Typografická a jazyková stránka práce je vcelku kvalitní. Problém vidím v realizačním výstupu a zvolených detekčních metodách, které, dle mého názoru, nevedou příliš ke smysluplným a využitelným výsledkům. V práci mi také chybí podrobnější diskuze k některým bodům - zejména monitorování nad reálnou sítí a podrobnější popis a vyhodnocení datasetů, kde se výsledky detekce řádově odlišují od state-of-the-art hodnot, bez podrobnějšího komentáře, proč tomu tak je. Celkově hodnotím práci jako dostatečnou (E).

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

V Brně dne: 2. června 2022

Grégr Matěj, Ing., Ph.D.
oponent