Posudek oponenta diplomové práce

Student: Snášel Daniel, Bc.
Téma: Identifikace mobilních aplikací v šifrovaném provozu (id 25031)
Oponent: Burgetová Ivana, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání diplomové práce hodnotím jako obtížnější, protože vyžaduje komplexní zpracování problematiky identifikace mobilních aplikací v šifrovaném provozu. Student se musel seznámit s dostupnými metodami, navrhnout vlastní způsob vytváření otisků aplikací a tento způsob otestovat a vyhodnotit pomocí vlastních nástrojů. Za tímto účelem musel také připravit vlastní datové sady.

2. Splnění požadavků zadání **zadání splněno**

Student splnil zadání ve všech bodech.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **78 b. (C)**

Prezentační úroveň technické zprávy je velmi dobrá. Zpráva je čtivá a jednotlivé kapitoly na sebe dobře navazují. Bohužel však tato zpráva obsahuje mnoho nepřesností, které zhoršují pochopitelnost pro čtenáře, zejména v kapitolách 5 a 6. Zde se často rozchází informace v textu s informacemi prezentovanými v přiložených tabulkách nebo v přílohách práce (např. tabulky č. 5.11, 6.3, 6.4, 6.7, 6.8, 7.2).

5. Formální úprava technické zprávy **89 b. (B)**

Z jazykového a typografického pohledu se jedná o velmi kvalitní práci.

6. Práce s literaturou **92 b. (A)**

Seznam literatury je přiměřeně obsáhlý, student prostudoval potřebné zdroje a převzaté prvky jsou řádně odlišeny od vlastních výsledků a úvah.

7. Realizační výstup **93 b. (A)**

V rámci realizačního výstupu vznikly skripty potřebné pro tvorbu datasetu s otisky aplikací a pro identifikaci otisků ze síťového provozu (detekci aplikací). Vytvořené skripty jsou plně funkční. Kromě těchto skriptů student v rámci diplomové práce vytvořil potřebné datasety, na jejichž základě určil atributy vhodné pro tvorbu otisků mobilních aplikací. Těmto atributům také přiřadil vhodné váhy na základě provedených experimentů.

8. Využitelnost výsledků

Jedná se o práci, která přináší nové poznatky v oblasti tvorby otisků mobilních aplikací a jejich detekce v šifrované komunikaci. V rámci práce byl navržen a implementován způsob vytváření potřebných otisků, způsob jejich identifikace. a také způsob aktualizace využívané databáze otisků. Podle dosažených výsledků je navržená metoda velmi přesná.

9. Otázky k obhajobě

- Jakým způsobem vybíráte ze síťového provozu pro tvorbu otisků právě ta TLS spojení, která jsou charakteristická pro danou aplikaci?
- Neuvažoval jste o využití atributů, které generují falešně pozitivní hodnoty, pro potvrzení toho, že byla aplikace správně identifikována?

10. Souhrnné hodnocení **91 b. výborně (A)**

Předložená diplomová práce komplexním způsobem řeší detekci mobilních aplikací v šifrovaném provozu. Student vybral vhodné atributy pro tvorbu otisků mobilních aplikací, přiřadil jim váhy a navrhl způsob porovnávání otisků. S tímto způsobem dosáhl vysoké přesnosti identifikace mobilních aplikací. Proto i přes nesrovnalosti v technické zprávě navrhuji hodnocení stupněm A.

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

V Brně dne: 1. června 2022

Burgetová Ivana, Ing., Ph.D.
oponent