Posudek oponenta bakalářské práce

Student: Babic Radovan
Téma: Detekce mobilních aplikací pomocí profilů komunikace (id 23992)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** **průměrně obtížné zadání**
   Práce se zabývá vytvořením otisků z SSL komunikace. Zadání hodnotím jako průměrně obtížné.
2. **Splnění požadavků zadání** **zadání splněno s drobnými výhradami**
   Drobné výhrady mám ke splnění bodu 3 zadání. Student měl vytvořit datovou sadu a vybrat vhodné položky pro vytvoření profilu. V práci nicméně tento bod není příliš diskutován a automaticky se využívá přímo otisk JA3 pro SSL. Nicméně tento způsob nemusí být jediný možný a očekával bych podrobnější diskuzi daného problému.
3. **Rozsah technické zprávy** **je v obvyklém rozmezí**

4. **Prezentační úroveň předložené práce** **70 b. (C)**
   Práce je logicky členěná. Některé informace bych ale pro lepší přehlednost prezentoval čtenáři jiným způsobem - např. v 3.2 se student zmiňuje o chybějícím SSL rozšíření elliptic_curves aby v kapitole 5 upozornil, že dané rozšíření v datech je, pouze se jmenuje jinak.
5. **Formální úprava technické zprávy** **70 b. (C)**
   Typograficky je práce standardní, dle šablony LateX s několika drobnými prohřešky (např. dělení zkratky IPFIX v závěru práce). Práce je psaná slovensky, dle mých znalostí bez větších chyb.
6. **Práce s literaturou** **60 b. (D)**
   Práce cituje pouze tři zdroje. Řadu dalších věcí cituje jako poznámky pod čarou. Zde bych očekával spíše odkaz do literatury.
7. **Realizační výstup** **65 b. (D)**
   Programové řešení obsahuje několik skriptů napsaných v jazyce Python, které zpracují pcap soubory a vypočtou otisky z SSL komunikace. Skripty nejsou příliš komentované. Logické členění také není, podle mého názoru, vždy nutné - např. Utility.py obsahuje pouze jednu triviální funkci. Některé části nejsou dopracovány.
8. **Využitelnost výsledků**
   Výsledky práce lze využít jako další zdroj dat pro detekci aplikací ze síťové komunikace.
9. **Otázky k obhajobě**
   - Jaký dopad bude mít na detekci nasazení šifrovaného Client Hello? (draft-ietf-tls-esni)
10. **Souhrnné hodnocení** **65 b. uspokojivě (D)**
    Práce vytváří ze zachycené SSL komunikace otisky, které mohou být dále použity pro detekci aplikací. Práce je napsána pochopitelně. Realizační výstup obsahuje několik skriptů v jazyce Python, které automatizují daný proces. Práci celkově hodnotím jako uspokojivou (D).

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

V Brně dne: 3. června 2021

Grégr Matěj, Ing., Ph.D.
oponent