Hodnocení vedoucího diplomové práce

Student: Kočí Jan, Bc.
Téma: Monitorování mobilních aplikací pomocí otisků TLS (id 24834)
Vedoucí: Matoušek Petr, doc. Ing., Ph.D., M.A., UIFS FIT VUT

1. **Informace k zadání**
   Cílem práce bylo využít otisky TLS k detekci mobilních aplikací v rámci monitorování toků IPFIX. Student měl vytvořit databázi TLS otisků a na základě dat z monitorovacích sond IPFIX detekovat mobilní aplikace v šifrovaném provozu. Dále bylo úkolem ověřit přesnost detekce a využít znalost mobilních aplikací k profilování uživatelů, detekci nebezpečných aplikací apod. Hlavním cílem bylo nasadit vytvořený systém na reálné síti a ověřit jeho chování. Zadání považuji za středně obtížné. Studentovi se však nepodařilo splnit hlavní body zadání.
2. **Práce s literaturou**
   Student využíval doporučené studijní zdroje.
3. **Aktivita během řešení, konzultace, komunikace**
   Během letního semestru přišel student na konzultaci spíše výjimečně. Místo zpracování dat ze sondy a detekci aplikací v provozu se student zaměřil na zkoumání, jak porovnat hodnoty SNI z otisku TLS, což nebylo hlavním cílem projektu. Další body zadání nestihl. Reálné nasazení do provozu a experimenty s detekcí aplikací v šifrovaném provozu nebyly vůbec provedeny.
4. **Aktivita při dokončování**
   Práce nebyla dokončena v termínu, poslední části textu nebyly konzultovány. Z výsledků experimentů není jasné, jak probíhalo vyhodnocení přesnosti detekce, kolik známých a neznámých aplikací se nacházelo v datasetu a podle čeho se počítaly hodnoty v tabulkách 9.1 a 9.2. V části experimentů (kapitola 10) jsou výstupy bez vyhodnocení přesnosti. Také není jasné, co vyjadřují hodnoty v tabulkách 10.2-10.4 a jak k nim autor přišel. Chybí také popis nasazení detekčního systému do provozu, způsob čtení vstupních dat, jejich zpracování a zobrazení výsledků detekce.
5. **Publikační činnost, ocenění**
   Práce nebyla publikována.
6. **Souhrnné hodnocení** **nevyhovující (F)**
   Student se ve své práci zaměřil na porovnání hodnoty SNI z komunikace TLS, na kterou aplikoval dvě metody detekce podobnosti: Jaccard Index a TF-IDF. Výpočet skóre podle mne nebude správně fungovat pro neznámé aplikace, protože v popisu výpočtu v kapitole 7 není uveden práh spolehlivosti, tj. vybere se nejbližší vhodná aplikace (viz rovnice 7.5 na str. 36), což není v pořádku. Celkový výpočet skóre dle rovnice 7.10 na str. 40 také nedává smysl, tj. celkové skóre by nemělo být součtem skóre pro různé klasifikátory.

   Student splnil první část práce zaměřenou na trénování, tj. učení se otisků známých aplikací (bod 1), a dále prozkoumal možnosti IPFIX sondy (bod 2). V práci ale není ukázáno, jak probíhá sběr a zpracování dat získaných ze sondy (bod 3), jak aplikace provádí detekci na základě databáze otisků, jak úspěšné je profilování úživatelů, jak se chová systém při detekci neznámých aplikací apod. Zcela chybí výstupy z nasazení v reálném provozu (body 4 a 5).

   Protože nebylo dosaženo hlavního cílo práce, tj. využití monitorovaných dat IPFIX pro detekci mobilních aplikací v šifrovaném síťovém provozu, považuji práci za nevyhovující a hodnotím ji stupněm F.

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

V Brně dne: 2. června 2022

Matoušek Petr, doc. Ing., Ph.D., M.A.
vedoucí práce