Posudek oponenta diplomové práce

Student: Navrátil Petr, Bc.
Téma: Anonymizace PCAP souborů (id 23161)
Oponent: Hynek Jiří, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání hodnotím jako obtížnější. Student se musel seznámit s problematikou zpracování, ukládání a následné anonymizace síťové komunikace. Student prostudoval formát PCAP, detekoval atributy síťové komunikace na jednotlivých úrovních architektury síťového modelu, pomocí kterých by bylo možné identifikovat uživatele a podrobně prostudoval anonymizační metody. Za pomoci nástroje TShark dále vyřešil problém automatického zpracování vstupních souborů ve formátu PCAP pro různé komunikační protokoly. Práce je tak aplikovatelná až na 3000 různých protokolů. Oproti jiným nástrojům je možné nastavovat pomocí konfiguračních souborů vlastní anonymizační politiku (výběr atributů a metod). Výstupy hodnotím kladně.

2. Splnění požadavků zadání **zadání splněno**

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

4. Prezentační úroveň předložené práce **85 b. (B)**

Prezentační úroveň technické zprávy je na dobré úrovni. V první části práce student představuje architekturu síťového modelu a zmiňuje atributy, které by mohly hrát roli při identifikaci uživatele. Dále se zaobírá problematikou anonymizace a představuje nástroj TShark. V druhé části popisuje návrh, implementaci a testování. Některé pasáže mohly být popsány o něco ilustrativněji (popis anonymizačních metod, anonymizace TCP komunikace).

5. Formální úprava technické zprávy **85 b. (B)**

Po jazykové a typografické stránce je zpráva napsána kvalitně. Výjimečně se vyskytují překlepy. Oceňuji vektorové ilustrace, zejména obrázek 4.1. Naopak bych vytkl ilustrace v sekci 6.3, jejichž sémantika je obtížně pochopitelná.

6. Práce s literaturou **95 b. (A)**

Student cituje dostatečné množství publikací. Oceňuji, že se jedná převážně o odborné publikace.

7. Realizační výstup **95 b. (A)**

Realizační výstup je kvalitní. Anonymizační politiky je možné čitelně definovat pomocí konfigurací psaných v jazyce YAML. Oceňuji, že student kladl důraz na dobrý návrh modelu a rozhraní, což umožňuje rozšířit aplikaci v případě potřeby (např. přidáním nových anonymizačních metod).

8. Využitelnost výsledků

Výsledný software je využitelný firmou Flowmon Networks.

9. Otázky k obhajobě

1. Jak bezpečné jsou implementované anonymizační metody? Je možné prolomit tyto metody a získat tak původní hodnoty identifikující uživatele? Pokud ano, pokuste se uvést jednoduchý příklad.

10. Souhrnné hodnocení **92 b. výborně (A)**

Diplomová práce je až na některé výše zmíněné zanedbatelné nedostatky nadprůměrná jak z hlediska technické zprávy, tak z hlediska realizačních výstupů, které jsou prakticky využitelné firmou Flowmon Networks. Navrhuji hodnocení **stupněm A**.

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

V Brně dne: 27. června 2020

Hynek Jiří, Ing., Ph.D.
oponent