Review of Bachelor's Thesis

Student: Zbořil Jan
Title: IoT Gateways Network Communication Analysis (id 24407)
Reviewer: Perešíni Martin, Ing., DITS FIT BUT

1. Assignment complexity — **less demanding assignment**

Práca sa zaoberá problematikou analýzy sieťovej komunikácie IoT zariadení. Prácu hodnotím ako **menej náročnú**, náročnosť z hľadiska výberu vhodnej metodiky a časovo náročnosť na manuálnu analýzu získaných dát.

2. Completeness of assignment requirements — **assignment fulfilled**

Zadanie považujem za **splnené**, študent si naštudoval koncepty sieťovej komunikácie IoT zariadení, analyzoval existujúce metodiky možného odchytu sieťovej komunikácie a vytvoril prostredie na zachytávanie komunikácie. Študent vo vytvorenom prostredí zozbieral údaje a následne ich vhodne analyzoval. Na základe vykonanej analýzy vyvodil možné problémy súvisiace so sieťovou komunikáciou IoT zariadení a porovnal ním získané výsledky s existujúcimi štúdiami. Pozitívne hodnotím aj vypracovanie práce v anglickom jazyku.

3. Length of technical report — **in usual extent**

Rozsah technickej správy je približne 70 normostrán. Dĺžka práce je teda v rámci **bežného rozsahu** bakalárskej práce. Technická správa uvázda relevantné informácie.

4. Presentation level of technical report — **80 p. (B)**

Práca má logickú štruktúru. Rozsah a poradie kapitol sú vhodne zvolené a celkovo je práca napísaná tak, aby bola pre čitateľa **zrozumiteľná**. Výhradu mám k tomu, že v texte je použitých príliš veľa odsekov, aj keď odsek obsahuje len jednu alebo maximálne dve vety, čo pôsobí rušivo na čítanie textu. Bolo by tiež vhodné občas použiť štylizáciu textu vo forme tučného písma, aby sa upriamila pozornosť na text, alebo písmo textového režimu (texttt) v prípade povedzme dlhých slov, skratiek (napr. TLS_AES_256_GCM_SHA384). Chcelo by to do textu vniesť aj lepšiu štábnu kultúru kultúru a prezentačnú logiku, aby bol text heterogénnejší. Okrem iného, napr. výčet IoT brán je nadbytočný s tabuľkou 5.1, stačilo by ich v texte len spomenúť, keďže sú opomenuté v tabuľke hneď pod ním, atď. Chcel by som tiež upozorniť na nefunkčný odkaz v práci na zozbieranú dátovú sadu, ktorý odkazuje na FIT Nextcloud. Hlavnú kritiku/pripomienky mám ku kapitole Výsledky experimentov. V tejto kapitole je príliš veľa hutného faktografického textu, ktorý sťažuje čitateľovi pohodlné čítanie, osobne nemám záujem presne vedieť o počete bajtov a 12 rôznych doménových názvoch, ktoré mi aj tak nepomôžu k vyvodeniu záverov. Buď by som vybral najdôležitejšie zistenia v každej časti a zvyšok by som dal do príloh, alebo by som úplne prepracoval logickú štruktúru textu. Oceňujem, že na konci kapitoly je aspoň zhrnutie zistení. Inak nemám k práci žiadne ďalšie výhrady.

5. Formal aspects of technical report — **85 p. (B)**

Text práce je napísaný v **angličtine**. Jazyková úroveň práce je dobrá, až na niektoré drobné nedostatky alebo nevhodné vetné konštrukcie a niekedy gramatické chybky alebo príliš zložité súvetia. Postupne sa však jazyková úroveň textu zlepšila.

6. Literature usage — **90 p. (A)**

Študent využíva relevantné zdroje v dostatočnom množstve, pričom čerpá informácie z odborných textov a dokumentácie, ale aj z webových stránok a návodov dostupných najmä na internete. Jediné, čo by som vytkol, je to, že niektoré internetové citácie odkazujúce na webové stránky výrobkov by bolo lepšie presunúť do textu ako poznámky pod čiarou, a nie ako citácie. Prácu s literatúrou hodnotím ako **kvalitnú**.

7. Implementation results — **90 p. (A)**

Realizačný výstup je **uspokojivý** a spĺňa špecifikáciu. Výstupom implementácie je vytvorenie dátovej sady zozbieraných údajov o sieťovej komunikácii 4 rôznych IoT brán. Okrem vytvoreného datasetu študent vytvoril aj akúsi MS Excel tabuľku na analýzu údajov (tá však nie je zverejnená) + analyzoval a vizualizoval dáta pomocou rôznych nástrojov, ako je Zeek.

8. Utilizability of results

Výsledky tejto práce sa pravdepodobne použijú na rozsiahlejšiu analýzu zozbieraných dát a prípadne na identifikáciu jednotlivých IoT zariadení (fingerprinting). Vidím taktiež potenciál na zverejnenie dátovej sady (opublikovanie údajov), prípadne jej ďalšie rozšírenie o väčší počet rôznych IoT zariadení; vytvoriť akýsi IoT lab.

9. Questions for defence

1. Prečo ste na analýzu údajov nepoužili nejaké automatizované metódy (strojové učenie, ...)?

2. Aký by bol najhorší dopad, ak by bol niektorý z opísaných útokov na IoT brány úspešný?

10. Total assessment **90 p. excellent (A)**

Študent splnil všetky povinné body zadania. Práca dosahuje kvalitu z hľadiska rozsahu, úpravy textu a prevedenia (s výnimkou drobných chýb). Práca bola napísaná v anglickom jazyku a jazyková úroveň napísaného textu je dobrá, čo hodnotím pozitívne. Výsledky vyzerajú sľubne a majú potenciál odhaliť zaujímavé súvislosti IoT brán a zariadení a otestovať rôzne klasifikačné metódy na identifikáciu IoT zariadení v sieti. Celkovo hodnotím výsledok ako **kvalitný** a navrhujem študentovi známku **A**.

In Brno 1 June 2022

Perešíni Martin, Ing.
reviewer