Posudek oponenta diplomové práce

Student: Slámová Hana, Bc.
Téma: Forenzní analýza prostředí IoT ze stop síťové komunikace (id 24167)
Oponent: Matoušek Petr, Ing., Ph.D., M.A., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Součástí práce bylo nainstalovat prostředí s vybranými chytrými zařízení, prozkoumat možnosti konfigurace (manuální chování, týdenní režim), odchytit a analyzovat síťovou komunikaci a navrhnout způsob detekce změn chování na základě dostupných dat. Protože většina komunikace je šifrovaná, studentka využívala statistické vlastnosti typu velikost paketů, četnost zasílání vybraných zpráva apod.

2. Splnění požadavků zadání **zadání splněno**

Výstupem práce bylo vytvořit datasety s chováním zařízení, implementovat nástroj na detekci a vyhodnotit úspěšnost detekce. Zadání bylo splněno.

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

4. Prezentační úroveň předložené práce **75 b. (C)**

Členění technické zprávy, zejména části 4 (detekce) a 5 (implementace) není z pohledu čtenáře vhodná, protože obsahy obou kapitol se vzájemně doplňují a čtenář musí neustále skákat mezi popisy v části 4 a 5. Vhodnější by bylo kapitoly sloučit do jednoho logického celku. Názvy podkapitol zabývající se chytrými žárovkami jsou stejné, i když obsah se liší podle typu, viz kapitoly 3.3 a 3.4., 4.1 a 4.2, 5.3 a 5.4 apod. Bylo by hodné dát do nadpisu rozlišení.

Při popisu detekce aktivit chytrých zařízení na základě zadaných pravidel je vhodnější použít např. vývojový diagram či rozhodovací strom než slovní popis algoritmu, který může být pro čtenáře méně srozumitelný.

5. Formální úprava technické zprávy **65 b. (D)**

Práce obsahuje větší množství pravopisných chyb zejména v diakritice či formulaci vět a souvětí, čímž se některé části stávají těžko srozumitelnými.

6. Práce s literaturou **85 b. (B)**

Studentka využívala relevantní zdroje. U citace na str. 16 (popis NTP) je nepřesný odkaz na standard TLS. V literatuře není nutné uvádět u každého citovaného díla URL odkaz a dostupnost, to se týká pouze online zdrojů, které nelze jinak citovat. Neplatí to pro standardy, časopisecké články, apod.

7. Realizační výstup **75 b. (C)**

Ve zdrojovém kódu chybí označení autora a není vždy jasné, které kódy vytvořila studentka sama a které převzala (např. parsery kaitai a další).

Při vyhodnocení úspěšnosti (kapitola 6) by bylo vhodné použít anotovaný soubor s uživatelskými aktivitami a hodnotit počet správně a nesprávně detekovaných aktivit, tj. počítat hodnoty TP, FP a FN. Přehledné srovnání úspěšnosti detekci na jednotlivých zařízeních a pomocí různých metod v práci chybí a čtenář to musí hledat na více místech u jednotlivých PCAP souborů.

8. Využitelnost výsledků

Jedním z výstupů je sada souborů PCAP s odchycenou komunikací chytrých zařízení. Sada je k dispozici pro další výzkum přes portál IEEE Dataport.

9. Otázky k obhajobě

1. V práci používáte pro detekci zařízení a změn např. interval posílání ARP dotazů, interval posílání keep-alive TCP paketů apod. Je možné tyto hodnoty na zařízení nastavit nebo jsou dané výrobcem? Jak je to s expirací ARP či DNS cache?
2. Zkoušela jste vytvořit více nezávislých běhů daného zařízení, aby bylo možné zjistit, zda zkoumané velikosti paketů či intervaly jsou typické pro dané zařízení a aktivitu?

10. Souhrnné hodnocení **75 b. dobře (C)**

Studentka připravila různé scénáře chování chytrých zařízení a odchytila jejich komunikaci pro analýzu chování. Navržené metody detekce aktivit vycházejí z experimentů na několika zařízeních a ukazují možnosti použití statistických metod pro detekci chování chytrých zařízení. Celkově hodnotím práci stupněm C.

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

V Brně dne: 8. června 2021

Matoušek Petr, Ing., Ph.D., M.A.
oponent