Review of Master's Thesis

Student: Koscielniak Jan, Bc.
Title: Detection of Timing Side-Channels in TLS (id 23189)
Reviewer: Malík Viktor, Ing., DITS FIT BUT

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

Zadanie práce spočívalo v rozšírení frameworku tlsfuzzer o nový spôsob testovania, ktorý by umožnil odhaliť zraniteľnosti SSL/TLS frameworku cez časové postranné kanály. Keďže detekcia tohoto typu chýb je všeobecne známa svojou náročnosťou, považujem zadanie za mierne náročnejšie.

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

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

4. Presentation level of technical report — **85 p. (B)**

Práca je pomerne dobre logicky členená, kapitoly a sekcie na seba nadväzujú. Výhradu mám k názvom kapitol 5-7, kde by generické názvy "Design", "Implementation" a "Testing" mali byť nahradené názvami, ktoré lepšie vystihujú skutočný obsah kapitol.

5. Formal aspects of technical report — **90 p. (A)**

Práca je písaná v angličtine, ktorá je, až na drobné chyby, veľmi dobrá a text je bez problémov pochopiteľný. Z formálneho hľadiska je práca taktiež na veľmi vysokej úrovni, s minimom typografických nedostatkov. Jedinú väčšiu výhradu mám k formátovaniu ukážky kódu na strane 37, kde chýba odsadenie, čo činí kód veľmi zle čitateľným.

6. Literature usage — **80 p. (B)**

Práca s literatúrou je na dobrej úrovni. Zdrojmi sú prevažne RFC špecifikácie, prípadne vedecké publikácie, čo považujem vzhľadom na charakter práce za dostatočné. Všetky prevzaté časti textu sú riadne ocitované. Čo mi však v práci chýba, je detailnejšia analýza a popis existujúcich riešení pre odhaľovanie časových postranných kanálov.

7. Implementation results — **95 p. (A)**

Realizačný výstup je najsilnejšou časťou práce. Obzvlášť by som vyzdvihol metodický prístup študenta, keď pred implementáciou samotného rozšírenia do nástroja tlsfuzzer najskôr vytvoril prototypovú aplikáciu, na ktorej porovnal a vyhodnotil rôzne možnosti odhaľovania časových postranných kanálov. Vďaka tomuto kroku je potom vlastné rozšírenie kvalitnejšie. Samotná implementácia a jej testovanie je na vysokej úrovni, čo potvrdzujú aj viaceré kontroly kvality kódu používané v projekte tlsfuzzer.

8. Utilizability of results

Keďže odhaľovanie zraniteľností cez časové postranné kanály je veľmi náročné, práca má jednoznačne veľký potenciál byť využitá v praxi. Tento potenciál tiež zvyšuje fakt, že výstupom je rozšírenie do frameworku tlsfuzzer slúžiaceho na testovanie SSL/TLS implementácií. Bohužiaľ, v práci úplne chýba experimentálne porovnanie predstaveného riešenia s existujúcimi riešeniami odhaľovania časových postranných kanálov a preto nie je možné určiť, či táto práca prináša nejaké zásadné zlepšenie v danej oblasti.

9. Questions for defence

- Vyžadovalo by Vaše riešenie nejaké úpravy, aby bolo možné ho použiť pre detekciu časových postranných kanálov v TLS verzii 1.3? Ak áno, tak aké?
- Ako by v kontexte vašej práce bolo možné použiť fuzz testovanie (ktoré je cieľom frameworku tlsfuzzer)?

10. Total assessment — **85 p. very good (B)**

Prácu navrhujem hodnotiť stupňom **B (veľmi dobre)**. Toto hodnotenie zohľadňuje kvalitu programového riešenia a rovnako aj textovej časti. Celkovo sa jedná o dobre zvládnuté nadpriemerne náročné zadanie.

In Brno 25 June 2020

Malík Viktor, Ing.
reviewer