

## Review of Bachelor's Thesis

**Student:** Hejzman Lukáš  
**Title:** Fingerprinting and Identification of TLS Connections (id 23922)  
**Reviewer:** Kocnová Jitka, Ing., DCSY FIT BUT

- 1. Assignment complexity** **more demanding assignment**  
Zadání hodnotím jako obtížnější, neboť práce vyžadovala nastudovat problematiku šifrovaného provozu na sítích, především pak protokol TLS a fingerprinting, a taktéž existující metody pro identifikaci procesů. Zároveň bylo třeba přijít s novým způsobem efektivní identifikace procesů.
- 2. Completeness of assignment requirements** **assignment fulfilled**  
Zadání bylo splněno ve všech bodech.
- 3. Length of technical report** **in usual extent**  
Rozsah technické zprávy je v rozmezí obvyklém pro bakalářskou práci. Po obsahové stránce je práce informačně bohatá a k řešené problematice jsou uvedeny pouze relevantní a nezbytné informace.
- 4. Presentation level of technical report** **100 p. (A)**  
Práce je vhodně rozdělena na teoretickou, návrhovou a implementační část. Jednotlivé kapitoly na sebe dobře navazují.
- 5. Formal aspects of technical report** **80 p. (B)**  
Práce je psaná v angličtině. Úroveň angličtiny je dobrá, v textu se občasné vyskytují chyby, nevhodně zvolená slova a překlepy.  
Z typografického hlediska práce obsahuje jen drobné množství nedostatků.
- 6. Literature usage** **90 p. (A)**  
Práce s literaturou je dle citačních zvyklostí a prameny jsou voleny vhodně s ohledem na téma práce.
- 7. Implementation results** **90 p. (A)**  
Realizační výstup práce je funkční a byl validován na reálných datech. Byl vytvořen nový přístup k identifikaci klientů a procesů využívajících komunikaci pomocí TLS protokolu. Tento přístup byl úspěšně otestován jako modul pro NEMEA framework.
- 8. Utilizability of results**  
Metoda byla testována na reálných datech a je plně využitelná pro další práci. Výsledky získané během práce byly publikovány na Excel@FIT a student plánuje zaslat i článek na mezinárodní konferenci.
- 9. Questions for defence**
  - Plánujete práci dále rozšiřovat? Pokud ano, jak?
- 10. Total assessment** **90 p. excellent (A)**  
Výsledkem práce je funkční modul pro framework NEMEA, který úspěšně identifikuje klienty a procesy komunikující na síti pomocí TLS protokolu. Výsledky byly publikovány na Excel@FIT. Vzhledem k dobrému zpracování obtížnějšího zadání navrhuji hodnotit stupněm **A**.

In Brno 27 May 2021

Kocnová Jitka, Ing.  
reviewer