Posudek oponenta bakalářské práce

Student: Mikula Ondřej
Téma: Obnova sdílených klíčů protokolu Wireless M-Bus (id 24440)
Oponent: Matoušek Petr, doc. Ing., Ph.D., M.A., UIFS FIT VUT

1. **Náročnost zadání** — **průměrně obtížné zadání**
   Cílem práce bylo implementovat modul do nástroje Hashcat pro obnovu hesel protokolu WM-Bus.
2. **Splnění požadavků zadání** — **zadání téměř splněno s drobnými výhradami**
   V práci chybí ověření výsledku například na různých scénářích, např. slovníku hesel o různé délce klíče, vypočítání náročnosti ověření klíče pro různé kombinace znaků a délky klíče, či diskuze o využití vytvořeného implementovaného modulu v praxi.
3. **Rozsah technické zprávy** — **téměř splňuje minimální požadavky**
   .
4. **Prezentační úroveň předložené práce** — **60 b. (D)**
   Logická struktura technické zprávy je v pořádku, některé kapitoly nejsou dotažené. V kapitole 2 chybí popis vlastního protokolu WM Bus s vysvětlením polí, které obsahuje. V kapitole 5 (implementace) by bylo vhodné ukázat schéma vytvořeného nástroje a způsob začlenění do Hashcatu. Ověření implementace a testování není vhodně navrženo, např. měření rychlosti generování hesel v tab. 6.2 a 6.3 neříká nic jiného, než že rychlost generování hesel v čase je konstatní, v tabulce 6.4. a grafech 6.1 až 6.4 vidíme, že výsledky lámání hesla na GPU jsou lepší než na CPU a při nastavení vyššího parametru výkonu W, což není nic překvapivého. Očekával bych spíše návrh různých scénářů použití a měření času pro nalezení hesla z určité sady možných hesel (slovníku) o zadané délce, struktuře znaků apod.
   V dokumentaci chybí popis instalace a specifikace systému, na kterém vytvořená aplikace běží.
5. **Formální úprava technické zprávy** — **70 b. (C)**
   Typografická a jazyková stránka technické zprávy je na přijatelné úrovni. Text je psán bez velkých pravopisných chyb a překlepů, autor však používá nadbytečně čárky ve větě, což snižuje srozumitelnost textu. Není jasné, proč podkapitoly na třetí úrovni nepoužívají desetinné číslování. V textu jsou některé stránky poloprázdné (např. str. 22 či 33), některá slova jsou špatně přeložená ("digest" jako "ochutnávka") či nesprávně vytvořená, např. "soukromnost", "limitace". Pro zvýraznění myšlenek v textu není zvykem používat tučné písmo, obvykle se doporučuje kurzíva.
6. **Práce s literaturou** — **80 b. (B)**
   Student využíval velké množství zdrojů, které dobře cituje. Pro popis standardu WM Bus není vhodné odkazovat se na Wikipedii ale přímo na daný standard. U zdroje [19] je špatně autor "Česko".
7. **Realizační výstup** — **60 b. (D)**
   Realizační výstup zahrnuje skripty pro generování hesel, což je triviální implementace v jazycích C a Python. Hlavním přínosem je modul pro WM Bus do nástroje Hashcat. Zde chybí u zdrojových textů název autora, takže není snadné odlišit již vytvořené zdrojové soubory od autorova díla. Zdrojové texty nejsou komentované a je těžké se v nich orientovat. Kód je přeložitelný a spustitelný, student demonstroval funkčnost aplikace.
8. **Využitelnost výsledků**
   .
9. **Otázky k obhajobě**
   -
10. **Souhrnné hodnocení** — **65 b. uspokojivě (D)**
    Student splnil zadání projektu. Výsledky nejsou ověřené na vybraných scénářích a chybí také popis využití, což je u takové práce škoda.

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

V Brně dne: 1. června 2022

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