Posudek oponenta bakalářské práce

Student: Večeřa Vojtěch
Téma: Obnova hesel archivů ZIP s využitím GPU (id 18211)
Oponent: Veselý Vladimír, Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** — **průměrně obtížné zadání**
   Zadání navazuje na nástroj vyvinutý v rámci ukončeného grantu Sec6net (Moderní prostředky pro boj s kyberkriminalitou Internetu nové generace - řešitel dr. Matoušek) a rozšiřuje jeho činnost o lámání hesel archivů ZIP a 7z.
2. **Splnění požadavků zadání** — **zadání splněno**
   Všechny body zadání byly splněny.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
   Práce má i s pomocnými provozy dohromady 36 stránek v husté LaTeXové šablonce. Je tedy v obvyklém rozsahu.
4. **Prezentační úroveň předložené práce** — **80 b. (B)**
   Technická zpráva je logicky členěna a autor postupně přibližuje řešenou problematiku. Avšak kapitoly 6 a 7 obsahující návrh a popis implementace by si zasloužily možná trochu více detailů.
5. **Formální úprava technické zprávy** — **70 b. (C)**
   Po typografické stránce je práce v pořádku. Po stránce jazykové se v práci vyskytují kostrbatě vysvětlované pasáže či nadužívání jednoho slova ve více po sobě jdoucích větách. Vložené médium obsahuje, co je slíbeno v příloze práce.
6. **Práce s literaturou** — **80 b. (B)**
   Student v práci cituje z relevantních zdrojů. Některé reference na objekty však v textu nejsou dále rozvedeny (např. Tabulka 8.3) a jejich obsah bez komentáře zhoršuje pochopitelnost. Hodilo by se studium a použití dalších souvisejících publikací na téma kryptografického zabezpečení a obnovy hesel dokumentů.
7. **Realizační výstup** — **90 b. (A)**
   Realizační výstup v C/C++ je funkční. Zdrojové texty jsou komentované. V implementační části mi přišlo, že:

   * se student málo zakousnul do problémů, které při testování vyvstaly;
   * neimplementoval všechny možné kryptografické kombinace, které formáty podporují.

   Studentův příspěvek se dá vyjádřit kvantitativně na stovky řádků kódu, některé z nich ovšem korektně převzaté z implementace programu 7-zip.
8. **Využitelnost výsledků**
   Práce rozšiřuje možnosti nástroje vyvíjeného zde na fakultě, který byl již úspěšně prezentovaného v několika publikacích. Dá se očekávat, že studentův přínos bude hladce integrován do nové verze nástroje.
9. **Otázky k obhajobě**
   1. Zhodnoťte složitost obnovy hesla pro formát RAR. V čem by bylo Wrathion nutné rozšířit, aby tento formát podporoval?
10. **Souhrnné hodnocení** — **80 b. velmi dobře (B)**
    Práci hodnotím na pomezí dobře (C) a velmi dobře (B) s tím, že nechávám na komisi finální verdikt. Práce je každopádně poctivé a kvalitní dílo hodné úspěšného bakaláře naši fakulty.

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

V Brně dne: 31. května 2016

.....
podpis