Posudek oponenta diplomové práce

Student: Mráz Patrik, Bc.
Téma: Analýza technologií pro distribuci výpočtu při lámání hesel (id 21860)
Oponent: Veselý Vladimír, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Body zadání jsou komplementem k dosavadnímu snažení na projektu TARZAN (dr. Matoušek), v rámci kterého se vyvíjí obdobné řešení (software FITcrack), jenž místo MPI využívá jako podvozek framework BOINC.

2. Splnění požadavků zadání **zadání splněno**

Všechny body zadání byly splněny.

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

Práce má 53 stran textu a i s pomocnými provozy v podobě příloh pak dohromady 71 stránek v husté LaTeXové šablonce. Je tedy v požadovaném rozmezí. Ovšem některé obrázky (např. 2.2, 3.1, 4.2 či 4.3) jsou dle mě zbytečně velké nebo působí jako doprovodné dekorace (než že by sdělovaly něco zásadního).

4. Prezentační úroveň předložené práce **81 b. (B)**

Práce je logicky členěna do kapitol, které postupně odrážejí dílčí části jednotlivých bodů zadání práce. Kapitoly na sebe přirozeně navazují a dobře vedou čtenáře celou problematikou zpracovávanou prací.

5. Formální úprava technické zprávy **86 b. (B)**

Práce je psána ve slovenštině, jazykově se čte velmi dobře, avšak gramatickou stránku věci nejsem sto schopen správně posoudit (snad až několik očividně zapomenutýc interpunkčních znamének). Co se týče typografie, anotování obrázků a diagramů, tak se zdá býti bez prohřešků.

6. Práce s literaturou **70 b. (C)**

Student v práci cituje z relevantních zdrojů. Nicméně:

- některým z nich (online stránky [1]-[5]) by spíš slušela forma poznámky pod čarou než plnohodnotné citace;
- u [6] není jasné, o jaký typ citace se jedná;
- [9] a [19] určitě nejsou originální specifikace (spíš bych sázel na dokumenty od NIST než RFC).

Mnohdy se jedná i o literárně nepříliš stravitelná RFC, jejichž pochopení studentem je v práci patrné. Kromě standardních citací obsahuje práce i celou řadu souvisejících poznámek pod čarou.

7. Realizační výstup **84 b. (B)**

Primárním výstupem jsou zdrojové kódy v jazyce Python, které představují implementovaný server (rozdělující práci) a klient (wrapper pro spouštění hashcat a reportovač práce), jež si spolu povídají pomocí MPI. Zdrojové kódy jsou účelně komentované a výstupy byly úspěšně demonstrovány (a korektnost činnosti ověřena) i nad oponentovými daty (vlastní hashe a formáty k zlomení).

8. Využitelnost výsledků

Dá se očekávat, že výsledky práce budou ku prospěchu dalšímu rozvoji problematiky lámání hesel v rámci projektu TARZAN, ale i mimo něj.

9. Otázky k obhajobě

- Diskutujte funkcionalitu Vašeho řešení v kontextu slovníkového útoku. Uvažujte přitom různé velikosti slovníku - 100 MB, 1 GB, 10 GB, 100 GB. Naznačte případná řešení.

10. Souhrnné hodnocení **81 b. velmi dobře (B)**

Celkovou práci hodnotím jako velmi dobrou (tedy stupněm B). Kromě hezkého textu oceňuji zejména bezproblémové implementaci, která jasně ukazuje, že není nutné použít těžkopádná řešení jako BOINC k distribuci úlohy lámání hesel.

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

V Brně dne: 6. června 2019

Veselý Vladimír, Ing., Ph.D.
oponent