Posudek oponenta diplomové práce

Student: Kos Ondřej, Bc.
Téma: Obnova hesel v distribuovaném prostředí (id 18213)
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 distribuce úlohy lámání na více paralelně běžících strojích.

2. Splnění požadavků zadání **zadání splněno**

Zadání bylo ve všech bodech splněno.

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

Práce má i s pomocnými provozy 52 stránek v husté LaTeXové šablonce, je tedy v obvyklém rozsahu.

4. Prezentační úroveň předložené práce **70 b. (C)**

Práce je logicky členěna do kapitol, které postupně odrážejí body plnění zadání. Tabulka 2.3 i vzhledem k hodnotám v ní obsaženým má spíše dekorativní charakter. V sekci implementace oceňuji komentované použití pseudokódu, které zpřehledňuje vstupy OpenMPI do původního kódu. Kapitola o experimentech podává výsledky vágnější formou - testovat se dalo detailněji (např. výkonnost pro různé podporované formáty).

5. Formální úprava technické zprávy **60 b. (D)**

Práce je psána česky, nicméně na této části je patrné mírné odbytí. Text obsahuje již znatelné množství překlepů a interpunkčních chyb. Stylisticky autor opakuje slova a především nadužívá dlouhá souvětí (mnohdy několik řádků, viz např. str. 35 či 40), ve kterých se ztrácí původní zamýšlené sdělení. Po typografické stránce použitá šablona špatně zalamuje české slabiky a na některých místech slova přetékají okraje textu (viz např. str. 28). Vložené médium obsahuje, co je slíbeno v příloze práce. Anglický abstrakt obsahuje periodicky opakující se prohřešek proti pravidlu SVOMPT.

6. Práce s literaturou **75 b. (C)**

Student v práci cituje z relevantních zdrojů (místy i vědeckých publikací), jejichž pochopení je v práci patrné.

7. Realizační výstup **80 b. (B)**

Realizační výstup v C/C++ s OpenMPI je funkční. Zdrojové texty jsou přehledné a místy komentované. Studentův příspěvek se dá vyjádřit kvantitativně na desítky řádků nového kódu.

8. Využitelnost výsledků

Téma i řešení jsou aktuální (většina komerčního SW je limitováno tím, že je single-user single-machine), a tak úspěšná paralelizace má vysokou přidanou hodnotu. Nicméně aktuálnímu výsledku ubírá nemožnost spouštět distribuované lámání za použití GPU, kde ta samá úloha jen na CPU nemůže být víc než jen proof-of-concept.

9. Otázky k obhajobě

1. V práci uvádíte (str. 36), že distribuovaná varianta Wrathionu dosahuje rychlosti 35 000 hesel/s. K lámání jakého formátu se toto číslo vztahuje? Prováděl jste měření i pro jiné formáty?
2. Popište metodiku měření zátěže síťového provozu. Jaká data jsou v tomto provozu majoritně obsažena?
3. Tvrdíte (str.40), že GPU variantu se nepodařilo zprovoznit, protože je limit na přenos zkompilovaných kernelů (obvykle o velikosti < 5MB) z hlavního uzlu na zbývající. Vzhledem k faktu, že každý uzel může mít potenciálně jiné prostředí (různá GPU), tak by bylo vhodnější specifické kernely kompilovat až na cílových uzlech. Co Vám bránilo upravit takto Wrathion a vyhnout se problému, na který jste narazil?

10. Souhrnné hodnocení **70 b. dobře (C)**

Práci je dle mě na pomezí dobře (C) a uspokojivě (D), s tím, že nechávám na komisi finální verdikt i s přihlédnutím k odpovědím diplomanta. Praktický výstup diplomové práce hodnotím velice kladně, nicméně mu ubírá na síle funkční řešení distribuce úlohy i pro GPU. Textové části škodí zbytečné formální nedostatky.

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

V Brně dne: 3. června 2016

.....
podpis