Posudek oponenta diplomové práce

Student: Večeřa Vojtěch, Bc.
Téma: Strategie distribuovaného lámání hesel (id 21556)
Oponent: Pluskal Jan, Ing., UIFS FIT VUT

1. Náročnost zadání **značně obtížné zadání**

Cílem práce bylo nastudovat způsoby distribuovaného lámání hesel a optimalizovat nástroj FITcrack na základě zjištění při měření výkonnosti různých typů grafických karet, doporučení a strategií. Zadání považuji za velmi obtížné, protože systém FITcrack je vyvíjen týmem výzkumníků a nalézt v něm výkonnostní problémy by mělo být obtížným úkolem.

2. Splnění požadavků zadání **zadání splněno s podstatným rozšířením**

Student splnil všechny body zadání a navíc provedl velmi detailní měření šesti typů grafických karet, což považuji za podstatné rozšíření práce.

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

Práce je v obvyklém rozsahu cca 65 normostran, doplněna o 14 stran detailního měření v přílohách.

4. Prezentační úroveň předložené práce **90 b. (A)**

Práce je členěna do logických celků, které reflektují jednotlivé body zadání. Kapitoly na sebe navazují a text práce je pro čtenáře čitelný.

5. Formální úprava technické zprávy **90 b. (A)**

Práce je psaná v anglickém jazyce. Objevuje se nepatrné množství gramatických chyb a stylistických chyb, jako např. nedodržení větné skladby. Možnost šíření informací uvedených v této práci díky použitému jazyku však převažuje drobné nedostatky.

6. Práce s literaturou **90 b. (A)**

Student používá kvalitní literární zdroje, které korektně cituje. Technické detaily a zejména doporučení lámacích strategií je podloženo relevantními online zdroji.

7. Realizační výstup **100 b. (A)**

Programový výstup je verzován systémem git, tedy je dohledatelný přínos autora na zdrojovém kódu, který považuji za značný. Kód vytvořený studentem je čitelný, dobře strukturovaný a přehledný. Vše se zdá býti použito v souladu s licenčními podmínkami použitých knihoven třetích stran.

8. Využitelnost výsledků

Práce přináší porovnaní výkonnosti při obnově hesel nástrojem Hashcat na state-of-the-art grafických kartách. Výsledky práce rozšiřují nástroj FITcrack o poznatky získané z výkonnostního měření a analýzy nástroje. Výstup vytváří podklady pro slibnou vědeckou publikaci, jejíž základ byl již publikovaný na konferenci Excel@FIT. Student dále participoval na konferenčním článku SPI a podílel se na třech technických zprávách.

9. Otázky k obhajobě

1. Jaká je škálovatelnost Vašeho řešení?
2. Jaká je cílená infrastruktura pro kterou si představujete hypotetické použití?
3. Jaké jsou/existují limitující faktory, které by bránily nasazení nástroje FITcrack na veřejném cloudu? Uvažujte neomezený rozpočet na provoz.

10. Souhrnné hodnocení **95 b. výborně (A)**

Student se úspěšně vypořádal s náročným zadáním optimalizace nástroje pro distribuovanou obnovu hesel. Výkonnostní měření nástrojů Hashcat a FITcrack, které student provedl, považuji za vynikající a převyšující požadavky zadání. Student dále nejen optimalizoval nástroj FITcrack, ale opravil i nalezené chyby. Všechny body zadání jsou splněny. Navrhuji hodnotit práci jako výbornou - A.

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

V Brně dne: 4. června 2019

Pluskal Jan, Ing.
oponent