Posudek oponenta bakalářské práce

Student: Sedlo Ondřej
Téma: Útok na šifrované diskové oddíly s využitím GPU (id 19362)
Oponent: Holkovič Martin, Ing., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Súčasťou práce bolo naštudovanie nástroja Fitcrack vyvíjaného v rámci výzkumnej skupiny NES@FIT, ktorý slúži pre obnovu hesiel. Tento nástroj študent rozšíril o podporu obnovu hesiel zo zašifrovaných diskových oddielov nástrojom TrueCrypt. K vytvoreniu nástroja musel študent naštudovať viacero hashovacích a šifrovacích algoritmov a implementovať ich pre CPU aj GPU.

2. Splnění požadavků zadání **zadání splněno s vážnými výhradami**

Študent vytvoril nástroj, ktorého funkcionalita mi bola predvedená. Vzhľadom k časovej náročnosti jednotlivých testov nebolo možné predviesť všetky podporované algoritmy. Výhrady mám k testovaniu vytvoreného nástroja. Niektoré testy v práci chýbajú (napríklad test východzieho nastavenia programu TrueCrypt), niektoré sú zle postavné (porovnávanie hashovacích algoritmov) a niektoré sú vyslovene nesprávne (porovnanie šifrovaích algoritmov).

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

4. Prezentační úroveň předložené práce **55 b. (E)**

Niektoré sekcie by bolo vhodné prehodiť pretože v aktuálnej podobe sa niektoré pojmy vysvetlujú až po ich použití. Kapitoly 5 a 6 majú veľmi krátky rozsah, pričom v nich chýba popis niektorých dôležitých častí z vyvíjaného nástroja.

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

Pochopiteľnosť textu často zhoršovalo umiestnenie výpočtov priamo v texte, chýbajúce zvýraznenie premenných z výpočtov v texte (napríklad šikmým písmom). Taktiež zobrazené kódy by mali byť vhodne oddelené od textu a označené popisom.

6. Práce s literaturou **75 b. (C)**

Prácu s literatúrou zvládol študent dobre. Práca obsahuje nadpriemerný počet dobre zvolených zdrojov.

7. Realizační výstup **50 b. (E)**

Základná varianta nástroja funguje podľa očakávania. Všetky možnosti nástroja nebolo možné z časových dôvodov pri predvedení študentom otestovať. Výsledky testov zamerané na porovnanie všetkých možností nástroja umiestnené v textovej správe sú bohužiaľ nesprávne - všetky algoritmy (a dokonca aj ich kombinácie) vraj majú rovnakú náročnosť. Preto je kompletnú fukčnosť nástroja ťažké zhodnotiť.

8. Využitelnost výsledků

Práca spočívala v implementácií dobre známych hashovacích a šifrovacích algoritmov, použitých podľa špecifikácie TrueCrypt. Po odstranení pochybností s výkonnosťou jednotlivých algoritmov je možné nástroj priamo integrovať do nástroja Fitcrack.

9. Otázky k obhajobě

1. V texte je uvedené, že algoritmus SHA-512 je z dôvodu nevyrovnaných prejavov akcelerácie najrýchlejšie vypočítateľný z použitých algoritmov. Môžete pojem "nevyrovnané prejavy akcelerácie" a celé toto tvrdenie objasniť?
2. Podľa výsledkov z testovania trvá overenie jedného hesla algoritmom AES asi 1.62ms, algoritmom Twofish rovnako asi 1.62ms. Avšak zároveň overenie jedného hesla algoritmom AES a následne Twofish (t.j. použitie oboch sériovo) trvá znovu 1.62ms. Ako je možné, že pridávanie ďalších algoritmov nespomaľuje overenie jedného hesla?

10. Souhrnné hodnocení **59 b. dostatečně (E)**

Textová správa je z dôvodu typografických chýb a občasného zlého poradia podkapitol v texte miestami zle pochopiteľná. Kapitoly číslo 5 a 6 sú veĺmi krátke a chýba v nich popis niektorých dôležitých prvkov vyvíjaného nástroja. Kapitola popisujúca testovanie má veľké nedostatky a namiesto potvrdenia správnosti vytvoreného nástroja len priniesla nové otázky. Celkovo práca nepôsobí dobrým dojmom a preto navrhujem hodnotenie 59 bodov (E).

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

V Brně dne: 2. června 2017

.....
podpis