Doc. Ing. Ladislav Hudec, CSc., Ústav počítačového inžinierstva a aplikovanej informatiky,
Fakulta informatiky a informačných technológií STU, Mlynská dolina, SK-842 16 Bratislava

---

Oponentský posudok dizertačnej práce

Dizertant: Ing. Radek Hranický, Fakulta informačních technologií, Vysoké učení technické v Brně
Názov práce: Digitální forenzní analýza: zrychlení lámání hesel (Digital forensics: the acceleration of password cracking)

Bezpečnostné mechanizmy na zaistenie dôvernosti a integrity digitálnych údajov často využívajú kryptografické nástroje, do ktorých ako vstupné parametre vstupujú heslá. Či už ide o zaistenie dôvernosti prostredníctvom šifrovania alebo integrity prostredníctvom šifrovania alebo hešovania. Takýmto spôsobom sa zabezpečujú rôzne objekty (napr. zariadenia, systémy, dokumenty). Ak pri forenznej analýze potrebuje vyšetrovateľ preskúmať objekt chránený heslom, potrebuje toto heslo získať od vlastníka objektu. Ak vlastník objektu heslo nie je schopný heslo vyšetrovateľovi poskytnúť, pre potreby forenznej analýzy je nevyhnutné heslo prelomiť. Dizertácia sa zaoberá urýchľovaním procesu lámania hesiel. Téma dizertácie je vysoko aktuálna a spadá do odboru Výpočtová technika a informatika.

Predložená dizertačná práca je nadštandardne veľkého rozsahu. Obsahuje 6 kapitol vrátane zoznamu literatúry, dve prílohy a 221 citovaných zdrojov. Celkovo má 202 strán.

Strategickým cieľom dizertačnej práce je urýchlenie lámania hesiel. Dizertant navrhol a implementoval nástroj Fitcrack, ktorý pracuje v hybridnom distribuovanom prostredí a využíva BOINC framework. Uzly distribuovaného prostredia sa skladajú od štandardných výpočtových prostriedkov až po špecializované výkonné prostriedky GPGPU (General-Purpose computing on Graphics Processing Unit). Jednotlivé uzly nástroja Fitcrack využívajú „lámací stroj“ hashcat.

Prvým pôvodným prínosom dizertanta je návrh 6 algoritmov (v dizertácii referencované ako Algoritmus 1 až Algoritmus 6) pre implementáciu nástroja Fitcrack. Rozloženie výpočtovej záťaže na jednotlivé uzly distribuovaného systému môže využívať viacero schém. Fitcrack používa dynamickú distribúciu blokov kandidátskych hesiel s progresívnym priradením kľúčového priestoru. Systém na to využíva adaptívny plánovací algoritmus na vytvorenie presne prispôsobených spracovateľských jednotiek, ktoré odpovedajú aktuálnemu výkonu každého hostiteľa. Experimenty ukázali, že mechanizmus umožňuje výpočtovým uzlom efektívne spracovávať úlohy a zvládať neočakávané udalosti, ako je napríklad náhla zmena výkonu uzla. Navrhnuté stratégie distribúcie pre rôzne spôsoby tvorby kandidátskych hesiel fungujú podľa plánu a umožňujú systému presne riadiť distribúciu kľúčového priestoru (kandidátskych hesiel) medzi výpočtové uzly. Boli však zistené isté rozdiely, ktoré vyplývajú zo špecifických vlastností jednotlivých spôsobov tvorby kandidátskych hesiel. Výkonnosť nástroja Fitcrack bola porovnaná s výkonnosťou nástroja Hashtopolis pre hešovacie algoritmy SHA-1, BCrypt a slovníky rockyou.txt a adobe100.txt.

Druhým pôvodným prínosom dizertanta v oblasti urýchlenia lámania hesiel je návrh spôsobu redukcie počtu kandidátskych hesiel. Vychádza z práce Weira, ktorý na tvorba kandidátskych

hesiel využil schému pravdepodobnostnej bezkontextovej gramatiky PCFG (Probabilistic Content-Free Grammar). Táto schéma je založená na znalostiach získaných automatizovanou analýzou existujúcich hesiel. Prepisovacie pravidlá gramatiky slúžia priamo na generovanie kandidátskych hesiel. Napriek mnohým vylepšeniam tejto schémy, aktuálne riešenia boli ťažko použiteľné na skutočné lámanie hesiel z dôvodu nízkej výkonnosti a chýbajúceho riešenia pre lámanie hesiel v paralelnom alebo distribuované prostredí. Na základe analýzy dizertant navrhol viacero vylepšení, ktoré sú vyjadrené aj tromi návrhmi algoritmov (v dizertácii referencované ako Algoritmus 9 až Algoritmus 11). Modifikácia existujúcej metódy Weira umožnila paralelné spracovanie a efektívne využitie všetkých dostupných procesorových jadier. Ďalším zaujímavým výstupom sú metódy, ktoré umožňujú distribuované lámanie hesiel vytvorených na báze PCFG. Riešenie využíva distribúciu preterminálnych štruktúr a umožňuje priame spustenie lámania hesla pomocou nástroja hashcat alebo iných nástrojov. Navrhnuté postupy boli overené. Experimenty ukázali, že navrhované vylepšenia priniesli výrazné urýchlenie procesu lámania hesiel.

V súvislosti s riešenou témou dizertant publikoval v rokoch 2016 až 2020 celkom 6 prác. Dve práce boli publikované v zahraničných časopisoch, tri príspevky na zahraničných konferenciách, jeden príspevok na domácej medzinárodnej konferencii a dizertant je spoluautorom jednej technickej správy vypracovanej pre pracovisko. V týchto prácach bola pojednávaná otázka návrhu nástroja Fitcrack, ktorý bol implementovaný ako distribuovaný systém na lámanie hesiel využívajúci framework BOINC a nástroj na lámanie hesiel hashcat. Tiež bolo opísané vylepšenie algoritmu prípravy kandidátskych hesiel metódou PCFG.

Na základe predloženej dizertačnej práce ako aj celkovej publikačnej činnosti dizertanta možno konštatovať, že dizertant je pracovník s vedeckou erudíciou. Predložená dizertačná práca dokumentuje nielen schopnosť dizertanta, že ovláda vedecké metódy práce a priniesol nové vedecké poznatky, ale aj schopnosť vykonávať vysoko odbornú inžiniersku a vývojovú prácu.

Otázky na dizertanta:

1. Bolo by možné zovšeobecniť spôsoby tvorby kandidátskych hesiel a takýto všeobecný spôsob implementovať v nástroji Fitcrack? Čo bráni v zovšeobecnení spôsobov tvorby kandidátskych hesiel?
2. Uvažoval dizertant so špecializáciou výpočtových uzlov v distribuovanom systéme na jednotlivé typy hešovacích funkcií? Mohla by takáto špecializácia priniesť zvýšenie výkonnosti, resp. ďalšie urýchlenie lámania hesiel?
3. Mohol by dizertant uviesť aktuálny stav v publikačnej činnosti týkajúci sa výstupov dizertácie?

Celkové hodnotenie dizertačnej práce.
Dizertačnú prácu Ing. Radka Hranického považujem za prínosnú pre aktuálnu problematiku urýchlenia lámania hesiel a konštatujem, že práca zodpovedá všeobecne uznávaným požiadavkám pre udelenie akademického titulu.

V Bratislave, dňa 4.10.2021 podpis oponenta