Lámání hesel pomocí algoritmu PRINCE v systému Fitcrack

Dávid Bolvanský, Školiteľ: Ing. Radek Hranický

Fakulta informačních technologií VUT v Brně

Motivácia

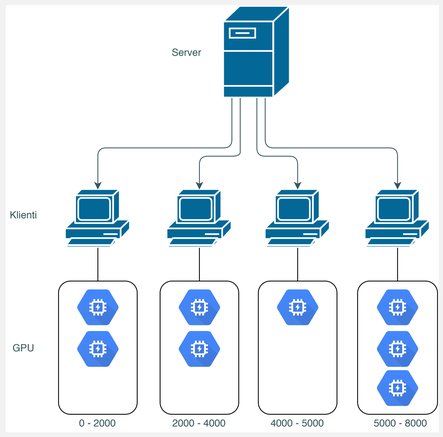
Algoritmus PRINCE je pokročilejšou formou kombinačného útoku. Algoritmus je všeobecne veľmi rýchly a výrazný rozdiel sa prejavuje najmä pri pomalých hešovacích algoritmoch a pri viacslovných kandidátnych heslách.
Nedistribuované lámanie hesiel v praxi naráža na svoje limity a jeho použiteľnosť na reálne úlohy sa znižuje kvôli stúpajúcim nárokom na výpočtové zdroje zariadenia.

Cieľ práce

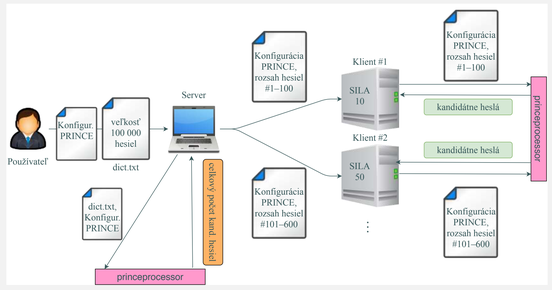
Cieľom práce je navrhnúť distribuovanú verziu útoku pomocou algoritmu PRINCE ako rozšírenie systému Fitcrack, ktorý slúži na distribuované lámanie hesiel.

Návrh distribúcie úlohy

Distribuovanosť úlohy s útokom PRINCE je založená na možnostiach nástroja **princeprocessor**. Každému klientovi sa priradí rozsah hesiel, ktoré bude spracovávať.



Distribúcia útoku v systéme Fitcrack



Experimenty

- Experimenty s konfiguračnými možnosťami PRINCE
- Experimenty skúmajúce škaľovatelnosť útoku
- Porovnanie PRINCE s inými typmi útokov
- Porovnanie implementácií útoku PRINCE v systéme Fitcrack a Hashtopolis

HW použitý na experimenty

Operačný systém	Windows 7
CPU	Intel Core i5-3570K, 3,4 GHz
GPU	Nvidia GTX 1050 Ti
RAM	DDR3, 8 GB

Tabuľka: Hardvérová konfigurácia počítačov použitých na experimenty.

Operačný systém	Ubuntu 18.04.4 LTS
CPU	AMD Ryzen 5 2600X, 3,6 GHz
GPU	Nvidia RTX 2080, GTX 1050 Ti
RAM	DDR4, 16 GB

Tabuľka: Hardvérová konfigurácia servera použitého na experimenty.

Konfiguračné možnosti PRINCE

maximálna dĺžka hesiel	doba výpočtu s 1 klientom	doba výpočtu s 10 klientami
8	4 minúty	1 minúta
10	3 hodiny	37 minút
12	85 hodín	9 hodín

Tabuľka: Vplyv zmeny maximálnej dĺžky hesiel na dobu výpočtu úlohy s jedným a s desiatimi klientami.

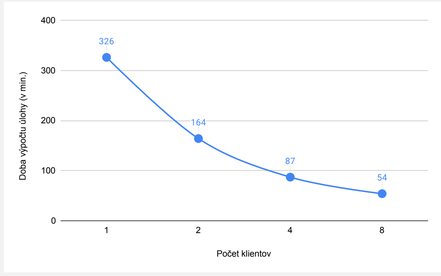
max. počet prvkov v reťazci	doba výpočtu s 1 klientom	doba výpočtu s 10 klientami
4	12 hodín	1 hodina
5	73 hodín	7 hodín

Tabuľka: Vplyv zmeny maximálneho počtu prvkov v reťazci na dobu výpočtu úlohy.

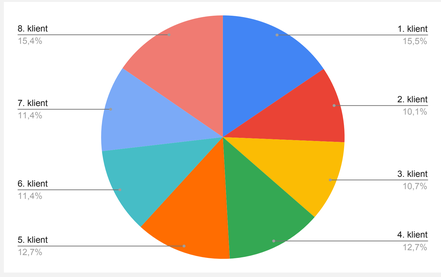
kontrola duplicít	doba výpočtu s 10 klientami
povolená	9 hodín
zakázaná	28 hodín

Tabuľka: Výsledky experimentu s povolenou / zakázanou kontrolou duplicitných hesiel so slovníkom s duplicitami.

Škáľovateľnosť útoku



Graf: Doba výpočtu úlohy pri rôznom počte klientov.



Graf: Distribúcia úlohy s útokom PRINCE medzi 8 klientov.

Porovnanie útoku s inými typmi útokov

Pomalý hešovací algoritmus bcrypt:

metrika výpočtu	PRINCE	kombinačný	slovníkový
efektivita	99 %	99 %	99 %
doba	9 hodín	20 hodín	13 hodín

Tabuľka: Porovnanie útokov pri 1 klientovi.

metrika výpočtu	PRINCE	kombinačný	slovníkový
efektivita	93 %	98 %	94 %
doba	5 hodín	11 hodín	5 hodín

Tabuľka: Porovnanie útokov pri 2 klientoch.

metrika výpočtu	PRINCE	kombinačný	slovníkový
efektivita	90 %	91 %	91 %
doba	2 hodiny	4 hodiny	2 hodiny

Tabuľka: Porovnanie útokov pri 4 klientoch.

PRINCE: Fitcrack vs. Hashtopolis

Rýchly hešovací algoritmus SHA-1:

metrika výpočtu	Fitcrack	Hashtopolis
efektivita	97 %	N/A
doba	8 hodín, 47 minút	8 hodín, 53 minút

Tabuľka: Porovnanie útoku v systéme Fitcrack a Hashtopolis - 10 klientov.

Výstup práce a využitie v praxi

Výstupom práce je nový distribuovaný útok založený na algoritme PRINCE. Výsledky experimentov ukazujú, že implementované riešenie je efektívne. Na sade experimentov bol skúmaný vplyv rôznych konfiguračných možností na celkové množstvo kandidátnych hesiel. Útok bol taktiež porovnaný so slovníkovým a kombinačným útokom. Výsledky lámania pomalých heší ukázali, že útok PRINCE bol najrýchlejší z tejto trojice útokov.