Excel@FIT 2017

OBNOVA HESEL NA ZÁKLADĚ PRAVIDEL

Motivace

- Hesla tvoří jednu z nejdůležitějších a nejpoužívanějších prostředků k ochraně dat.
- Zapomenuté nebo ztracené heslo trápí nejen běžné uživatele, ale i vyšetřovatele během vyšetřování trestných činů.
- K obnově hesla můžeme použít mnoho různých metodik, avšak problém současných řešení je časová náročnost.

I FORGET MY PASSWORD

Existující řešení

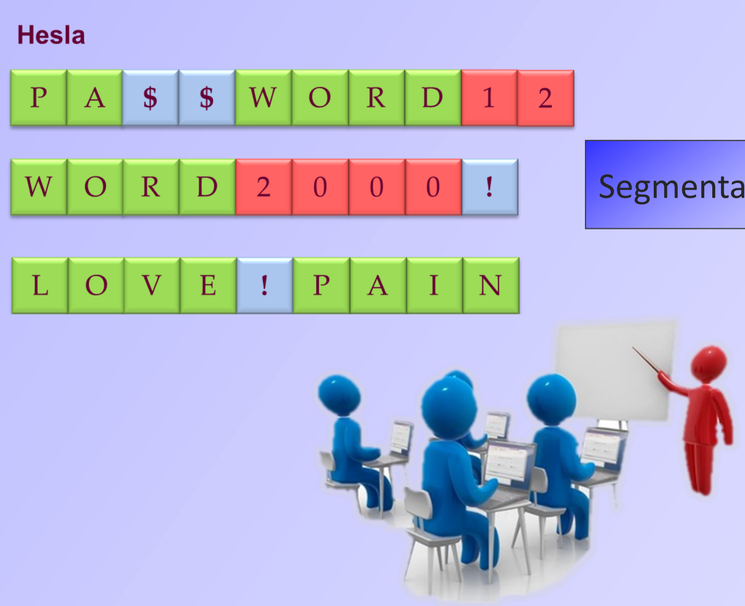
- Obnova pomocí **brute-force** metody je jednoduchá, ale velmi časově náročná.
- **Slovníkový útok**, při které se používají předgenerovaná nebo získaná hesla, exceluje při prolamování jednoduchých a často používaných hesel. Avšak je velmi omezena velikostí použitého slovníku.
- Chytré metody jako **Markovovy řetězce** a **Klávesové vzory** tvoří rozumný kompromis mezi omezeností slovníkového útoku a časovou náročností brute-force metody

Naše řešení

- Patří mezi chytré metody
- Postup se dělí se na dvě fáze — učení a generování hesel.
- Metoda vyžaduje trénovací množinu hesel.
- Pravděpodobnější hesla jsou vygenerována dříve.

Fáze učení

- Nejdůležitější fáze.
- Rozhoduje o výsledné síle generátoru hesel.
- Rozložení každého hesla na fragmenty.
- Fragmenty se dělí na číselné, písmenné a fragmenty speciálních znaků.
- Vytvoření šablony hesel — přepsání hesel na zástupné znaky (písmena — L, číslice — D, speciální znaky — S)
- Setřídění fragmentů a šablon podle počtu výskytů.



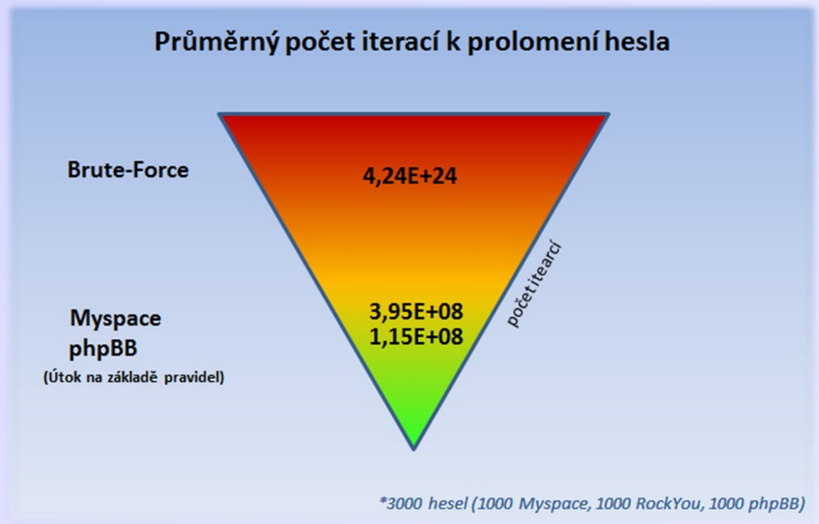
Generování

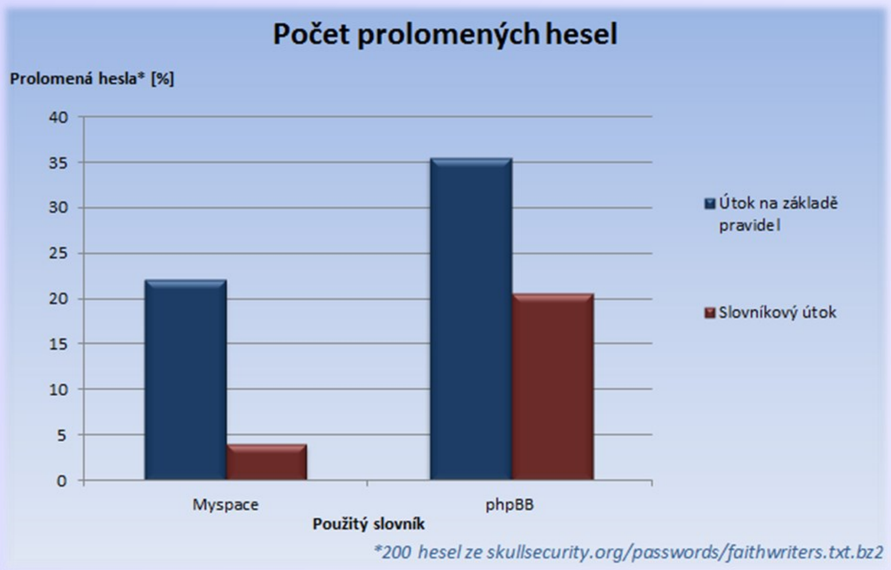
- Dosazování fragmentů do získaných šablon podle pravděpodobnosti.
- Vytváření permutací fragmentů původních hesel.

Výsledky

- Překvapivě dobré!

RYCHLEJŠÍ NEŽ BRUTE-FORCE!





ÚSPĚŠNĚJŠÍ NEŽ SLOVNÍKOVÝ ÚTOK!

Karel Jiránek 20