Pokročilé metody lámání hesel

Radek Hranický
Lukáš Zobal
Michal Eisner
Jiří Veverka

9. 9. 2019

Úniky uživatelských hesel

Na prodej je 32 milionů hesel z Twitteru. Firma některé účty blokuje

10. června 2016 15:02

Kolem 32 milionů přihlašovacích údajů k účtům na sociální síti Twitter nabízí k prodeji neznámý útočník. Společnost již reaguje tím, že omezuje přístup k některým účtům.

iDNES.cz / MAGAZÍNY Ona Auto Bydlení Revue **Technet** Mobil Cestování Hobby Xmar

Technet.cz Technika Věda Vesmír Vojenství Testy Internet Audio foto video Hardware Sc

Největší únik dat. Yahoo hlásí kompromitaci informací u miliardy lidí

15. prosince 2016 10:05

Společnost Yahoo oznámila, že v roce 2013 byla z jejích stránek odcizena data asi miliardy uživatelů.

Ilustrační snímek | foto: Jiří Benák, iDNES.cz

LUPA.cz server o českém Int

Rychlost Internetu Články Aktuality Video Podcast Nabídky práce v IT Nástroje Lupa.

Lupa.cz » Měli jste účet na MySpace? 427 milionů hesel je na prodej za 2 800 dolarů

Měli jste účet na MySpace? 427 milionů hesel je na prodej za 2 800 dolarů

Autor: Shutterstock, podle licence: Rights Managed

30. 5. 2016

Rok 2016 začíná vypadat náramně, co se úniků (a vymyšlených úniků) hesel týče. Pokud je tento případ skutečný, tak je to také rekordní únik.

Doba čtení: **3 minuty**

Repozitáře hesel online

https://wiki.skullsecurity.org/index.php?title=Passwords

Leaked passwords

Passwords that were leaked or stolen from sites. I'm hosting them because it seems like nobody els these; I simply found them online, removed any names/email addresses/etc (I don't see any reason I'll see if I have them.

The best use of these is to generate or test password lists.

Note: The dates are approximate.

Name	Compressed	Uncompressed
Rockyou	rockyou.txt.bz2 (60,498,886 bytes)	n/a
Rockyou with count	rockyou-withcount.txt.bz2 (59,500,255 bytes)	n/a
phpbb	phpbb.txt.bz2 (868,606 bytes)	n/a
phpbb with count	phpbb-withcount.txt.bz2 (872,867 bytes)	n/a
phpbb with md5	phpbb-withmd5.txt.bz2 (4,117,887 bytes)	n/a
MySpace	myspace.txt.bz2 (175,970 bytes)	n/a
MySpace - with count	myspace-withcount.txt.bz2 (179,929 bytes)	n/a
Hotmail	hotmail.txt.bz2 (47,195 bytes)	n/a
Hotmail with count	hotmail-withcount.txt.bz2 (47,975 bytes)	n/a
Faithwriters	faithwriters.txt.bz2 (39,327 bytes)	n/a
Faithwriters - with count	faithwriters-withcount.txt.bz2 (40,233 bytes)	n/a
Elitehacker	elitehacker.txt.bz2 (3,690 bytes)	n/a
Elitehacker - with count	elitehacker-withcount.txt.bz2 (3,846 bytes)	n/a
Hak5	hak5.txt.bz2 (16,490 bytes)	n/a
Hak5 - with count	hak5-withcount.txt.bz2 (16,947 bytes)	n/a
Älypää	alypaa.txt.bz2 (5,178 bytes)	n/a
alypaa - with count	alypaa-withcount.txt.bz2 (6,013 bytes)	n/a
Facebook (Pastebay)	facebook-pastebay.txt.bz2 (375 bytes)	n/a
Facebook (Pastebay) - w/ count	facebook-pastebay-withcount.txt.bz2 (407 bytes)	n/a

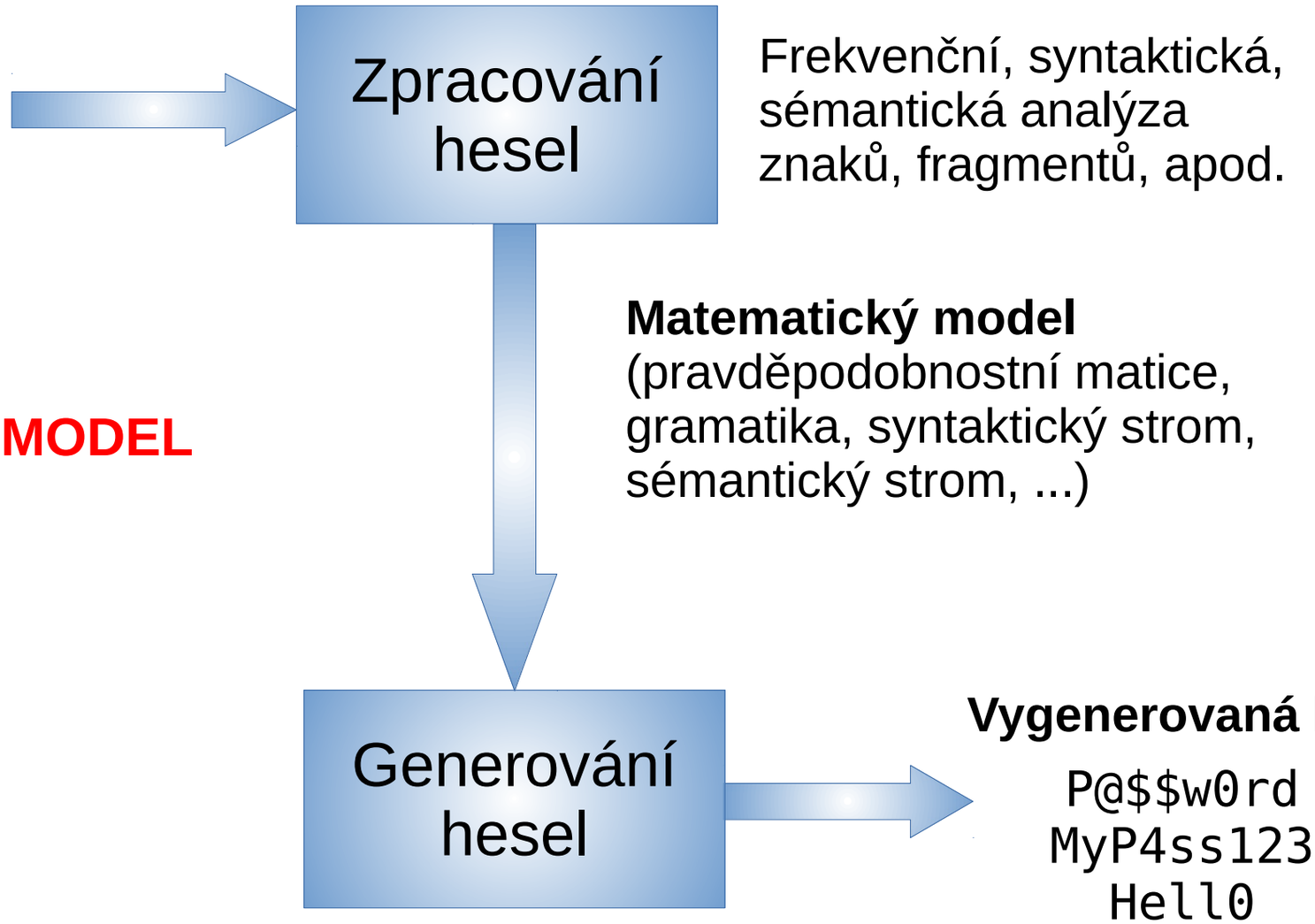
Inc. [US] | https://github.com/danielmiessler/SecLists/tree/master/Passwords

Common-Credentials	find . -name '*_*' -exec rename 's/_/-/g' "{}" \;
Cracked-Hashes	Quick rename of files
Default-Credentials	New Default Password List
Honeypot-Captures	Quick rename
Leaked-Databases	Better filenames
Malware	Close #291 - Fix encoding issues
Permutations	rename 's/_/-/g'
Software	Close #291 - Fix encoding issues
WiFi-WPA	Add "-" to split up words, moved files since PR accepted
Keyboard-Combinations.txt	Add "-" to split up words, moved files since PR accepted
Most-Popular-Letter-Passes.txt	Add "-" to split up words, moved files since PR accepted
PHP-Magic-Hashes.txt	Adding sha256 magic hash
README.md	removes exec. bits
SCRABBLE-hackerhouse.tgz	Add scrabble
UserPassCombo-Jay.txt	"Passwords/" Clean up
bt4-password.txt	Close #291 - Fix encoding issues
cirt-default-passwords.txt	Fix for #201 - _ -> _
clarkson-university-82.txt	Quick rename of files
darkc0de.txt	Close #291 - Fix encoding issues
darkweb2017-top10.txt	Add "-" to split up words, moved files since PR accepted
darkweb2017-top100.txt	Close #291 - Fix encoding issues
darkweb2017-top1000.txt	Close #291 - Fix encoding issues
darkweb2017-top10000.txt	Close #291 - Fix encoding issues
der-postillon.txt	Add worlds-safest-password list by Der Postillon
mssql-passwords-nansh0u-guardicore...	Add MSSQL from guardicore: labs_campaigns-Nansh0u

Princip pokročilých metod

1. ZPRACUJ EXISTUJÍCÍ HESLA

Existující slovník hesel



2. VYTVOŘ JEJICH MODEL

3. POUŽIJ JEJ PRO TVORBU NOVÝCH

PCFG

- Původní uživatelská hesla:

```
pass!word, love@love
```

- Pravděpodobnostní gramatika (model):

```
G = {M, T, R, S, P}
M = {S, A4, 01}
T = {pass, word, love, @, !}
R(P) = {S → A401A4 (100%),
        A4 → word (25%) | pass (25%) | love (50%),
        01 → @ (50%) | ! (50%)}
S = {S}
```

- Nově vygenerovaná hesla:

```
love!love       love@pass       pass@pass
love@love       love@word       pass@word
pass!love       love@pass       word!pass
pass@love       love@word       word!word
word!love       pass!pass       word@pass
word@love       pass!word       word@word
```

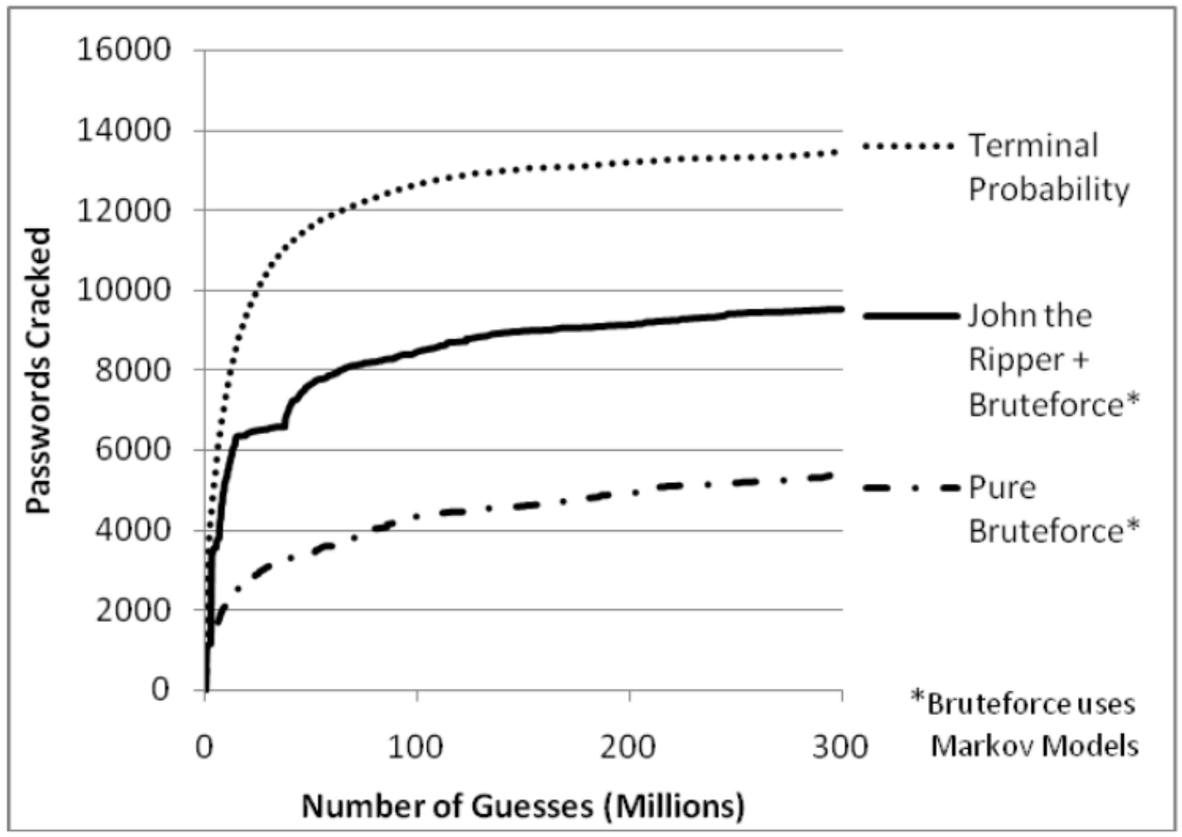
Výhody PCFG

- **Každé možné** heslo má **pravděpodobnost**
- Můžeme vygenerovat **n** nejpravděpodobnějších hesel

  → lepší cílení útoku!

  - Vyšší úspěšnost při vyzkoušení stejného počtu hesel
  - Nemusím zkoušet vše, abych dosáhl úspěchu

MySpace:



Weir, Matt, et al. "Password cracking using probabilistic context-free grammars." 2009 30th IEEE Symposium on Security and Privacy. IEEE, 2009.

Pozvánka na DEMO

- **Jak vypadá gramatika vytvořená ze slovníku?**
- **Jaká hesla z ní vytvoříme?**
- **Jak hesla zároveň generovat a zkoušet?**
- **Jak hesla generovat paralelně?**
- **Jak úlohu chytře rozdělit na více uzlů?**
- **Jak můžeme integrovat PCFG do systému Fitcrack?**

To vám ukáže skupina **Fitcrack** v rámci demonstrace
”**Pokročilé metody lámání hesel**”

Dotazy?

Pokročilé vs. tradiční metody

- **Slovníkový útok**
  - Omezený počet hesel
  - Nutnost přesné shody → Co není ve slovníku, nevyzkoušíme
- **Útok hrubou silou**
  - Klasická verze nezohledňuje předchozí znalosti o heslech
  - Příliš velký počet hesel
  - Složitý algoritmus + netriviální heslo → nepřijatelné trvání