OD DOMÁCEHO MILÁČIKA, CEZ SOCIALISTICKÉ HESLÁ AŽ K ČIPOVANIU POPULÁCIE

TOMÁŠ KUBLA

20.9.2018

Kto som?

- Škola
  - ZŠ Košická
  - GJH
  - Matfyz
- Práca
  - Slovak Telekom
  - GJH – ešte stále?
- Hobby
  - Folklór
  - Swing

Autentifikácia

proces, ktorý zabezpečuje a potvrdzuje totožnosť používateľa

Pre fajnšmerkov: aký je rozdiel medzi autentifikáciou a autorizáciou?

- Niečo čo viem
- Niečo čo mám
- Niečo čo som

Najpoužívanejšia? Prečo?

Prieskum

- Koľko účtov máte?
  - GJH, gmail, FB, banka, Linkedin, Instagram, Skype, Dropbox, Deezer/Spotify, Netflix, …
  - Alza, Aliexpress, Ticketportal, DropBox, WizzAir, AppleID, Uber, Airbnb, Blablacar, Môj telekom, …
- Koľko hesiel máte?
- Koľko rôznych hesiel máte?

- Štatistika*
  - 1 email ~ 118 účtov
  - Každých 5 rokov sa počet zdvojnásobuje
  - Počet hesiel
    - 11% jedno heslo
    - 49% dve heslá (senzitívne a nesenzitívne)
    - 40% čo služba to heslo

*https://digitalguardian.com

Top Heslá (2015)*

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. Starwars

*SplashData

Top Heslá (2016)*

1. 123456
2. password
3. 12345 (+2)
4. 12345678 (-1)
5. football (+2)
6. qwerty (-2)
7. 1234567890 (+5)
8. 1234567 (+1)
9. princess (+12)
10. 1234 (-2)
11. login (+9)
12. welcome (-1)
13. solo (+10)
14. abc123 (-1)
15. admin (nové)
16. 121212 (nové)
17. flower (nové)
18. passw0rd (+6)
19. dragon (-3)
20. sunshine (nové)
21. master (-4)
22. hottie (nové)
23. loveme (nové)
24. zaq1zaq1 (nové)
25. password1 (nové)

*SplashData

Top Heslá (2017)*

1. 123456
2. password
3. 12345678 (+1)
4. qwerty (+2)
5. 12345 (-2)
6. 123456789 (nové)
7. letmein (bolo v 2015)
8. 1234567
9. football (-4)
10. lloveyou (nové)
11. admin (+4)
12. welcome
13. monkey (bolo v 2015)
14. Login (-3)
15. abc123 (-1)
16. starwars (bolo v 2015)
17. 123123 (nové)
18. dragon (+1)
19. passw0rd (-1)
20. master (+1)
21. hello (nové)
22. freedom (nové)
23. whatever (nové)
24. qazwsx (nové)
25. trustno1 (nové)

*SplashData

Trendy

- Muži vs. ženy
- Vek

- Mená rodinných príslušníkov
- Mená domácich miláčikov
- Dovolenkové destinácie
- Dátumy narodenia

Komplexita

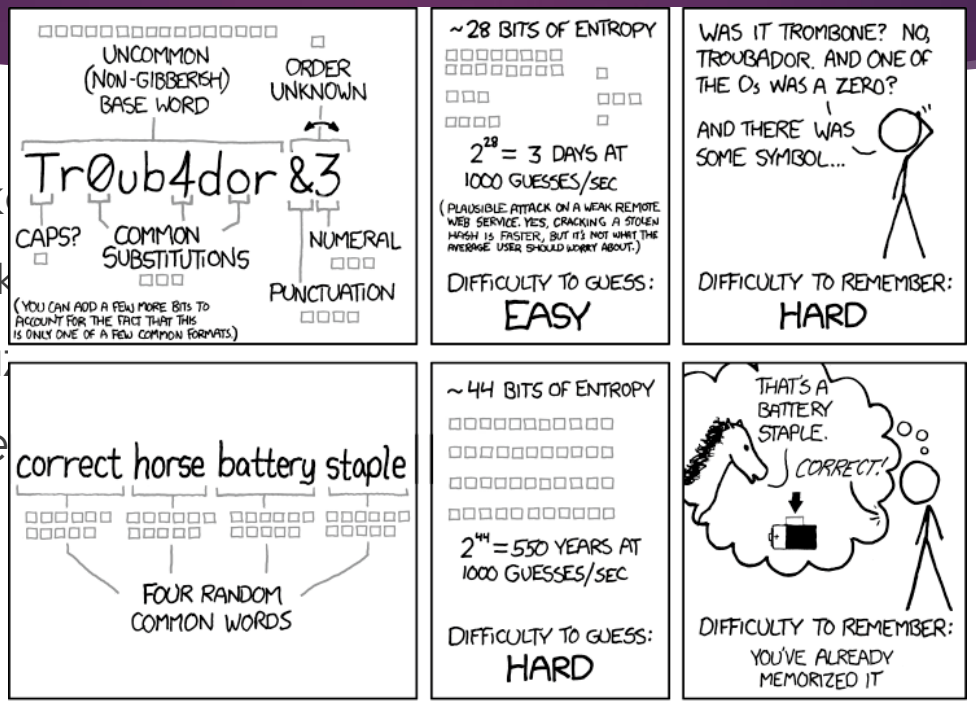
- Ale veď nové registrácie mi nedovoľujú dať tak ľahké heslo
- Heslová politika
- Politika? V informatike?
  - Aj dĺžka hesla
  - Aj dĺžka platnosti
- Malé znaky
- Veľké znaky
- Čísla
- Špeciálne znaky

Dobre heslo! Dobre heslo?

- Vysoká komplexita ~ dobré heslo?
  - Nie tak celkom
- Veta, fráza, replika
- *nech-Zije-1.maj-sviatok-prace*
- Nemeniť

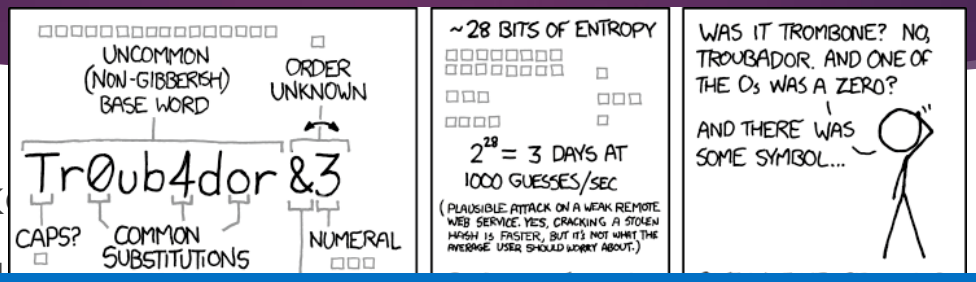
Dobre heslo! Dobre heslo?

- Vysoká k
  - Nie tak
- Veta, fra
- *nech-Zije*
- Nemenit'



Dobre heslo! Dobre heslo?

- Vysoká k
  - N
- Vet
- *nec*
- Ner

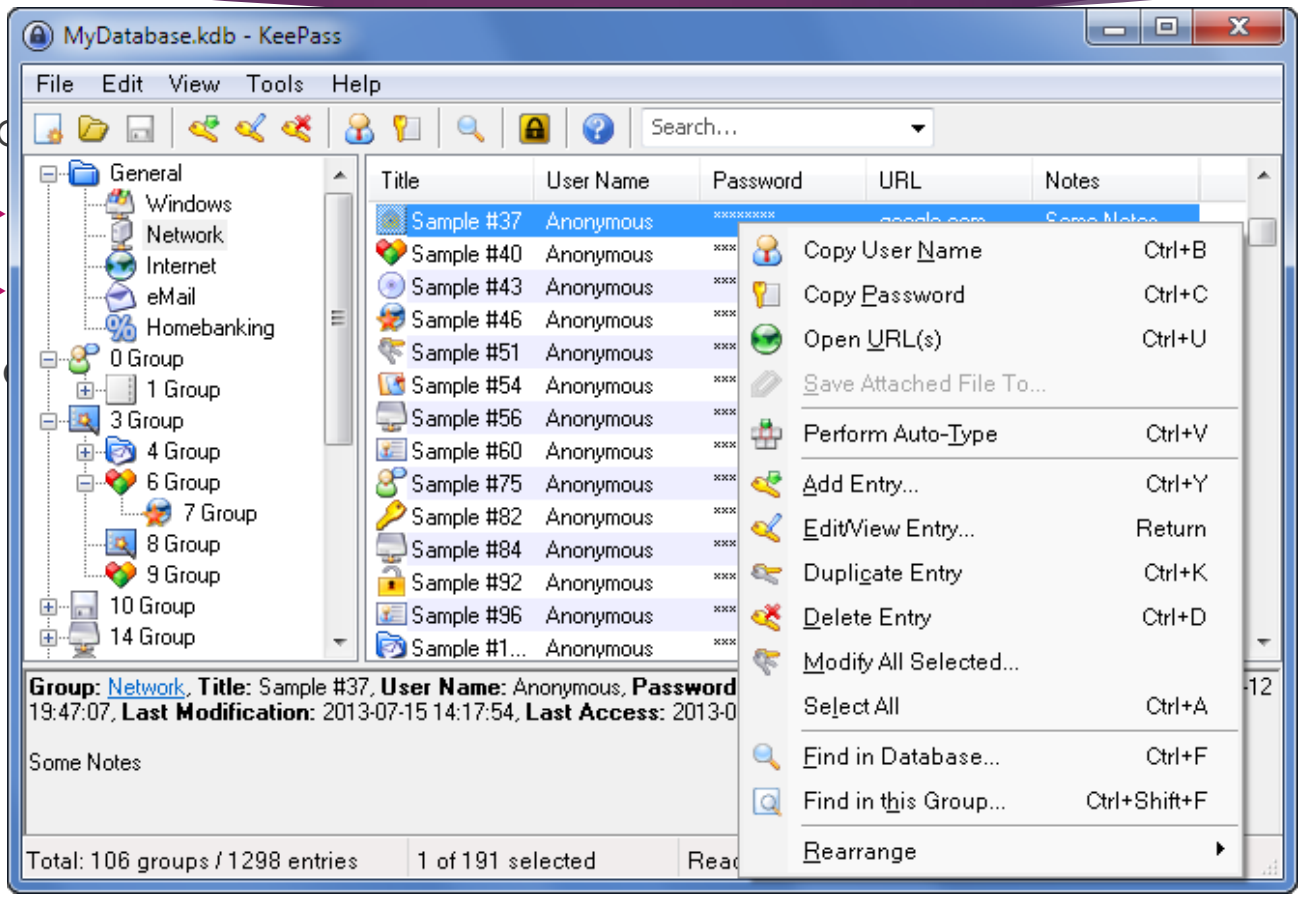


A ako si to zapamätám?

- Password manger
  - 1 heslo extra super ultra náročné, ktoré si pamätám
  - Ostatné (hlavne nezapamätatelné) v databáze
- Demo

A ako si to zapamätám?

- Po
  -
  -
- D



Útoky I

Sociálne inžinierstvo

- Mail
- Telefonát

Onálepkovaný monitor

Oko vidí


210
209
208
207
206
1

Útoky II

- Kamera / diktafón
- Sociálne inžinierstvo (áno, znova)
  - Syndróm muža s rebríkom
  - Syndróm muža v reflexnej veste
- Key logger (sw,hw)
  - 36$ (free shipping)
- Počúvam na sieti (COAX)

Útoky III

- Online / offline
  - Uniknutá databáza
- Hrubá sila (brute-force)
- Slovníky
  - Top 1mil.
  - Mená
  - Psy, mačky, rybičky
  - Chemické zlúčeniny
- Hybrid – paterny

- Extra herný PC (solídny MD + 8x GPU)
  - MD5 - 200.3 GH/s
  - SHA1 - 68.77 GH/s
  - SHA3 - 6.4956 GH/s
  - PBKDF2-HMAC-SHA512 - 3450.1 kH/s
- Pre fajnšmekrov:
  - Hash
  - Time–memory trade-off

Skutočne chceme iba heslá?

- Máme aj iné metódy (niečo čo mám, niečo čo som)
  - Smart karty
  - Tokeny
  - Otlačky
  - Podkožné čipy
- 2FA

Zaujímavosti

- nbusr123
- Vymenili mi monitor, neviem sa prihlásiť
- Na “verejných miestach“ - video
- Maximálna dĺžka hesla
- Odtlačok mŕtveho muža

Ďakujem za pozornosť

OTÁZKY & ODPOVEDE