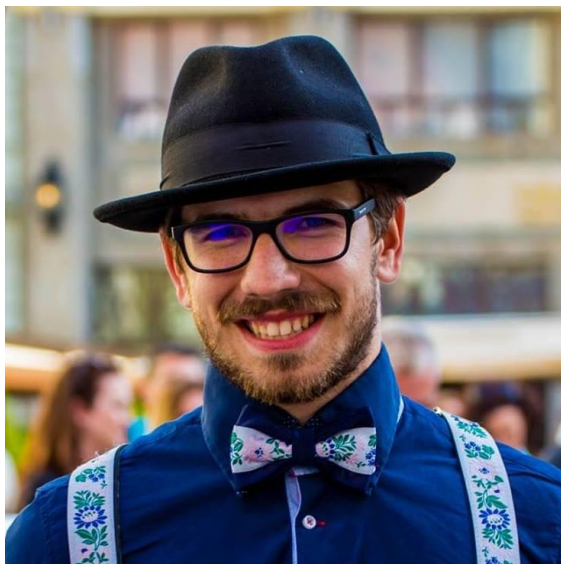


OD DOMÁCEHO MILÁČIKA, CEZ SOCIALISTICKÉ HESLÁ AŽ K ČIPOVANIU POPULÁCIE

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


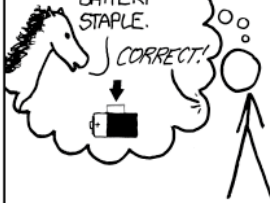
- ▶ Ale veď nové registrácie mi nedovoľujú dať tak ľahké heslo
- ▶ Heslová politika
- ▶ Politika? V informatike?
 - ▶ Aj dĺžka hesla
 - ▶ Aj dĺžka platnosti
- ▶ Malé znaky
- ▶ Veľké znaky
- ▶ Čísla
- ▶ Špeciálne znaky

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
- ▶ Nemeniť

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor & 3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Dobre heslo! Dobre heslo?

- ▶ Vysoká k
- ▶ Nie
- ▶ Veto
- ▶ ne
- ▶ Ner

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS? COMMON SUBSTITUTIONS NUMERAL

~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?

AND THERE WAS SOME SYMBOL...

PASSWORDS ARE LIKE
UNDERPANTS



~~Change them often~~ keep them private and never share them with anyone.

A ako si to zapamätám?

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

A ako si to zapamätám?

- ▶ PC
- ▶
- ▶
- ▶
- ▶ D

The screenshot shows the KeePass application window titled "MyDatabase.kdb - KeePass". The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar with icons for file operations and search, and a search box. On the left, a tree view shows a hierarchy of groups: General, Windows, Network, Internet, eMail, Homebanking, and several numbered groups (0 Group to 14 Group). The main pane displays a table of entries with columns for Title, User Name, Password, URL, and Notes. The entry "Sample #37" is selected, and a context menu is open over it, listing actions such as "Copy User Name", "Copy Password", "Open URL(s)", "Perform Auto-Type", "Add Entry...", "EditView Entry...", "Duplicate Entry", "Delete Entry", "Modify All Selected...", "Select All", "Find in Database...", "Find in this Group...", and "Rearrange". The status bar at the bottom indicates "Total: 106 groups / 1298 entries" and "1 of 191 selected".

Title	User Name	Password	URL	Notes
Sample #37	Anonymous	XXXXXXXXXX	google.com	Some Notes
Sample #40	Anonymous	XXXXXX		
Sample #43	Anonymous	XXXXXX		
Sample #46	Anonymous	XXXXXX		
Sample #51	Anonymous	XXXXXX		
Sample #54	Anonymous	XXXXXX		
Sample #56	Anonymous	XXXXXX		
Sample #60	Anonymous	XXXXXX		
Sample #75	Anonymous	XXXXXX		
Sample #82	Anonymous	XXXXXX		
Sample #84	Anonymous	XXXXXX		
Sample #92	Anonymous	XXXXXX		
Sample #96	Anonymous	XXXXXX		
Sample #1...	Anonymous	XXXXXX		

Group: Network, Title: Sample #37, User Name: Anonymous, Password: 19:47:07, Last Modification: 2013-07-15 14:17:54, Last Access: 2013-07-15 14:17:54

Some Notes

Total: 106 groups / 1298 entries 1 of 191 selected Rearrange

Útoky I

Sociálne inžinierstvo

- Mail
- Telefonát

Onálepkovaný monitor



Oko vidí



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 sieť (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 fajňšmekrov:
 - ▶ 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