

# Hesla včera, dnes a zítra

Ondřej Caletka



3. prosince 2018



Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

# Když se řekne heslo

- autentizační prvek
  - slouží k ověření, že jsme tím, za koho se vydáváme
- tajemství, které nikdo kromě nás nezná
  - nejlépe ani ten, kdo jej ověřuje
- tajemství, které nikdy nezapomeneme

- dlouhé
- náhodné
- unikátní
- zapamatovatelné
- bezpečně zapsané pro nečekané okolnosti

# Míra entropie

System  $S$ , který může nabývat  $n$  stavů, každý s pravděpodobností  $P(s_i)$ , má entropii  $H(S)$  shannonů (bitů):

$$H(S) = - \sum_{i=1}^n P(s_i) \log_2 P(s_i) \quad (1)$$

Jsou-li všechny stavy stejně pravděpodobné,  $P(s_i) = \frac{1}{n}$  pro  $\forall i$ , pak:

$$H(S) = \log_2 n \quad (2)$$

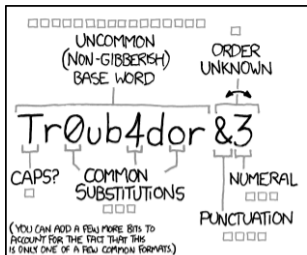
znaků	entropie	lámání 1000/s	znaků	entropie	lámání 30mld./s
4	24 bitů	7 hodin	8	48 bitů	2 hodiny
5	30 bitů	19 dnů	9	54 bitů	7 dnů
6	36 bitů	3 roky 4 měsíce	10	60 bitů	14 měsíců
7	42 bitů	214 let	11	66 bitů	78 let
8	48 bitů	13 tisíc let	12	70 bitů	1200 let

# Entropie běžného hesla

- výrazně nižší než ideální
- jednotlivé znaky nejsou na sobě nezávislé
- slovníková slova mají entropii danou velikostí slovníku
- běžné náhrady (e → 3, i → 1) entropií moc nezvyšují
- lidé jsou předvídatelní v používání číslic a speciálních znaků

DICTIONARY ATTACK!





~28 BITS OF ENTROPY

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

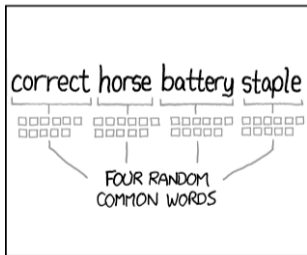
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.

# Zapamatovatelné bezpečné heslo

- zcela náhodný výběr z 4096 slov (12 bitů na slovo)
- aspoň 60 bitů entropie → 5 slov

## Příklady

- byty mám jakmile člověk zpátky
- zabývá přednost diváků rameny konstatoval
- pádu uvidí budovy muž listopadu
- stole co vlastnictví modely zdroje
- zákon tímto podlehl řešit alespoň

# Unikátnost hesla

- únik hesla z *nedůležité* služby umožní průnik do *důležitější* služby
- kombinace dat z *nedůležitých* služeb umožní cílený útok na *důležitější* služby

## Způsoby uložení hesla na straně služby

prostý text / šifrování / obfuskace

zachrání nás jen unikátnost

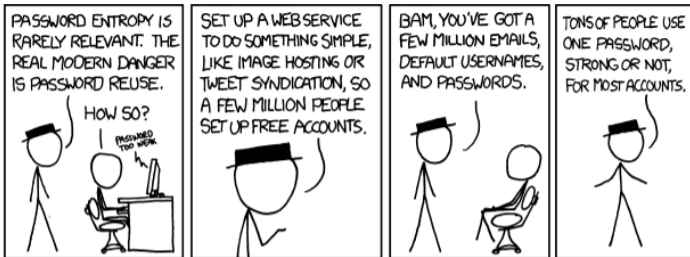
rychlá hashovací funkce (MD5, SHA1) s/bez soli

hesla s vysokou entropií jsou v bezpečí

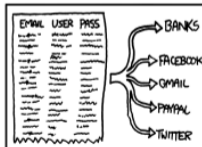
pomalá hashovací funkce (bcrypt, Argon, PBKDF)

stačí i výrazně nižší entropie hesla (~40 bitů)





USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.



YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.



WELL, THAT'S WHERE I GOT STUCK. YOU DID THIS? WHY DID YOU THINK I HOSTED SO MANY UNPROFITABLE WEB SERVICES?



I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS CAREFULLY. BUT RESEARCH SHOWS MORE MONEY DOESN'T MAKE PEOPLE HAPPIER, ONCE THEY MAKE ENOUGH TO AVOID DAY-TO-DAY FINANCIAL STRESS.



# Internetem Bezpečně



Příručka pro děti od 6 do 12 let

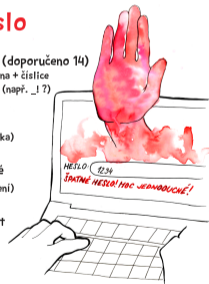
## Heslo

Tvoje heslo je jako klíč od domu. Když je ten klíč kvalitní, nikdo si bez něj dveře do domu neotevře. Bude-li ale špatně zhotovený, nebude mít zloděj s otevřením dveří moc práce.

Bezpečné heslo by se proto mělo skládat ze znaků, které nikdo nezjistí ani neuhodne.

### Bezpečné heslo

- má minimálně 8 znaků (doporučeno 14)  
malá písmena + velká písmena + číselce  
+ má v sobě i speciální znak (např. \_! ?)
- není uhodnutelné  
(jako je jméno tvého mazlíčka)
- není snadno zjistitelné  
(jako je datum tvého narození)
- není běžná posloupnost  
(jako je 12345, abcd)



## Vytvoř si 3 okruhy hesel

1. okruh

router  
heslo do počítače  
heslo do mobilního telefonu nebo tabletu

Nejtajnější hesla z nejtajnějších ...

2. okruh

email  
sociální sítě  
(facebook, snapchat, instagram aj.)

Nikam je nepiš a nezapomínej se odhlašovat.

3. okruh

chaty  
hesla do počítačových her  
hesla do internetových obchodů

Také tajná hesla, ale měla by být jiná než předešlá.

12-13

## Jak vytvořit heslo? Snadno!

Vymyslet neprůstřelné heslo není jen tak. A zapamatovat si ho - to vyžaduje hodně práce. Nebo ne?  
Koukni na tenhle jednoduchý postup, jak na to:

Vymysli si krátkou větu s číslovkou:

**Můj pes má čtyři nohy a jeden ocas.**

Z každého slova použij první písmeno a číslovky změň na čísla.

**mpm4na1o**

Některá písmena udělej velká.

**MpM4Na1o** <- hustokrutopřísné heslo :)

Jak si zapamatuješ více hesel? Stačí jedno trochu pozměnit, koukej!  
[ml\\_MpM4Na1o](#) heslo do emailové schránky  
[MpM4Na1o\\_fb](#) heslo do sociální sítě facebook  
[MpM4Na1o\\_game](#) heslo do počítačové hry

**Nikdy, nikdy, nikdy!**

Hesla nikdy nikomu nepošleš přes internet (emailem apod.).  
Hesla si nikam nepiš - zapamatuj si je.  
Nepoužívej stejné heslo k více službám najednou.  
Nikdy nenechávej heslo dlouho beze změny - pravidelně ho měň.

**Jak si zapamatuješ více hesel? Stačí jedno trochu pozměnit, koukej!**

**ml\_MpM4Na1o** heslo do emailové schránky

**MpM4Na1o\_fb** heslo do sociální sítě facebook

**MpM4Na1o\_game** heslo do počítačové hry

**Nikdy, nikdy, nikdy!**

Hesla nikdy nikomu neposílej přes internet (emailem apod.).

Hesla si nikam nepiš - zapamatuj si je.

Nepoužívej stejné heslo k více službám najednou.

Nikdy nenechávej heslo dlouho beze změny - pravidelně ho měň.

**Jak si zapamatuješ více hesel? Stačí jedno trochu pozměnit, koukej!**

ml\_MpM4Na1o heslo do emailové schránky

MpM4Na1o\_fb heslo do sociální sítě facebook

MpM4Na1o\_game heslo do počítačových her

**Nikdy, nikdy, nikdy!**

**Nikdy, nikdy, nikdy!**

Hesla nikdy nikomu neposílej přes internet (emailem apod.).

Hesla si nikam nepiš - zapamatuj si je. **hlavní heslo si zapiš**

Nepoužívej stejné heslo k více službám najednou. **ani odvozené**

~~Nikdy nenechávej heslo dlouho beze změny - pravidelně ho měň.~~



**KoLeDiPeOk**



**Ko1Le2Di3Pe4Ok5**



## Odvozování dalších hesel podle Jak na Internet

Pro další služby a účty můžete používat své dosavadní heslo, k němuž jednoduše přidáte znaky odpovídající dané službě nebo účtu. Například:

- Ko1Le2Di3Pe40k5**Fa** → **Facebook**
- Ko1Le2Di3Pe40k5**Wi** → **Wi-Fi**
- Ko1Le2Di3Pe40k5**Em** → **Email**
- Ko1Le2Di3Pe40k5**Cl** → **Cloud**

Toto řešení **není ideální**, ale pokud máte problém pamatovat si různá hesla, je přeci jen bezpečnější než používání stále téhož hesla.

Zdroj: Jak na Internet, CZ.NIC



## Doporučení podle Google

- „Starý traktor“ můžete napsat jako „St@RyTr@K+0r“.
- „Extraliga“ můžete napsat jako „E\*Tr4L!g4“.

Zkrajte větu. Vymyslete si nějaké sdělení a vytvořte heslo z prvního písmene každého slova. Příklad: „Strýček Otakar nikdy nedokončil historku, kterou začal vyprávět“ můžete napsat jako „S0nNH,kZv“.

Používejte dlouhá hesla. Delší hesla jsou bezpečnější. Vzhledem k tomu, že jsou povoleny mezery, můžete použít snadno zapamatovatelné věty nebo části oblíbených písní, básní apod. Příklad:

- „M0je <3 bije pr0 KATKU“
- „Štěstí = krásná věc, ale \$ si za něj nekoupíš“
- „Za 100 let v rameni bezmasém, svaly mi v železo ztuhly“

# Doporučení NIST SP800-63B

- pravidelné změny hesel snižují bezpečnost
- požadavky na složení hesel ze znaků určitých skupin jsou kontraproduktivní, místo toho je třeba kontrolovat
  - nejpoužívanější hesla
  - slovníky uniklých hesel
  - triviální hesla
  - kontextově závislá hesla (jméno služby, uživatele, atd.)
- bezpečnostní otázky je třeba zrušit bez náhrady
- hádání hesel by mělo být znemožněno
- hesla mají být uložena bezpečně
- podporovat vícefaktorové ověření
  - SMS není spolehlivý druhý faktor

Root.cz: Nový standard pro přihlašování: nenuťte uživatele měnit hesla

# Vícefaktorové ověření

**první faktor** něco, co znám → heslo, PIN

**druhý faktor** něco, co mám → mobil, token, biometrie

- nejčastěji pomocí jednorázových SMS kódů
- lepší varianta HOTP/TOTP, případně speciální aplikace
- FIDO U2F
- silné jednofaktorové ověření FIDO2 - *něco, co mám*, namísto hesla



Obrázek: YubiKey.cz



# Co je špatného na použití SMS?

- v GSM síti lze SMS celkem snadno odposlouchávat
  - útočník ale musí být blízko
- malware krade autentizační SMS zprávy přímo ze smartphone
  - velmi oblíbený způsob útoku na česká online bankovníctví
- SIM-swap: útoky sociálním inženýrstvím na operátora
  - „ztratil jsem telefon, prosím převedte mé číslo na novou SIM kartu“
  - oblíbený způsob hlavně v zahraničí
  - pro oběť je obtížné získat číslo zpět

# Hlava není na hesla

- v paměti udržíme maximálně jednotky hesel
- abychom je nezapomněli, musíme je často používat
- když nevíme, **nezkoušíme postupně všechna hesla**, co známe
- je správné, mít hesla zapsaná
  - v bezpečném správci hesel
  - na papíře **na bezpečném místě**



Rob Price  
@robaeprice

Follow

A password for the Hawaii emergency agency was inadvertently published in an @AP photo in July 2017 after being written on a post-it note.

[uk.businessinsider.com/hawaii-emergen ...](http://uk.businessinsider.com/hawaii-emergen...)



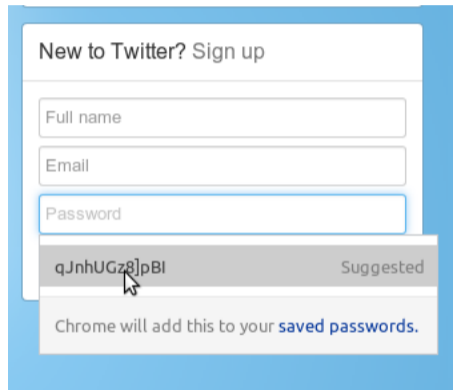
8:27 PM - 16 Jan 2018

# Správci hesel

- KeePass
- 1Password
- LastPass
- *SuperGenPass*
- **vestavěný ve webovém prohlížeči**

Kromě bezpečného uchování také **generuje bezpečná hesla.**

Zdroj: Chromium Password Generation



- délka hesla je důležitější, než množina znaků, ze kterých je složeno
- používání stejného hesla pro víc služeb je větší problém, než slabé heslo
- správce hesel je **nutnost**; prohlížeče ho mají vestavený
- bezpečné hlavní heslo je dobré mít zapsané **na bezpečném místě**

## Další čtení

- Michal Špaček: Hlava není na hesla
- Per Thorsheim: Hakuna Matata - Account Lifecycle Management
- Root.cz: Nový standard pro přihlašování: nenuťte uživatele měnit hesla



Děkuji za pozornost

**Ondřej Caletka**  
**Ondrej.Caletka@cesnet.cz**  
**[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)**

