Hesla včera, dnes a zítra

Ondřej Caletka

cesnet

13. apríla 2019

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

cesnet

Způsob autentizace

Běžný přenos

- typické pro web
- vyžaduje zabezpečený kanál
- ověřovatel může hesla ukládat bezpečně
- náchylné k phishingu

Vzájemné ověření

- například HTTP Digest, MSCHAPv2
- není třeba zabezpečený kanál
- heslo musí být čitelné pro obě strany
- odolné proti phishingu

cesnet

Ukládání hesel na straně služby

Článek: "If you want, I can store the encrypted password." A Password-Storage Field Study with Freelance Developers

Ukládejte heslo bezpečně!

- Base64 - 8 vývojářů
- AES - 3 vývojáři
- 3DES - 3 vývojáři
- MD5 - 10 vývojářů - většina bez soli
- SHA - 6 vývojářů
- PBKDF - 5 vývojářů
- bcrypt - 7 vývojářů
- Argon2 - 0 vývojářů

cesnet

Správné ověřování hesla

- použití náhodné soli – stejná hesla mají různý otisk
  - ideálně netriviálně promíchané s heslem, např. HMAC
- použití pomalé hashovací funkce
  - MD5: 30 Mhash/s
  - bcrypt: 1 khash/s

cesnet

Silné bezpečné heslo

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

cesnet

Míra entropie

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

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

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

$$H(S) = \log_2 n \tag{2}$$

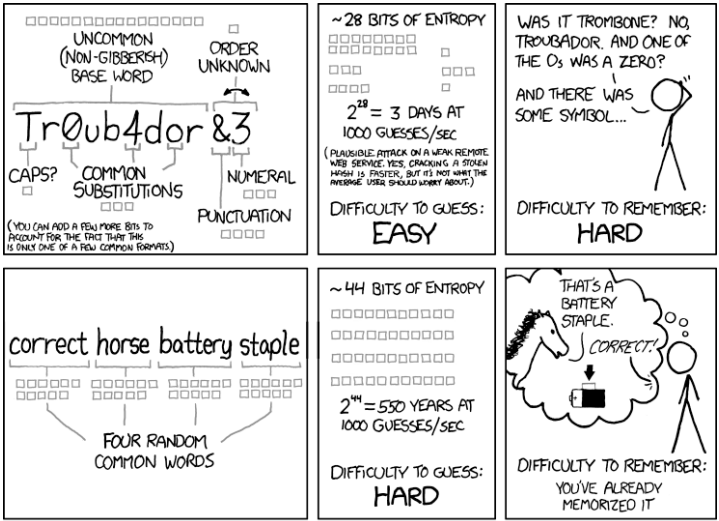
znaků	entropie	lámání 1000/s	znaků	entropie	lámání 30mld./s
4	24 bitů	7 hodin	8	48 bitů	2 hodiny
5	30 bitů	19 dnů	9	54 bitů	7 dnů
6	36 bitů	3 roky 4 měsíce	10	60 bitů	14 měsíců
7	42 bitů	214 let	11	66 bitů	78 let
8	48 bitů	13 tisíc let	12	70 bitů	1200 let

cesnet

Entropie běžného hesla

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

cesnet



Zdroj: xkcd 936, Randall Munroe, CC-BY-NC

Zapamatovatelné bezpečné heslo

- zcela náhodný výběr z 4096 slov (12 bitů na slovo)
- aspoň 60 bitů entropie $\rightarrow$ 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

cesnet

Unikátnost hesla

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

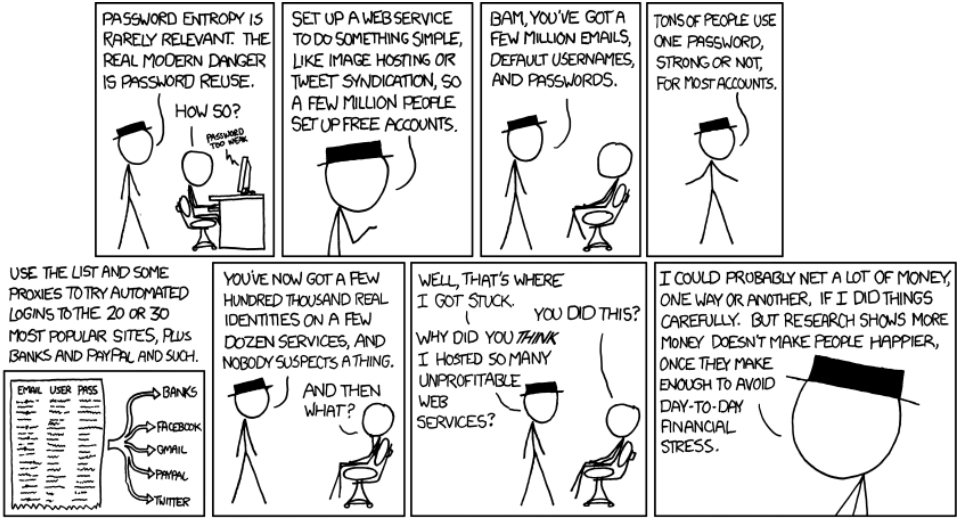
Způsoby uložení hesla na straně služby

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)

cesnet



Zdroj: xkcd 792, Randall Munroe, CC-BY-NC

Roman Kohout
Sandra Kubíčková

Internetem Bezpečně

Příručka pro děti od 6 do 12 let

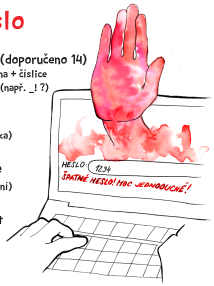
Heslo

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 + číslice
  + 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)



Zdroj: Internetem Bezpečně, Roman Kohout CC-BY-NC-ND

cesnet

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:

NÁVOD

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!
m!_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.

cesnet

Zdroj: Internetem Bezpečně, Roman Kohout CC-BY-NC-ND

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.

Zdroj: Internetem Bezpečně, Roman Kohout CC-BY-NC-ND

cesnet

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

ml_MpM4Na1o heslo do emailové schránky

MpM4Na1o_fb heslo do sociální sítě fa

MpM4Na1o_game heslo do poč

Nikdy, nikdy, nikdy!

Nikdy, nikdy, nikdy!

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

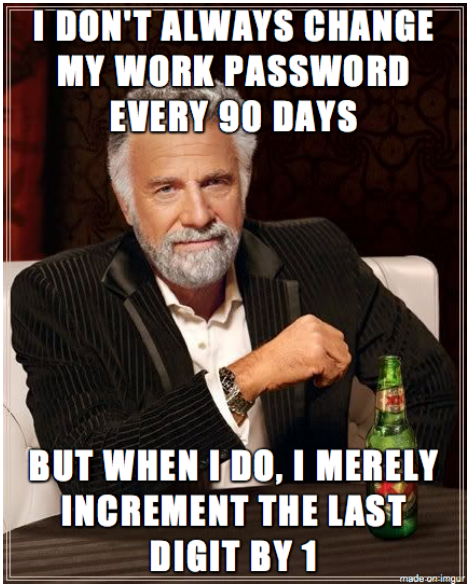
Hesla si nikam nepiš - zapamatuj si je. hlavní heslo si zapiš

Nepoužívej stejné heslo k více službám najednou. ani odvozené

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

Zdroj: Internetem Bezpečně, Roman Kohout CC-BY-NC-ND

cesnet


I DON'T ALWAYS CHANGE MY WORK PASSWORD EVERY 90 DAYS
BUT WHEN I DO, I MERELY INCREMENT THE LAST DIGIT BY 1
made on imgur

cesnet

Zdroj: Jak na Internet, CZ.NIC

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:

- `Ko1Le2Di3Pe40k5Fa` → **Fa**cebook
- `Ko1Le2Di3Pe40k5Wi` → **Wi**-Fi
- `Ko1Le2Di3Pe40k5Em` → **Em**ail
- `Ko1Le2Di3Pe40k5Cl` → **Cl**oud

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

cesnet

Doporučení podle Google

- „Vianocne sviatky“ zmeňte na „V1@n0CneSv1@tKy“
- „Cauky mnauky“ zmeňte na „c@Uky+mN@ukY“

Skráťte vetu: Vymyslite si vetu a použite prvé písmeno z každého slova. Príklad: „Ujo Peter má rád čokoládu a lieskové orechy“ zmeňte na „uPmrC@10“.
Dlhšie heslá sú silnejšie. Tieto tipy vám pomôžu vytvoriť dlhšie heslá, ktoré sa ľahšie pamätajú. Vyskúšajte text skladby alebo básne, zmysluplný citát z filmu alebo prejavu, úryvok z knihy,skupinu slov, ktorej rozumiete, skratku (vytvorte heslo z prvých písmen slov vo vete).

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

Zdroj: Vytvorenie silného hesla, Google

cesnet

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

cesnet

cesnet

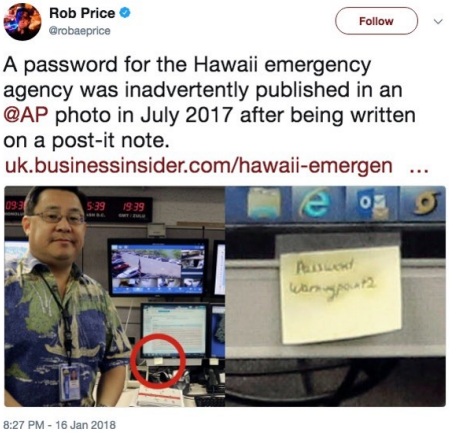
Co je špatného na použití SMS?

- 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 bankovnictví
- SIM-swap: útoky sociálním inženýrstvím na operátora
  - „ztratil jsem telefon, prosím převeďte mé číslo na novou SIM kartu“
  - oblíbený způsob hlavně v zahraničí
  - pro oběť je obtížné získat číslo zpět

cesnet

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**

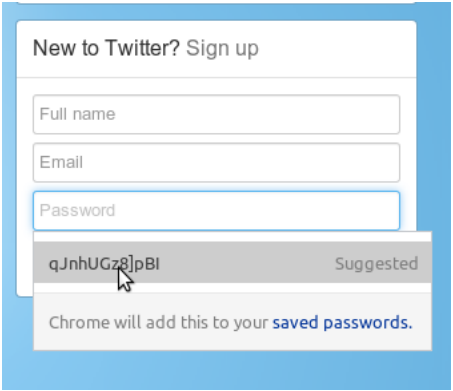


cesnet

Správci hesel

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

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



Zdroj: Chromium Password Generation

cesnet

Shrnutí

- 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

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.

14.1.2019 SK-NIC pripravuje spustenie služby DNSSEC

Po uskutočnení významnej investície do nových systémov a hardvéru prispeje v roku 2019 spoločnosť SK-NIC, a. s. aj k zvýšeniu bezpečnosti slovenského internetu. Na Slovensko pritom prinesie najmodernejšiu verziu technológie DNSSEC.

Od marca tohto roka si budú môcť slovenské firmy a občania zabezpečiť svoje webové sídla s doménou .SK proti tomu, aby ich klientov hackeri nemohli tak jednoducho presmerovať na falošné webstránky. Umožní to pripravované **spustenie služby DNSSEC**, ktorá umožňuje zabezpečiť používanie domén (napr. www.nejakyweb.sk) na internete proti podvrhnutiu (tzv. 'spoofing') a úmyselnej manipulácii.