Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Techniky autentizácie a overovania

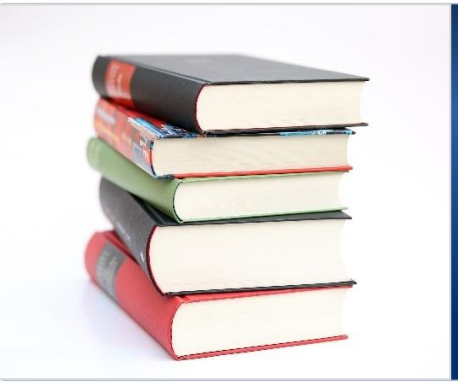
Identifikácia a autentizácia (Blok III)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

doc. Ing. Gabriel Koman, PhD.

KC KYB UNIZA, https://kc.uniza.sk

gabriel.koman@uniza.sk



Obsah

- Typy autentizačných faktorov
- Význam a spôsoby overenia digitálnej totožnosti (elektronické a kvalifikované elektronické podpisy)
- Heslá a ich šifrovanie
- Prehľad autentizačných metód
- Prehľad technológií a protokolov používaných v AAA (RADIUS, TACACS+)
- Nastavenie a testovanie autentizačných mechanizmov na príkladoch z verejnej správy

Typy autentizačných faktorov

Typy autentizačných faktorov

- Autentizačné faktory sa delia na tri hlavné kategórie:
  - **Niečo, čo viete**
    - Heslá
    - PIN kódy
    - Bezpečnostné otázky
  - **Niečo, čo máte**
    - Smartfóny
    - Bezpečnostné tokeny
    - Čipové karty
  - **Niečo, čo ste**
    - Odtlačky prstov
    - Skenovanie tváre
    - Skenovanie dúhovky

Typy autentizačných faktorov

- **Niečo, čo viete**
  - **Heslá**
    - Najbežnejší autentifikačný faktor
    - Kombinácia číslic, písmen, príp. špeciálnych znakov
    - Overenie totožnosti používateľka
    - Heslá by mali byť dostatočne silné, aby sa zabránilo ich uhádnutiu alebo dešifrovaniu
  - **Slabé heslo**
    - Krátke, jednoduché, ľahko uhádnuteľné
      - Napríklad „123456“ alebo „password“, a preto je veľmi zraniteľné. Útočníci môžu tieto heslá uhádnuť veľmi rýchlo, najmä pri použití automatických nástrojov.
  - **Silné heslo**
    - Dostatočne dlhé (minimálne 12 znakov)
      - Kombinácia veľkých a malých písmen, číslic a špeciálnych znakov (napr. !, @, #).
      - Silné heslá sú ťažšie na uhádnutie a sú odolnejšie voči útokom, ako je napríklad **brute force**
        - Útok, pri ktorom sa vyskúša každá možná kombinácia znakov

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy autentizačných faktorov

- **Niečo, čo viete**
  - **PIN kódy**
    - Personal Identification Number
    - Krátky číselný kód
    - Zvyčajne má 4 až 6 číslic, čo ho robí jednoduchším na zapamätanie, ale zároveň aj zraniteľnejším voči útokom
  - **Slabý PIN kód**
    - Číselná kombinácia, ktorú útočník ľahko uhádne
    - PIN kódy sú zvyčajne kratšie, čo znižuje počet možných kombinácií, a tým aj bezpečnosť
  - **Silný PIN kód**
    - Nie je ľahko uhádnuteľný, ako napríklad rok narodenia alebo sériové číslo
    - Dobrý PIN by mal byť náhodný a nemal by obsahovať zrejmé sekvencie:
      - „1234“ alebo „0000“
  - Použitie:
    - Kde je potrebné rýchlo overiť identitu používateľa:
      - Mobilné zariadenia, bankomat, smartfón a pod.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy autentizačných faktorov

- **Niečo, čo viete**
  - **Správa hesiel**
    - Významný aspekt kybernetickej bezpečnosti
    - Používa sa množstvo rôznych online účtov:
      - E-mail, bankovníctvo, sociálne siete, online nákupy
      - Zapamätanie si hesiel, najmä ak majú byť silné a jedinečné pre každý účet
      - Používanie rovnakého hesla pre viacero účtov
      - Jednoducho zapamätateľné heslá zvyšujú riziko neoprávneného prístupu
    - **Tradičná správa hesiel a možné problémy s tým spojené:**
      - Používanie rovnakého hesla na viacerých účtoch
        - Napadnutie viacerých účtov, čo zvyšuje riziko zneužitia
      - Používanie slabých hesiel
        - Slabé heslá, ako napríklad "123456" alebo "password", sú veľmi ľahko uhádnuteľné
      - Zapamätanie si mnohých rôznych hesiel
        - Zapamätanie si môže byť náročné, najmä ak je potrebné pamätať si desiatky online účtov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy autentizačných faktorov

- **Niečo, čo viete**
  - **Správa hesiel**
    - **Používanie správcov hesiel**
      - Nástroj, ktorý pomáha používateľom bezpečne uchovávať a spravovať ich heslá
      - Môže generovať silné a jedinečné heslá pre každý účet
        - Používateľ si nemusí pamätať každé heslo, len hlavné heslo na prístup do správcu hesiel
      - Základné výhody správcov hesiel:
        - Generovanie silných hesiel
          - Automaticky generujú silné, náhodné a jedinečné heslá pre každý účet, ktoré obsahujú kombináciu písmen (veľkých aj malých), čísel a špeciálnych znakov
        - Bezpečné uchovávanie hesiel
          - Správca hesiel šifruje uložené heslá, t. j. len používateľ môže získať prístup k svojim heslám
        - Jednoduchý prístup k heslám
          - Stačí, keď si používateľ zapamätá jediné silné heslo – hlavné heslo na prístup do správcu hesiel
        - Zníženie rizika zneužitia slabých hesiel
          - Každé heslo je jedinečné a dostatočne silné na ochranu účtu, t. j. výrazne sa znižuje riziko neoprávneného prístupu
        - Bezpečné zdieľanie hesiel
          - Možnosť bezpečne zdieľať heslá s inými používateľmi bez toho, aby museli byť zdieľané prostredníctvom nešifrovaných kanálov (ako e-mail alebo textová správa)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

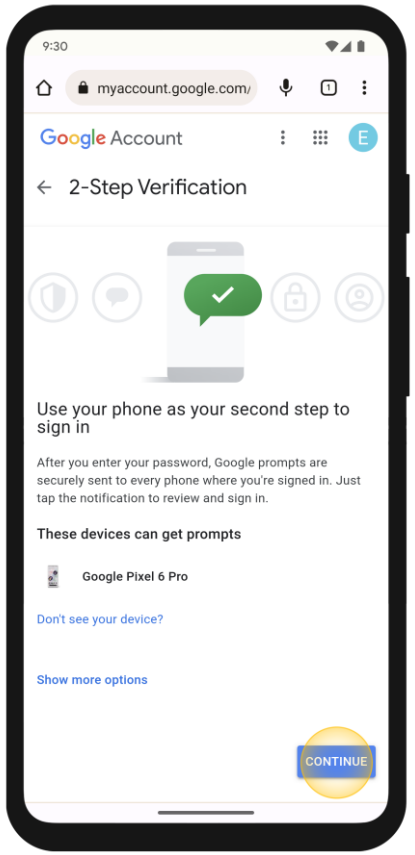
Typy autentizačných faktorov

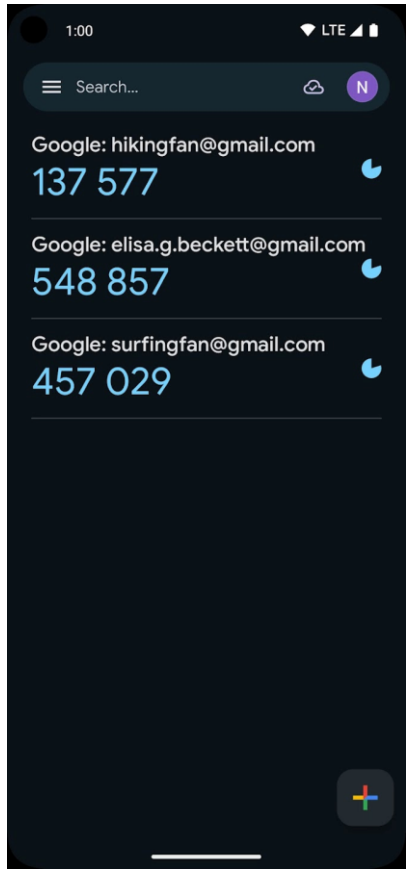
- **Niečo, čo viete**
  - **Správa hesiel**
    - **Používanie správcov hesiel**
    - **Príklady správcov hesiel**
      - LastPass
        - Šifrovanie na úrovni zariadení a jednoduchá synchronizácia medzi rôznymi zariadeniami
      - 1Password
        - Jednoduchý s robustnými bezpečnostnými funkciami
      - Dashlane
        - Okrem správy hesiel ponúka aj monitorovanie únikov údajov a bezpečnostný audit
      - Bitwarden
        - Open-source správca hesiel, ktorý poskytuje vysokú úroveň bezpečnosti a šifrovania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy autentizačných faktorov

- **2FA – dvoj faktorová autentizácia / MFA – viac faktorová autentizácia**
  - používa sa súčasne s heslom
  - zvyšuje bezpečnosť - je potrebné mať fyzicky prístup k dodatočnému zariadeniu/niečo vlastniť
  - **Niečo čo máte**
    - **Smartfón**
      - OTP – jednorazový kód meniaci sa v čase (30s)
      - Potvrdenie prihlásenia aplikáciou
    - **Bezpečnostný token**
      - zariadenie vo forme USB kľúča
        - Pripojenie do PC, aktivované dotykom na zlatú plôšku
      - samostatné zariadenie generujúce PIN
    - **Čipová / bezkontaktná karta**
      - vloženie do zariadenia
      - priloženie (dosah pár cm)





Typy autentizačných faktorov

- **2FA – dvoj faktorová autentizácia / MFA – viac faktorová autentizácia**
  - **Niečo čo ste**
    - **Biometria**
      - Biometrické údaje: Jedinečné fyziologické alebo behaviorálne charakteristiky jednotlivca (napr. odtlačky prstov, rozpoznávanie tváre, skenovanie dúhovky a sietnice, hlasové vzory).
      - Biometrické overenie: **Proces** porovnania biometrických údajov s uloženými vzormi v databáze za účelom potvrdenia totožnosti.
    - **Výhody biometrického zabezpečenia**
      - Vysoká úroveň zabezpečenia: Jedinečnosť biometrických údajov sťažuje ich falšovanie alebo krádež.
      - Pohodlie: Rýchle a jednoduché overovanie totožnosti bez potreby hesiel alebo prístupových kariet.
    - **Nevýhody**
      - Ochrana súkromia: Riziko zneužitia biometrických údajov, krádeže identity a podvodov.
      - Biometria sa môže ľahko poškodiť (porezanie sa, úraz...)
      - Nutnosť presného zberu a spracovania údajov, aby boli spoľahlivé.
    - **Príklady využitia**
      - Mobilné zariadenia: Odomykanie telefónov pomocou odtlačkov prstov alebo rozpoznávania tváre.
      - Založenie účtu v banke: pokročilejšie snímanie pohybu tváre
      - Kontrola prístupu: Zabezpečenie vstupu do budov alebo systémov pomocou skenovania dúhovky alebo odtlačkov prstov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Význam a spôsoby overenia digitálnej totožnosti (elektronické a kvalifikované elektronické podpisy)

Digitálna totožnosť

- Spôsob identifikácie ako v reálnom svete
  - Meno
  - Priezvisko
  - Rodné číslo
  - Adresa
  - Podpis
- Zvyčajne kombinácia viacerých parametrov, ktoré **jednoznačne** identifikujú osobu, alebo jej konanie (napr. podpísanie dokumentu)
- V digitálnom svete nie je možné získať biologický identifikátor
  - Podoba
  - Vlastnoručný podpis

Digitálny podpis

- Elektronický ekvivalent vlastnoručného podpisu
  - Potvrdenie/overenie dokumentu
- Elektronický podpis nie je grafický podpis!
- Využíva sa asymetrická kryptografia
  - Súkromný kľúč je uložený u používateľa
    - Napr. Občiansky preukaz s čipom
  - Týmto kľúčom je podpísaný dokument
  - Na základe overenia verejným kľúčom používateľa vieme jednoznačne určiť podpisujúceho

- **Predpoklad:** Súkromný kľúč (alebo médium na ktorom je uložené) nebol ukradnutý

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kvalifikovaný elektronický podpis

- Kvalifikovaný elektronický podpis je právnym ekvivalentom vlastnoručného podpisu

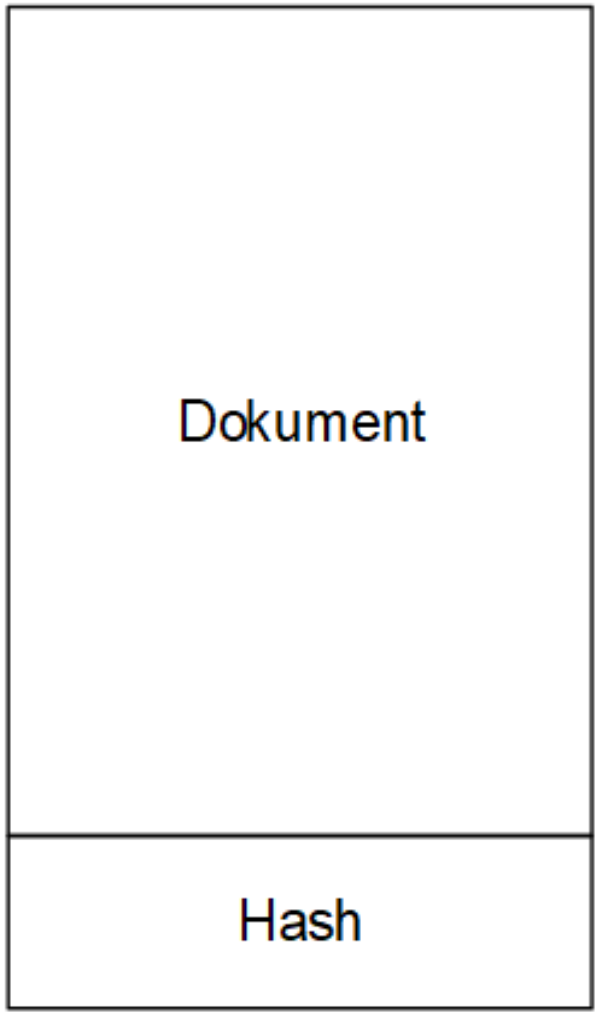
- Zabezpečí možnosť
  - overenia identity subjektu
  - preukázania nemennosti údajov uvedených v dokumente
  - určenia zodpovednosti za podpis pripojený k elektronickému dokumentu.

- Prijatím zákona č. 272/2016 Z. z. sa pojem zaručený elektronický podpis zmenil na kvalifikovaný elektronický podpis.

Technický princíp fungovania elektronického podpisu

1) Vytvorím z dokumentu odtlačok (tzv. Hash)
2) Zašifrujem Hash svojím súkromným kľúčom
3) Pripojím zašifrovaný Hash k dokumentu

- Podpis je k dokumentu pripojený ako príloha
- Obsahuje
  - Čas podpisu
  - Kryptografické informácie o podpise
  - Zvyčajne aj verejný kľúč (certifikát) podpisujúceho



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Overenie elektronického podpisu

1) Získam podpísaný dokument
2) Získam verejný kľúč odosielateľa
3) Overím verejný kľúč odosielateľa
   - Platnosť
   - Či nebol odvolaný - CRL (Certificate Revocation List)
4) Vypočítam Hash z dokumentu
5) Dešifrujem získaným kľúčom priložený Hash
6) Porovnám Hash hodnoty

§ Ak sa Hash hodnoty nerovnajú, dokument bol počas prenosu zmenený alebo podpis nie je pravý

Heslá a ich šifrovanie

Ako vytvoriť bezpečné heslo

- **Sila hesla zásady:**
  - Nepoužívať slová zo slovníka ani mená v žiadnom jazyku
  - Nepoužívať bežné preklepy slov zo slovníka (“Misspellings“)
    - "h3llo" namiesto "hello"
  - Ak je to možné, používať špeciálne znaky, ako sú ! @ # $ % ^ & * ( )
  - Nepoužívať názvy počítačov ani názvy účtov
  - Používať heslo s viac ako desiatimi znakmi
- Na obrázku je uvedená rýchlosť prelomenia hesla na základe jeho zložitosti podľa Kompetentné a certifikačné centrum kybernetickej bezpečnosti

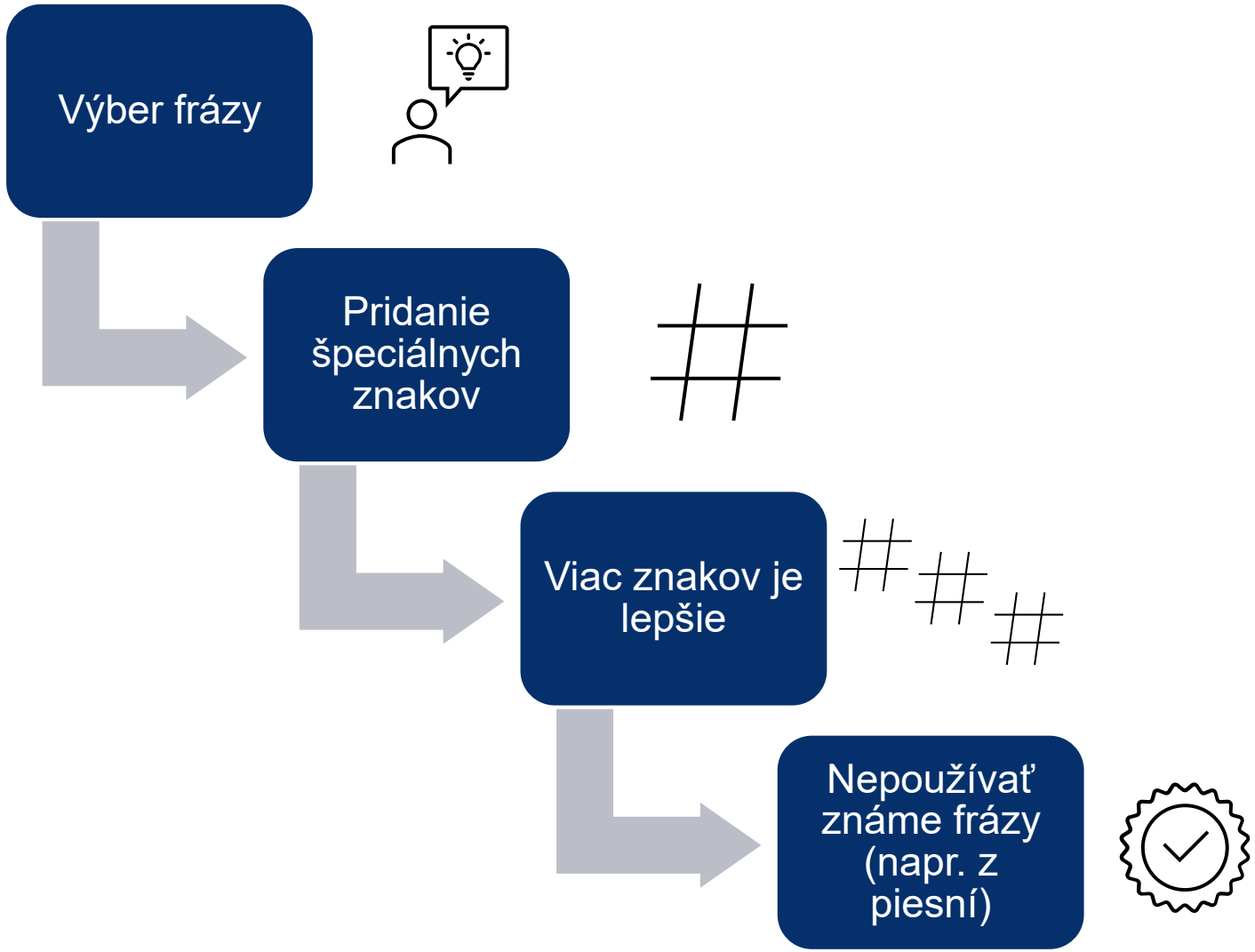
Počet znakov \ Typ znakov	Iba číslice	Malé písmená	Veľké a malé písmená	Čísla, veľké a malé písmená	Čísla, veľké a malé písmená, symboly
4	Okamžite	Okamžite	3 sekundy	6 sekundy	9 sekúnd
5	Okamžite	4 sekundy	2 minúty	6 minút	10 minút
6	Okamžite	2 minúty	2 hodiny	6 hodín	12 hodín
7	4 sekundy	50 minút	4 dni	2 týždne	1 mesiac
8	37 sekúnd	22 hodín	8 mesiacov	3 roky	7 rokov
9	6 minút	3 týždne	33 rokov	161 rokov	479 rokov
10	1 hodina	2 roky	1 tis. rokov	9 tis. rokov	33 tis. rokov
11	10 hodín	44 rokov	89 tis. rokov	618 tis. rokov	2 mil. rokov
12	4 dni	1 tis. rokov	4 mil. rokov	38 mil. rokov	164 mil. rokov
13	1 mesiac	29 tis. rokov	241 mil. rokov	2 mld. rokov	11 mld. rokov
14	1 rok	766 tis. rokov	12 mld. rokov	147 mld. rokov	805 mld. rokov
15	12 rokov	19 mil. rokov	652 mld. rokov	9 bil. rokov	56 bil. rokov
16	119 rokov	517 mil. rokov	33 bil. rokov	566 bil. rokov	3 brd. rokov
17	1 tis. rokov	13 mld. rokov	1 brd. rokov	35 brd. rokov	276 brd. rokov
18	11 tis. rokov	350 mld. rokov	91 brd. rokov	2 trl. rokov	19 trl. rokov

Zdroj: www.cybercompetence.sk

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako vytvoriť bezpečné heslo

- **Fráza ako heslo**
  - Menej zraniteľná voči útokom
  - Dlhšia ako typické heslo
  - Napríklad: „Acat th@tlov3sd0gs
  - A cat that loves dogs



Ako vytvoriť bezpečné heslo

- **Tvorba hesiel**
  - The United States National Institute of Standards and Technology (NIST)
  - Národný inštitút pre normy a technológie
  - Požiadavky na heslá:
    - Aspoň 8 znakov
    - Bežné heslá by sa nemali používať (heslo, abc123...)
    - Zviditeľnenie hesla pri jeho zadaní
    - Všetky znaky a medzery by mali byť povolené
    - Nemala by existovať nápoveda k heslu
    - Nemal by existovať časový limit na platnosť hesla
    - Nemala by existovať autentifikácia založená na znalostiach
    - Odpovede na tajné otázky
    - Overovanie histórie transakcií atď.

Ako vytvoriť bezpečné heslo

- **Tvorba hesiel – Generátor hesiel**

Vygenerujte si svoje bezpečné heslo

Veľmi silné

.Lw!iHY$He7w%x^ KOPÍROVAŤ

Dĺžka hesla 15

Veľké písmená Malé písmená Čísla Symboly

Automatický online generátor hesiel

NÁŠ TIP: Ako vymyslieť dobré heslo

Algoritmus	
Vysloviteľné:	◉
Náhodné:	○

Množiny symbolov				
Malé písmená	Áno	◉	○	Nie
Veľké písmená	Áno	◉	○	Nie
Číslice	Áno	◉	○	Nie
Špeciálne symboly	Áno	◉	○	Nie

Možstvo a dĺžka		
Počet hesiel na vygenerovanie:	6	max 255
Minimálna dĺžka hesla:	8	max 255
Maximálna dĺžka hesla:	14	max 255

Náhodné dáta definované používateľom	
Dávka:	

Zrušiť uložené nastavenia ○ Uložiť nastavenia do cookie ○

Generovať

Vygenerované heslá

```
VojCioc9
shtulvyuhedNu
opsIdIlmaf
diaciavUd1
CytNouptogtoo
Ucdoquauccus
```

Powered by Platon webhosting

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Riziká používania rovnakého hesla viackrát

- **Riziko reťazového útoku**
  - Ak sa útočníkovi podarí prelomiť jedno (napríklad pri úniku dát z webovej stránky), získa prístup ku všetkým účtom používateľa, kde používa rovnaké heslo
  - Týmto spôsobom môže útočník rýchlo získať kontrolu nad e-mailovými účtami, bankovými účtami, sociálnymi médiami a ďalšími online službami

  - **Príklad:** Ak niekto ukradne prihlasovacie údaje používateľa zo sociálnej siete, môže sa pokúsiť použiť rovnaké heslo na prihlásenie do e-mailu, bankového účtu alebo iných služieb. To znamená, že získa prístup k viacerým účtom bez toho, aby musel uhádnuť nové heslo.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riziká používania rovnakého hesla viackrát

- **Útoky typu credential stuffing**
  - Technika, pri ktorej útočníci používajú databázy uniknutých prihlasovacích údajov (napr. zo starších únikov údajov) a skúšajú ich na rôznych webových stránkach
  - Ak používateľ používa rovnaké heslo na viacerých stránkach, útočník môže získať prístup k viacerým účtom vďaka tomu, že heslo bolo opakovane použité

  - **Príklad:** Ak bolo heslo používateľa odcudzené pri úniku z jedného online obchodu, útočník môže vyskúšať toto heslo na rôznych stránkach, ako je napríklad bankový účet používateľa alebo sociálne siete. Tieto údaje môžu byť zneužité, ak sú heslá rovnaké.

  - Email: https://haveibeenpwned.com/
  - Heslo: https://haveibeenpwned.com/Passwords
  - Web: https://haveibeenpwned.com/PwnedWebsites

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riziká používania rovnakého hesla viackrát

- **Riziko zneužitia citlivých informácií**
  - Ak používateľ používa rovnaké heslo pre viacero účtov, útočník, ktorý získa prístup k jednému účtu, môže získať prístup k citlivým údajom vo viacerých oblastiach života používateľa:
    - Osobné údaje
    - Finančné informácie
    - Pracovné dokumenty
    - Prístup k službám, ktoré by mali byť chránené atď.

  - **Príklad:** Ak útočník získa prihlasovacie údaje používateľa k jeho e-mailovej schránke (ktorá je často základom pre obnovenie hesiel na iných službách), môže si jednoducho obnoviť heslá na iných účtoch, ako sú bankové aplikácie, online nákupy alebo iné citlivé systémy.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riziká používania rovnakého hesla viackrát

- **Znížená bezpečnosť v prípade napadnutia**
  - Ak je jeden z účtov používateľa napadnutý, všetky ďalšie účty, ktoré používajú rovnaké heslo, sú už v podstate kompromitované
  - Útočníci môžu získať prístup k účtom, ktoré inak nie sú priamo ohrozené pretože používateľ nezabezpečil svoje účty rôznymi heslami

  - **Príklad:** Ak hacker získa prihlasovacie údaje používateľa z online obchodu a toto heslo používa aj na sociálnych sieťach, hacker môže začať zneužívať účty používateľa, dokonca bez toho, aby vedel jeho úplne iné informácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riziká používania rovnakého hesla viackrát

- **Útoky hrubou silou a slovníkové útoky**
  - Útočníci používajú automatizované nástroje na skúšanie rôznych kombinácií hesiel (útoky hrubou silou) alebo na skúšanie bežných slov a fráz (slovníkové útoky)
    - Ak používateľ používa rovnaké heslo na viacerých stránkach, zvyšujete pravdepodobnosť, že útočník heslo uhádne
- **Phishingové útoky:**
  - Útočníci sa snažia oklamať používateľov, aby im prezradili svoje heslá prostredníctvom falošných e-mailov alebo webových stránok (phishing)
    - Ak používateľ používa rovnaké heslo na viacerých stránkach, útočník môže použiť získané heslo na prístup k ďalším účtom
    - Zvyšuje sa efektivita Phishingových útokov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

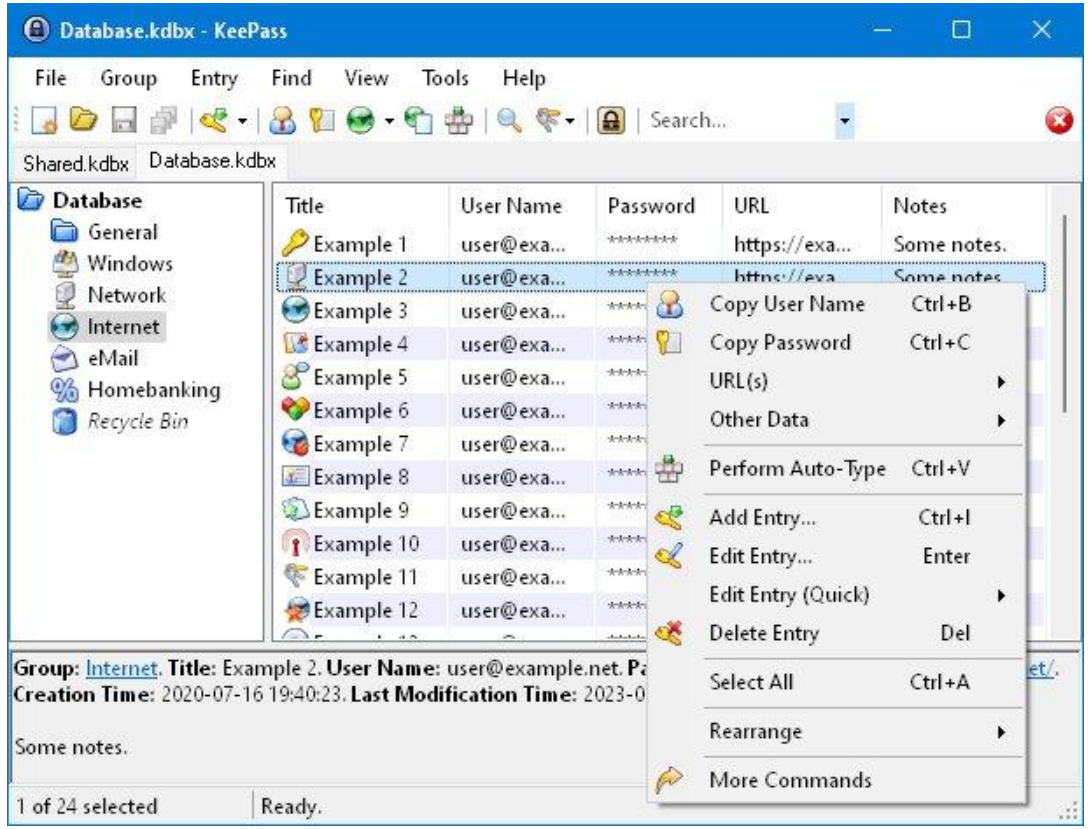
Riziká používania rovnakého hesla viackrát

- **Predchádzanie rizikám používania rovnakého hesla viackrát**
  - Používanie jedinečných hesiel pre každý účet
  - Používanie správcov hesiel
  - Dvojfaktorová autentifikácia (2FA)
  - Pravidelná zmena hesiel
    - Najmä pri podozrení na kompromitáciu/zneužitie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako spravovať heslá pomocou správcu hesiel

- Password Manager
  - Program na správu hesiel
  - Jedným "globálnym" heslom sa odomkne databáza hesiel
  - Môže byť
    - Personálny - súkromný pre jedného človeka
    - Skupinový - zdieľaný pre skupinu, napr. tím ľudí v práci

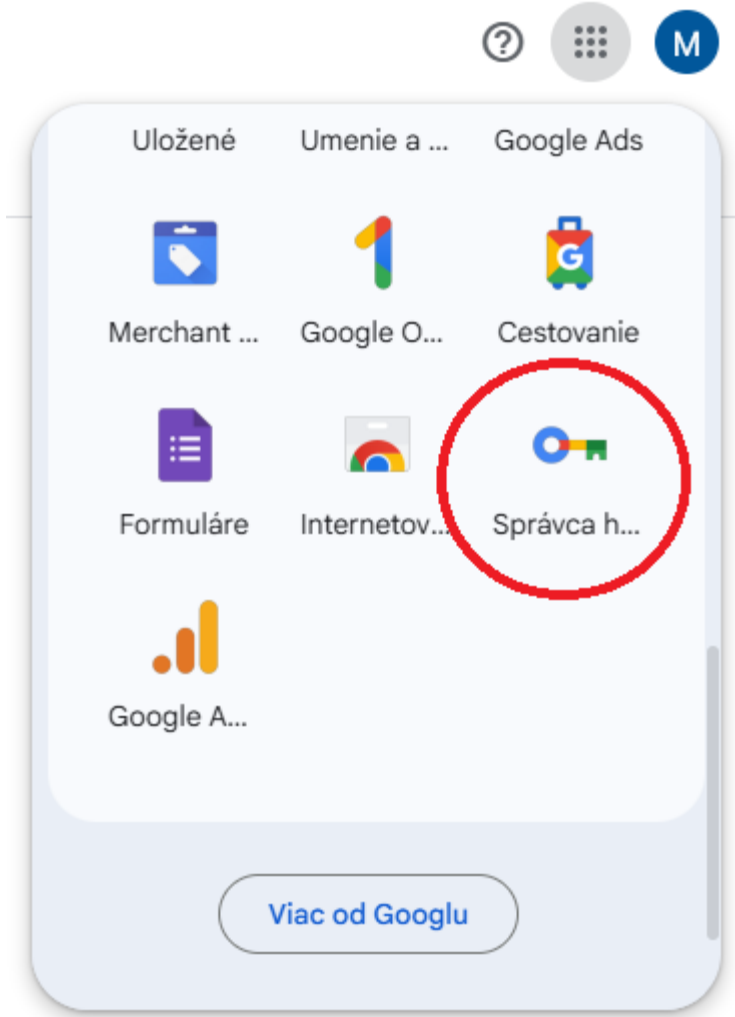


- Password Manager dovoľuje
  - Ukladanie mena, hesla, URL
  - Generovanie hesiel
    - Malé písmená, veľké písmená, čísla, špeciálne znaky, dĺžka hesla, ...
  - Integrácia do prehliadača

Ako spravovať heslá pomocou správcu hesiel

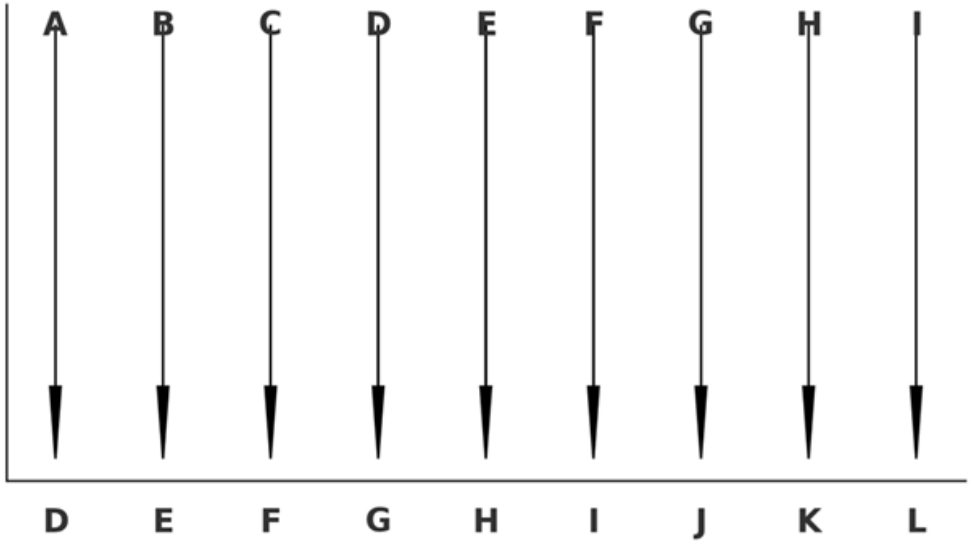
- Online
  - Google password manager (passwords.google.com/)
  - Proton Pass (proton.me/pass)
  - Ďalšie platené

- Aplikácia vo Vašom PC
  - KeePass
  - KeePassXC
  - Enpass
  - BitWarden
  - 1Password



Ako sa heslá ukladajú a šifrujú

- **Šifrovanie**
  - Proces prevodu údajov/informácií do nečitateľnej formy pre neoprávneného používateľa
  - Iba oprávnená osoba
  - Tajný kľúč alebo heslo na dešifrovanie
- Nezabráni zachyteniu údajov
- Zabráni v zobrazení/prístupe



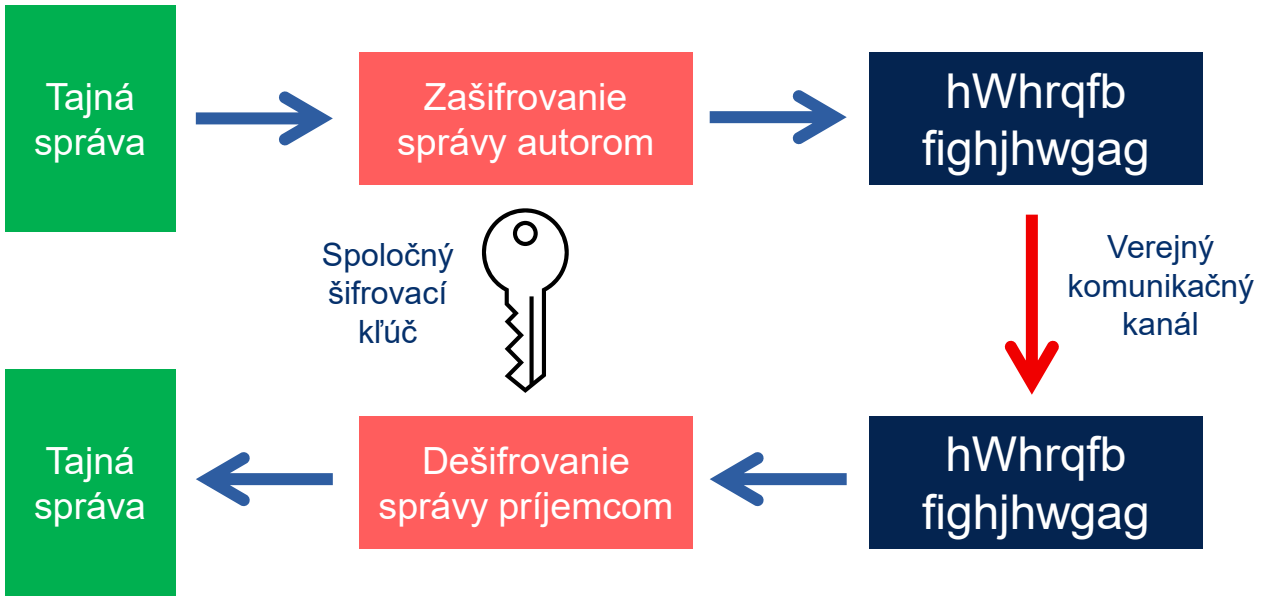
- **Príklad:** Ceasarova šifra = 2 sady abecedy, písmeno posunuté o 3 miesta (a->d), kľúčom bol počet miest v zmene

Ako sa heslá ukladajú a šifrujú

- Každá metóda šifrovania používa na šifrovanie a dešifrovanie správ špecifický algoritmus, ktorý sa nazýva **šifra.**
- **Šifra = séria dobre definovaných krokov na šifrovanie/dešifrovanie**
  - Transpozícia
    - Preusporiadanie písmen
  - Náhrada
    - Nahradenie písmen
  - Jednorazový blok
    - Čistý text v kombinácii s tajným kľúčom vytvorí nový znak, ktorý sa skombinuje s otvoreným textom

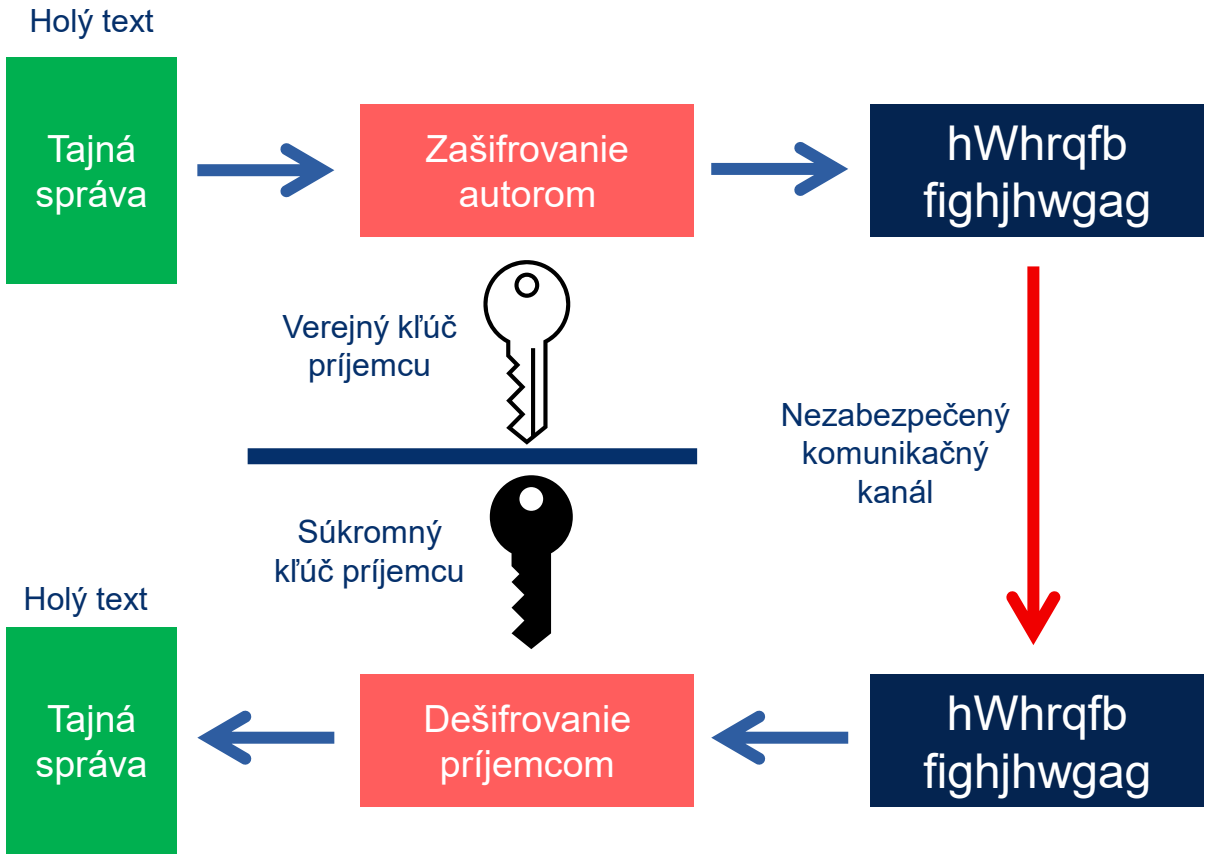
Ako sa heslá ukladajú a šifrujú

- Triedy šifrovacích algoritmov
  - **Symetrické algoritmy**
    - Šifrovanie a dešifrovanie na základe rovnakého vopred zdieľaného kľúča
    - Odosielateľ aj príjemca poznajú vopred zdieľaný kľúč skôr, ako začne akákoľvek šifrovaná komunikácia
    - Šifrovacie algoritmy, ktoré používajú spoločný kľúč, sú jednoduchšie a vyžadujú menej výpočtového výkonu



Ako sa heslá ukladajú a šifrujú

- Triedy šifrovacích algoritmov
  - **Asymetrické algoritmy**
    - Používajú jeden kľúč na šifrovanie údajov a iný kľúč na dešifrovanie údajov
    - Jeden kľúč je verejný a druhý súkromný
    - V systéme šifrovania s verejným kľúčom môže každá osoba zašifrovať správu pomocou verejného kľúča príjemcu a príjemca je jediný, kto ju môže dešifrovať pomocou svojho súkromného kľúča
    - Strany si vymieňajú zabezpečené správy bez toho, aby potrebovali vopred zdieľaný kľúč
    - Tieto algoritmy sú náročné na zdroje a ich vykonávanie je pomalšie



Ako sa heslá ukladajú a šifrujú

- **Rozdiel medzi symetrickým a asymetrickým šifrovaním**

Symetrické	Asymetrické
• Algoritmy zdieľaného tajného kľúča	• Algoritmy verejného kľúča
• 80 – 256 bitov	• 512 – 4 096 bitov
• Odosielateľ aj príjemca zdieľajú tajný kľúč	• Odosielateľ aj príjemca nezdieľajú tajný kľúč
• Algoritmy pomerne rýchle (jednoduché matematické operácie)	• Algoritmy pomalé (náročné výpočtové algoritmy)
• DES, 3DES, AES, IDEA, RC/2/4/5/6, Blowfish	• RSA, ElGamal, eliptické krivky, DH

Ako sa heslá ukladajú a šifrujú

- Ako zašifrovať svoje údaje:
  - Šifrovací softvér
  - Šifrovanie na úrovni disku
  - Šifrovaný cloud
  - Šifrovane emailov
  - Heslá a biometrické údaje
  - Zálohovanie šifrovaných údajov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako sa heslá ukladajú a šifrujú

- **Hashovanie (hashing)**
  - Proces, pri ktorom sa vstupné údaje (napríklad heslo alebo súbor) prevedú do jedinečného reťazca pevnej dĺžky, ktorý je reprezentáciou týchto údajov
    - Tento reťazec sa nazýva **hash**
    - Jednosmerný proces
      - Nie je možné získať pôvodné údaje zo získaného hash kódu.
      - Hashovanie sa používa v rôznych oblastiach, najmä v oblasti bezpečnosti, na ukladanie hesiel alebo na zabezpečenie integrity údajov
      - SHA-256 (Secure Hash Algorithm 256-bit) - Jeden z najbežnejších algoritmov na hashovanie
        - Napríklad na zabezpečenie hesiel v databázach
  - **Príklad:** Chceme zahashovať heslo: P@ssw0rd123
    Po aplikovaní algoritmu SHA-256 na tento text dostaneme výsledný hash:

6CB75F652A9B52798EE4D8F1B4C5E91B9B9B6AB6F1F4E0F60A5C2A0E4536D1F3

Ako sa heslá ukladajú a šifrujú

- **Vlastnosti hashovania**
  - Jednosmerné
    - Po získaní hash hodnoty nie je možné získať späť pôvodné heslo
  - Deterministické
    - Pre rovnaký vstup vždy dostaneme rovnaký hash
  - Rýchlosť
    - Algoritmus je navrhnutý tak, aby rýchlo generoval hash z akéhokoľvek vstupu
  - Neexistuje kolízia
    - Dobrý hashovací algoritmus má veľmi nízku pravdepodobnosť, že rôzne vstupy povedú k rovnakéj hash hodnote

Ako sa heslá ukladajú a šifrujú

- **Význam hashovania**
  - Bezpečnosť
    - Pri kompromitovaní databázy s heslami útočník získa hash hodnoty, nie samotné heslá
    - Bez použitia správneho algoritmu nie je možné získať pôvodné heslo z hash hodnoty
  - Rýchlosť
    - Hashovanie je efektívny spôsob, ako generovať jedinečné hodnoty pre rôzne vstupy a zabezpečiť údaje
- **Moderné algoritmy:**
  - Algoritmus Message Digest 5 (MD5)
    - Jednosmerná funkcia, ktorá uľahčuje výpočet hashu z daných vstupných údajov
    - Vytvára 128-bitovú hash hodnotu
  - Secure Hash Algorithm (SHA)
    - Algoritmus špecifikovaný v SHS
    - NIST publikoval SHS prvýkrát v 1994
    - SHA-2 má 4 funkcie (SHA-224; SHA-256; SHA-384; SHA-512)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako sa heslá ukladajú a šifrujú

- **Solenie (salting)**
  - Používa sa na zvýšenie bezpečnosti hashovaných hesiel a iných citlivých údajov, aby sa zabránilo niektorým typom útokov, ako je rainbow table útok alebo brute-force útok
  - Proces, pri ktorom sa pred hashovaním pridáva **náhodný reťazec znakov** k vstupnému heslu alebo iným údajom
    - Tento reťazec sa nazýva **soľ** a zaručuje, že aj rovnaké heslá budú mať rôzne hashe, pretože soľ je jedinečná pre každý používateľský účet
- **Príklad:** Chceme zahashovať heslo: P@ssw0rd123
  Solenie resp. generovanie soli: rAnD0mS0lt!
  Nové solené heslo: P@ssw0rd123rAnD0mS0lt!
- Po aplikovaní algoritmu SHA-256 na tento text dostaneme výsledný hash:

  a29da90931f834df13fd9528e8ccf5e28a7c2a8a1e6edd2922020413832a53b9

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako sa heslá ukladajú a šifrujú

- **Význam solenia**
  - **Zabraňuje útočníkovi použiť:**
    - Slovníkový útok
    - Použitie vyhľadávacích tabuliek
      - Ukladá vopred vypočítané hodnoty hash hesiel v slovníku hesiel
    - Použitie spätného vyhľadávania
      - Vyhľadávacia tabuľka vykreslí každý hash z hesla z databázy narušených účtov
    - Použitie Rainbow Tables
      - Menšia tabuľka, ktorá môže uložiť riešenia pre viac hashov na rovnakom priestore

Prehľad autentizačných metód

Jednokroková autentizácia, viacfaktorová autentizácia

- **Jednofaktorová autentifikácia (Single-Factor Authentication, SFA)**
  - Základný spôsob overovania identity používateľa
  - Na potvrdenie totožnosti používateľ poskytne len jeden faktor
  - Priebeh jednofaktorovej autentifikácie:
    - Používateľ zadá svoj identifikátor (napr. používateľské meno alebo e-mail)
    - Používateľ poskytne jeden autentifikačný faktor (napr. heslo alebo PIN)
    - Systém overí tento faktor
  - Príklady jednofaktorovej autentifikácie:
    - Prihlásenie do e-mailu - používateľské meno a heslo
    - Bankomat (ATM) prístup - PIN kód do bankomatu
    - Prihlásenie do webovej aplikácie - používateľské meno a heslo
  - **Výhody jednofaktorovej autentifikácie:**
    - Jednoduchosť - žiadne špeciálne zariadenia alebo technológie
    - Pohodlie - zapamätanie si iba jedného faktora
    - Rýchlosť prihlásenia - bez nutnosti ďalších krokov, stačí jeden faktor

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Jednokroková autentizácia, viacfaktorová autentizácia

- **Riziká jednofaktorovej autentifikácie**
  - Nízka úroveň bezpečnosti
    - Heslá môžu byť slabé, opakované alebo ľahko uhádnuteľné
    - V prípade získania hesla môže útočník pristúpiť k účtu bez ďalších obmedzení
  - Riziko krádeže alebo úniku údajov
    - Ak používateľovo heslo alebo PIN kód unikne alebo je ukradnuté, útočník môže získať úplný prístup k účtu bez ďalších ochranných vrstiev
  - Neexistujúce dodatočné vrstvy ochrany
    - Jednofaktorová autentifikácia neponúka ďalšiu vrstvu bezpečnosti
- V dnešnej dobe sa jednofaktorová autentifikácia považuje **za nedostatočnú** pre zabezpečenie dôležitých účtov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Jednokroková autentizácia, viacfaktorová autentizácia

- **Viacfaktorová autentifikácia (Multi-Factor Authentication, MFA)**
  - Bezpečnostný proces, ktorý vyžaduje od používateľa, aby poskytol dva alebo viac nezávislých faktorov na overenie svojej identity
  - Faktory v MFA:
    - Niečo, čo viete
    - Niečo, čo máte
    - Niečo, čo ste
  - Priebeh viacfaktorovej autentifikácie:
    - Prvý faktor (niečo, čo viete) – Používateľ zadá svoje heslo alebo PIN kód
    - Druhý faktor (niečo, čo máte alebo biometria) – Po zadaní hesla systém požaduje druhý faktor, ktorým môže byť: bezpečnostný kód, biometrické údaje, fyzické zariadenie
    - Overenie a prístup – Ak oba faktory (alebo viac) zodpovedajú správnym hodnotám, používateľovi sa umožní prístup k systému alebo účtu
  - **Výhody viacfaktorovej autentifikácie:**
    - Vyššia bezpečnosť
    - Ochrana pred krádežou hesla
    - Zlepšenie dôvery používateľov

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

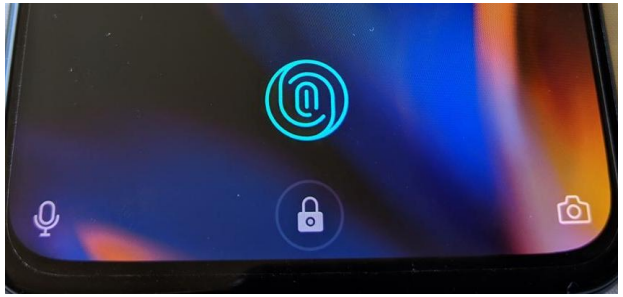
Jednokroková autentizácia, viacfaktorová autentizácia

- **Riziká viacfaktorovej autentifikácie**
  - Zložitosť pre používateľa
    - Prihlásenie bude trvať dlhšie a bude menej pohodlné
    - Problémy so zapamätaním si rôznych kódov alebo s prístupom k zariadeniam, ktoré sa používajú na získanie druhého faktora
  - Možné technické problémy
    - Problém prihlásiť sa do účtu v prípade straty zariadenia na generovanie kódov
    - Komplikácie pri obnove účtu pri strate / zabudnutí druhého faktora
  - Náklady a implementácia
    - Nákladná a časovo náročná implementácia, najmä pre menšie organizácie
    - Potreba ďalších bezpečnostných technológií
- Viacfaktorová autentifikácia (MFA) je silná bezpečnostná technika, ktorá výrazne zvyšuje ochranu účtov tým, že vyžaduje viacero nezávislých faktorov na overenie používateľa

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady viacfaktorovej autentizácie

- SMS verifikácia
- Biometrická autentifikácia
  - Odtlačok prsta pre odomknutie smartfónu
- Aplikácia v smartfóne
- Hardvérový token
  - Yubikey
- Čítačka karty
  - Tatra banka
- OTP – One time password



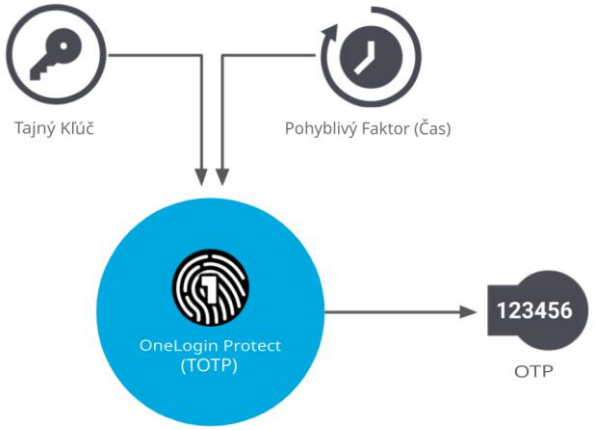
Vhodné kombinácie autentizačných faktorov

- Meno a heslo + OTP kód
- Meno a heslo + hardvérový bezpečnostný token USB
- Meno a heslo + hardvérový bezpečnostný token generujúci PIN
- Prihlasovacie ID + PIN + Mobilná aplikácia
- PIN + otlačok prsta + skenovanie tváre + vzorka hlasu

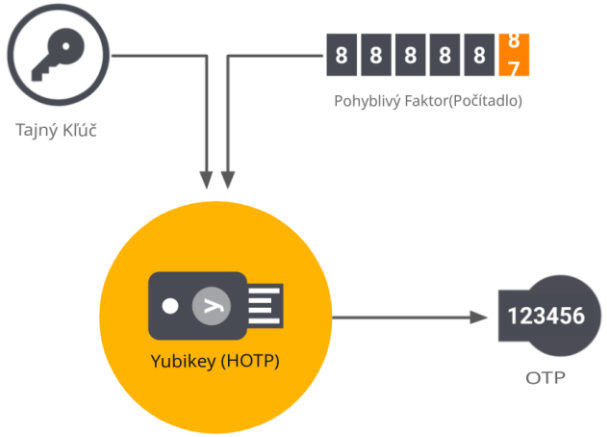
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aplikácie typu One Time Password

- One Time Password (OTP) – PIN, ktorý je použiteľný vždy len 1 raz
- Poznáme viaceré druhy:
  - **TOTP** (jednorázový PIN založený na tajnom kľúči a čase)
    - 6/8 miestny PIN, platný vždy len 30 sekúnd
    - každých 30 sekúnd nový PIN
    - Aplikácia, ktorá PIN vytvára je nainštalovaná v Smartfóne/PC
    - Zariadenie, na ktorom je autentifikačná aplikácia musí mať nastavený presný čas



  - **HOTP** (jednorázový PIN založený na tajnom kľúči a počítadle)
    - 6/8 miestny PIN, platný iba pre jeden pokus prihlásenia
    - počítadlo sa po každom vygenerovanom PINe zvýši
    - Po pokuse prihlásenia server tiež zvýši počítadlo
    - Po úspešnom prihlásení si aplikácia a server zosúladia počítadlo



Prehľad technológií a protokolov používaných v AAA (RADIUS, TACACS+)

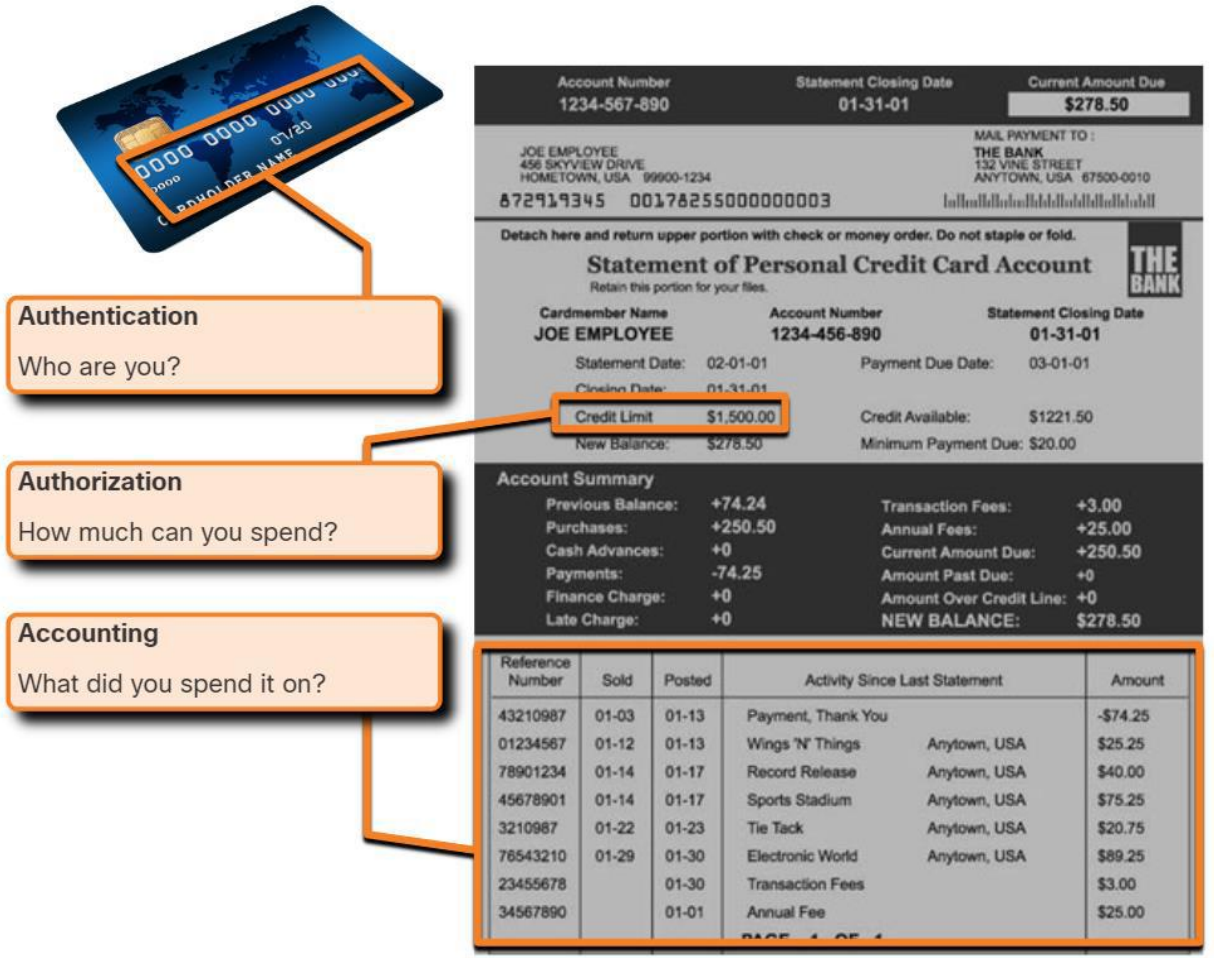
Riadenie prístupu

- Riadenie prístupu = Mechanizmus a politiky, ktoré regulujú, kto môže zobrazovať alebo používať zdroje v rámci informačného systému
  - Aplikujú sa selektívne obmedzenia pre každé miesto, zdroj alebo aktívum

- Kľúčové komponenty riadenia prístupu:
  - Authentication (Autentifikácia)
  - Authorization (Autorizácia)
  - Accounting (Účtovanie)

Prehľad mechanizmu AAA

- Zmysel AAA mechanizmu
  - Authentication (Autentifikácia)
    - Kto sa môže pripojiť k informačnému systému
    - Admini, zamestnanci, návštevníci...
  - Authorization (Authorization)
    - Aké práva sú pridelené prihláseným používateľom v IS
    - Možnosť čítania, zapisovania, vykonania zmien údajov v IS...
  - Accounting (Účtovanie)
    - História aktivity v IS
    - Kto/kedy/kde vykonal zmeny v IS



Authentication (Autentifikácia)

- **Autentifikácia =** overenie totožnosti na zabránenie neoprávnenému prístupu

- Zvyčajne dvojica prihlasovacie meno/ ID a :
  - Niečoho, čo používatelia poznajú
    - heslo, PIN,...
  - Niečo, čo používatelia majú:
    - Token, karta, prístupový čip...
  - Niečo, čím používatelia sú:
    - Biometria : odtlačky prstov, rysy tváre, DNA, hlas...

- Príklady:
  - **Single Sing-On (SSO) -** jednorazové prihlasovanie do viacerých systémov
  - Autentifikácia pomocou **Biometrie**
  - **Multi-faktorová autentifikácia**
  - **Protokoly:**
    - **Radius, Tacacs+, Kerberos, 802.1x...**

Authorization (Autorizácia)

- **Autorizácia =** Pridelenie práv konkrétnemu používateľskému účtu v rámci IS.

- Autorizácia hovorí o tom, aké úlohy môže vykonávať konkrétny používateľ v konkrétnom IS.:
  - **Admin ->** vykonávanie zmien v IS
  - **Bežný používateľ ->** povolenie na čítanie v IS, zamietnutý prístup k vykonávaniu zmien v rámci IS

- Príklady:
  - **ACL (Access Control List)** – zoznam príkazov na kontrolu prístupu
  - Viacero techník na riadenie prístupu: napr.: Riadenie prístupu na základe roly/atribútov v IS
  - **Protokoly:**
    - **Radius, Tacacs+**

Accouting (Účtovanie)

- **Účtovanie =** záznam o vykonaní aktivít prihláseným používateľom v IS

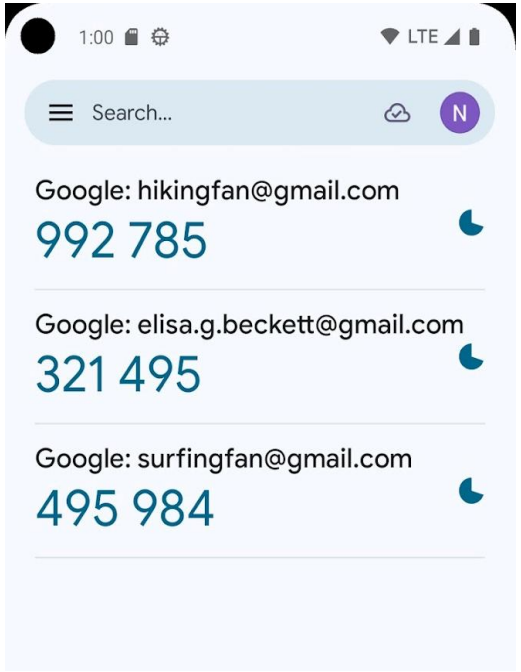
- Záznamy zvyčajne:
  - Kto vykonal činnosť v IS
  - Kedy vykonal činnosť v IS
  - Aké zmeny boli vykonané
  - Aký dlhý časový úsek strávil používateľ vykonávaním činnosti

- Príklady:
  - **SNMP** (Simple Network Management Protocol)
  - **Syslog**
  - **Protokoly:**
    - **Radius logging, Tacacs+, NetFlow...**

Nastavenie a testovanie autentizačných mechanizmov na príkladoch z verejnej správy

Príklad konfigurácie OTP autentifikátora na Android

1. Stiahnite z Obchodu Play aplikáciu Google Authenticator
2. Otvorte aplikáciu a vpravo dole vyberte voľbu "+" a vyberte možnosť naskenovať QR kód
3. Fotoaparátom zosnímajte QR kód
4. V aplikácii sa vám zobrazí položka "KIS_FRI_Skolenie: Vzorovy QR kod"
5. 6 miestny PIN sa zmení každých 30 sekúnd



Otvorená reflexia

Ktorý z nasledujúcich príkladov patrí medzi autentizačný faktor „niečo, čo viete“?

A) Odtlačok prsta

B) Smartfón

C) Heslo

D) USB token

Otvorená reflexia

Čo je slabé heslo podľa dokumentu?

A) P@ssw0rd2023!

B) 123456

C) H$kf92!kd

D) Fráza dlhšia ako 16 znakov

Otvorená reflexia

Ktoré tvrdenie o 2FA je pravdivé?

A) Vyžaduje iba jeden faktor na overenie

B) Vyžaduje dva nezávislé faktory

C) Používa sa iba pri bankových aplikáciách

D) Je nahradené biometrickými údajmi

Otvorená reflexia

Ktorá vlastnosť platí pre hashovaciu funkciu?

A) Reverzibilná

B) Jednosmerná

C) Dešifrovateľná

D) Používajú ju len banky

Otvorená reflexia

Čo je TOTP?

A) Jednorazové heslo založené na čase

B) Šifrovací algoritmus

C) Heslo typu biometria

D) Typ správy hesiel

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Techniky autentizácie a overovania

Identifikácia a autentizácia (Blok III)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

doc. Ing. Gabriel Koman, PhD.

KC KYB UNIZA, https://kc.uniza.sk

gabriel.koman@uniza.sk