Bevezetés a kiberbiztonságba - Biztonságtudatosság

Jelszavak kezelése

Bonifert Tamás

2023. 04. 13.

Tartalom

Jelszavakkal kapcsolatos tudnivalók

- Jelszavakkal, jelszó hash-ekkel kapcsolatos általános tudnivalók
- Biztonságos jelszótárolás
- Jelszó policyk
- Jelszófeltörési technikák
- Jelszómenedzser megoldások
- Alkalmazás hitelesítés

Milyen minőségű jelszavak használatosak?

80%

Jelszavakkal kapcsolatos megállapítások

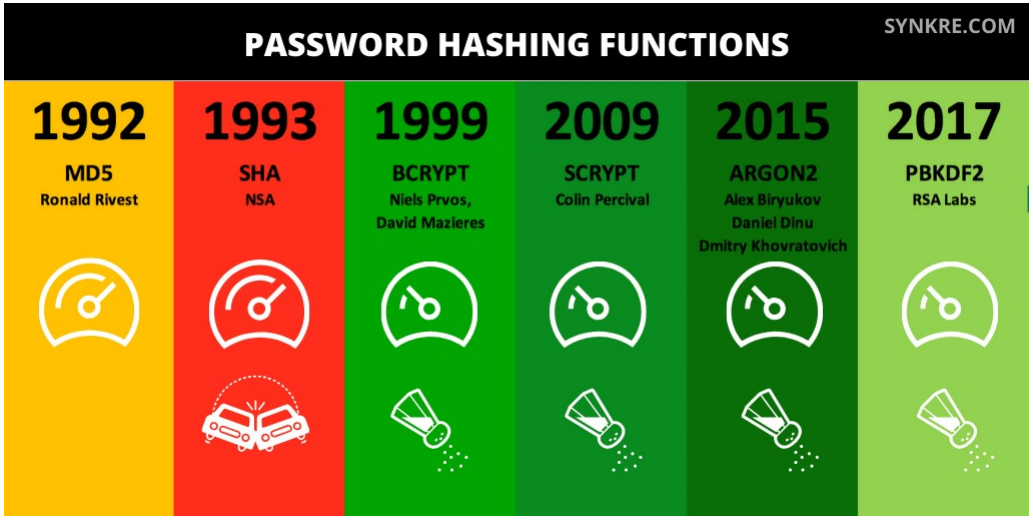
- A különböző vizsgálatok eredményei alapján rossz minőségű jelszavak használatosak
- Oktatás szerepe -> jelszóképzési technikák ismertetése
- Jelszavakra vonatkozó szabályok körültekintő kialakítása
- Üzemeltető állomány felelőssége
  - Jelszavakkal kapcsolatos operációs rendszer szintű beállítások
  - Kiemelt jogosultságok körültekintő használata
  - Jelszó blacklistek létrehozása
  - A technikai fejlődés figyelembe vétele

Jelszótárolás elvi lehetőségei

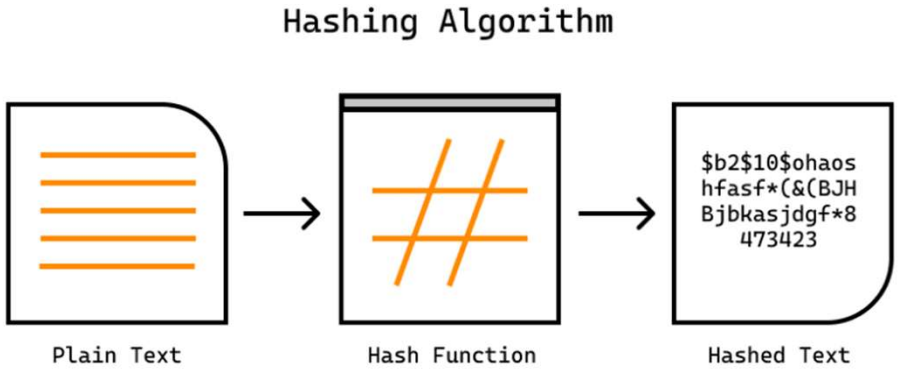
- Clear text 
- Titkosított jelszótárolás 
- Jelszóhash 

Hash algoritmusok fajtái

- Jelszavak hashelésére **nem** alkalmas függvények
  - MD5
  - SHA-1, SHA-256, SHA-512 stb.
- Jelszavak hashelésére szolgáló függvények
  - Bcrypt, Scrypt
  - Argon2, PBKDF2

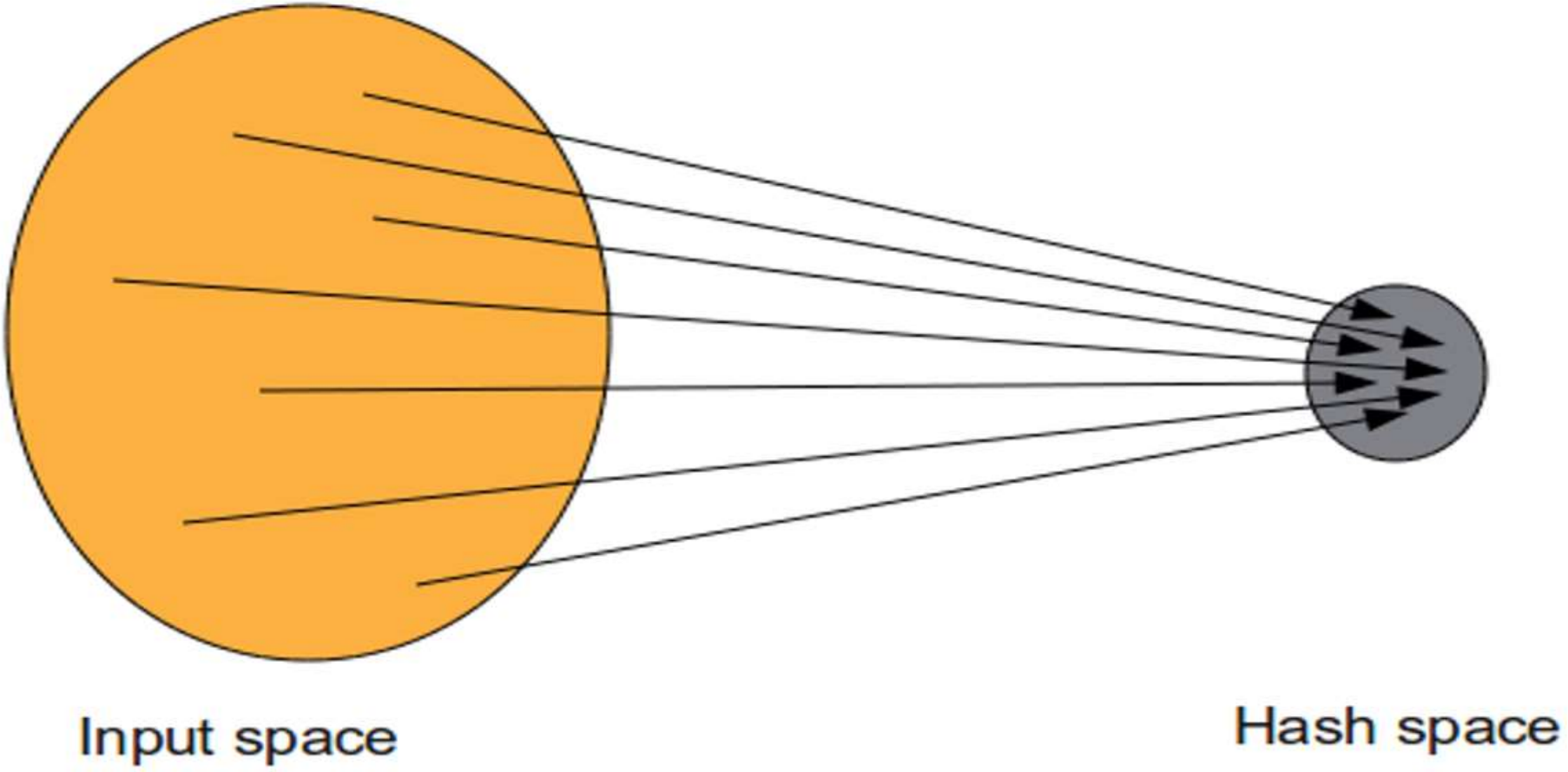


Hash algoritmusok jellemzői



- Egyirányú kódolási rutin
- Adott bemenetből mindig ugyanaz a kimenet képződik
- A kimeneti adat egyértelműen utal a bemeneti adatra…
- …de a kimeneti adatból nem állítható elő a bemeneti adat
- A bemeneti adat legkisebb változása teljesen más kimenetet eredményez

Hash értékkészlet jellemzői



Jelszó hash algoritmusok

- LM (Windows NT 1.0)
- NTLM v1 (Windows NT 3.1)
- NTLM v2 (Windows NT 4.0)
- KRB5TGS (Kerberos)

- B-crypt, S-crypt
- Argon2

Adaptív jelszóhash

Jelszóképzés szempontjai

- Ideális jelszóhossz
- Hosszú vs. összetett jelszó: melyik preferáljuk?
- Jelszavakra vonatkozó szabályok körültekintő kialakítása
- Jelszócsere: az új jelszó ne hasonlítson az előző jelszóra!
- Divatos jelszóképzési technikák: valóban biztonságos?
  - Budapest12 -> Bud@p$st12
- Feketelisták jelentősége
- Kódmondaton alapuló jelszavak
  - Afm100%iv

Hosszú vs. összetett jelszó

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Eltúlzott biztonsági beállítások következményei

-Kérem, adja meg jelszavát!
alma
-Sajnálom, a jelszónak legalább 8 karakterből kell állnia.
-reszelt alma
-Sajnálom, a jelszónak tartalmaznia kell legalább egy számot.
-50reszeltalma
-Sajnálom, a jelszónak legalább egy nagybetűt kell tartalmaznia.
-50KIBASZOTTreszeltalma
-Sajnálom, a jelszóban nem követhetik egymást nagybetűk.
-50Kibaszott,ReszeltAlma,FeldugvaAseggedbe!
-Sajnálom, a jelszó nem tartalmazhat írásjeleket.
-50KibaszottReszeltAlmaRohaggymegHaNemFogadodElEztSe
-Sajnálom, a jelszó már foglalt.

Biztonsági problémák a gyakorlatban

- Legacy rendszereknél alapértelmezett lehet az NTLM v1
- A jelszóhash-ek sok esetben megszerezhetők (hálózati forgalom, lokál gép)
- 8 karakteres jelszó egy közepes vga-val akár 350 milliárd (!) hash legenerálható
- … azaz egy 8 karakter hosszúságú, bármilyen bonyolultságú jelszó 5-6 óra alatt törhető, ha megvan a hash

Jelszóházirend beállítások

- Enforce password history: >24
- Maximum password age: >360
- Minimum password age: 1 day
- Minimum password lenght: >12
- Password must meet complexity: Enabled (?)
- Store password using reversible encryption: Disabled

Password manager programok jellemzői

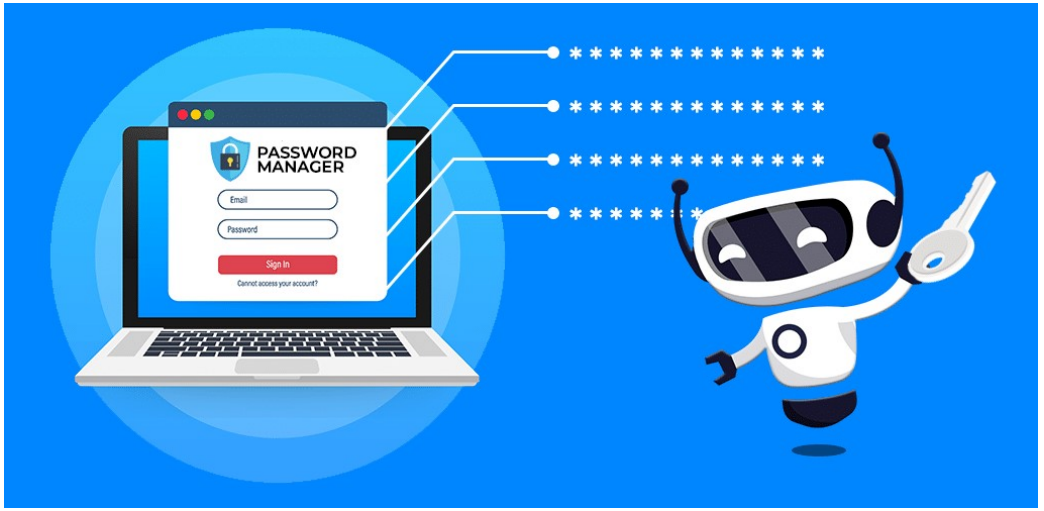
- Automatikus (biztonságos) jelszóképzés
- Jelszavak titkosított adatbázisban történő tárolása
- Mesterjelszóval történő (akár automatizált) hozzáférés a jelszavakhoz
- Lehet felhős vagy lokális tárolású megvalósítás is

Követelmények

- Jelszó adatbázis és mesterjelszó erős algoritmussal történő titkosítása (AES-256 stb.)
- Gyártói támogatás (sérülékenység menedzsment)
- Biztonsági mentés lehetősége
- Kétfaktoros hitelesítés
- Felhős változat esetén:
  - Zero-knowledge architektúra
  - Local only encryption/decryption

Ajánlott password manager alkalmazások

- 1Password
- KeePass
- Dashlane
- LastPass
- Syspass



- Különböző PAM megoldások (pl. Thycotic, Thalos)

KÖSZÖNÖM A FIGYELMET!

Kérdések?