Jelszóbiztonság statisztika szinopszis

Előző napokban került a kezembe egy fiktív adatbázis. Az adatbázisban közel 55ezer felhasználó adatai találhatóak meg.
Készítettem egy kisebb statisztikát a felhasználók jelszavairól, elég meglepő eredmények jöttek ki.

Az 55ezer felhasználóból:
közel 51 000 jelszó sikerült megfejteni és 3 500db maradt máig ismeretlen.

Kis érdekesség:
Az adatbázisban közel 27 000 nő és 28 000 férfi adatai található. Szóval a jelszavak eloszlása valószínűleg hasonló.

Kis kitérő a jelszavak titkosításáról és törhetőségéről. A jelszavak saltolva (sózva) voltak a felhasználónevekkel, ami lassítja a törést, viszont a maximum hosszúság 8karakter, a minimum 3 volt. A titkosítás case-insensitive, vagyis nem számítanak különbségnek a kis és nagybetűk.
A karakterkészlet körülbelül a következőkből épült fel: [a-z0-9_] plusz ékezetes betűk. A törés sebességének tudatában könnyen kiszámolhatjuk, hogy egy jelszó lehetőségeinek száma 3nap alatt elfogy, vagyis a maximális törési idő jelszavanként maximálisan 3nap!

Törésre fordított idő: 147 nap
Használt processzor: Intel Pentium 4 (3Ghz)

Ez az idő 49 bonyolult (végletekig elbújt terület a kulcstérben) jelszóra lenne elegendő idő, ehelyett 51 000darabot sikerült megfejteni, 1041x-szer többet, már itt érezhető a jelszavak gyengesége.

A jelszavak kiosztásakor egy analógiát követtek azok akik ezt megtették. Ezek a jelszavak felhasználónévre megbecsülhetők adatbázis tartalma alapján.
Az adatbázis 34 500 default jelszót tartalmazott.

Leggyakrabban használt jelszavak:

Összesített nemek (24db):

111111	80
12345	80
(cenzúrázott)	43
macika	36
123456	35
020101	32
attila	31
eszter	30
anita	28
jelszo	26
55555	25
viktor	24

Férfiak (12db):

111111	75
12345	49
020101	27
123456	22
(cenzúrázott)	22
jelszo	15
attila	14
tomika	13
55555	13
(cenzúrázott)	13
zolika	12
lacika	12

Nők (12db):

macika	33
eszter	22
(cenzúrázott)	21
12345	21
tigris	19
csillag	19
marci	19
macska	18
anita	18
attila	17
judit	17
nyuszi	17

kicsim	24
tigris	24
marci	23
petike	23
macska	23
nyuzsi	22
judit	22
gabor	21
csillag	21
cicus	21
zolika	21
lacika	21

Jelszavak karakterszám szerinti eloszlása:
1-4 karakter hosszan 0db
5karakteres hosszúságú: 4481db
6karakteres hosszúságú: 5028db
7karakteres hosszúságú: 2658db
8karakteres hosszúságú:2797db

Csak angol abc karaktereit tartalmazó jelszavak: 11284db
Jelszavak amik tartalmaznak számokat és betűket egyaránt (alfanumerikus): 1313db

A töretlen jelszavak vagy egy ~150nap alatt el nem ért kulcstérbe tartoznak, vagy olyan karaktereket tartalmaznak, amiket nem tartalmazott a karakterkészlet.
Konklúzióként levonhatjuk, hogy 20% használ maximális hosszúságú jelszavakat, közel 33% gyengébb 6karaktereseket. 80% nem szereti a számokat a jelszavukba. 10% próbált meg valamelyest biztonságosabb jelszót választani.
Sajnos a kriptofüggvény ismeretében kijelenthetem, hogy jelen esetben nincs ésszerű biztoságos jelszó választás, mivel azok a karakterek amiket nem használunk a törési karakterkészletben, azok a karakterkódolási táblákban változhatnak, szóval számítógép- és számítógép, operációsrendszer- és operációsrendszer között eltérhet, ezért nem ajánlott átlagos felhasználók által való használatra.

Javaslat:

Erősebb kriptográfiai algoritmus alkalmazása - jelenlegi jelszavak csak egy erősebb (lasabb és case-sensitive) algoritmus mellett lennének biztonságosabbak.

vagy

Megint csak algoritmikus változtatás és a jelszavak hosszabbítása minimum 12karakterre.

Bucsay Balázs – http://www.rycon.hu – earthquake[at]rycon[dot]hu