JELSZAVAKRÓL – IPARÁGI LEGROSSZABB GYAKORLATOK

PASSWORDS – WORST PRACTICES IN USER AUTHENTICATION

KESZTHELYI ANDRÁS LÁSZLÓ egyetemi docens
Óbudai Egyetem Keleti Károly Gazdasági Kar

Abstract

Our age may well be called as the age of cyber crime, so our need for security has become very important. In information security one of the main fields is user authentication, including the use of passwords, which is the oldest method. Analysing the password related security incidents of the near past and investigating the different password related rules of different companies we find an alarming situation: as if only bad and worse practices existed. Re-thinking some old rules seems to be carved in stone we can find simple and efficient solutions for handling passwords both on user and system administrator side.

1. Bevezetés

A felhasználók gépi azonosításának eljárásai három fő csoportba sorolhatók: a tudás és a birtoklás alapú eljárások mellett napjainkra a biometrikus eljárások is jelentősen elterjedőben vannak. Különféle helyzetekben más-más fajta eljárások lehetnek a legmegfelelőbbek, nem lehet általános érvényű rangsort felállítani. Van azonban néhány – általános – szempont, amit érdemes szem előtt tartani, mint például a programbonyolultság, az ár, a döntés bizonyossága.

A tudás alapú eljárások alapvetően és nagyjából ingyenesnek tekinthetők, amennyiben általában semmilyen kiegészítő eszközre az amúgy is meglévőeken túl nincs szükség. A birtoklás alapú eljárásoknál felhasználónként külön birtokolandó eszközre van szükség és belépési pontonként egy vagy – az átbocsátóképesség elvárt szintjétől függően – több eszközolvasóra. A biometrikus eljárások esetében pedig a biometrikus jegyet olvasó eszközre van szükség.

A tudás és a birtoklás alapú eljárások esetében a programbonyolultság, ebből fakadóan a hibavalószínűség csekély: az egyszerű keresés tételének alkalmazására, vagy nagyobb felhasználószám esetén egyszerű adatbázis select műveletre van szükség. A biometrikus eljárások esetében azonban a leolvasott biometrikus jellemző feldolgozása meglehetősen bonyolult eljárás, olyannyira, hogy itt jelenik meg a fals pozitív és a fals negatív gyakoriság érték (FAR, FRR), mint a megvalósítás minőségét jellemző két mutatószám.

A fentiek alapján feltehetjük, hogy a jelszavak használata, mint egyszerű, biztos és igen olcsó azonosítási eljárás még sokáig fennmarad. Mivel nagyon régi, kiforrott eljárás, kimondottan furcsa, hogy napjainkban is számos téveszme és hibás gyakorlat van forgalomban a tudás alapú azonosítási eljárásokkal (jelszavakkal) kapcsolatban. Érdemes ezek közül néhány kirívót alaposabban szemügyre venni és átértékelni, különösen a közelmúlt néhány, jelszavakat is valamilyen módon érintő biztonsági incidenseinek, illetve általánosan hirdetett téves rendszabályok kapcsán, messze nem a teljesség igényével.

2. Jelszavakat is érintő biztonsági incidensek

A közelmúlt néhány év során számos olyan biztonsági incidens vált ismertté, amelyek valamilyen módon jelszavakkal voltak kapcsolatban, összefüggésben.

A Websense arról írt már 2011-ben, hogy szerintük a kérdés nem az, hogy bekövetkezik-e, hanem az, hogy mikor történik meg a mi vállalatunk ellen is a sikeres támadás. 2011 márciusában 40 millió RSA-felhasználó, ugyanezen év áprilisában 20 millió Google-felhasználó, májusban pedig 100 millió Sony-felhasználó adatait lopták el (és ez csak a jéghegy csúcsa). Nagy mennyiségű, valódi felhasználói adat, ténylegesen használt jelszó nyilvánosságra kerülésének az egyik következménye, hogy a jelszóválasztási szokások elemezhetők, meghatározhatók a tipikus jelszófajták, jelszószerkezetek, ez pedig jelentősen elősegítheti a hatékony jelszótörést.[1] Ezen esetekben a jelszavak napvilágra kerülése járulékos következmény, az incidens bekövetkezése maga független a jelszavak helyes vagy helytelen használatától, illetve kezelésétől.

2013-ban az Adobe mintegy 150 millió felhasználójának az adatait lopták el, és a teljes jelszóállományt sikerült megfejteniük a támadóknak, ugyanis az Adobe „sózott árnyékjelszavak" helyett közönségesen titkosítotva tárolta a felhasználók jelszavait.[2] Hogy, hogy nem, a támadóknak sikerült megfejteniük az ellopott jelszóadatbázis titkosítását. A Telenor, pontosabban az online.telenor.hu ugyancsak tárolja a felhasználók jelszavait visszaállítható formában. A szerző saját tapasztalata, 2014 áprilisában sikertelen bejelentkezési kísérleteket követően az „elfelejtett jelszó" lehetőséggel élve a telenor.hu közönséges emilben elküldte az igazi, eredeti jelszót. Ez előrevetíti, hogy egy (közel)jövőbeli sikeres támadás következtében a telenor.hu felhasználói adatai – ide értve a visszafejthető módon tárolt jelszavakat is – illetéktelen kezekbe, illetve napvilágra kerülhetnek. Üzemeltetői oldalon a felhasználói jelszavaknak bármilyen visszaállítható formában való tárolása súlyos felelőtlenség.

2008-ban Barack Obama, az Amerikai Egyesült Államok elnökének feltörték a twitterfiókját. A sikeres támadó, egy francia férfi azt a módszert alkalmazta, hogy nyilvános forrásból összegyűjtötte a személyhez kapcsolódó jelszó-lehetőségeket (pl. születési dátum), és ezeket rendre kipróbálta, ez esetben sikerrel.[3] Pár évvel előbb egy munkanélküli francia férfi a francia központi bank hitelezési rendszerébe lépett be – véletlenül – az 123456 jelszó megadásával.[4] Ezen példák – és a sort lehetne folytatni – esetében a felhasználó felelőssége állapítható meg: túl kézenfekvő jelszót használt, és ez tette lehetővé a sikeres támadást.

3. Elméleti háttér

A felhasználók jelszavas azonosításának már a kezdetén rájöttek[5] arra, hogy a felhasználók jelszavait nem szabad tárolni, mert ha bárki, bármilyen okból és módon hozzáfér ezekhez, akkor onnantól bármely felhasználót megszemélyesítheti minden további nehézség nélkül. Ezt úgy lehet megnehezíteni, hogy a jelszó helyett annak egy lenyomatát (hash) tárolják. Ezt a lenyomatot, az árnyékjelszót (shadow passoword) egy olyan függvény állítja elő, amelyiknek nincs inverze.

Ha tehát egy támadó sikeresen hozzáfér is az árnyékjelszavakhoz, akkor sem tudja ezekből visszafejteni az eredeti jelszavakat. Egyetlen dolgot tehet: egyenként veszi a legvalószínűbb jelszavakat, kiszámítja a lenyomatukat, és ellenőrzi, hogy azonos-e valamelyik ellopott lenyomattal. Ha igen, akkor sikeresen megtalálta az adott lenyomathoz tartozó jelszót.

Lássuk, milyen lehetőségei vannak a támadónak a jelszó megtippelésre, kitalálására. A biztos eljárás a nyers erő módszere, azaz ha kipróbál minden lehetséges karaktersorozatot, mert ebben az esetben egészen bizonyosan meg fogja találni a jelszót – a kérdés csak az, hogy mennyi idő alatt. A felhasználó kellően körültekintő jelszóválasztása és az üzemeltető gondossága esetén ez az időigény reménytelen, világegyetemünk életkorának a sokszorosa is lehet. Minden más eljárás ehhez képest jelentősen egyszerűsítheti és megkönnyítheti a támadó dolgát, ezen esetekben azonban a felhasználónak fokozott felelőssége van nem elég körültekintő jelszóválasztása okán.

Így tehát a leggyakoribb jelszavak kipróbálásával fogja kezdeni a támadó, mint pl. asdfgh, 123456 stb.

A következő lépésben a felhasználó személyéhez köthető jelszavakat érdemes kipróbálni (születési dátum, kedvenc színész(nő) neve stb.), majd a felhasználói név egyszerű toldalékolásait (admin – admin, admin – admin12 stb.), legvégül pedig érdemes lehet jelentésbeli kapcsolatot feltételezni (mehemed – soselátotttehenet) és kipróbálni.

Ha ezen próbálkozások – és eddig néhány száz próbálkozásról lehet szó – nem vezettek eredményre, akkor lépésenként egyre nagyobb és bővebb szótárak szóállományát kell végigpróbálni – ez elérheti a tízezres nagyságrendet is.

Ezután még a továbbfejlesztett szótár alapú támadás következhet, amikor a szótári alapszavak egyszerű toldalékolásait is kipróbálja. Ezen a ponton segíthet sokat a már ismertté vált nagy tömegű jelszavak szerkezeti elemzése és a leggyakoribb szerkezettípusok meghatározása. A rockyou.com napvilágra került jelszavainak szerkezeti elemzése azt mutatta, hogy a leggyakoribb jelszavak a 8, 6 és 7 kisbetűből állóak, és ezek együttesen a 32 milliós jelszóállomány mintegy 13%-át teszik ki.[6]

Mindebből következik, hogy ha a felhasználó olyan jelszót választott magának, amit a támadó meg tudott találni a nyers erő módszerét megelőző, lényegesen könnyebb találgatási módszerekkel, akkor a felhasználó nem elég körültekintően járt el. Következik mindebből az is, hogy a jelszóválasztáskor ezek szem előtt tartásával a jelszót úgy kell megválasztani, hogy a nyers erő módszerének is kellő ideig ellenálljon.

Ezen a ponton igen fontos megállapítani, hogy ha a támadónak bármilyen többletismerete van egy jelszóról, az alapvetően befolyásolhatja a törési kísérlet sikerességét. Az alábbiakban ismertetendő hibás gyakorlatok egyben ezt is példázzák.

4. Téveszmék és hibás gyakorlatok

A jelszavak használatával kapcsolatos – felhasználói és üzemeltetői – háttér elméletileg tiszta, világos és egyszerű. Az elmúlt évtizedekben azonban végbementek olyan változások, amelyek nem hagyhatók figyelmen kívül, legelsősorban is a reálisan rendelkezésre álló számítási teljesítmény korábban hihetetlen mértékű megnövekedése. Emiatt egyes, régi szabályokat célszerű pontosítani és az új helyzethez igazítani. Emellett azonban – ismeretlen okból és ismeretlen módon – általánosan elterjedté vált néhány téveszme, továbbá igen tekintélyes forrásokban látott napvilágot néhány nyilvánvalóan hibás elgondolás, melyeket ezen források követendő szabályként javasolnak. Lássunk ezek közül néhányat az alábbiakban.

A legelsőként említendő, hogy szinte mindenhol – Gmail, Twitter, Google, OTP stb. – a legfontosabb követelményként a jelszó vegyes összetételét követelik meg (legyen benne kis- és nagybetű, számjegy, írásjel és egyéb jel, vagy ezek közül legalább háromféle).[7,8,9,10,11,12] Ez önmagában persze nem ártalmas, de elég kevéssé segíti elő a nyers erőnek kellően ellenálló jelszó választását.

Hogyan lehet kiszámolni a nyers erő alkalmazása esetén az időigényt? Egyszerűen: a kipróbálandó karakterkombinációk számát osztani kell az időegység alatt elvégezhető próbák számával.

Az előbbi értelemszerűen a lehetséges karakterek darabszámának a hatványa annyiadik kitevőn, ahány jelből áll a jelszó. Az utóbbi, a törési sebesség két tényezőtől függ: az árnyékjelszó képzéséhez használt hash függvény számításigényétől és a rendelkezésre álló számítási teljesítménytől. 2012 végén Jeremi Gosney 25 db AMD Radeon videokártya alkalmazásával NTLM hash esetén 348 milliárd próba/másodperc sebességet tudott elérni. Ezt alapul véve a törési sebességet feltételezzük legalább 10^{12} próba/másodpercnek (a biztonság irányába hibázzunk). Ha az üzemeltető bcrypt hash függvényt alkalmazna (de felhasználóként ebben nem lehetünk biztosak), abban az esetben ez a sebesség csak kb. 72 000 próba/másodperc lenne, tehát még jóval biztonságosabb lesz a nagyobb törési sebességre méretezett jelszó.

A jelszó összetételében a normál billentyűzeten könnyen elérhető karaktereket (kis- és nagybetűk, számjegyek, írásjelek és egyéb jelek) szerepeltethetjük, ezek száma kb. 80. Ha a jelszó hossza 8, akkor a kipróbálandó karakterkombinációk száma $80^8 \sim 10^{15}$ db. Ez azt jelenti, hogy egy 15 jegyű szám, amely csak a tízféle számjegyből áll, ugyanolyan erősségű, mint a 8 hosszúságú, nyolcvanféle jelből álló jelszavak. Evvel megdőlt az az állítás, hogy a jelszó jóságát vegyes összetétel határozná meg.

A törési időigény $80^8 / 10^{12} = 1.678$ másodperc, szűk fél óra. Ha a választható karakterkészlet számosságát egynegyedével növeljük, 80-ról 100-ra, akkor az időigény szűk három órára növekszik. Ha ellenben maradunk a nyolcvanféle karakternél, de a hosszúságot növeljük, ugyancsak negyedével, 8-ról 10-re, akkor viszont már négy hónapra (!) nő az időigény. Ebből az következik, hogy a jelszó hossza sokkal fontosabb, mint az összetétel vegyessége, hiszen az exponenciális függvény „sokkal gyorsabban" növekszik a hatványfüggvénynél (80^x vs. x^8).

A Hewlett-Packard 2003-ban jelentetett meg egy programot, amely mindmáig elérhető a honlapjukon, és azt állítja, hogy gyönge jelszavakból erős jelszót tud csinálni.[13] Az itt alkalmazott és javasolt eljárás a következő: a program egy nagyon egyszerű jelszót összefűz a kiszolgáló nevével (pl. asdfgh + gmail.com), majd abból MD5 hash-t számol, nyomtatható karakterekre konvertálja (base64 eljárással), majd levágja 12 jel hosszúságúra. Így vegyes összetételű, véletlenszerűnek látszó jelszó keletkezik, a felhasználónak ellenben mégis elég nagyon egyszerű, önmagában nyilvánvalóan alkalmatlan jelszót megjegyeznie. Csakhogy ha a támadó feltételezi, vagy felteheti, hogy a célszemély ezt a programot alkalmazza – látta a gépén –, akkor nyilván nem a 12 karakter hosszú, vegyes összetételű jelszavakat fogja nyers erővel próbálgatni, hanem a néhány száz legvalószínűbb és legegyszerűbb jelszóval (és a domain névvel) fog játszadozni, éspedig jó eséllyel pillanatok alatt sikeresen.

A HVG idén nyáron közölt egy írást „Próbálja ki: így csinálhat 1 perc alatt könnyen megjegyezhető jelszót, amit senki nem fog kitalálni" címmel. Ebben a cikkben a Stanford Egyetem informatikusait idézi, hogy: „A legbiztosabb módszer tehát, és erre biztatják most a felhasználókat a Stanford Egyetem biztonsági szakértői is, ha néhány egymástól teljesen független kifejezést választunk jelszónak, ezt mutatja a fenti ábra is, ahol a felhasználó jelszava a «narancs sas kulcs cipő»."[14] Sajnos a Stanford, a világ tíz legjobb egyetemének egyike, tényleg ezt javasolja a hallgatóinak.[15] Csakhogy!

Ha az így gyártott 22 karakteres, csupa kisbetűs jelszót nyers erővel törjük, a becsült időigény $\sim 4*10^{13}$ év lenne. De ha egy támadó a fejébe veszi, hogy a Stanford felhasználóinak bejelentkezéseit fogja törni, feltételezheti, hogy a felhasználók számottevő hányada megfogadja az egyetem tanácsát, és így készíti a saját jelszavát. Épp ezért nem a 20 karak-

ter és még hosszabb jelszavak amúgy is reménytelen törését fogja megkísérelni, hanem abból indul ki, hogy a jelszó 4 egyszerű szótári szó összetétele lehet. Kétezer szavas alapszótárt feltételezve a lehetséges négyszavas összetételek száma $2000^4 = 16*10^{12}$, a törés időigénye tehát pontosan 16 másodperc az árnyékjelszó birtokában. És ha a felhasználó különlegesen választékos, tízezres szókincsből választja a négy szót, a törési időigény akkor is csak szűk három óra lenne...

Szokták javasolni a kedvenc vers kezdőbetűiből különféle cserékkel és továbbképzésekkel való jelszógyártást is, de ezek általában túl bonyolult eljárások, ezért megjegyzésük és alkalmazásuk nehézkes.

Üzemeltetői oldalon rendszeresen előforduló hiba a felhasználókat arra kényszeríteni, hogy aránylag rövid időközönként változtassák meg jelszavaikat akkor is, ha semmilyen gyanús körülmény nem merült föl. Bruce Schneier szerint ez azonban arra fogja késztetni a felhasználókat, hogy könnyen megjegyezhető jelszavakat válasszanak (jelszavam_jan, jelszavam_feb...), amelyek egyúttal könnyebben megtippelhetők is lesznek. Lássuk be, hogy általános esetben, ha egy támadónak sikerül megszereznie a hozzáférést valamely jelszóval védett erőforráshoz, akkor azt azonnal birtokba veszi (kiüríti a bankszámlát). Ha viszont a támadó szeretné feltűnés nélkül, a jogos felhasználóval párhuzamosan használni az erőforrást (kémkedni a helyi hálózaton), akkor a – bárhogyan – megszerzett jelszó birtokában rangemelést fog végrehajtani, hátsó kaput létrehozni a rendszerben a saját céljaira. Azaz általános esetben nincs sok értelme a jelszó időnkénti megváltoztatásának, ellenben biztonsági incidens gyanúja esetén azt azonnal szükséges megtenni.[16]

5. Legjobb gyakorlat

A fentiek alapján aránylag könnyű megfogalmazni, mi (lenne) a legjobb gyakorlat mind a felhasználó, mind az üzemeltető oldalán. Legelsősorban is a fentebb – nem a teljesség igényével – említett hibák kiküszöbölése.

A felhasználó tehát úgy válasszon jelszót, hogy az csak nyers erővel legyen törhető, ha pedig a jelszava elég hosszú, akkor ez reménytelen vállalkozás. Fontos, hogy a jelszavait meg is tudja jegyezni. Célszerű tehát valamilyen nem szokványos eljárást választani a jelszó előállítására, például két-három szó (esetleg különböző nyelvekből) legalább három helyen toldalékolva megnyugtatóan jó eljárásnak látszik: 1848TalpraIIImagyar15!!, 2martinies_dry_drei! A hossz legyen legalább 16-20 karakter hosszúságú, minél hosszabb, annál jobb.

Értelemszerűen nem szabad ugyanazt a jelszót több fontos helyen használni.

A fentiek maradéktalan betartása sem ér semmit, ha gépünkre billentyűnaplózót sikerült tennie a támadónak (hardveres vagy szoftveres), vagy az álmennyezetbe mini kamerát, esetleg mi magunk adjuk meg egy adathalász emilben küldött link végén lévő ál-oldalon...

Az üzemeltető oldalán a következőkre célszerű figyelemmel lenni:

Jelszót tárolni semmilyen visszafejthető formában nem szabad, ez kirívóan súlyos üzemeltetési felelőtlenség. Az árnyékjelszó előállításához használt hash függvény legyen számításigényes: ha egy támadónak sikerült valahogyan megszereznie az árnyékjelszavakat, nagyon nem mindegy, hogy másodpercenként 10^{12}, vagy 10^4 próbát tud csinálni a reálisan elérhető számítási teljesítménnyel.[17,18]

Amikor a felhasználó jelszót választ, az új jelszót célszerű ellenőrizni a leggyakoribb jelszavak és egyszerű toldalékolásaik feketelistája alapján, és az ilyen, túl egyszerű jelszavakat elutasítani.

Tovább fokozza a biztonságot, ha a jelszavakat a lenyomat kiszámolása előtt „sózzák”, azaz toldalékolják egy egyedi szövegelemmel, például a felhasználónévvel. Ez azt eredményezi, hogy a különböző felhasználók esetleg azonos jelszavainak a lenyomatai különbözőek lesznek – ennek nagy felhasználói létszám esetén van jelentősége, mert így a támadó egyszerre csak egyetlen jelszót fog tudni megfejteni.

Általánosságban, túllépve a felhasználó és az üzemeltető technikai szintű lehetőségein a kockázatkezelés jelentőségét kell hangsúlyoznunk.[19] Továbblépve az oktatás fontosságát és jelentőségét emelhetjük ki, különösen annak fényében, hogy hazánkban – de Közép-Európában is – a diákok tudásszintje ezen a területen (is) riasztó állapotokat mutat.[20,21] Figyelembe véve, hogy korunk ifjúsága alkotja a Z-generációt, hétköznapi életük szerves része a digitális/virtuális világba való tartozás, a folyamatos ott időzés, a kapcsolattartás – többnyire mobil eszközök segítségével –, számukra kiemelkedően fontos (lenne) az információbiztonság, elsődlegesen a magánszféra védelme szempontjából, azaz közvetlen, személyes érintettség okán, ennek ellenére a helyzet messze van az ideálistól.[22]

S hogy mit hoz a jövő, még gyorsabb és még olcsóbb processzorokat, vagy akár a kvantumszámítógépet, ki tudja? Mivel mindennapi életünk során valamennyien egyre jobban függünk a digitális és/vagy virtuális világtól, mivel korunk egyre inkább a netbűnözés kora is, nem elégedhetünk meg avval, ha – úgy, ahogy – ismerjük a jelenleg érvényes szabályokat, mert ha holnap nem, holnaputánra már változhatnak. A magabiztos és aktív alkalmazkodás az egyre újabb kihívásokhoz nem képzelhető el a folyamatos tanulás és továbbképzés nélkül, sőt: a biztonság több, mint megtanulandó tananyag, a kultúra részévé kell válnia.[23] Különben végünk.

Jegyzetek

1. It is no longer a question of ’if’ but ’when’! Websense, 2011. 05. 24. http://view.websense-email.com/view_email.aspx?j=fe5815727d6200787d11&m=fefc1177756502&ls=fdf01078716c077d7713737d&l=fec117787c66057a&s=fe2111757c620c78761170&jb=ffcf14&ju=fe2d157274640675721079&cmpid=Emerging-No-longer-a-Q-Prosp-24May11&wsid=0032000000NsbQ6AAJ&linkid=View+as+a+Web+Page
2. Ducklin, P. Anatomy of a password disaster – Adobe’s giant-sized cryptographic blunder http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/
3. Mesquita, R. Frenchman convicted for hacking Obama’s Twitter, The Boston Globe, 2010. 06. 25., http://www.boston.com/business/technology/articles/2010/06/25/frenchman_convicted_for_hacking_twitter/
4. Weitzenkorn, B. Bank of France’s Accidental Hacker Acquitted, http://www.technewsdaily.com/8140-accidental-hacker-bank-france.html
5. Morris, R., Thompson, K. Password Security: A Case History. Bell Laboratories, 1978. 04. 03. cm.bell-labs.com/cm/cs/who/dmr/passwd.ps
6. Keszthelyi A. About passwords. Acta Polytechnica Hungarica, Vol. 10, No. 6, 2013. http://www.uni-obuda.hu/journal/Keszthelyi_44.pdf
7. Lord, B. Keeping our users secure, 2013. 02. 01. http://blog.twitter.com/2013/02/keeping-our-users-secure.html
8. Ködmön J. (2007): Biztonságosabb felhasználóazonosítás az egészségügyben, IME – Az egészségügyi vezetők szaklapja, 6. évf., 9. szám, 2007. nov., pp. 46–51.
9. The Gmail Team. Choosing a smart password. http://gmailblog.blogspot.hu/2009/10/choosing-smart-password.html, 2009. 10. 07.

10. https://accounts.google.com/PasswordHelp, dátum nélkül.
11. Make Computer Security One of Your New Year's Resolutions, http://www.consumer.ftc.gov/blog/make-computer-security-one-your-new-years-resolutions, 2013. 01. 03.
12. Keeping Your Account Secure, https://support.twitter.com/articles/76036-keeping-your-account-secure# 2013. 02. 05.
13. Karp, Alan H.: Site-Specific Passwords, Hewlett-Packard Company, 2003. http://www.hpl.hp.com/personal/Alan_Karp/site_password/index.html
14. Próbálja ki: így csinálhat 1 perc alatt könnyen megjegyezhető jelszót, amit senki nem fog kitalálni. HVG, 2014. 06. 10. http://hvg.hu/tudomany/20140610_nagyon_eros_jelszo_keszitese_gyorsan/
15. https://weblogin.stanford.edu/pwstrength.html
16. Schneier, B. Changing Passwords. Schneier on Security blog, 2010. 11. 11. https://www.schneier.com/blog/archives/2010/11/changing_passwo.html
17. Update: New 25 GPU Monster Devours Passwords In Seconds, http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds/ 2012.12.04.
18. New 25-GPU Monster Devours Strong Passwords In Minutes, http://it.slashdot.org/story/12/12/05/0623215/new-25-gpu-monster-devours-strong-passwords-in-minutes 2012. 12. 05.
19. Tóth-Laufer, E., Takács, M. Rudas, I. J. (2013): "Interactions Handling Between the Input Factors in Risk Level Calculation" in Proc. of the IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2013), Herl'any, Slovakia, January 31–February 2, 2013, pp. 71–76, ISBN: 978-1-4673-5926-9.
20. Kiss, G.: Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course / TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4. ISSN: 2146 – 7242, pp. 222-235.
21. Kiss, G.: Comparison of the Programming Knowledge of Slovakian and Hungarian Students / Procedia of Social and Behavioral Science Journal különszám, ISSN: 1877-0428, p. 10.
22. Fehér-Polgár, P. (2014): Data security of mobilephones, from the aspect of university students, in: Management, Enterprise and Benchmarking in the 21st Century 2014 (szerk. Michelberger P.) Óbuda University, Budapest, 2014, 393-401 ISBN: 978-615-5460-06-7
23. Lazányi Kornélia (2014): A biztonsági kultúra, TAYLOR Gazdálkodás- és szervezéstudományi folyóirat, A Virtuális Intézet Közép-Európa Kutatására Közleményei, in press.

Felhasznált irodalom

Az online tartalmak elérhetőségét 2014. október 10. és 12. között ellenőriztem, ahol ettől eltérő jelzés nincs.

Ducklin, P. Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Fehér-Polgár, P. (2014): Data security of mobilephones, from the aspect of university students, in: Management, Enterprise and Benchmarking in the 21st Century 2014 (szerk. Michelberger P.) Óbuda University, Budapest, 2014, 393-401 ISBN: 978-615-5460-06-7

https://accounts.google.com/PasswordHelp, dátum nélkül.

https://weblogin.stanford.edu/pwstrength.html

It is no longer a question of 'if' but 'when'! Websense, 2011. 05. 24. http://view.websense-email.com/view_email.aspx?j=fe5815727d6200787d11&m=fefc1177756502&ls=fdf01078716c077d7713737d&l=fec117787c66057a&s=fe2111757c620c78761170&jb=

ffcf14&ju=fe2d157274640675721079&cmpid=Emerging-No-longer-a-Q-Prosp-24May11&wsid=0032000000NsbQ6AAJ&linkid=View+as+a+Web+Page
Karp, Alan H.: Site-Specific Passwords, Hewlett-Packard Company, 2003. http://www.hpl.hp.com/personal/Alan_Karp/site_password/index.html
Keeping Your Account Secure, https://support.twitter.com/articles/76036-keeping-your-account-secure# 2013. 02. 05.
Keszthelyi A. About passwords. Acta Polytechnica Hungarica, Vol. 10, No. 6, 2013. http://www.uni-obuda.hu/journal/Keszthelyi_44.pdf
Kiss, G.: Comparison of the Programming Knowledge of Slovakian and Hungarian Students / Procedia of Social and Behavioral Science Journal különszám, ISSN: 1877-0428, p. 10.
Kiss, G.: Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course / TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4. ISSN: 2146 – 7242, pp. 222-235.
Ködmön J. (2007): Biztonságosabb felhasználóazonosítás az egészségügyben, IME – Az egészségügyi vezetők szaklapja, 6. évf., 9. szám, 2007. nov., pp. 46–51.
Lazányi Kornélia (2014): A biztonsági kultúra, TAYLOR Gazdálkodás- és szervezéstudományi folyóirat, A Virtuális Intézet Közép-Európa Kutatására Közleményei, in press.
Lord, B. Keeping our users secure, 2013. 02. 01. http://blog.twitter.com/2013/02/keeping-our-users-secure.html
Make Computer Security One of Your New Year's Resolutions, http://www.consumer.ftc.gov/blog/make-computer-security-one-your-new-years-resolutions, 2013. 01. 03.
Mesquita, R. Frenchman convicted for hacking Obama's Twitter, The Boston Globe, 2010. 06. 25., http://www.boston.com/business/technology/articles/2010/06/25/frenchman_convicted_for_hacking_twitter/
Morris, R., Thompson, K. Password Security: A Case History. Bell Laboratories, 1978. 04. 03. cm.bell-labs.com/cm/cs/who/dmr/passwd.ps
New 25-GPU Monster Devours Strong Passwords In Minutes, http://it.slashdot.org/story/12/12/05/0623215/new-25-gpu-monster-devours-strong-passwords-in-minutes 2012. 12. 05.
Próbálja ki: így csinálhat 1 perc alatt könnyen megjegyezhető jelszót, amit senki nem fog kitalálni. HVG, 2014. 06. 10. http://hvg.hu/tudomany/20140610_nagyon_eros_jelszo_keszitese_gyorsan/
Schneier, B. Changing Passwords. Schneier on Security blog, 2010. 11. 11. https://www.schneier.com/blog/archives/2010/11/changing_passwo.html
The Gmail Team. Choosing a smart password. http://gmailblog.blogspot.hu/2009/10/choosing-smart-password.html, 2009. 10. 07.
Tóth-Laufer, E., Takács, M. Rudas, I. J. (2013): "Interactions Handling Between the Input Factors in Risk Level Calculation" in Proc. of the IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2013), Herl'any, Slovakia, January 31–February 2, 2013, pp. 71–76, ISBN: 978-1-4673-5926-9.
Update: New 25 GPU Monster Devours Passwords In Seconds, http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds/ 2012.12.04.
Weitzenkorn, B. Bank of France's Accidental Hacker Acquitted, http://www.technewsdaily.com/8140-accidental-hacker-bank-france.html