Szakmai Jelentés
UNIVERSITY OF CAMBRIDGE
Számítógép Laboratórium

A JELSZAVAK MEGJEGYEZHETŐSÉGE ÉS BIZTONSÁGA NÉHÁNY GYAKORLATI EREDMÉNY

Jianxin Yan, Alan Blackwell, Ross Anderson, Alasdair Grant

2000. szeptember

Kivonat. A jelszavakkal kapcsolatosan sok „jól ismert” tény van: a felhasználók nem tudnak megjegyezni nehéz jelszavakat; a jelszó, amire emlékeznek, az könnyen kitalálható. Mindenesetre úgy látszik, kifejezetten hiányzik a téma kutatása, mely megfelelne az alkalmazott pszichológia követelményeinek.

Beszámolunk egy kísérletről, melyben négy, 100 elsőéves egyetemistából álló csoport vett részt. Három csoportot egy formális kísérlethez toboroztunk, ebből két csoportnak megfelelő tanácsokat kapott a jelszó kiválasztásához. A gyenge jelszavak gyakoriságát a jelszó-állomány feltörésével határoztuk meg, míg az elutasítások számánál a rendszerbe való belépést vettük figyelembe.

Megfigyeltünk néhány jelenséget, mely az eddig megalapozott filozófiának ellentmond. Például az emlékezeterősítő mondaton alapuló jelszavak majdnem olyan nehezen feltörhetőek, mint a véletlen jelszavak mégis ugyanolyan könnyen megjegyezhetőek, mint a naiv felhasználó által választottak.

1. Bevezetés

Számos hiányossága a jelszó hitelesítő rendszereknek az emberi memória korlátjaiból ered. Ha az emberektől nem kérnék a jelszó megjegyzését, akkor a legbiztonságosabb a maximális entrópiájú jelszó lenne: egy olyan hosszú karakterlánc, amekkorát még a rendszer engedélyez, az összes lehetséges karakter felhasználásával és oly módon kiválasztva, hogy ne legyen benne ismétlődés - pl. teljesen véletlenszerű kiválasztás.

Mindegyike ezeknek a követelményeknek ellentétben áll az emberi memória jól ismert tulajdonságaival. Először is, az emberi memória adatok sorozatára nézve időben korlátolt [1], kis kapacitású, körülbelül hét plusz-mínusz két adatot képes megjegyezni rövid idő alatt [2]. Másodszor, amikor az ember megjegyez egy adatsorozatot, azok nem lehetnek tetszőlegesek és szokatlanok, hanem ismerős ‘darabokat’ kell tartalmazniuk: szavakat vagy ismerős szimbólumokat [2]. Harmadszor, az emberi memória a redundanciával (ismétlődéssel) fejlődik a leggyorsabban - sokkal jobban megjegyezzük azokat az információkat, amelyek többféleképpen kódolhatóak [3].

A jelszó hitelesítés látszólag magába foglal egy kompromisszumot. Egyes jelszavak könnyen megjegyezhetőek (pl. egyetlen szó a felhasználó anyanyelvén), de ugyanakkor nagyon könnyen kitalálhatóak szótárból való kereséssel. Ezzel ellentétben bizonyos jelszavak nagyon biztonságosak a találgatásra nézve, de nehéz őket megjegyezni. Az utóbbi esetben a kiválóbb jelszó biztonságát veszélyezteti az emberi korlátozottság, mivel a felhasználó megőrizhet egy biztonság nélküli írott feljegyzést vagy igénybe vehet biztonság nélküli jelszó-felderítő eljárásokat, ha elfelejti azt[1].

Ezen írás egy gyakorlati vizsgálata a lehetséges kompromisszumoknak a jelszavakat használók körében. A megismerő pszichológia területén végzett kutatás során sok korlátot határoztak meg az emberi teljesítményre- ezen kísérlet során a személyeket véletlenszerű és pszeudo-véletlenszerű szimbólumsorozatok megjegyzésére kérték.

Nagyon nehéz általánosítani ilyen kutatásokból a jelszavakat használókra, akik saját maguk választhatják ki a kódszót, azt el tudják ismételni memorizálás közben, és hosszú idő után szabályos időközönként fel kell idézzék.

---

[1] Ez nem azt jelenti, hogy mi elfogadjuk azt a közismert elméletet, hogy leírni a jelszót az minden esetben hiba. Azon gépek számára, melyek nyilvános nem elérhetőek, értelmes dolog lehet egy hosszú véletlen betöltendő jelszó leírása egy borítékba, a géphez ragasztva, ezek után kell egy szigorú adatvédelmi politika: a jelszót semmilyen körülmények között nem szabad felfedni telefonon. Mindenesetre a ‘szociális-mérnöki’ támadások megelőzése egy különálló kutatási téma.

Megmutatjuk, hogy ezen felhasználói környezet hozzájárul a jelszómegjegyzést segítő emlékezeterősítő stratégiák kiaknázásához. Sok sikeres emlékezeterősítő stratégia létezik, amelyeket fel lehet használni lenyűgöző teljesítmények elérésére látszólag véletlenszerű sorozatok megjegyzése esetén. Olyan jelszóváltozatok, mint „Pass Faces" (Arc kód) a magasabb rendű emberiarc-memóriát használja ki, lásd [4]. Mindenestre, a jelszó hitelesítési eljárás megváltoztatása helyett inkább javasoljuk a változtatást azon tanácsokban, amiket a felhasználónak a jelszó kiválasztásakor adnak.

2. Létező tanácsok a jelszó kiválasztásához

Számos terjedelmes szervezet ad sajátos tanácsokat az új felhasználóknak, hogyan válasszanak „jó jelszavakat". A jó jelszó, a fenti tárgyalást követve, elegendően hosszúnak kell lennie, megfelelően nagy karakterkészletet kell használnia és mindezek mellett könnyen megjegyezhető kell maradjon. Tovább bonyolítható a dolog aszerint, hogy a támadó több jelszóval próbálkozik a hálózaton keresztül, vagy megszerzett egy másolatot a jelszó állományról és offline töri fel, de mi eltekintünk ezektől a jelenlegi tanulmány céljaiért.

Készítettünk egy tájékoztató jellegű felmérést a nagyobb kiterjedésű oldalak által az új felhasználóknak adott tanácsok alapján, a weben keresve a „choose" (válasszunk), „good" (jó), és „password" (jelszót) kifejezéseket. Sok oldal nem ismeri fel a jelentőségét a megjegyezhetőségnek, csupán az ellenállást helyezi előtérbe a brute-force (nyers-erő) kereséssel szemben. Néhány tipikus tanács:

„[Egy jó] jelszó lehetőleg vegyes karakterekből vagy speciális karakterekből áll, és nincsenek benne szótárban megtalálható szavak. Ha lehet, ne írjuk le könnyen elérhető helyre és különösen nem az azonosítóval együtt. Mindegyik lehet nagy vagy kis betű"

„Használdd a kimenetét egy véletlenszerű jelszógenerátornak. Válassz egy olyan véletlenszerű karaktersort, amit ki lehet ejteni és könnyű megjegyezni. Például a találomra létrehozott 'adazac' szót ki lehet ejteni, mint a-da-zac és meg tudod jegyezni, mint 'A-to-Z'. Tegyél közéjük nagybetűket is, hogy létrehozd a saját változatodat, például aDAzac.2"

„Jó jelszavaknak látszanak a véletlenszerű karakterek. Minél szélesebb a változatossága a karaktereknek, annál jobb. Keverve a betűket számokkal, jobb, mint a betűk magukra. Még jobb, ha keverjük a speciális karaktereket számokkal és betűkkel."

Egy ajánlás, ami egyre nagyobb népszerűségnek örvend, az a jelszógenerálás „kódmondat"-tal való megközelítése. Egy tipikus leírása ennek a következő:

„Egy jó technika a jelszó kiválasztásában az, hogy használjuk egy mondat szavainak első betűit. Mindenesetre ne válasszunk egy jól ismert mondatot, mint 'An apple a day keeps the doctor away' (Aaadktda) — 'A doktorhoz nem kell menni, csak naponta almát enni' (Adnkmcsnae).Helyette valami mást válassz, mint például'My dog's first name is Rex' (MdfniR) —'A kutyusom neve Morzsa.' (AknM), vagy'My sister Peg is 24 years old.' (MsPi24yo)—'A lánytestvérem, Peg 24 éves' (AlP24e)."

Természetesen ezen felmérés nem foglalja magába azokat az oldalakat, ahol egyáltalán nem adnak tanácsot a jelszóválasztást illetően. Szerintünk sok oldal csak minimális követelményeket ad meg egy érvényes jelszóhoz (hosszúság és karakterkészlet), és nem ad további tanácsot a biztonság, illetve a megjegyezhetőség szempontjából. Mások, tapasztalataink alapján, olyan szabályokat vezetnek be, mint:

„A jelszónak legalább nyolc karakter hosszúnak kell lennie, és tartalmaznia kell két nem betű karaktert. Továbbá havonta legalább egyszer meg kell változtatni."

A megszokott válasz erre a felhasználó részéről egy sajátos jelszógenerálás, erre egy egyszerű példa a Julia03 március, Julia04 április esetén és így tovább. Ez jól láthatóan gyenge. Más próbálkozások a magatartás megváltoztatására visszafelé sültek el. Például, Patterson számolt be egy ilyen esetről: a felhasználókat rákényszerítették a jelszó megváltoztatására és figyelmeztették az előbbi változatok elkerülésére, mire ők gyakran cseréltek jelszót, hogy kimerítsék az előző jelszavak listáját, majd visszatértek a kedvenc jelszavukhoz. A válaszlépés, hogy ne lehessen kicserélni a jelszót 15 napon belül, azt jelentette, hogy a felhasználó nem tudta cserélni a jelszót a rendszergazda segítsége nélkül [9].

Így a kivitelezése a felhasználóknak adott tanácsoknak és a rendszer-szintű rákényszerítésnek - ami az előző kiegészítése lehet, komoly problémát jelentenek, és újabb, kifinomultabb kérdéseket tesznek fel az alkalmazott pszichológia területéről, melyekre a válasz nem magától értetődő.

A létező irodalom a jelszó kiválasztását illetően meglehetősen kevés. Grampp és Morris a Unix biztonságáról szóló klasszikus írásukban jelentették, hogy miután a szoftverek elérhetőek lettek—ami azt eredményezte, hogy a jelszavaknak legalább hat karakter hosszúságúaknak kellett lenniük és legalább egy nem betű karaktert kellett tartalmazniuk—, ők készítettek egy állományt a 20 legelterjedtebb női névvel, mindegyiket megtoldva egy számjeggyel. Ezen 200 jelszó közül a megvizsgált néhány tucat gépen legalább egy használatban volt [5].

Klein beszámol 13797 jelszó-állomány Unix rendszerekből való összegyűjtéséről és támadás alá vételéről kimerítő kereséssel; körülbelül egynegyedét sikerült feltörnie. Jelszómenedzsment útmutatója az amerikai Védelmi Osztálynak (US Department of Defense) [7] ajánlotta a gépi generálású véletlen jelszavak használatát.

Zviran és Haga [8] az általuk végzett kísérletben 106 egyetemistát kértek meg, hogy válasszanak jelszót és írják azt le egy kérdőívre. A kérdőív tartalmazott egy találomra kiválasztott jelszót is és azt kérték tőlük, jegyezzék meg mindkettőt. Három hónap múlva, a következőket tapasztalták:

	Saját választás	Véletlenszerű
Sikeresen megjegyezte:	35%	23%
Leírta:	14%	66%

Mindenesetre, az egyetemisták nem használták a jelszavakat a három hónap alatt. Így amellett, hogy - számszerű adatokat felhasználva - tájékoztat a véletlen jelszavak nehézségéről, nem modellez közelebbről egy valós működésű környezetet.

3. Kísérleti tanulmány

Ezen kompromisszumos tényezők egy valós alkalmazás keretén belül történő kivizsgálása érdekében, vezettünk egy kísérletet, bevonva 400 elsőéves egyetemistát a mi egyetemünkről. A kísérlet során összehasonlítottuk a jelszóválasztásnál a három csoport különböző tanácsokkal való ellátásának eredményeit. Továbbá mértük ezen tanácsoknak a három csoportra kifejtett hatását a biztonság és a memorizálhatóság tekintetében.

A kísérlet alanyai olyan egyetemisták, akik a Természettudományi Karon kezdték meg tanulmányaikat, ezen kar fizikát, kémiát, geológiát és anyagtudományokat foglal magába. Minden karunkon tanuló egyetemista kap egy azonosítót a központi számítógépre, ami egy felhasználói névből és egy találomra generált kezdeti jelszóból áll. Több szolgáltatáshoz is hozzáférhetnek. Amíg ezen nyilvántartással kapcsolatos tudnivalókat megkapják, az egyetemistákat általában ellátják tanáccsal, hogy miként válasszanak saját jelszót. Vannak, akik ezt a tájékoztatást kézbesítve kapják - a karukon vagy otthoni címükre kiküldve - a rendszergazdától. Sok hallgató egy bevezető előadáson vesz részt a központi szolgáltatással kapcsolatosan, amit egy oktatói óra követ a bemutatók felügyelet mellett.

4. Módszer

A bevezető előadás során, 1999 októberében, az egyetemistáknak megmondták, hogy ők kísérleti alanyai lesznek egy jelszó kiválasztási tanulmánynak (saját beleegyezésük esetén).

Az oktatói órán megkérdezték őket beleegyeznek-e, és véletlenszerűen beosztották őket a három kísérleti csoport egyikébe. Mindegyik hallgatót elláttak egy tájékoztató lappal, annak függvényében, hogy melyik csoportba osztották be. A három különböző típusú tanács a következő volt:

– a kontrollcsoportba tartozó hallgatók ugyanazokat a tanácsokat kapták, mint előző években, ami egyszerűen ennyiből állt: ‘A jelszónak legalább 7 karakter hosszúságúnak kell lennie, és tartalmaznia kell legalább egy nem betű karaktert.’

– a véletlenszerű jelszavak csoportjába tartozóak egy lapot kaptak, melyen az A-Z betűk és a 0-9 számjegyek ismételten voltak felírva. Ki kellett válasszanak egy véletlen jelszót úgy, hogy becsukott szemmel találomra vettek nyolc karaktert. Még azt a tanácsot kapták, hogy írják le egy papírra és hordják magukkal mindaddig, míg meg nem jegyzik.

–a kódmondat csoportba levőknek annyit mondtak, hogy jelszavukat egy arra emlékeztető mondat alapján válasszák.

A csoportoknak megfelelő utasítások szövegét a függelék tartalmazza.

Arra az eredményre vártunk, hogy a véletlenszerű jelszavak csoportjának erősebb jelszavai lesznek, mint a kódmondat csoportjába tartozóknak, viszont nehezebben jegyzik meg és/vagy könnyebben elfelejtik; továbbá a kódmondatos csoport tagjai hasonlóan viszonyulnának a kontrollcsoport tagjaihoz.

Egy hónappal az oktatói óra után vettük az összes jelszó-állományt és négyféle támadásnak vetettük alá:

1. Szótári támadás: Egyszerűen szótár-állományokat használtunk a jelszavak feltöréséhez. Ezt a támadást minden jelszóra kipróbáltuk.

2. Szavak és számjegyek permutációja: minden szótár-állománybeli szót permutáltunk a 0, 1, 2 és 3 számjegyekkel, hogy létrehozzunk lehetséges jelszavakat. Ugyanakkor olyan megszokott helyettesítéseket is elvégeztünk, mint I helyett 1, S helyett 5 stb. Ezen támadást is minden jelszón kipróbáltunk.
3. Felhasználói információn alapuló támadás: A jelszó-állományokból összegyűjtött felhasználói adatokat -pl. azonosító, teljes név, és ennek egy része- használtuk a jelszó feltöréséhez. Minden jelszón kipróbáltuk.
4. Brute force (nyers erő) támadás: ezen támadást csak a hat karakternél hosszabb jelszavak esetében próbáltuk.

Minden csoportban adatokat gyűjtöttünk a jelszavak hosszúságáról, valamint a feltört jelszavak számáról. Figyelemmel követtük azon esetek számát, amikor a felhasználó kérte a rendszergazdát a jelszavának újraállításáért — azon feltételezés alapján, hogy a nehezen megjegyezhető jelszavakat elfelejthetik. Ilyen esetben a felhasználó vagy kéri jelszavának újraállítását, vagy nem használja a központi rendszert máshol biztosított szolgáltatás véve igénybe. Mindemellett, minden kísérleti alany részt vett egy e-mailen keresztüli felmérésen, amit négy hónappal a konzultációs óra után végeztünk el, megkérdezve őket, hogy volt-e bármilyen nehézségük a jelszavuk megjegyzésében. Ezen felmérésben a következőket kérdeztük:
1. Milyen nehéznek találtad a jelszavad megjegyzését egy 1-től (triviális) 5-ig (lehetetlen) tartó skálán?
2. Mennyi ideig kellett magadnál tartsad a jelszavadnak az írásos másolatát? Kérjük, becsüldd meg az időt hetekben.

A kísérletünk érvényességét ellenőriztük, végrehajtva ugyanazon támadásokat egy 100 elsőéves egyetemistából álló csoporton, akik nem vettek részt a bevezető előadáson vagy egyáltalán nem kaptak gyakorlati utasítást.

5. Eredmények

A 300 megkérdezett hallgatóból 288 beleegyezett, hogy részt vegyen a kísérletben. Őket véletlenszerűen szétválogattuk a kísérleti csoportokba a következőképpen:

Kontrollcsoport	95
Véletlenszerű jelszavak csoportja	96
Kódmondat csoport	97

A kiválasztott jelszavak átlagban 7 és 8 karakter hosszúságúak (7,6; 8,0; 7,9 – a csoportnak megfelelően), a három csoport közötti lényeges különbség nélkül. Az összes csoport által választott jelszavak alig voltak hosszabbak, mint a későbbi 100 hallgatóé, akik nem vettek részt oktatói órán (közepes hossz 7,3; a különbség statisztikailag $t= 4,53$, $p<,001$ esetén jelentős).

A legsikeresebb feltörési módszer a permutált szótári támadás bizonyult. A felhasználóról szerzett ismeretekre támaszkodó feltörés nem volt sikeres egyik esetben sem, valószínűleg a jelszó állományok nagyon korlátozott információtartalma miatt (ezek nem tartalmaztak például keresztnevet).

Minden hat karakterből álló jelszót a brute force támadással sikeresen feltörtünk. A következő összesítő a feltört jelszavak számát tartalmazza (a brute force —nyers erő — támadást külön tárgyalva:)

Kontrollcsoport	30 (32%) + 3 brute force
Véletlenjelszavak csoportja	8(8%) + 3 brute force
Kódmondat csoport	6(6%) + 3 brute force
Összehasonlítási csoport	33 (33%) + 2 brute force

Minden hat karakterből álló jelszó ki van téve a brute force támadásnak. Ezeknél nem hatásosak a kísérlet során adott jelszó-kiválasztási tanácsok. Mindegyik kísérleti feltételnél kis számú felhasználó nem vette figyelembe a tanácsot a jelszó hosszát illetően, és nem megbízható jelszót választott. Ez előfordult az összehasonlítási csoport esetén is.

A hat karakternél hosszabb jelszavak esetén sokkal többet sikerült feltörni a kontrollcsoportnál, mint a véletlen jelszavak csoportjánál vagy kódmondat csoportnál (lényeges $\chi^2=24,8$; $p <,001$ esetén). A feltört jelszavakra vonatkozó arány a kontrollcsoportban kisebb volt, mint az összehasonlítási csoport esetén (például

13% az összehasonlító csoportban hat karakter hosszúságú jelszót használt a kontrollcsoport 5% -hoz képest, míg 13 jelszó az összehasonlítási csoportnál szószerinti szótári szó volt, míg a kontrollcsoportnál 3).

Azok a jelszavak, melyeket sikeresen feltörtünk a véletlenszerű jelszavak és a kódmondat csoportnál, mind szótárbeli szavak voltak vagy azok számokkal való permutációi — ami a hallgatóknak adott tanácsoknak nem felelt meg. Ezen eredmények, együtt a hat karakteres jelszavakkal, megbecsülik a jelszóválasztással kapcsolatos tanácsot meg nem fogadó felhasználók szintjét.

Megfigyeltük, hogy szinte senki sem használt speciális karaktereket (pl. betű, szám), kivéve a kódmondat csoport, akiknek az utasításoknál példák voltak adva az írásjelek használatára. Így a betűk, számok és speciális karaktereket vegyesen tartalmazó jelszavak használatára való felhívás ajánlatos.

Nagyon kevés felhasználó kérte a rendszergazdát a jelszó újraállításához.

A konzultáció utáni három hónap alatt a rendszergazda általi újraállítások száma az egyes csoportokban a következő volt:

Kontrollcsoport	2
Véletlen jelszavak csoportja	1
Kódmondat csoport	3

242 hallgató válaszolt az email-felmérőre, amelyek közül 13 válasz utalt arra, hogy nem használták az azonosítójukat vagy kiestek a kurzusokról.

Az érvényes válaszok alapján tisztán látszott a különbség a csoportok között:

		Nehézség	Hetek
Kontrollcsoport	80	1,52	0,7
Véletlen jelszavak csoportja	71	3,15	4,8
Kódmondat csoport	78	1,67	0,6

A véletlen jelszavak csoportjába osztott felhasználók jelentették, hogy jelszavaikat sokkal nehezebben megjegyezhetőeknek találták (jelentős $t=8,25$; $p< 0,001$esetén) és azt, hogy ők sokkal tovább hordozták jelszavaik írott másolatát (jelentős $t=6,41$; $p<0,001$esetén). Ez megerősíti Zviran és Haga eredményeit egy működőképes beállításra vonatkozólag.

A különbségek a válaszok között nem jelentősek, ezért mi nem hisszük, hogy eredményeink lényegesen eltorzítottak a véletlen jelszavak csoportjába tartozó hallgatók által, akik tanácsainkat olyan bonyolultnak találták, hogy lemondtak a számítógép által nyújtott lehetőségek használatáról.

Semmit sem ér, hogy sokan a véletlen jelszavak csoportjából még a felmérő időpontjában is magukkal hordozták a jelszó írott másolatát — azaz képtelenek voltak megjegyezni a jelszavukat.

- **Tárgyalás**

Ez a tanulmány igazol bizonyos számú széles körben elterjedt népi hiedelmet a jelszavakról, és másokat megsemmisít.

1. Az első népi hiedelem az, hogy a felhasználók nehézségekbe ütköznek a véletlen jelszavak megjegyzésénél. Ez a hiedelem bebizonyosodott.
2. A második népi hiedelem az, hogy az emlékezeterősítő (kódmondatos) jelszavak nehezebben találhatóak ki, mint a naivul kiválasztott jelszavak. Ez a hiedelem is bebizonyosodott.
3. A harmadik népi hiedelem az, hogy a véletlenszerű jelszavak jobbak, mint azok, amelyek emlékeztető mondatokon alapulnak. Mégis, úgy látszik mind a kettő egyformán erős jelszó. Így ezen hiedelmet lelepleztük.
4. A negyedik népi hiedelem az, hogy az emlékezeterősítős jelszavak nehezebben megjegyezhetőek, mint a naivul kiválasztottak. Mindenesetre, úgy látszott, hogy az egyiket is és a másikat is egyforma könnyen megjegyezhetik. Így e hiedelem szintén alaptalan volt.
5. Az ötödik népi hiedelem arról szól, hogy a felhasználót arról oktatva, hogy használjon véletlen vagy kódmondaton alapuló jelszavakat, jelentősen növelhetjük a biztonságot. Mindemellett, mindkét véletlenszerű jelszó esetén 10% (beleértve a túl rövid jelszavakat és a nem megfelelő utasításoknak megfelelően választott jelszavakat) nem vette figyelembe a tanácsokat. Míg ez jobb, mint az a 35%, ami azon hallgatók esetében kaptunk, akik felületes kiképzés mellett választottak rossz jelszót, nem igen nagy javulás. A támadónak lehet háromszor olyan keményen kell dolgoznia, de a jelszó politika kényszerítő

mechanizmusának hiányában úgy tűnik nincs út arra, hogy a támadókat ezerszer nehezebben dolgoztassuk. Tulajdonképpen a mi kísérleti csoportunk lehetett a legmegfelelőbb egy rendszergazda elvárásainak. Így ennek a hiedelemnek is véget vetettünk.

Ebben az írásban leirt munka csupán az első lépés a számítástechnikai biztonság alkalmazott pszichológiai vetületeinek jobb megértése felé. Sok kérdés vár még válaszra, mi tervezzük a kísérletek folytatását újabb csapatok bevonásával. Addig is a mi javaslataink a rendszergazdáknak a következők:

- A felhasználót arrafelé kellene irányítani, hogy válassza a kódmondaton alapuló jelszót, mivel ugyanolyan könnyen emlékezetbe véshetők, mint a naivul kiválasztottak, de pontosan olyan nehéz kitalálni, mint a véletlenszerűen létrehozottakat. Azaz mindkét részről a legtöbbet hozzák.
- A méret számít. Olyan rendszerek esetén, mint Unix, ahol eleve meghatározott a jelszó hosszának maximális hossza: nyolc karakter, a felhasználónak meg kell mondani, hogy válasszon pontosan nyolc karakterből álló jelszót. Olyan rendszereknél, mint a Netware, amely 14 karaktert enged meg, de nem tesz különbséget kis és nagybetű között, biztatni kell a felhasználókat, hogy tíz vagy annál több karakterhosszúságú jelszót válasszanak, remélhetőleg ez bátorítani fogja az emlékezeterősítő módszer használatára (Ez a következő évek kísérleteinek témája, ahogy általánosan a kényszerítés is).
- A karakterre eső entrópia is számít. A felhasználónak meg kell mondani, hogy válasszanak olyan jelszót, amely tartalmaz számokat és speciális karaktereket, úgyszintén betűket. Ha ilyen útbaigazítást nem adnánk, akkor a legtöbbjük által választott jelszó hossza csak töredéke lesz a jelszó lehetséges hosszának.
- A kompromisszum, egyetértés a legkritikusabb probléma. Olyan rendszerekben, ahol a felhasználó csak saját magát teheti ki a rizikónak, megfontolandó a saját megérzésükre bízni a dolgot. Ebben az esetben számíthatunk arra, hogy 10% gyenge jelszót választ az adott tanácsok ellenére. Olyan rendszerekben, ahol egy felhasználó hanyagsága más felhasználót is érint (például egy rendszerben miután egy behatoló megszerzi egyetlen felhasználó jelszavát, könnyen rendszergazdai jogokat szerezhet, jól ismert és elterjedt trükköket használva), figyelembe kell venni a jelszó minőségét kikényszerítő rendszermechanizmusokat.
- Ha haszna van központilag kiadott véletlenszerű jelszavak használatának, ez abból a tényből jöhet, hogy a központi hozzárendelés (ami megköveteli az egyetértést) jobban elfogadott, mint a véletlenszerű generálás (ami csak kódmondatokon alapulhat).

Egy érdekes és fontos kihívás megtalálni együttműködésre kész kikényszerítő mechanizmusokat, melyek jól működnek emlékezeterősítő választással. Úgy reméljük, hogy a jelszó-ellenőrző, amely leellenőrzi, hogy a jelszó nem része-e egy ismert gyenge résznek a jelszó halmazból, egy hatékony szerszám lehet. Egy kísérleti teszt ezen elvárások irányában egyike a jövő évi terveinknek.

Referenciák

1. GJ Johnson, in *Psychological Review* v 98 no 2 (1991) pp 204-217
2. GA Miller, „The magical number seven, plus or minus two: Limits on our capacity for processing information" in *Psychological Review* v 63 (1956) pp 81-87
3. A Paivio, „The empirical case for dual coding" in *Imagery, Memory and Cognition: Essays in honor of Allan Paivio*, JC Yuille (Ed), Erlbaum, Hillsdale, NJ (1983); pp 307-322
4. H Davis, „Physiognomic access control", in *Information Security Monitor* v 10 no 3 (Feb 95) pp 5-8
5. FT Grampp, RH Morris, „UNIX Operating System Security", *AT&T Bell Laboratories Technical Journal* v 63 no 8 (Oct 84) pp 1649-1672
6. DV Klein, „Foiling the Cracker; A Survey of, and Improvements to Unix Password Security", Proceedings of the USENIX Security Workshop. Portland, Oregon: USENIX Association, Summer 1990; `http://www.deter.com/unix/`; expanded as a technical report from SEI, 1992
7. Department of Defense, '*Password Management Guideline*', CSC-STD-002-85 (1985)
8. M Zirvan, WJ Haga, „A comparison of password techniques for multilevel authentication mechanisms", in *Computer Journal* v 36 no 3 (93) pp 227-237
9. B. Patterson, letter to *Communication of the ACM* v 43 no 4 (Apr 2000) pp 11-12

Függelék

Itt található a három útmutatás szövege a három csoport részére.

Kontrollcsoport

Ez a lap néhány tanácsot ad, hogyan válasszunk jó jelszót. Ezt a lapot a bevezetőben bemutatott jelszóbiztonsággal foglalkozó kísérlet részeként adjuk neked. Különböző emberek különböző tanácsokat kapnak (de mindegyik tanács legalább olyan biztonságos jelszót eredményez, mint amilyent választottál volna, ha nem veszel részt a kísérletben). Kérünk, ne beszélj a barátaiddal a kísérletről, a kapott tanácsról, vagy az általad választott jelszóról.

Kérünk, lépjél be a kezdeti jelszóval, majd válassz egy új jelszót, amit nem ismer senki. A 'Windows NT Tutor' megmondja, hogyan teheted ezt meg az 1.6-1.7 oldalakon.

A jelszavad legalább hét karakter hosszú kell legyen és tartalmaznia kell legalább egy nem betű karaktert.

Ha már kicserélted a kezdő jelszavadat és az új jelszó megfelel a követelményeknek, akkor nem kell újból megváltoztatnod. Mindenképpen felhívjuk figyelmedet, hogy időnként változtasd meg a jelszavadat – legalább egyszer félévente. Mivel a kísérlet az akadémiai év végéig tart, kérjük tartsd meg ezt a lapot, és használdd a tanácsokat újból, amikor kiválasztod az új jelszavadat Nagyböjt és Húsvét idején.

6.1 Véletlen jelszavak csoportja

Ez a lap néhány tanácsot ad, hogyan válasszunk jó jelszót. Ezt a lapot a bevezetőben bemutatott jelszóbiztonsággal foglalkozó kísérlet részeként adjuk neked. Különböző emberek különböző tanácsokat kapnak (de mindegyik tanács legalább olyan biztonságos jelszót eredményez, mint amilyent választottál volna, ha nem veszel részt a kísérletben). Kérünk, ne beszélj a barátaiddal a kísérletről, a kapott tanácsról, vagy az általad választott jelszóról.

Egy biztonságos jelszó olyan, amit nehéz kitalálni. Szótári szavak, emberek és helyek nevei könnyen kitalálhatóak. A legnehezebben kitalálható jelszavak véletlenszerű betűk sorozata. Hogy segítsünk kiválasztani egy véletlen jelszót, kinyomtattunk egy rácsot véletlen betűkkel a hátoldalon. Hunyd be a szemed, és véletlenszerűen mutass a rács egy pontjára. Ezen módszerrel válassz nyolc karaktert és írdd le egy papírszeletre.

Lépjél be a kezdeti jelszavaddal és cseréldd ki arra az új véletlenszerű jelszóra, amit választottál. A 'Windows NT Tutor' megmondja, hogyan teheted ezt meg az 1.6-1.7 oldalakon.

Jelszavad nehezen megjegyezhetőnek tűnhet. Győződjél meg róla, hogy a papírdarab, amire leírtad az egy biztonságos helyen van, mint például az erszényedben vagy pénztálcádban.

Meglátod, miután sokszor beléptél, képes leszel megjegyezni. Miután megbizonyosodtál, hogy sikerült megjegyezni, semmisítsd meg a papírdarabkát, amire leírtad a jelszót.

Végezetül, felhívjuk figyelmedet, hogy időnként cseréld a jelszavadat - legalább egyszer félévente. Mivel a kísérlet az akadémiai év végéig tart, kérjük tartsd meg ezt a lapot, és használdd a tanácsokat újból, amikor kiválasztod az új jelszavadat Nagyböjt és Húsvét idején.

6.2 Kódmondat csoport

Ez a lap néhány tanácsot ad, hogyan válasszunk jó jelszót. Ezt a lapot a bevezetőben bemutatott jelszóbiztonsággal foglalkozó kísérlet részeként adjuk neked. Különböző emberek különböző tanácsokat kapnak (de mindegyik tanács legalább olyan biztonságos jelszót eredményez, mint amilyent választottál volna, ha nem veszel részt a kísérletben). Kérünk, ne beszélj a barátaiddal a kísérletről, a kapott tanácsról, vagy az általad választott jelszóról.

Hogy szerkessz egy jó jelszót, alkoss egy nyolcszavas mondatot, majd építsd fel a jelszavadat a szavakból vett betűkből. Veheted a kezdő vagy az utolsó betűket, tehetsz nagybetűket, hogy jelszavad nehezen kitalálható legyen; és legkevesebb egy számot vagy speciális karaktert is iktass be! Használd ezt a módszert, hogy generálj egy 7 vagy 8 karakterből álló jelszót.

Például az „It's 12 noon I am hungry" mondat segítségével összeállíthatjuk a következő jelszót: "I's12&Iah" („Déli 12 óra van, nagyon éhes vagyok" – „D12o&nev"), amely bárki másnak nagyon nehéz kitalálni, de neked nagyon könnyű a megjegyzése. Ha ismersz idegen nyelvet, használdd: a „AwKdK.Md" jelszót a következő mondatból kaptuk: „Anata wa Kyuuketsuki desu ka … Miyu desu". Keverhetsz szavakat akár különböző nyelvekből is. Mindenképpen ne csak egy szót használjál vagy neveket az idegen nyelvből. Igyekezz kreatív lenni!

Lépjél be a kezdeti jelszavaddal, majd cseréld ki az általad választott új jelszóra. A 'Windows NT Tutor' megmondja, hogyan teheted ezt meg az 1.6 -1.7 oldalakon.

Ne írdd le az új jelszavadat!

Végezetül, felhívjuk figyelmedet, hogy időnként cseréld a jelszavadat - legalább egyszer félévente. Mivel a kísérlet az akadémiai év végéig tart, kérjük tartsd meg ezt a lapot, és használdd a tanácsokat újból, amikor kiválasztod az új jelszavadat Nagyböjt és Húsvét idején.

fordította: Bartha Ágnes, neska@mad.hu, 2003. február