Biztonságosabb felhasználóazonosítás az egészségügyben

Dr. Ködmön József, Bodnár Károly, Debreceni Egyetem, Egészségügyi Kar, Nyíregyháza

A cikk alapos elemzés után megmutatja, hogy az egyszerű jelszavas felhasználóazonosítás nem ad elegendő informatikai biztonságot a nagy tömegű érzékeny egészségügyi adat védelméhez. A szerzők javasolnak a jelszavas azonosítás helyett egy olyan alternatívát, ami szabványos mobil aláírást alkalmaz.

This paper analyses and shows that the simple username-password authentication system does not provide high security for storing large amount of sensitive medical data. Instead of password authentication authors suggest a solution applying the standard mobile signature.

BEVEZETÉS

A számítógépek előtt ülő felhasználók azonosítása klasszikusan nehéz informatikai probléma. A hálózatban működő megoldások óriási mértékű térnyerése miatt rendkívüli mértékben megnőtt a felhasználóazonosítási hibákból eredő károkozás lehetősége. A személyes és különleges adatokat kezelő hálózati alkalmazások használatának kockázata az utóbbi időben jelentősen emelkedett, hiszen az ilyen adatok nyilvánosságra kerülése, illegális felhasználása súlyos törvénysértést jelent.

Igényes informatikai alkalmazások is gyakran belefutnak abba a csapdába, hogy nagy tömegű személyes adatot mindössze egyetlen jelszó véd, elfelejtkezve az azonosítás komplex informatikai környezetéről. Kiemelten fontos hangsúlyozni, hogy az elvárt informatikai biztonság csak a fizikai, az algoritmusos és az ügyviteli védelem megfelelő együttes alkalmazásával érhető el.

Egy informatikai rendszer fizikai védelmét a hardver és szoftver elemek, ezek között különösen a számítógépek, a hálózati elemek, a nyomtatók, az adathordozók, dokumentumok és dokumentációk, valamint ezek közvetlen környezetének fizikai hatások elleni védelmét jelenti.

Az algoritmusos védelem azokból az eljárásokból, protokollokból áll, amelyek a rendszer szolgáltatásaival egyidejűleg, velük szorosan együttműködve látják el a védelmi feladatokat. Gyakran az informatikai biztonság megteremtésének egyetlen eszközeként alkalmazzák a teljes védelemnek ezt az elemét. Ez a megoldás azonban – ami gyakran csak jelszó ismeretéhez köti a magasabb szintű jogosultságokat is – erősen eltúlozza az algoritmusos védelem jelentőségét.

Az ügyviteli védelem az informatikai rendszert üzemeltető szervezet ügymenetébe épített védelmi intézkedések, biztonsági szabályok, tevékenységi formák együttese, amelyet szabályzatban szokás rögzíteni. A védelemnek ezt a területét szokták adminisztratív védelemnek is nevezni.

Míg a fizikai védelem a rendszerbe való engedélyezett belépési pontokat jelöli ki, addig az ügyviteli védelem a belépési pontok igénybevételének elfogadható, elvárt formáit rögzíti. Az ügyviteli védelem mintegy összekapcsolja a fizikai és algoritmusos védelem eszközrendszerét, ezzel valósítva meg az informatikai biztonság teljességét.

Különösen nagy jelentőségűek a hatékony informatikai biztonsági megoldások az egészségügy területén, ahol nagy jelentőségű, komplex alkalmazások kezelnek óriási mennyiségű különleges adatot.

A jelszó hatékony informatikai biztonságot nyújtó alkalmazása körül sok a bizonytalanság. Még az informatikai szakemberek körében is előfordulnak téves elképzelések a jelszó használatáról. Még több gondot okoz a felhasználók képzetlenségből eredő felelőtlensége.

A JELSZAVAK ELLENTMONDÓ TULAJDONSÁGAI

A jelszavakat titokban szokás tartani, ezért keveset tudunk mások jelszavának szerkezetéről és egyéb tulajdonságairól. A titkosság követelménye miatt nem helyes a jelszót feljegyezni, tehát olyan jelszót igyekszünk választani, amit nehézség nélkül emlékezetünkből bármikor fel tudunk idézni. Itt kezdődnek a problémák. A szakemberek természetesen mindenféle jó tanáccsal ellátnak, számos publikáció foglalkozik a jelszóválasztás témájával.

Az ideálisan jó jelszó tulajdonságai az alábbiak:

- legalább 8-10 karakter hosszúak,
- nem tartalmaznak értelmes szavakat, kifejezéseket,
- tartalmaznak különféle betűket, számokat és egyéb jeleket is,
- könnyen megjegyezhetők,
- rendszeresen megváltoztatják őket.

A felsorolásból látható, hogy ezeket a feltételeket nem egyszerű dolog teljesíteni. Ha megnézzük, hogy a szakirodalom milyen jelszavakat nem ajánl, az alábbi tulajdonságokat találjuk:

- 8 karakternél rövidebbek,
- a jelszó tulajdonosához kapcsolódó (vagy nem kapcsolódó) értelmes szavakat, kifejezéseket tartalmaznak,
- csak betűkből állnak, esetleg néhány számot is tartalmaznak, de egyéb jelek nem szerepelnek bennük,
- könnyen megjegyezhetők,
- hosszú ideig nem változtatják meg őket.

A két felsorolásból szembetűnő, hogy a legnagyobb problémát a jelszavak megjegyzése jelenti, hiszen egy telje-

sen értelmetlen, kisbetűket, nagybetűket, számokat és még egyéb írásjeleket is tartalmazó, legalább 8 karakter hosszú „szöveget” fejben tartani nem könnyű feladat.

Ebből az alaphelyzetből adódik, hogy a felhasználók hajlamosak valahová felírni a jelszót, az sem ritka, hogy telefonon, e-mail-ben vagy SMS-ben továbbítják azt egymás között. Nyilvánvalóan fennáll annak a veszélye, hogy valamelyik – akár magas jogosultságú – felhasználót sikerül megszemélyesítenie egy rosszindulatú betolakodónak.

Az egyik legismertebb egyszerű megoldás a jelszó megjegyzésére az úgynevezett memoriter módszer, amihez egy kívülről megtanult verssornak, slágerszövegnek, egy idegen nyelvű mondatnak vagy más hasonló jól megtanult szövegnek a biztos felidézésére van csupán szükség. Ha a versrészlet az, hogy „Még nyílnak a völgyben a kerti virágok“, akkor a jelszó lehet: MNAVAKV. Tehát a memoriter felidézése közben a szavak kezdőbetűit leírjuk a billentyűzeten. Ez már ebben a formában is elfogadható jelszónak számít. Ha még hozzáteszünk néhány számot vagy írásjelet, és némelyik betűt kisbetűre változtatjuk, akkor már szinte tökéletes jelszót kapunk. Az előbbi memoritert kiegészítve kérdőjellel és a billentyűzet numerikus része egyik átlójában elhelyezkedő három számmal (MNaVaKV?159), akkor már elegendően biztonságos jelszót kaphatunk a legmagasabb jogosultsággal rendelkező rendszergazda számára is.

Létezik néhány más módszer is, de a felhasználók viszonylag ritkán alkalmazzák ezeket, inkább felírják a jelszót egy „nagyon biztonságos” helyre, vagy olyan jelszót választanak, amit biztosan nem felejtenek el. A leggyakoribbak a keresztnevekből és dátumokból álló jelszavak, amelyek kötődnek a felhasználó személyéhez, ezért ezek az elfogadhatatlanul rossz kategóriába esnek.

Egy jelszó biztonságának mértékét például az [1] honlapon vizsgálhatjuk meg, ahol tanácsokat is kaphatunk a helyes jelszóválasztáshoz.

A jelszavak gyengeségeit kihasználja néhány szoftvergyártó, és olyan szolgáltatásokat ajánl (például [2] és [3] honlapok) amelyekkel a gyenge jelszavakat – főként az Office-csomag fájlmegnyitást akadályozó jelszavait – rövid idő alatt hatástalaníthatjuk. Bizonyos esetekben meglepően jó eredményeket szolgáltat, főként angol nyelvű környezetben.

Ezek után kijelenthető, hogy a megfelelő informatikai biztonság megteremtésére a jelszó önmagában nem alkalmas. Következésképp, az olyan egészségügyi adatokat kezelő alkalmazások, amelyek egyetlen adatvédelmi eleme a jelszó használata, jelentős biztonsági kockázatot jelentenek a működtető számára.

Ezek után joggal merül föl a kérdés: mi a megfelelő informatikai biztonságot nyújtó megoldás a felhasználók azonosítására az egészségügyben? A jó megoldás három elemű:

- Komplex szemlélet: fizikai, algoritmusos és ügyviteli védelem együttes alkalmazása.
- A felhasználók és üzemeltetők megfelelő tájékoztatása, képzése.
- A „valamivel rendelkezik, és valamit tud” elv alkalmazása a felhasználóazonosításban.

Ez utóbbi azt jelenti, hogy a rendszerbe történő bejelentkezéskor minden felhasználó alkalmaz egy eszközt (például bankkártya, egyéb azonosító kártya, ujjlenyomat) és beírja – lehetőleg jó minőségű – jelszavát is.

Természetesen igen fontos tényező a költséghatékonyság is. A bankkártyák elég jól működnek, nyilvánvaló gyengeségük, hogy a jelszó ebben a rendszerben a mindössze négy számból álló PIN. Egy hasonló rendszer a hazai egészségügyben jelenleg nehezen képzelhető el, bár vannak ilyen – jelentős egyszeri beruházást igénylő – jól működő chipkártyás alkalmazások Európában.

Van olyan megoldás is, ami egyszerűbb eszközökkel valósítja meg az említett elvet.

KRIPTOGRÁFIAI ALAPOK

A jelszó biztonságos működéséhez szükséges kriptográfiai építőkövek helyes kiválasztása és megfelelő alkalmazása nagyban befolyásolja a megvalósítható informatikai biztonság minőségét. Az egyik fontos elem az *f* egyirányú függvény, amelynek *f(x)* függvény értékét könnyű kiszámítani *x* ismeretében, de az *f(x)* érték birtokában csaknem lehetetlen meghatározni a hozzá tartozó *x* értéket. Az egyirányú függvény működése hasonlítható egy húsdarálóhoz, amibe néhány húsdarabot rakva előállítjuk a pépesre megdarált húst, majd ebből szeretnénk valahogyan visszakapni az eredeti néhány húsdarabot, ami nyilvánvalóan lehetetlen.

Az *f* függvény egy fontos tulajdonsága az úgynevezett lavina hatás, aminél az *x* input egy bitjének megváltozása az *f(x)* bitjei legalább felének megváltozását eredményezi. Lényeges még, hogy a függvényérték tetszőlegesen nagy input esetén is ugyanolyan kicsi méretű, tipikusan 128, 256 vagy 512 bit. Ezért a függvényértéket szokták üzenetkivonatnak, esetleg ujjlenyomatnak is nevezni. Klasszikus, jól működő egyirányú függvény az MD5 (RFC 1321) és az SHA (RFC 3174) függvénycsalád. Hazai fejlesztésű, Codefish nevű egyirányú függvény is létezik (lásd [4] honlap). Szövegek üzenetkivonatának elkészítését például az [5] honlapon próbálhatjuk ki, ahol a legismertebb megoldások függvényértékeit hasonlíthatjuk össze.

A jelszó működéséhez szükséges másik fontos építőelem a véletlenszám-generátor, ami olyan bitsorozatokat állít elő, amelyekben a bitek megjósolhatatlanul követik egymást. Ilyen – valóban véletlen – sorozatot számítógéppel előállítani nem egyszerű feladat. A biztonságosnak tekinthető alkalmazások is megelégednek úgynevezett álvéletlen (pszeudorandom) generátorok alkalmazásával, amelyek megfelelő algoritmusokkal, általában valódi véletlen bitsorozatok felhasználásával állítanak elő kriptográfiailag megbízható álvéletlen számokat. Ilyen módszert ír le például a NIST SP 800-90 ajánlás. Magyar fejlesztésű, Numberfish nevű álvéletlen generátor is létezik (lásd [4] honlap).

Nélkülözhetetlen a helyes jelszavas védelem korrekt használatához egy bizonyítási módszer, amelynek neve nullaismeretű bizonyítás (zero knowledge proof). Az ilyen bizonyítási eljárás során az egyik fél (Bizonyító) úgy győzi meg a másikat (Ellenőrző) egy titok ismeretéről, hogy a másik félnek nem árulja el a titkot, de az mégis kénytelen elhinni, hogy partnere azt ismeri.

Egy bank ügyfele hasonlóképpen győzi meg bankkártyája elfogadóhelyét arról, hogy ismeri PIN-jét, anélkül, hogy a bankrendszer tudná azt. Ha egy felhasználó – nevét és jelszavát megadva – bejelentkezik egy számítógépes rendszerbe, szintén ezt a bizonyítási módot alkalmazza. A rendszer üzemeltetői természetesen nem ismerik a felhasználó jelszavát, mert az sehol nincs tárolva.

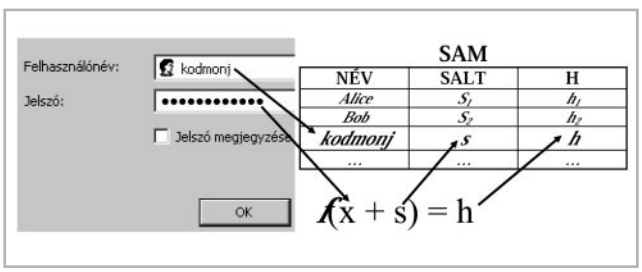
Az ilyen megoldások megengedhetnek néhány téves bizonyítási kísérletet, hiszen 2-3 eltévesztett PIN vagy jelszó lényegesen nem csökkenti a módszer hatékonyságát.

A JELSZÓ HELYES MŰKÖDÉSE

A jelszó működését az 1. ábra segítségével tudjuk szemléltetni, ahol az *f* az egyirányú függvény, *s* egy kriptográfiailag megbízható álvéletlen szám, *h* pedig az üzenetkivonat. A felhasználónevet, az *s* és a *h* értéket speciális módon tárolja a rendszer egy SAM (Security Access Modul), esetleg Security vagy egyéb más nevű adatfájlban.

Ha egy új felhasználó kerül egy rendszerbe, akkor a név megadásakor a SAM-ban tárolódik felhasználóneve, a jelszó megadásakor pedig a rendszer előállítja az *s* értéket, azonnal hozzáírja konkatenációval az *x* jelszóhoz *(x+s)*, elvégzi a leképezést az *f* függvénnyel, letárolja a *h* értéket, majd végül letárolja az *s* értéket is a SAM-ban. Látható, hogy a jelszó a lehető legrövidebb ideig tárolódik a memóriában, és egyáltalán nincs tárolva a rendszerben, ami megadja a lehetőséget a nullaismeretű bizonyítás módszerének alkalmazására.

Ha egy felhasználó bejelentkezik nevének és jelszavának megadásával, akkor a rendszer a felhasználónév alapján kikeresi a SAM táblázat megfelelő sorát, az ott található *s* értéket azonnal hozzáírja a jelszóhoz *(x+s),* és elvégzi az *f(x+s)* érték kiszámítását. Ha ez megegyezik a felhasználónév sorában tárolt *h* értékkel, akkor a felhasználó helyes jelszót adott meg.



1. ábra

Mivel az *f* függvény egyirányú, az *f(x+s) = h* értékből teljesen reménytelen kiszámítani az *x+s* értéket, majd felhasználva *s* értékét meghatározni az *x* jelszót. Az *f* függvény tulajdonságai és a nullaismeretű bizonyítás módszere együttesen garantálják a jelszó titkosságát úgy, hogy lehetséges annak ellenőrzése, annak ellenére, hogy a jelszó nincs tárolva a rendszerben.

A különféle hálózati operációs rendszerekben a SAM-fájl általában egyedi módon kezelt, ezért a hozzáférés és a fájl szerkezetének megismerése nehéz feladat.

Mivel a jelszó működésének leírása általában nem nyilvános, ezért nem lehetünk biztosak abban, hogy az egyes informatikai alkalmazásokban a fent ismertetett módszert használják. Különösen problémás lehet a speciális fájlok (például Office-csomag fájljai, Acrobat pdf-fájlok) felhasználási jogosultságát kezelő jelszavak konstrukciója, ahol az üzenetkivonat és a salt tárolása – a hordozhatóság miatt – kizárólag magában a fájlban lehetséges.

Nagy biztonsági kockázatot jelenthet az egyedi gyártók által készített kórházi integrált rendszerek, a háziorvosi szoftverek és egyéb más, egészségügyben alkalmazott szoftverek jelszóellenőrző megoldásainak működése, amelyek általában szintén nem nyilvánosak.

Egy információbiztonsági megoldás akkor számít kielégítő minőségűnek, ha ismert, hosszú időn keresztül kifogástalanul működő módszereket és algoritmusokat alkalmaz. Ha egy biztonsági megoldás működését senki sem ismeri, akkor annak használatát a felhasználóknak el kell utasítani, hiszen megengedhetetlenül nagy kockázatot jelenthet számukra. Mivel tökéletes biztonság nem létezik, csak a szakmai nyilvánosság jelenthet kielégítő biztonsági garanciát.

A JELSZAVAS AZONOSÍTÁS KOMPROMITTÁLÓDÁSÁNAK LEHETŐSÉGEI

A jelszavas védelem feloldására számos lehetőség van. A jelszót meg lehet szerezni a felhasználótól és abból a számítógépes rendszerből, ahol azt használják.

Talán a legegyszerűbb a felhasználó emberi gyengeségeinek, hanyagságának és képzetlenségének kihasználásával megszerezni a jelszót. Hasonlóan egyszerű és hatékony, ha megfigyelik a felhasználó által a billentyűzeten beírt jelszóhoz tartozó karaktereket (keylogging). Ehhez a módszerhez igen hatékony, háttérben működő szoftverek is léteznek, amelyek tárolnak minden billentyűleütést egy adatfájlban, és még az is lehetséges, hogy ezt automatikusan elküldik egy megadott e-mail címre. Többek között ezért is fontos, hogy az egyes számítógépes munkahelyeken csak ellenőrzött, ismert szoftverek működjenek.

Lehetséges egy jelszót feltörni, ami egy adott felhasználónévhez tartozó jelszó teljes mértékű ismeretét, birtoklását jelenti. Ezáltal lehetséges egy felhasználó teljes mértékű megszemélyesítése. Ezt gyakran összetévesztik a jelszó hatástalanításával, ami nem jelenti a jelszó birtoklá-

sát, csupán a védett jogosultságok – valamilyen más módszerrel történő – megszerzését, anélkül, hogy a jelszót feltörnék.

A hatástalanítást általában könnyebb kivitelezni, és többnyire így is megvalósítható a megszemélyesítés.

A feltöréshez két jól ismert módszer létezik, ezeket gyakran kombinálják is.

A nyers erő módszer végigpróbálgatja a jelszó összes pozíciójában a lehetséges karakterek minden változatát, ezért nem túlságosan hatékony. A 95 nyomtatható karaktert felhasználó, 8 hosszúságú jelszó nyers erővel történő feltörése körülbelül 210 évet vesz igénybe. Az ugyanilyen összeállítású, de 5 hosszúságú jelszó feltörése már csak 2 perc. A kizárólag kisbetűkből álló 8 illetve 5 hosszúságú jelszó pedig 2 nap és 10 óra, illetve 12 másodperc alatt törhető fel. Mindegyik példában olyan számítógépet és szoftvert feltételeztünk, ami másodpercenként egymillió jelszó megvizsgálására képes, ami teljesen reálisnak tekinthető teljesítmény.

A másik módszer az összehasonlítások hatékonyságának növelésére speciális szótárakat és hatékony nyelvészeti algoritmusokat használ. A különféle nyelvi környezetekben alkalmazott helyesírásellenőrzők szótárait és algoritmusait bővítik ki a felhasználókkal kapcsolatba hozható szövegekkel és speciális keverő – a felhasználók vélhető szokásaihoz igazodó – algoritmusokkal. Ez a módszer hihetetlenül hatékony lehet, főként akkor, ha nagymértékben ismertek a felhasználók adatai és különféle szokásai.

A feltörés és hatástalanítás bármelyik módszerének alkalmazásához azonban szükséges az egyirányú függvény ismerete, továbbá a SAM-fájl birtoklása és szerkezetének ismerete, hiszen ezek hiányában a vélt és valódi jelszó összehasonlítása nem lehetséges.

A jelszó feltörését és hatástalanítását gyakran a legnagyobb biztonsági kockázatnak tartják. A fentiekből azonban látható, hogy ez nem így van, hiszen ehhez igen jelentős szakértelem, naprakész ismeretanyag szükséges, nem elegendő beszerezni egy kellően nagy teljesítményű szoftvert, ahogyan azt egyes szoftvergyártók (lásd [2, 3] honlap) állítják.

Az igazi nagy kockázatot a felhasználók és üzemeltetők felelőtlensége, hanyagsága és képzetlensége, röviden az emberi tényező jelenti.

GYAKORI PROBLÉMÁK A JELSZAVAKKAL

Tekintettel a fenti módszerekre és konkrét feltörési adatokat tartalmazó példákra, látható, hogy nagyon komoly kockázatot jelent a túl rövid vagy értelmes szavakat is tartalmazó jelszó, főként, ha az összefüggésbe hozható a felhasználó személyével. Az ilyen típusú problémák alkotják a jelszavas védelemmel kapcsolatos felhasználó oldali rossz megoldások túlnyomó részét.

Az üzemeltető rendszergazdák felelőssége is igen nagy, hiszen általában lehetőségük van megfelelő rendszerbeállításokkal kikényszeríteni, hogy a felhasználók milyen hosszúságú, milyen összetételű jelszót használhatnak, továbbá milyen időközönként kell azt kicserélniük, és hány különböző jelszócsere után használhatják ismét ugyanazt a jelszót.

Nyilvánvaló azonban, hogy a rendszergazdák ezekkel a lehetőségekkel kevéssé élnek, hiszen a felhasználók jelszavaikkal kapcsolatos problémáikkal őket hívnák segítségül, amivel munkájuk nagy mértékben megszaporodna. Az is nyilvánvaló, hogy a jelszókezelési szabályok sarkos kikényszerítése esetén a felhasználók még kevésbé tartanák be azokat, még gyakoribb lenne a jelszó feljegyzése, átadása, illetve közös vagy csoportos jelszavak használata.

Gyakran előforduló, de szintén rossz megoldás, hogy a felhasználónév és a jelszó csak néhány karakterben különbözik. Ekkor a feltöréshez használatos szótárat kibővítik a lehetséges felhasználónevekkel, és nyelvészeti keverő algoritmusokkal növelt hatékonyságú próbálgatással könnyen feltörik a jelszót.

A különféle rossz megoldások kezelésére ki lehetne egészíteni a felhasználónevet és jelszót kérő beléptető rendszert egy jelszóminősítő résszel, ami minden alkalommal figyelmeztetné a felhasználót, hogy felhasználóneve és jelszava nem felel meg a minimális elvárásoknak. Nagyobb kockázatú hiányosságok esetén pedig kikényszerítené a jelszó megváltoztatását, mindaddig, míg az nem teljesíti a rendszer üzemeltetői által beállított minimális feltételeket.

Sajnos ilyen komplex – a felhasználónevet és a jelszót is együttesen figyelő – minősítő biztonságirendszer-elemekkel az egészségügyi és más alkalmazásokban alig találkozunk.

A szakmai szempontból kielégítő kompromisszumot nagyon nehéz megtalálni, az is lehetséges, hogy nincs is ilyen megoldás.

Egy tavalyi reprezentatív felmérés tanulmánya [6] kimutatta, hogy az átlagos jelszavak 7,8 karakter hosszúak, 57,9 százalékuk tartalmaz személynevet vagy értelmes szót, 77,6 százalékuk számot, 14,1 százalékuk kis- és nagybetűket is, és csak 2,1 százalékukban van az előző kategóriáktól eltérő karakter. Mindössze 1 százalékot tett ki azoknak a száma, akik a jelszóadás alapszabályai szerint jártak el, vagyis a felsorolt kategóriák mindegyikét használták jelszavukban.

Az idézett felmérésből kiderül, hogy az irodai alkalmazottak negyede feljegyzi jelszavát, 15,5 százalékuk valahol a számítógépén – például egy szöveges fájlban – , 13,9 százalékuk külső eszközön, gyakran mobiltelefonon tárolja azt. És ami még ennél is érdekesebb, a megkérdezett felhasználók több mint harmada igenis használja a különféle hálózati alkalmazások jelszómegjegyző funkcióját.

Hasonló eredményre jutott a világhírű kriptográfus, Bruce Schneier is [7] írásában, aki a MySpace közösségi portál 34 ezer felhasználójának bejelentkezési adatait elemezhette, amelyek adathalász támadás miatt kerültek nyilvánosságra.

A JELSZAVAS FELHASZNÁLÓAZONOSÍTÁS ALTERNATÍVÁI

Az eddig leírtak alapján a jelszó jól működő alternatívája nehezen képzelhető el. Valóban nem sok lehetőség létezik, a gyakorlatban csupán a jelmondat és a dinamikus jelszó van használatban.

A jelmondat (passphrase) tulajdonképpen egy hosszú – általában legalább 20 karakteres – jelszó funkciójú szöveg, azzal a lényeges eltéréssel, hogy értelmes szavakat, kis- és nagybetűket és írásjeleket tartalmaz. A jelmondat tehát általában egy értelmes mondat, amit sokkal könnyebb megjegyezni, mint a jelszót, és mégis nehéz feltörni. A szótáras feltörés veszélye miatt használatánál csak arra kell vigyázni, hogy szólás-mondás gyűjteményben, vagy hasonló ismert szöveggyűjteményekben ne legyen megtalálható. Hátránya, hogy nehéz vakon beírni, és sok rendszer nem támogatja, mert korlátozott a jelszó hossza, mivel jelmondat beírására a fejlesztők nem gondolnak.

A jelszó vagy a jelmondat tehát nem képes elfogadható informatikai biztonságot teremteni, igazi áttörést csak másfajta módszerek alkalmazása jelenthet.

A felhasználóazonosításnál a „valamivel rendelkezik és valamit tud" elv alkalmazásával érhető el a megfelelő szintű informatikai biztonság. Ezt alkalmazzák például a bankkártyák használatánál az elfogadóhelyek, hiszen a bankkártya készpénz helyetti elfogadásához a tulajdonosnak meg adni a PIN-t, amit a kártyatulajdonos tud. A PIN tulajdonképpen egy igen gyenge jelszó, de a kártya birtoklása és a PIN ismerete együtt megfelelő szintű biztonságot nyújt.

Ezt az elvet és a nullaismeretű bizonyítás módszerét alkalmazza az úgynevezett dinamikus jelszó, amely alapvetően eltér a hagyományos változattól. A dinamikus jelszó használata tulajdonképpen egy többlépéses protokoll végrehajtását jelenti.

Ebben az esetben nem a jelszó a felhasználó által produkálandó ismeret, hanem a felhasználóhoz rendelt matematikai kifejezés, képlet. A felhasználóazonosítás abból áll, hogy a felhasználó megad egy hagyományos jelszót, amelynek hatására az azonosító szerver egy véletlen számot küld a felhasználónak, és ugyanakkor ezt a véletlen számot a szerveren tárolt – felhasználóhoz tartozó – matematikai kifejezésbe helyettesíti. A felhasználó a birtokában lévő képletbe helyettesíti a szervertől kapott véletlen értéket, majd az így kiszámított eredményt visszaküldi a szervernek. Az összehasonlítja a visszakapott értéket az általa kiszámítottal, és egyezés esetén elfogadja a felhasználó bejelentkezését.

Ebben a konstrukcióban a felhasználó oldalán szükség van egy általa birtokolt megfelelő eszközre – például intelligens kártyára –, ami automatikusan elvégzi a titkos matematikai kifejezés helyettesítési értékének meghatározását. A szerveren pedig szükséges egy megbízható megoldás az egyes felhasználók titkos képleteinek megfelelő tárolására.

A dinamikus jelszó használata közben a kommunikációs vonalat figyelő lehallgató csak olyan adatokhoz tud hozzájutni, amely nulla információt ad az illegális hozzáférés megvalósításához, így nyílt vagy kevéssé védett kommunikációs csatornán is biztonságosan megoldható a felhasználó azonosítása.

A titkos képletek megfelelő tárolása és a helyettesítési értékek kiszámítása gondot okozhat. A felhasználó oldalán ezt egy intelligens kártya alkalmazásával szokás megoldani, a szerver oldalán – a védett környezet miatt – könnyebb és olcsóbb a megfelelően biztonságos megoldást alkalmazni.

Ne feledkezzünk meg arról, hogy szinte mindenki hord magánál egy intelligens kártyát, mégpedig mobiltelefonjában egy SIM kártyát, aminek segítségével az alapfunkciókon kívül sok egyéb is megvalósítható.

Erre a tényre alapoz a dinamikus jelszó egy változata, az úgynevezett mobil aláírás, ami olcsó és megfelelő biztonságú megoldást szolgáltat. A mobil aláírás egy egyszerűsített változatának protokoll-leírása a következő:

- A felhasználó kezdeményezi bejelentkezését biztonságos kommunikációs csatornán (például https-protokoll) egy szerverre: megadja felhasználónevét és jelszavát.
- A szerver ellenőrzi a felhasználónév alapján a jelszó helyességét. Ha a jelszó helyes, generál a felhasználó számára egy álvéletlen számot, amit rövid ideig tárol. Ha a jelszó rossz, akkor a hagyományos jelszóellenőrzés szabályait alkalmazza.
- Ha a jelszó helyes, a szerver egy másik biztonságos kommunikációs csatornán (például mobiltelefonon keresztül, automatikus SMS-ben) elküldi az álvéletlen számot a felhasználónak.
- A felhasználó a kapott álvéletlen számot megadja a bejelentkezéshez, elküldi azt az általa kezdeményezett biztonságos csatornán (például https-protokoll) a szervernek.
- A szerver a felhasználónév alapján ellenőrzi az álvéletlen szám helyességét.
- Ha a szerver által egyik biztonságos csatornán elküldött és másik biztonságos csatornán visszakapott álvéletlen szám egyezik, akkor elfogadja a felhasználó bejelentkezését, és azonnal törli a protokollban használt álvéletlen számot.

Ez a megoldás megfelelő biztonságot nyújthat a nagy tömegű személyes és különleges adatot kezelő egészségügyi alkalmazások számára is. A mobil aláírás fenti változata valószínűleg a felhasználóazonosítás egyik legolcsóbb, legegyszerűbb és elegendően biztonságos megoldása. Könnyen implementálható a meglévő alkalmazások kiegészítésével, a hazai mobilszolgáltatókkal egyedi szerződések köthetők az automatikus SMS-ek küldésének olcsó megoldására, a felhasználók általában rendelkeznek kizárólag saját fennhatóságuk alatt álló mobiltelefonnal. A pénzintézetek is szinte kizárólag ezt a megoldást alkalmazzák internetes házibank-szolgáltatásuk biztonságának fokozására.

A mobil aláírásnak létezik olyan változata is, ami képes egy dokumentum hitelesítésére elektronikus aláírás és más kriptográfiai megoldások segítségével. Ehhez azonban speciális SIM kártyára van szükség, ami a hazai mobiltelefonszolgáltatóknál is rendelkezésre áll.

A mobil aláírás részleteiről elsősorban a European Telecommunications Standards Institute (ETSI) honlapján [8] lehet további információkat találni, amelyek között témánk szempontjából a [9] dokumentum a legfontosabb.

ÖSSZEFOGLALÁS

Írásunkban bemutattuk, hogy a csupán jelszót alkalmazó felhasználóazonosítás nem nyújt elégséges informatikai biztonságot az egészségügyben keletkező nagy tömegű személyes és különleges adat kezeléséhez.

A lehetséges módszerek közül egy megfelelő biztonságot adó, olcsó, könnyen bevezethető megoldást javaslunk: a hagyományos felhasználónév és jelszó megadást erősítsük meg egy egyszerűsített mobil aláírással, és ne feledkezzünk meg arról, hogy az elvárt biztonság csak komplex védelem alkalmazásával érhető el.

Az európai trendek szerint valószínűleg nem kerülhető el az intelligens kártyás betegazonosítás és a szakdolgozók professzionális intelligens kártyával történő azonosítása. Ennek bevezetéséig az általunk ajánlott módszer alkalmazható, legalább a magasabb jogosultságú felhasználók és főként az üzemeltetők körében.

IRODALOMJEGYZÉK

[1] http://www.securitystats.com/tools/password.php
[2] http://www.decryptum.com/hu
[3] http://www.lostpassword.com
[4] http://www.kripto.hu
[5] http://www.johnmaguire.us/tools/hashcalc
[6] O. Fredstie: End Users Attitudes and Behaviours towards Password Management: Survey Report
[7] Bruce Schneier: Real-World Passwords, http://www.schneier.com/blog/archives/2006/12/realworld_passw.html
[8] http://www.etsi.org
[9] Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface (ETSI TS 102 204 szabvány)

A SZERZŐ BEMUTATÁSA

Dr. Ködmön József a debreceni Kossuth Lajos Tudományegyetemen szerzett 1979-ben matematika tanári diplomát, majd 1990-ben számítástechnika szakos középiskolai tanári képesítéssel egészítette azt ki. 1991-ben elkezdte munkáját Nyíregyházán a Debreceni Orvostudományi Egyetem Egészségügyi Főiskolai Karán, ahol részese volt az egészségügyi ügyvitelszervező képzés elindításának. Eleinte főként a tananyag kialakításában és oktatásszervezési feladatok ellátásában vett részt, később pedig önálló kutatási területként a kriptográfia számelméleti vonatkozásaival, majd egészségügyi alkalmazásával foglalkozott. 2004-ben PhD-fokozatot szerzett, értekezése kriptográfia témájú. Jelenleg a Debreceni Egyetem Egészségügyi Főiskolai Karán dolgozik, az Egészségügyi Informatika Tanszék vezetője.

Bodnár Károly 1998-ban szerzett matematika-számítástechnika szakos tanári diplomát, majd a Debreceni Egyetemen 2006-ban informatika tanári diplomát, jelenleg a Debreceni Egyetem Egészségügyi Kar Egészségügyi Informatika Tanszékének oktatója. A fiatal szakember szakközgazdász végzettséggel is rendelkezik, kutatási területe az egészségügyi informatika biztonsági vonatkozásaihoz is kötődik.