BÁNKI KÖZLEMÉNYEK
2. ÉVFOLYAM 3. SZÁM

Hálózati kommunikáció biztonságának becslése

Nőthig Ádám, Zentai Dániel
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mechatronikai és Járműtechnikai Intézet, Budapest, Magyarország
nothig.adam@gmail.com, zentai.daniel@bgk.uni-obuda.hu

Absztrakt

A tanulmány célja, hogy egy olyan következtetési rendszert építsen fel, ami képes egy számítógépes hálózat kommunikációjának biztonságát becsülni és azt egy felhasználó számára is érthető módon közölni. A következtetési rendszert alkalmazva könnyen demonstrálható, hogy milyen hatással van a jelszavak hossza, a kommunikáció médiuma, információ titkosítására szolgáló eljárás valamit az azonosítási faltorok száma a biztonságra.

Kulcsszavak: Fuzzy rendszerek, hálózati biztonság, Wi-Fi biztonság, autentikáció

1. BEVEZETÉS

Sok kutatás jut arra a következtetésre, hogy egy átlagos számítógép felhasználó nincs tisztában azzal, hogy egy gyenge jelszó vagy a nem megfelelő kommunikációs protokoll milyen hatással lehet az adatainak biztonságára. [1] [2] Tanulmányunkban egyszerű bemenetekből számítunk egy mindenki számára érthető biztonsági mutatót a kommunikáció titkosításának minőségére.

A következtetési rendszert a MATLAB Fuzzy Logic Toolboxban építettük fel. Míg az autentikációs faktorok száma diszkrét logikai faktor, ezzel szemben a jelszavak hossza és a kommunikációs megoldás nem az. Különböző források eltérő adatokat adnak meg optimális jelszó hosszként, a kommunikációs protokollok osztályozását pedig különálló revíziók teszik bonyolulttá.

2. JELSZAVAK - AZ ELSŐ HIBA

2.1. Jelszavak természete

A jelszó általában az első biztonsági réteg az azonosítás során, sok rendszer esetén ez az egyetlen azonosítási faktor. A jó jelszóval kapcsolatos követelmények változnak rendszerről rendszerre, de általában minimum 8 karaktert ajánlanak, különleges karakterekkel kiegészítve, valamint, hogy ne használjuk ugyanazokat a jelszavakat különböző rendszereken. A fő probléma ezzel, hogy a jelszó természeténél fogva az embereknek nehezére esik emlékezni rájuk még anélkül is, hogy a fent említett szabályokkal bonyolítanak rajta. Ebből következően, ha lehetőségük van, vagyis, ha a weboldal vagy a rendszer nem teszi kötelezővé az emberek többsége figyelmen kívül fogja hagyni ezeket a szabályokat/javaslatokat.

Ezt a problémát fokozandó a GPU teljesítmény növekedése miatt a számítógépek egyre jobbak a jelszavak kitalálásában. Arról nem is beszélve, hogy a crypot valuta bányász őrület után a nagy teljesítményű GPU-k relatívan olcsón beszerezhetőké váltak, annyira, hogy akár egy átlagember is építhet olyan gépet, ami percek alatt képes egy 8 karakteres jelszó feltörésére. Még abban az esteben is, ha egy MD5 algoritmussal lett hash-elve, ami, habár egy elavult megoldás még mindig elég sok esetben használják. De volt arra is precedens, hogy több milliárd dolláros cégek milliónyi felhasználó adatát nyílt szövegként tárolták. [3] Tehát előfordulhat, hogy a jelszó biztonsága a felhasználó hatáskörén kívül esik. A következőkben a lehetséges megoldásokat mutatjuk be.

2.2. Biztonságos jelszavak

A biztonságos jelszavak alapja, hogy nehéz kitalálni. Úgy gondolnánk, hogy ez mindenki számára egyértelmű. Tekintsük át, hogy ez megfelel-e a valóságnak.

2013-ban a Google publikált egy tanulmányt, amiből kiderült, hogy a legtöbb ember olyan jelszót választ, ami a közösségi média oldalakon elérhető adataikból egyszerűen kikövetkeztethető. Ilyen információk például a születésük helye, a kisállatuk vagy a gyermekük neve. Szintén itt derült ki, hogy az emberek 48%-a több oldalon vagy rendszerben is ugyanazt a jelszót használja és hogy 3% a számítógépre ragasztott Post-it cédulán hagyja a jelszavát. [1]

A fentiekkel ellentétben jó megoldás lehet 2 vagy több egymással kapcsolatban nem álló szót összefűzni. [4] Jeff Yan arra az eredményre jutott, hogy egy mondat szavainak kezdőbetűit egymásután írva egy nehezen kitalálható, de könnyen megjegyezhető jelszót kapunk. [5] A speciális karakterek vagy számok előírása viszont kétélű kard ugyanis gyakran az a következménye, hogy úgy nevezett Leet speak-ben (1337) adják meg a felhasználók a jelszavukat. Vagyis bizonyos betűket numerikus karakterekkel helyettesítenek, mint például az i-t egy 1-sel vagy az e-t egy 3-sal. Ez a módszer viszont széles körben ismert és épp ezért nem növeli a jelszó biztonságát. Az, hogy egy sorral eltoljuk a billentyűzeten a leütőt gombokat szintén nem megbízható megoldás. [6]

2.3. A jelszavak halála

Több prominens személy is megjósolta már hogy a jelszavak kora véget ért, többek közt Bill Gates 2004-ben [7] és a Google Információ biztonsági menedzsere Heather Adkins 2013-ban [8]. Általában valamilyen biometrikus vagy kétfaktoros azonosítást javasolnak helyére. Egyes szakértők szerint viszont semmilyen másik technológia nem tudja a jelszavakat helyettesíteni kényelmesség, gyorsaság és költséghatékonyság terén. [9]

3. KOMMUNIKÁCIÓS MEGOLDÁSOK

3.1. Kommunikáció médiumai

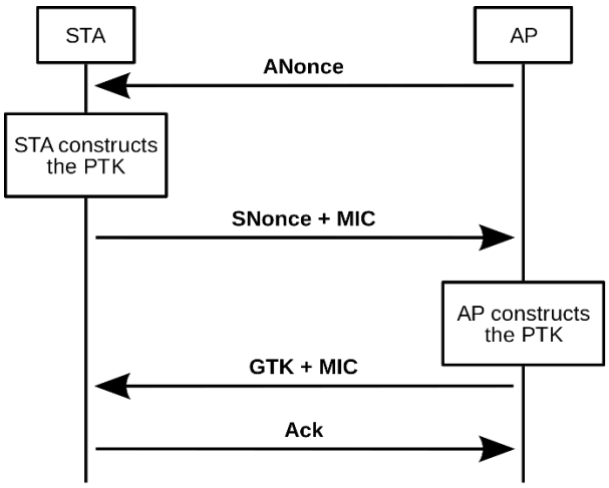
A tradicionális kábeles mellet egyre elterjedtebb a vezetéknélküli kommunikáció az IEEE 802.11 szabvány segítségével. Mivel az eszköz bárhova vihető kényelmet jelent használójának, mindemellett a legújabb Wi-Fi szabványok az 802.11ac és az 802.11ax képesek több GBit/s-es sebességre, amit a legtöbb felhasználó nem is tud maximálisan kihasználni. A rádióhullámos kommunikációval viszont új problémák jelentek meg.

Míg egy kábeles kommunikáció lehallgatásához általában fizikai hozzáférésre van szükség addig a rádióhullámokat bárki foghatja, aki hatókörön belül van és rendelkezik akár egy olcsó vevővel is. Ezért a jeleket valamilyen módszerrel titkosítani szükséges hacsak nem akarjuk, hogy a potenciálisan szenzitív adatainkhoz hozzáférjenek.

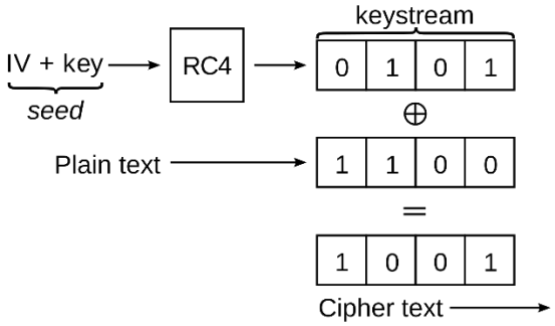
3.2. A 802.11 titkosítási szabványok

Az első titkosítási szabvány az WEP mely az eredeti 802.11-es szabvánnyal együtt jelent meg. A W(ired) E(quivalent) P(rivacy) nevű protokollnak a célja a vezetékessel egyező biztonság elérése volt.

A szabvány egy 64 bites RC4-es kulcsot generál a megadott jelszóból, ez későbbi verziókában akár 128 vagy 152 bites is lehet.



1. ábra WEP/WPA2 kézfogás protokoll



2. ábra WEP kulcs generálás

A rendszer hibája, ami a feltöréséhez is vezetett, hogy a kulcs generálás során egy 24 bites úgy nevezett Inicializáló vektort (IV) nyílt szövegként küld el, ezt a vektort nem szabad többször felhasználni, viszont egy 24 bites hossz nem elegendő az ismétlődések elkerülésére egy sűrűn használt hálózaton. Ráadásul a születésnap paradoxonból kifolyólag annak az esélye, hogy ezek az IV-k 5000 csomagonként ismétlik egymást 50%. Ennek ismeretében passzív módszerekkel is feltörhető kulcs.

A kulcs hosszának növelése nem jelent lényeges biztonság növekedést hiszen a támadás a kriptográfiai eljárás hibáját támadja nem a kulcsot. Az FBI 2005-ben nyilvánosan elérhető eszközökkel 3 perc alatt feltört egy WEP jelszót, [10] 2007-ben 45 millió felhasználó adatát lopták el a TK Maxx cégtől a WEP gyengeségeinek kihasználásával. [11] Az átlag felhasználó szerencséjére viszont az újabb routerek egyáltalán nem támogatják ezt a hitelesítési módot, de még sok régebbi modellben ez az alapbeállítás.

A látványos biztonsági hibák kijavítására a Wi-Fi Alliance 2013-ban bevezette a Wi-Fi Protected Access-t (WPA) mint egy átmeneti megoldás. A hosszútávú megoldást a WPA2 jelente mikor 2014-ben hivatalosan is része lett az IEEE 802.11i szabványnak. Ez a titkosítás már Temporal Key Integrity Protocol-t (TKIP) használ, vagyis minden csomagot más kulccsal titkosít, így megakadályozza az olyan jellegű támadásokat amik legyőzték a WEP-et.

Mint ahogy az az 1. ábrán is látszik a kézfogási protokollja megegyezik a WEP-el. A legnagyobb problémát bár kijavították, de az a megoldás még mindig sebezhető, passzív és offline támadásokkal szemben. Habár a kulcsot titkosítva küldik el, a protokoll nem akadályozza meg hogy elfogják és feltörjék a saját gépen. Nem kell még a hozzáférési ponttal sem kommunikálni.

Ahogy a kulcs rendelkezésre áll minden üzenet dekódolható, tehát ha megosztott a kulcs, mint például egy kávézóban vagy hotelben akkor egyáltalán nem biztonságos.

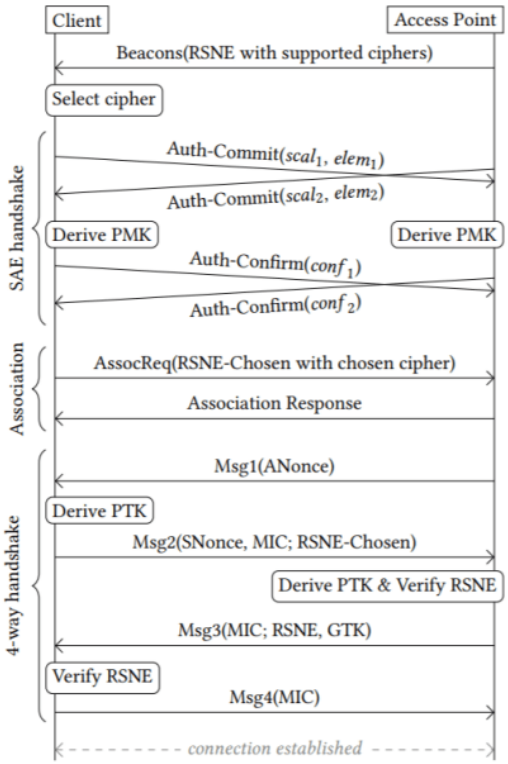
Egy 2017-ben publikált cikk bemutatta, hogy lehet lehallgatni az adásokat anélkül, hogy visszafejtenék a kulcsot ez az úgynevezett KRACK (Key Reinstallation Attacks) támadás, mely a WPA minden verzióját érintette habár különböző hatásai voltak a hálózatra az alkalmazástól függően. Ez a támadás a kézfogási protokoll egyik gyengeségét használta ki. [12] Emellett számos támadással szemben sebezhető mind hozzáférés mind denial of service (DoS) téren. Így a Wi-Fi Alliance is úgy tartotta, hogy ideje lecserélni ezt a több mint egy évtizede szolgáló protokollt.

2018-ban bemutatták a WPA3-at, ami orvosolni hivatott a kettes verzió hibáit. Az új rendszerrel elméletileg nem lehetséges az offline kulcs fejtés és biztosítja, hogy ha a kulcsot meg is fejtik akkor sem lehet az előző vagy jövőbeli üzeneteket vele visszafejteni. A protokollt azonban sokan már az elterjedése előtt temetik.

2019 áprilisában ugyanis ugyanaz a csoport, aki a KRACK támadást kifejlesztette, felfedezett 5 sebezhetőséget ezeket együttesen DRAGONBLOOD-nak nevezték el. 4 támadás az új DragonFly kézfogást támadja.

Ezek a támadások a 3. ábrán látható kézfogási protokoll második és harmadik lépéseit célozzak meg.

Mivel a piacon minden újonnan bevezetett eszköznek kompatibilisnek kell lennie a korábbi termékekkel, ezért a WPA3-as eszközökön megtalálható újításoknak is funkcionálnia kell a WPA2-es eszközökön. Ezt használja ki az utolsó publikált támadási módszer ami kényszeríti a hozzáférési pontot arra, hogy WPA2-vel azonosítson, így megkerülve a frissebb verzió offline kulcs fejtési korlátozásait. [13]



3. ábra WPA3 kézfogás protokoll

A támadások pontos eljárását még nem publikálták, először a Wi-Fi Alliance-et informálták róla, hogy azt javítani tudják, amit már meg is kezdtek.. Mivel ez a verzió még nem túl elterjedt a hibákat könnyebb korrigálni, mint az előző 2 verzió estén. Ezért talán még túl korai kijelenteni a protokollról, hogy a biztonsága nem megfelelő.

4. Azonosítási faktorok

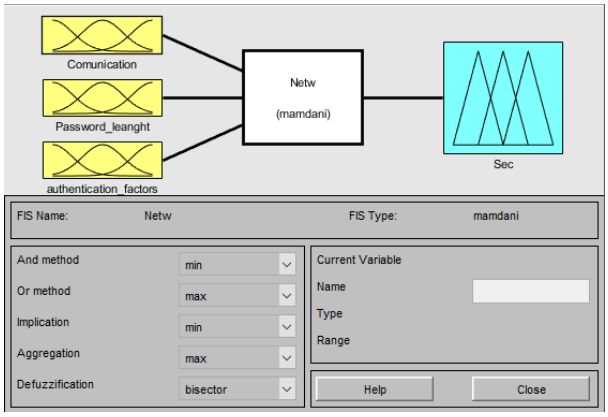
A jelszó a legelterjedtebb egyfaktoros azonosításai módszer. [14] A fentiek szerint ez gyakran nem elég biztonságos és ezért plusz azonosítási faktorokat is bevezethetnek, hogy javítsák a védelmet. A legelterjedtebb faktorok alapja, valami, amit tud a felhasználó (pl.: jelszó), valami a felhasználónál van (pl.: egyszer használatos kód generátorok), valami, ami a csak a felhasználóra jellemző (pl.: bio-metrikus). [15] Fontos megjegyezni, hogy ezek a faktorok nem egyenlőek. A bio-metrikus azonosítás például hajlamos a hamis elfogadásra amikor egy nem megfelelő személynek is hozzáférést add az esetek bizonyos százalékában. Valamint bio-metrikus adatokat relatíve könnyű ellopni. A több faktoros azonosítás támogatói szerint megfelelő kommunikációs protokollal kombinálva lényegesen csökkenthető az illetéktelen hozzáférések esélye.

5. A KÖVETKEZTETÉSI RENDSZER

A modellben Mamdani típusú következtetési rendszert alkalmaztunk, melyben a szakértői tudást a következő felépítésű szabályok reprezentálják:

IF x_1 *is* A_{1,i_1} *and ... and* x_n *is* A_{n,i_n} *THEN y is* $B_{i_1,\dots,i_n}$,

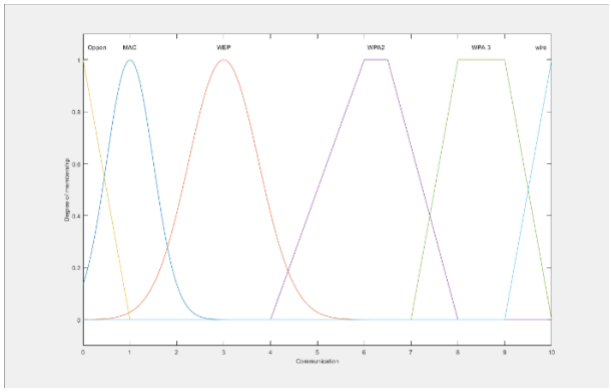
ahol A_{k,i_k} a k-adik bemenethez tartozó i_k-adik antecedens, $B_{i_1,\dots,i_n}$ az a fuzzy halmaz, amit a szabályok konzekvens részéhez rendelünk, $i_j = 1, \dots, n_j$; és n_j a j-edik bemenethez tartozó antecedens halmazok száma.



4. ábra következtetési rendszer áttekintése

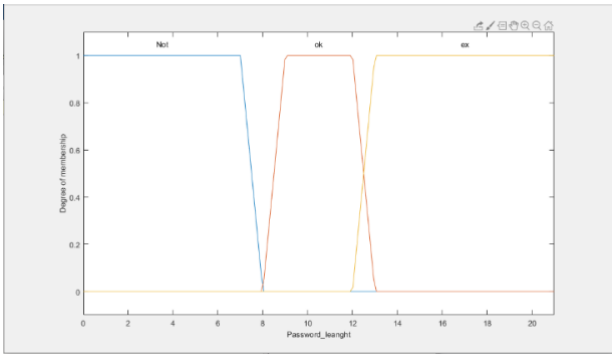
Ahogy az 1. ábrán is látható, a következtetési rendszernek 3 bemenete van, ami alapján a kommunikáció biztonságosságát értékeli. Ezek a bevezetésben említett jelszó hossz, kommunikáció módja és az azonosítási faktorok száma. Ebből a három bementi adatból értékel egy tízes skálán a rendszer. Tesztelés során a 1. ábrán látható operátorok hozták legkonzisztensebben jó eredményeket.

A bemenetek fuzzifikálására alkalmazott tagsági függvényeket a 2-4. ábrák szemléltetik.



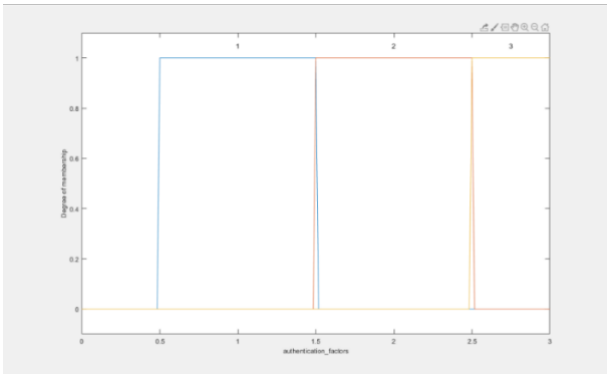
5. ábra tagsági függvények a kommunikációs bemenetnél

Az egyes protokollt egy tízes skálán osztályozzuk, hogy mérhető értékeket kapjunk belőle, így elvégezhetőek a számítások. A nyílt és a MAC szűrés nem nyújt biztonságot, a WEP könnyebben míg a WPA2 nehezebben, de feltörhető. A WPA3 és a vezetékes megoldások adják a legnagyobb biztonságot.



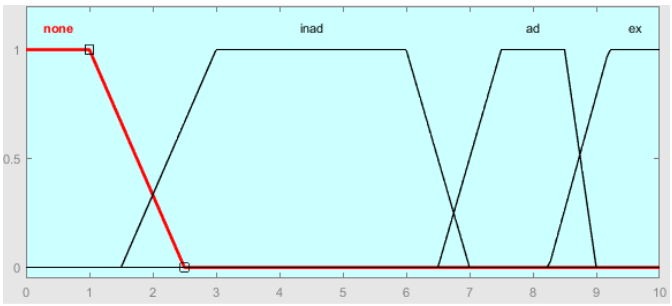
6. ábra tagsági függvények a jelszó hosszára

A jelszavak hosszát egyszerűen a karakterek mennyiségével reprezentáljuk, feltételezve, hogy azok az angol abc kis és nagy betűiből állnak és tartalmaznak speciális karaktereket is.



7. ábra tagsági függvények az autentikáció faktorok számára

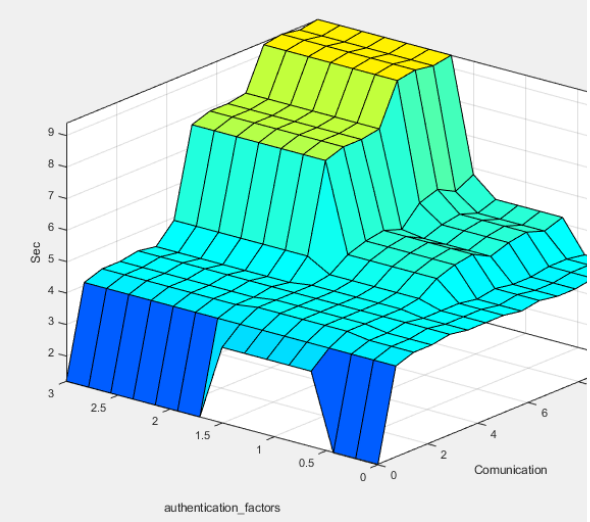
Az autentikációs faktorok száma diszkrét logikai elem a rendszerben, ezért az értékek átmenet nélkül váltanak a függvények között.



8. ábra kimeneti tagsági függvények

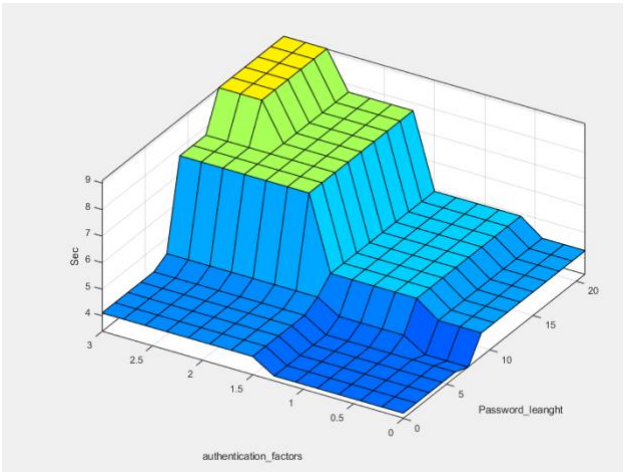
A biztonságot egy 10-es skálán értékel és a elfogadhatatlannak, nem megfelelőnek, megfelelőnek és kiválónak értékeli azt.

A szabályrendszert a program úgy nevezett Surface nézetén keresztül demonstráljuk az 9. *és 10. ábrán.*



9. ábra szabályrendszer 1

A rendszer a WPA 3-at még magasra értékeli hiszen az ellene irányuló támadások még nem publikusak. Ellentétben a kettes verzióval és a WEP-vel, ami nyilvánosan és ingyenes elérhető szoftverekkel támadható. Szintén magas értékelést kap a kábeles kommunikáció, hiszen ahhoz, hogy azt lehallgassák fizikai hozzáférés szükséges a hálózathoz.



10.ábra szabályrendszer 2

Több faktoros autentikáció nem értelmezhető bizonyos protokollok esetén. Mivel a jelszó hosszával exponenciálisán növekszik a feltöréséhez szükséges idő, így a jelentősebb pontokon lényegesen ugrás látható a biztonsági mutatóban. A rendszer nem viselkedik láncként, elemeinek a gyengeségeit lehet bizonyos mértékben kompenzálni más pontok erősítésével.

6. Összefoglalás

A rendszer a tapasztalatoknak megfelelő értéket képes megbecsülni a kommunikáció biztonságára vonatkozóan, hogy azt prezentálni lehessen a felhasználónak. Nem javasolt viszont ennek a segítségével tervezni a hálózati kommunikációt hiszen nagy általánosítással készül. Ez a megállapítás nem feltétlen helytálló az átlag felhasználó szempontjából, mivel ők nem véletlenszerű jelszavakat alkalmaznak és a különleges karakterek használata is ritka. [2]

További fejlesztési irány lehet például az említett jelszó minőség osztályozásra bemeneti függvények fejlesztése. Akár egy többszintű fuzzy függvénnyel, ami a jelszavak hosszát, karakter készletét, valamint a véletlenszerűségét is figyelembe veszi. Ugyanezt a számítási metódust lehet alkalmazni az azonosítási faktorokra, melyeknek csak a számát értékeljük, és figyelmen kívül hagyjuk a bio-metrikus azonosítás hibáit [16] (hamis elfogadás és könnyű hamisítás). Továbbá, ha például egy tűzfal osztályozó rendszerrel is kombinálnák melyekre, szinten léteznek fuzzy függvények és figyelembe vennénk egyéb sebezhetőséget is akkor a rendszer képes lehet akár teljes számítógépes hálózat biztonságának becslésére is.

A folyamat során a legnagyobb kihívás az emberi tényező korrekt osztályozása, hiszen az rengeteg komponenstől függ, mind az ismeretek a jelszó kezeléssel kapcsolatban vagy a rendszerek zárolása, ha a felhasználó azok felügyelet nélkül hagyja. Megfelelő elővigyázatossággal még a bio-metrikus azonosítók megszerzése is korlátozható így lényegesen javítva annak biztonságát.

Köszönetnyilvánítás

Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar és a Magyar Fuzzy Társaság támogatásával készült a tanulmány.

Irodalomjegyzék

[1] F. V. Allen, „The 10 Worst Password Ideas, as Revealed by Google,” 07 08 2013. [Online]. Available: https://www.techlicious.com/blog/the-10-worst-password-ideas-as-revealed-by-google/.

[2] M. Ehrenkranz, „The 25 Most Popular Passwords of 2018,” Gizmondo, 2018. [Online]. Available: https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705.

[3] A. Hern, „Facebook stored hundreds of millions of passwords unprotected,” 21 04 2019. [Online]. Available: https://www.theguardian.com/technology/2019/mar/21/facebook-admits-passwords-unprotected.

[4] M. E. Whitman és H. J. Mattord, Principles of Information Security, 2014.

[5] J. Yan, „Password Memorability and,” 2004.

[6] D. Lewis, Ctrl-Alt-Delete, 2011, p. 17.

[7] M. Kotadia, „ZDNet,” 2004. [Online]. Available: https://www.zdnet.com/article/gates-predicts-death-of-the-password/.

[8] D. Teriman, „Google security exec: 'Passwords are dead',” 2013. [Online]. Available: https://www.cnet.com/news/google-security-exec-passwords-are-dead/.

[9] C. Herley és P. v. Oorschot, A Research Agenda Acknowledging the Persistence of Passwords, 2012.

[10] Network Computing, „FBI Teaches Lesson In How To Break Into Wi-Fi Networks,” 2005. [Online]. Available:

https://www.networkcomputing.com/wireless-infrastructure/fbi-teaches-lesson-how-break-wi-fi-networks.

[11] T. Espiner, „Wi-Fi hack caused TK Maxx security breach," 2007. [Online]. Available: https://www.zdnet.com/article/wi-fi-hack-caused-tk-maxx-security-breach/. [Hozzáférés dátuma: 01 08 2019].

[12] M. Vanhoef, „Key Reinstallation Attacks," 2017. [Online]. Available: https://www.krackattacks.com/.

[13] M. Vanhoef, „DRAGONBLOOD," [Online]. Available: https://wpa3.mathyvanhoef.com/. [Hozzáférés dátuma: 13 06 2019].

[14] „SINGLE-FACTOR AUTHENTICATION (SFA)," [Online]. Available: https://doubleoctopus.com/security-wiki/authentication/single-factor-authentication/.

[15] R. Dias, „The 5 Factors of Authentication," 2017. [Online]. Available: https://medium.com/@renansdias/the-5-factors-of-authentication-bcb79d354c13.

[16] D. Thakkar, „Risk Factors Associated with Biometric Identification," BAYOMETRIC.