

XXXII. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Gödöllő, 2015. április 15-17.
Szent István Egyetem Gazdaság- és Társadalomtudományi Kar
Nemzeti Közszolgálati Egyetem

Beléptető rendszerek biztonságának vizsgálata

Jelige: BATMAN

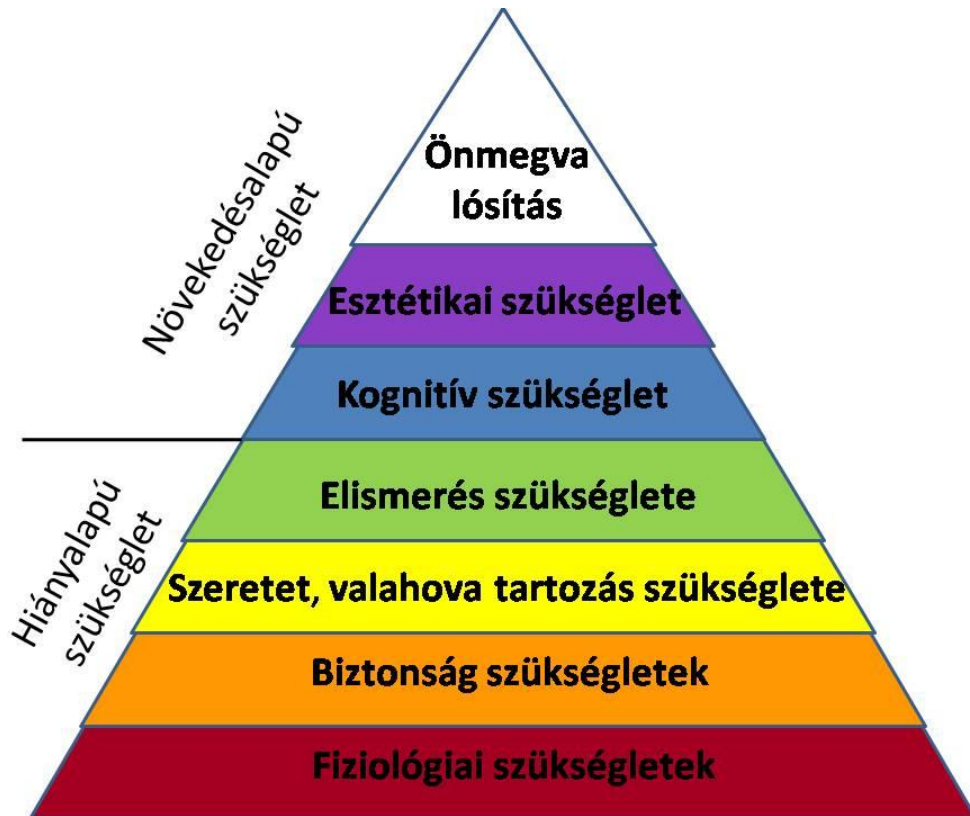
Pályamunka lezárásának ideje: 2014, június

2015.

Tartalomjegyzék

1. Bevezető.....	3
1.1. Témaválasztás	4
1.2. A téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása	5
1.3 Célkitűzések megfogalmazása	6
1.4 A dolgozat gyakorlati alkalmazása	7
2. A biztonságról általánosan	8
3. A beléptetésről általánosan.....	9
3.1. Mechanikai beléptetési rendszerek biztonsága	10
3.1.1. Hagyományos záruk biztonsága	11
3.1.2. Zártörés.....	13
3.2. Elektronikus beléptető rendszerek biztonsága	17
3.2.1. Tudás alapú elektronikus beléptető rendszer	18
3.2.2. Birtoklás alapú elektronikus beléptető rendszer.....	23
3.2.3. Biometrikus azonosítás	28
3.3. Élőerős beléptetés.....	32
3.3.1. Személyi tényező gyenge pontjai	34
4. Összefoglalás.....	36
5. Források.....	38

1. Bevezető



A fenti ábra a Maslow-piramisként elhíresült elméletet szemlélteti. A kidolgozója Abraham Maslow, a 20. század nagy pszichológusa, aki az emberi motiváció tényezőit vizsgálva jutott arra következtetésre, hogy vannak bizonyos szükségleteink, amelyek piramisszerűen épülnek egymásra. Az elméletből, azóta megannyi következtetést vontak le, ám ami számomra érdekes, hogy az alapvető fiziológiai szükségleteink után (légzés, evés, ivás, alvás, fajfenntartás), a biztonság megléte a második legalapvetőbb szükségletünk az életben. Épp ezért gondolom, hogy a biztonság szerteágazó témaköre mindig is aktuális volt és lesz is, illetve rendkívül fontos szerepe van mindannyiunk életében.

1.1. Témaválasztás

Dolgozatom témája a beléptetési rendszerek biztonságának vizsgálata, amiben bemutatom a biztonságot, mint alapvető fogalmat, majd konkrétan a beléptetési rendszerekkel általánosan illetve biztonsági szempontból is foglalkozom.

Bár dolgozatom címe és témája szigorúan véve csak a beléptetési rendszereket említi, de szorosan idevág a jogosultság ellenőrzése is, amit a szakirodalmak néha egybe, néha külön vesznek (angolul egyszerűen *access control*). Emiatt dolgozatom egyes elemei átnyúlnak a jogosultság vizsgálat témakörébe, de alapvetően igyekszem a választott témámnál maradni. Témaválasztásnál erősen befolyásolt, hogy tanulmányaimhoz köthető témát válasszak. Had-és biztonságtechnikai mérnök szakos hallgatóként, a biztonság gyakorlati megvalósulása mindenképp szakmámhoz köthető téma. Ezen túlmenően Katonai Informatika szakirányra specializálódtam, így érdekel az információ biztonságának témaköre, ugyanúgy, mint a digitális technika megvalósulása. Éppen ezért keltette fel figyelmem a beléptetési rendszerek vizsgálata, hisz ami egy látszólag egyszerű folyamat, valójában rengeteg részből épül fel, melyek együttes működése szükségeltetik a rendszer biztonságos működéséhez. Gondoljunk bele egy olyan intézménybe, ahol naponta több százan fordulnak meg, milyen komoly folyamatok zajlanak le, hogy a megfelelő emberek belépési jogosultságát biztosítsák. Nem kell messzire menni, a Zrínyi Miklós Laktanya és Egyetemi Campus, ahol jelenleg tanulmányaimat folytatom, rendelkezik ugyanúgy egy beléptetési rendszerrel, amivel nap, mint nap találkozom. Úgy érzem ez egy olyan témakör, amibe igazán érdemes belemélyülni és minél többet megtudni róla. A tanulmányaim közvetlenül nem térnek ki erre a témára, így megfelelő kutatómunkát igényel, de hosszútávon feltétlenül köthető az informatikai és biztonságtechnikai szakmához.

1.2. A téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása

Úgy vélem az általam választott témáról elmondható, hogy rendkívül általános, mindennapi, illetve egyszerűsített változatában előfordul mindenki életében.

Konkrét példával kezdenék, hiszen ha otthon rendelkezünk egy ajtóval, amit kulccsal zárunk, az már egyfajta beléptetési rendszer. Ezt már lehet elemezni biztonsági szempontból, például milyen lakatot használunk, kinek van kulcsa hozzá, hogy lehet megkerülni az ajtót, stb.. Ezen felül, napjaink információs társadalmában alapvető, hogy a legtöbben rendelkezünk különböző felhasználónevekkel és hozzá tartozó jelszavakkal. Ezek mind jó példák a különböző beléptetési rendszerekre. Ennek biztonsági elemzése egész könyveket is megtöltene, kezdve a jelszó feltörésétől, a rendszerbe való betörésen, őrség semlegesítésén vagy épp egy betonfal nyújtotta védelem áttöréséig mindent. A beléptetések üzemeltetése elengedhetetlen mindennapi életünkhöz, e nélkül a világon semmilyen érték se lenne biztonságban, hisz semmi sem gátolná a jogosulatlan belépést különböző objektumokba, beleértve a bankok széfjeihez, vállalatok központi adatbázisába, katonai objektumokba, a lista végtelen. Ezen túlmenően, a biztonságnak rengeteg aspektusa van, így ahhoz, hogy megfelelő betekintést nyújtsak a témába több tudományágat is érinteni fogok. Minden védelem annyit ér, mint a leggyengébb pontja, nincs ez másként a beléptetésnél sem, hisz lehet egy adott helyen ultra modern retina ellenőrző beléptetési rendszer kiépítve, ha két méterrel odébb bárki gond nélkül átmászik a kerítésen.

Összességében elmondható, hogy manapság, amikor információs társadalomban élünk, és kulcsfontosságúvá váltak a nyilvántartások, dokumentációk, adatbázisok megléte, a beléptetések rendszere is ebbe az irányba terelődik. Bár a megvalósulásának módszerei sokat változtak, pláne az utóbbi időkben, jelentősége semmint csökkent, sőt még inkább megnőtt a szerepköre.

1.3. A célkitűzések megfogalmazása

A dolgozatom megírásának első és legfontosabb célja saját ismereteimnek bővítése, látóköröm szélesítése, tapasztalatok szerzése gyakorlati feladatokkal, egyszóval tudásom gyarapítása.

Felmerült bennem, ezen kívül, a vágy, hogy kipróbáljam magam egy új területen, ami magába foglalja az anyagok gyűjtését, értelmezését, feldolgozását, összegzését. Célom egy olyan tudományos igényű dolgozat elkészítése, mely bemutatja a témában megszerzett ismereteimet. Fontosnak tartom, hogy teljes körű leírást adjak a választott témámról, részletbe menően elemezzem a különböző ágazatait, illetve az egészet esztétikailag is megfelelő formában prezentálni. Ezen kívül, szeretném, ha dolgozatomban leír eredményeim, akár csak részben, de hasznosíthatók legyenek mind elméletben, mind gyakorlatban.

Végezetül szeretném magam összemérni társaimmal a Tudományos Konferencia keretein belül, illetve bemutatni munkám eredményeit.

1.4. A dolgozat gyakorlati alkalmazása

Dolgozatom megírásakor igyekeztem odafigyelni, hogy ne legyen teljes mértékig elmélet orientált, hanem gyakorlatban is használható gondolatokat, ötleteket fogalmazzak meg.

A választott témának nagyon sokféle és fajta gyakorlati alkalmazása van, hiszen bizonyos fokú védelemre mindenhol szükség van, beléptetést pedig szintén általánosan elterjedten használnak. Konkrét példaként felmerül bármely objektum (otthonok, üzletek, munkahelyek, stb..), ahol beléptetési rendszert használnak. A dolgozatom magában foglalja, miként érdemes a gyakorlatban a beléptetést kiépíteni különböző helyzeteknek és céloknak megfelelően, miként lehet és érdemes ezek biztonságáról gondoskodni, figyelembe véve olyan sajátos tényezőket, mint a fenyegetettség, anyagi lehetőségek, vagy épp fizikai adottságok.

Dolgozatom során igyekszem végig gyakorlati példákkal szemléltetni egyes problémákat és azok megoldásait, amennyiben lehetséges, ezeket mindennapi és jól érthető szituációkkal bemutatni. Gyakorlatban foglalkozom, ezen túlmenően a védelem feltörésével, kizáróhatóságával, gyengepontjaival.

Úgy vélem, hogy amennyiben bebizonyítható, hogy adott beléptetési rendszer nem nyújt kellő védelmet, úgy alternatív megoldásokat kell keresni, melyeket megpróbálok javasolni minden helyzetben.

2. A biztonságról általánosan

Munkám legelején szeretnék foglalkozni azzal, hogy mit is jelent pontosan a biztonság. A biztonság leginkább úgy írható le, mint egyfajta védelem vagy ellenállás bizonyos károkozás(ok) ellen. A biztonság hagyományos formája a fizikai védelem, ellenben napjainkra egyre elterjedtebb és nagyobb szerepet játszik az információs védelem. Éppen ezért fontos, hogy ha egy adott téma (jelen esetben a beléptetési rendszerek) biztonságáról beszélünk, meg kell vizsgálnunk mindkét szempontból.

Azt már az elején ki kell kötni, hogy 100%-os biztonság nem létezik. Ellenben törekedni lehet, sőt adott esetben kell is, hogy egy elfogadható szintet megüssünk. Ehhez első lépésben mindenképp fel kell mérnünk, hogy milyen fenyegetettségekkel, veszélyekkel kell számolnunk. Példának okáért, egy katonai objektum esetében elvárható a fokozott biztonság, beléptetésnél legyenek biztonsági örök, hagyományos és digitális záruk, beléptető kapuk, esetleg biometrikus azonosítók, kamerák, stb... Ellenben, egy másik példa, ha a testvérünktől akarunk elzárni egy személyes naplót, bőven elegendő egy kisméretű zár a naplóra erősítve (hiszen ez is egyfajta vizsgálata a jogosultságnak, azáltal, hogy rendelkezik-e az illető kulccsal). Annak felmérésevel, hogy egy adott objektumra, szervezetre, személyre minden biztonsági kockázatok jellemzőek, a biztonság menedzsment hajtja végre. Ennek eredményét felhasználva tervezik meg a biztonsági rendszer kialakítását illetve felügyeletét.

Egy másik alapelv a biztonság tekintetében egy közismert mondás: "Minden lánc olyan erős, mint a leggyengébb láncszeme". A védelemmel kapcsolatban mindig külön-külön és együtt is vizsgálni az egyes elemeit. Nagyon jó példa erre, ha vásárolunk 50cm vastag titán páncélzatú ajtót, hozzá három különböző típusú zárral, de nyitva hagyjuk a hátsó ablakot, a védelmünk lényegében nulla. Ezért lényeges, hogyha beléptetési pontot akarunk kiépíteni, az egyes elemeit a fenyegetettség függvényében egyformán arányos kell kialakítani.



3. Beléptetésről általánosan

Amikor beléptetésről beszélünk több minden is az eszünkbe juthat, egyszerűbb példáktól kezdve az igen komplexekig bármi, ám először tisztáznunk kell, mit takar a fogalom. Beléptetés alatt egy adott objektum személy- és/vagy gépjárműforgalmának irányítása, koordinálása, ellenőrzése. Egy beléptetési folyamat az alábbi lépésekből épül fel:

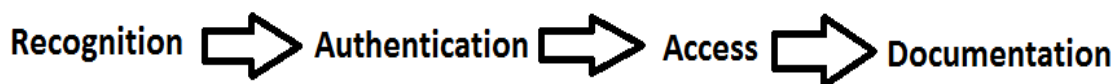
- Azonosítás
- Jogosultság ellenőrzése
- Áthaladás
- Dokumentálás

Minden lépés szükséges feltétele a beléptetés hibátlan működésének, a biztonság állandó fenntartásának. Ezen kívül, az alábbiak fajtái vannak a beléptetésnek:

- Mechanikai (zár, lakat)
- Elektronikai (számkódos terminál, mágneses kártya)
- Élőerős (portás, őrség)

Ezek alapján fogom dolgozatom további részében csoportosítani a témakört, részegységeként megvizsgálni mind általános, mind biztonság szempontból is.

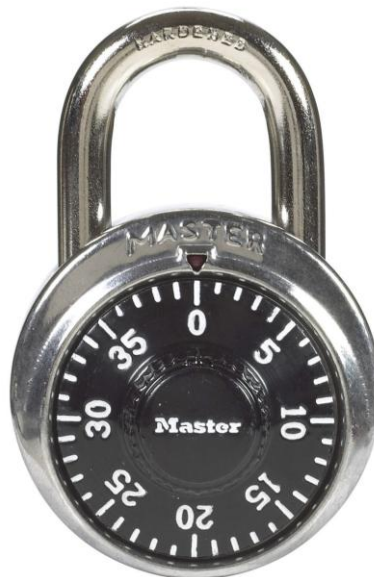
Összességében a beléptetés egy igen tág témakör, rengeteg fajtája létezik és van is használatban, mindezeket lehet többféle szempontból vizsgálni (fizikai, gazdaságosság, jogi, stb..), mindazonáltal úgy vélem, hogy alapvető rendeltetésük a biztonság, ezért ebből szemszögből nézve igyekszem bemutatni őket, illetve feltárni bizonyos gyakorlati hibákat, amelyek elkerülésével eredményesen építhetjük ki egy adott objektum beléptetését, illetve védelmének egyéb elemeit.



3.1. Mechanikai beléptetési rendszerek biztonsága

A következőkben azzal szeretnék foglalkozni, mitől függ egy beléptetési rendszer fizikai biztonsága, hogyan érdemes és célszerű kiépíteni, milyen elemei vannak, hogyan működnek általánosan.

Első sorban szeretném bemutatni, hogy hogyan épül fel egy beléptetési rendszer. Az alapja, hogy kiválassza kik jogosultak egy belépni egy adott területre vagy hozzáférni valamilyen anyaghoz. A legegyszerűbb példa, amit el lehet képzelni, az egy ajtóval elzárt terület, amelyhez csak bizonyos embereknek van jogosultsága hozzáférni. Nyilvánvaló, hogy önmagában egy ajtó nem fogja garantálni a jogosultság ellenőrzését, ehhez külön rendszert kell kiépíteni. Erre lehet jó példa, ha zárat teszünk az ajtóra, és csak bizonyos embereknek kapnak hozzá kulcsot. Természetesen, ha van egy elzárni kívánt aljtónk, akár állíthatunk elé őrséget is, vagy valamilyen elektronikus védelmi rendszert is, de tény, hogy a legelterjedtebb és legegyszerűbb megoldás a mechanikai eszköz (zár) alkalmazása. Innentől kezdve már beléptetési rendszerről beszélünk, hiszen valamilyen módon szűrve vannak a hozzáférésre jogosultak (kulcsok). Mechanikai eszközök tekintetében a birtoklásos módszeren kívül (kulcs), felmerülhet a tudás alapú módszer is (pl. számszár). Erre jellemző a nagyfokú biztonság, nehezen feltörhető/kijátszható, ellenben költséges, illetve ritkán használják, mert a helyét átvette a biztonságosabb számkód alapú terminálok, leginkább széfek esetében fordulnak még elő. A fent említett okokból a továbbiakban csak a kulcsot igénylő mechanikai zárok biztonságára fogok kitérni.

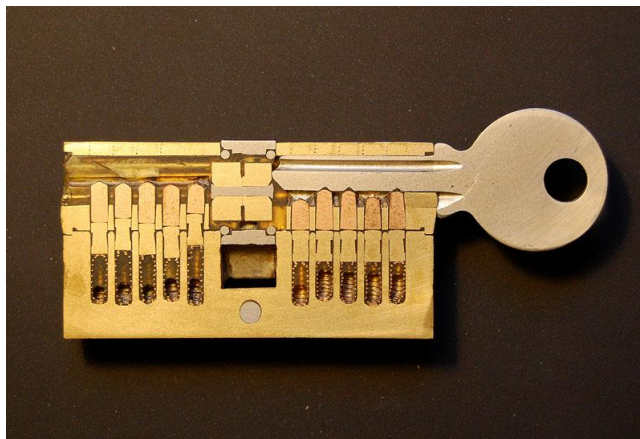


3.1.1. Hagyományos zárok biztonsága

Ebben a fejezetben a zárok biztonságáról ejtenék pár szót, annak előnyeiről és hátrányairól, illetve létjogosultságukról napjaink társadalmában.

A zárok története egészen az ókorig nyúlik vissza, hiszen a legalapvetőbb társadalmakban, ahol már megjelent a vagyon és a tulajdon fogalma, felmerült az óvásuk is, a személyi védelemről már nem is beszélve. A középkorban a lakatok, zárok készítése külön mesterséggé nőtte ki magát, innen ered a lakatos (angolul *locksmith*) szakma. Mindezzel párhuzamosan alakult ki egy másik szakma is, még hozzá a zártörés (angolul *lockpicking*). Amióta léteznek zárok, azóta léteznek zártörők is, ezek rengeteg film és videojáték témájává váltak. Nyilván, azóta rengeteget változtak mind a zárok felépítése, mind a zártörés módszerei. Manapság a legelterjedtebbek az úgynevezett cilinderzárok, hengerzárok (népszerű márka például *ELZETT*), illetve a trezorzárok. Zárossal mindenhol találkozunk, mindenki használja, mindenkinek vannak kulcsai, általában külön van zára az egész területet határoló kapunak, külön a háznak/lakásnak, és sokszor egyes szobáknak is. A biciklinket zárral óvjuk a tolvajoktól, sokszor fiókokat, ládákat, ékszeres dobozokat, szekrényeket is kulcsra zárunk. Miután így felvázoltam az általános és széles körben elterjedt helyzetét a zároknak mai világunkban, szeretnék szót ejteni azok biztonságáról.

A cilinder vagy henger zárok felépítése ábrán jól szemléltethető, legfontosabb része a forgó cilinder, amely elforgatásakor helyére kerül a retesz és ez által a zár bezárul. Ideális esetben, ez meggátolja a jogosulatlanok hozzáférését, ami által a zár eléri eredeti rendeltetését. Sajnos a valós életben ez még közel sem jelent kellőbiztonságot, ennek kijátszására számos mód létezik, mely közül bemutatnék, illetve el is magyaráznék néhányat.



Elsőként szeretném azzal kezdeni, amit már fentebb is említettem a „leggyengébb láncszem” kapcsán, hogy amennyiben van egyszerűbb és kézenfekvőbb mód és a bejutásra, megszerzésre, lehet, hogy nincs is szükség a zár feltörésére. Tegyük fel, hogy van egy törhetetlen zárunk, ellenben a kulcs hanyag módon van őrizve. Ez esetben logikusan következik, hogy valamelyik formában a kulcshoz próbálunk hozzájutni, így a zár nem kerül feltörésre, hanem annak rendje és módja szerint szabályosan lesz kinyitva. Ide tartozhatnak egyéb olyan módszerek is, mint például a kulcs valamely hordozóját megvesztegetéssel, zsarolással, vagy fenyegetéssel rávenni a zár nyitására. Számos egyéb módját lehet elképzelni a zár kijátszásának, ezek közül többet említek is dolgozat más részein, a továbbiakban viszont folytatnám a fizikai zártöréssel.

Ha zártörésről beszélünk a legegyszerűbb, legelemibb megoldás az úgynevezett *nyers erő* (angolul *brute force*) alkalmazása. Ilyenkor a zárat, a reteszt, illetve azon tárgyat melyre a zár lett felszerelve, fizikai erő hatására megrongáljuk, így biztosítván jogosulatlan hozzáférést. Ennek hatásossága függ a zár és az anyagok minőségétől is. Hagyományos értelemben *brute force* támadás lehet az is, ha például berúgunk egy ajtót és behatolunk, miközben a zár érintetlen marad. Másik gyakori támadási módszer, konkrét példával bemutatva, mikor betörnek egy kocsinak az ablakát, hogy aztán belülről kinyissák (természetesen korszerű autók fel vannak szerelve kellő védelemmel ilyen támadásokkal szemben). Ilyen esetben a támadás nem a zár ellen irányul, hanem annak kinyitását elősegítendő. Ilyen támadásokkal szemben leghatásosabb megoldás, a fizikai védelem javítása (több és erősebb zár, vastagabb falak, ajtók, ütésálló üvegek, stb..). Legnagyobb hátránya a nyers erő használatának, hogy könnyen észlelhető, hiszem maga a törés feltűnő, hangos, ráadásul nyomot is hagy. Ha éjszaka betörnek egy lakott házba, esélyes, hogy többen felriadnak, és van mód az illetéktelen behatoló ellen tevékenykedni. Ha viszont ugyanez a támadó egy finomabb módszert használ, könnyen lehet, hogy napok múlva tűnik csak fel a behatolás, és akkor sem a zár látszólagos sérülése miatt....

3.1.2. Zártörés

Valószínűleg már mindenki látta filmekben, ahogy a főhős egy hajtű vagy épp bankkártya segítségével könnyen átjut a zárt ajtókon is. Ezek a jelenetek általában kis túlzásokkal élnek, de az igazság az, hogy a legtöbb ma használatos zárat igencsak könnyű feltörni. Ehhez nem kellene kémfilmekbe illő csúcs technológiával készült felszerelések, se nem több éves képzések, mindössze otthon is előállítható eszközök és néhány hét gyakorlás. A következőkben az igen gyakori és elterjedt cylinder zárok feltörési technikáját mutatom be.

A ma használatos cylinderzárok legfontosabb elemei a forgó henger és rugó által vezérelt stífték. Amennyiben a megfelelő kulcsot behelyezzük a zárba, a stífték egyenletes helyzetet vesznek fel, amely által lehetővé válik a cylinder elfordítása, ezáltal a zár kinyitása. A stíftéket tartó rugók különböző erősségűek, ebből adódik a kulcs recés éle, hisz a stíftéket különböző mértékben kell eltolni, hogy egy vonalba kerüljenek.

Amennyiben valakinek célja, hogy a kulcs használata nélkül nyisson ki egy zárat, addig kell igazgatnia a stíftéket, míg a henger el nem fordul, és ki nem nyílódik a zár. Ahhoz azonban, hogy idáig eljusson valaki, több problémát is le kell küzdenie. Elsőként felmerül, hogy a zárok kisméretűek, a kulcs bemeneti nyílása pedig milliméterekben mérhető, emiatt szükség van egy alkalmas eszközre. Ennek megfelelő méretűnek kell lennie, hogy belemenjen a nyílásba, illetve kellőképp íveltnek kell lennie a végének, hogy azzal igazgatni lehessen a stíftéket. Ezt az eszközt hívják a szaknyelvben *pick*-nek, magyarul esetleg zártörőnek. Rengeteg fajtája létezik, a leginkább elterjedtek a *hook* (magyarul kampó, horog), *rake*, *diamond*, stb... Ezek az eszközök bizonyos mértékig eltérnek technikájukban, de rendeltetésük és végeredményük ugyanaz.



Ezen eszközöket más országokban (főként Egyesült Államok) gyártanak, lehet ilyeneket kapni vagy épp rendelhet is az ember magának, akár külföldről is. A dolog érdekessége, hogy némi leleményességgel és kellő ügyességgel otthon is előállítható ilyen *pick*. Legegyszerűbben egy egyszerű fűrészlapból célszerű készíteni, az anyaga pont megfelelő, könnyen formázható.

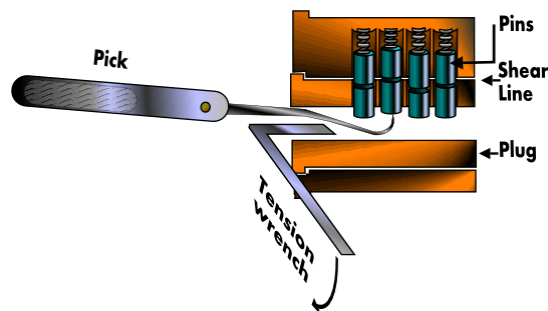
A probléma ezzel még nem oldódott meg, ugyanis aki már látott közelebbről ilyen zárat, az tudja, hogy a stiftok a rúgók miatt szabadon mozognak, ám utána vissza is állnak eredeti helyzetébe. Mikor kulcsot helyezünk a zárba, egyszerre fejtünk ki nyomást az összes stiftre, ezért sikerül elforgatni a hengert, ha viszont zártörővel próbálkozunk, nem tudjuk egyszerre mindegyiket elmozdítani. Ilyenkor jön kapóra a zárok azon tulajdonsága, hogy amennyiben kellő forgatónyomaték hat a hengerre, a stifteteket egyesével megfelelő helyzetbe lehet hozni, anélkül, hogy elmozdulnának. Ahhoz, hogy ilyen hatást elérjünk, szükség van egy másik eszközre, amelyet be tudunk helyezni a zárba, és arra forgatónyomatékot kifejteni. Ezt a szaknyelv *tension wrench*-nek hívja, magyar megfelelőjéről nem tudok. Ehhez is némiképp görbe, vagy elhajlított eszközre van szükség, amelynek egyik része belemegy a zárba, a másik kiálló részét pedig valamilyen irányba forgatni próbáljuk. A filmekben ehhez elhajlított hajtút vagy biztosító tűt szoktak használni, a gyakorlatban célszerűbb megint csak egy vékony fémlapból kialakított eszközt használni. Ehhez ideális lehet a szélvédő lemosójának merevítőjét használni, amihez bárki könnyen, olcsón (és teljesen legálisan) hozzájuthat, és két csavarással kialakítható belőle a megfelelő eszköz.



Most, hogy megvannak a kellő eszközök, csak némi gyakorlás kérdése, és bárki eljuthat odáig, hogy fel tudjon törni egy zárat.

Első körben érdemes megtudni, miféle zárral van dolgunk, illetve milyen stiftok vannak benne. A gyakorlatban használt zárokban a stiftok száma nagy valószínűséggel 4 és 6 között van, legtöbbször 5, ennél kisebb vagy nagyobb számban már nem nyújtanak kellő biztonságot. Ahhoz, hogy felmérjük a stifteteket, érdemes párszor végighúzni rajta a *pick*-et, így

érezhető, hogy mennyivel kell dolgozni, van-e esetleg olyan, amelyik akad vagy nehezebben mozog, stb.. Ha ezzel megvagyunk, lehet nekiállni a zártörésnek. Elsőként a *tension wrench*-et kell behelyezni és nyomást gyakorolni rá. Fontos, hogy megfelelő mértékű legyen, ha túl gyenge vagy épp túl erős, a stiftek nem fognak megakadni. Ez függ a zár minőségétől is, illetve gyakorlás is szükségeltetik, hogy valaki ráérezzen a megfelelő erősségre. A nyomás folyamatos gyakorlása mellett, nekiállunk a *pick*-kel elrendezni a stifteket. Fontos figyelembe venni, hogy adott sorrendben fognak beállni, és erre rá kell érezni, ki kell tapasztalni. Érdeemes még odafigyelni arra is, hogy ami egyszer beállt, egy rossz mozdulat következtében még visszaugorhat. Lényeges továbbá az is, hogy ha túl erősen nyomjuk be valamelyiket, az fennakadhat, és onnantól lehet előlről kezdeni. Mindeközben a forgatónyomatékokat folyamatosan fenn kell tartani, hol erősebben, hol gyengébben. Amennyiben mindent megcsináltunk, egy kattanást fogunk hallani és érezni, hogy a henger elfordul, a zár kinyílt.



A fent említett módszeren kívül, másképp is fel lehet törni egy zárat (tulajdonképpen lehetőségek egész tárháza adódik, dolgozatomban csak a legismertebbekről szólnék). A fent bemutatott *hook pick*-en kívül lehetséges a *rake pick* használata is, amelyet *snake*-nek (kígyónak) is hívnak, sajátos formája miatt. Ennek hátránya, hogy házilag elkészíteni roppant körülményes lenne, aki ilyennel szeretne próbálkozni, célszerű beszerezni valahonnan. Előnye, hogy nem igényel különösebb finomságot, érzéket, csupán be kell helyezni a zárba, és végigszántani (a *rake* szó jelentése gereblye) a stifteket. Ezzel a módszerrel egy teljesen kezdő, aki életében először próbál ilyesmit, könnyűszerrel felnyit egy zárat fél percen belül.



Használatos továbbá egy pick gun („zártörő pisztoly”) névre hallgató eszköz is, melynek formája első ránézésre valóban egy kézi lőfegyverre emlékeztet. Működési elve komplexebb, nem is szeretnék rá kitérni, mivelhogy a felhasználóját sem érinti a dolog. Ami lényeges, hogy a segítségével kb. 10 másodpercig tart egy zár feltörése, nem igényel semmilyen tudást vagy különösebb ügyességet. Hátránya, hogy meglehetősen zajos, a hagyományos zártörőkhöz képest, illetve házilag elkészíteni lehetetlen, csak is beszerezni lehet, és költségesebb is.



Amennyiben valaki a fent leírt módszerek egyikével tör fel egy zárat (szakmában roncsolásmentes zártörés), úgy annak semmi nyoma nem marad, látszólag olyan mintha valaki kulccsal nyitotta volna ki. A zár ezután ugyanúgy visszazárható, működik továbbra is rendesen, és ez által illetéktelen személyek nyomtalanul juthatnak át, akár beléptetési pontokon is. Természetesen a gyakorlatban, mint ahogy azt korábban említettem, egy adott védelemnek több aspektusa is van, (biztonsági őrség, kamerák elhelyezése, világítás használata, stb..) így nem valószínű, hogy egyetlen zár feltörésével bárki is képes lenne egy komplett védelmen túljutni. Mindazonáltal úgy vélem, hogy a hagyományos zárok biztonsága jócskán túl van értékelve, sokszor meglepően nagy fontosságú hozzáféréseket korlátoznak mindössze egy hagyományos zár védelmével, ami önmagában semmiképp sem nyújt kellő biztonságot.

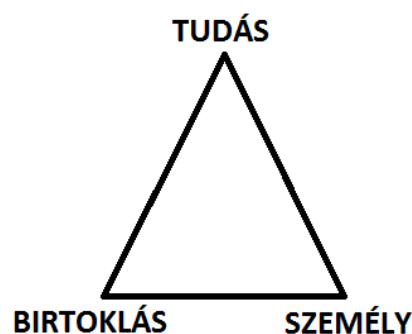
3.2. Elektronikus beléptető rendszerek biztonsága

A második ipari forradalom idején rengeteg új elektromossággal kapcsolatos találmány jelent meg, illetve rengeteg eszköz terjedt el. Ennek következményeként a biztonság terén is változások jöttek létre. Egyre több és több olyan elektronikai eszközt használtak, ami hozzájárult a védelemhez is (pl. rádió). Manapság pedig a technológiai lehetőség korlátlanok, ami korábban elképzelhetetlennek tűnt, (pl. egyetlen személy kamerákkal tudja figyelni egy többemeletes épület minden szintjét) az manapság teljesen normális és megszokott. Ezekről az eszközökről és a biztonságukról foglalkoznánk a továbbiakban.

Amikor elektronikus beléptetőkről beszélünk, háromféle tanúsítvánnyal igazolhatjuk jogosultságunk:

- Valami, amit tudunk
- Valami, amit birtokolunk
- Valami, ami sajt magunk vagyunk

Ezen tényezők egyébiránt a beléptetés egyéb módszereinél is előjöhetnek, viszont úgy érzem, hogy, ennél a résznél tudom a legjobb gyakorlati példákkal bemutatni őket. Ezen három módszer közül talán az utolsó a legbiztonságosabb azonosítási módszer, hiszen míg egy jelszót megtudhatnak, egy kulcsot elrabolhatnak, addig valakinek az ujjlenyomata az övé és csakis az övé (habár vannak módszerek a biometrikus beléptetési rendszerek kijátszására is, lásd később). Az, hogy ezek közül a módszerek közül melyiket alkalmazunk az több tényezőtől is függ (kockázatelemzés, anyagi lehetőségek, gyakorlati hasznosság). Adott esetben előfordulhat, hogy a lehetőségeket kombináltan használják, a nagyobb biztonság érdekében. Rengeteg helyen fordul elő, például irodaházakban, hogy az adott alkalmazott ujjlenyomat leolvasóval jut be az objektumba, mágneses kártyával nyitja az irodáját, és jelszóval lép be a számítógépébe (ez utóbbi nem tartozik szigorúan a dolgozatom témájához, de jól beleillik a példába). Felmerül viszont egy probléma, hogy amennyiben a biztonsági elemeket túlzottan felhalmozzuk, egy idő után nem a biztonság javára, hanem a gyakorlati működés kárára megy. Továbbiakban csoportosan mutatom be az egyes módszereket.



3.2.1. Tudás alapú elektronikus beléptető rendszer

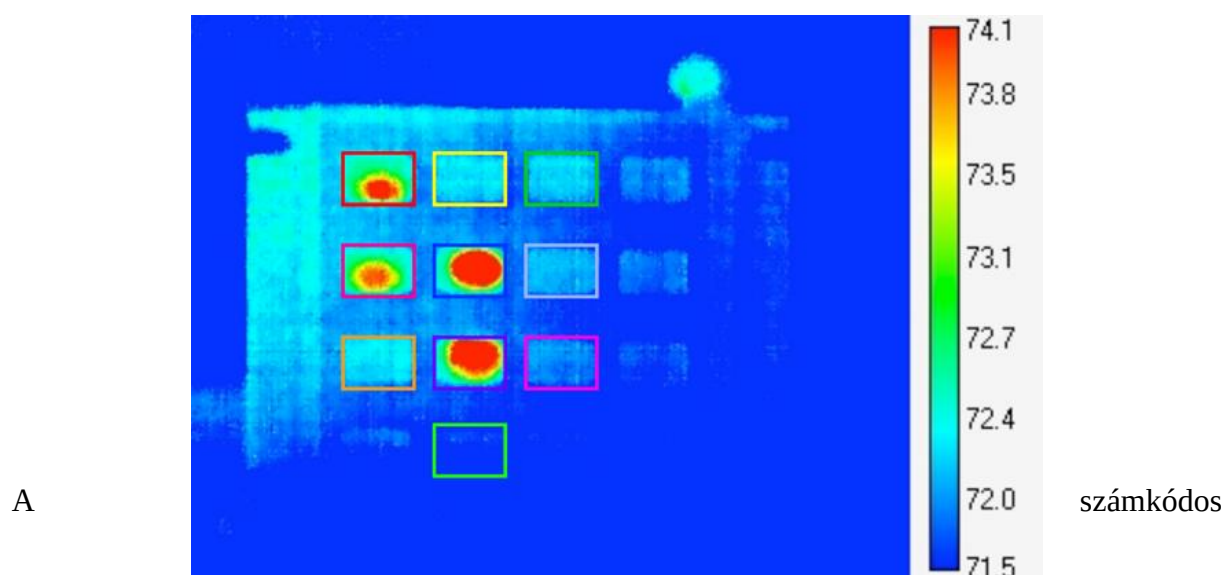
Ebben a témakörben a leginkább ismert megoldási módszer számkódos terminál. Ennek rengeteg fajtája létezik és kapható a piacon, de a működési elvük lényegében azonos. A belépéshez szükségeltetik egy, általában 4 számból álló jelszó ismerete és helyes megadása.

Biztonság szempontjából vizsgálva, a három megoldás közül ez számít a legkevésbé megbízhatónak. Az egyik legnagyobb hátránya, hogy ha valaki megtudja a jelszavunkat, arról nem szerzünk egyből tudomást, előfordulhat, hogy valakinek tudtán kívül hosszú ideig használják a jelszavát akár beléptetésnél, akár máshol. Egy kulcs vagy mágneskártya hiánya, például, egyből feltűnik, még ha csak véletlenre és nem rossz szándékra gyanakszunk, ennek függvényében lehet intézkedni (zárcsere, kártya letiltása, stb.). Jelszavas beléptetők működési elvét nem szeretném részletezni, sokkal lényegesebbek a hozzá tartozó biztonsági rések. Nagyobb objektumok esetében nem célszerű használni, torlódást, akadást okozhat a beléptetésben. Leginkább egy-egy szoba beléptetésénél célszerű használni, ahol a belépésre jogosultak száma alacsony. A legnagyobb biztonsági kockázat is ebből fakad, hiszen bárki képes kilesni a másik jelszavát, ehhez nem kell semmi tudás vagy felszerelés. Alapvető biztonsági követelmény, hogy jelszó, számkód megadásakor eltakarjuk a kezünket (nemcsak beléptetésnél, hanem például bankok PIN termináljánál is). Itt említenék egy példát, ami szigorúan véve a *Social Engineering* témakörhöz tartozik, de itt érthető meg a legjobban. Egy rossz szándékú illetéktelennek nem kell tudnia a jelszavunkat, könnyen előfordulhat, hogy az előtte belépő személy nyitva hagyja az ajtót udvariasságból. Emiatt is kiemelten fontos, hogy lehetőleg olyan esetekben használjuk, ahol kevés a belépésre jogosultak száma.

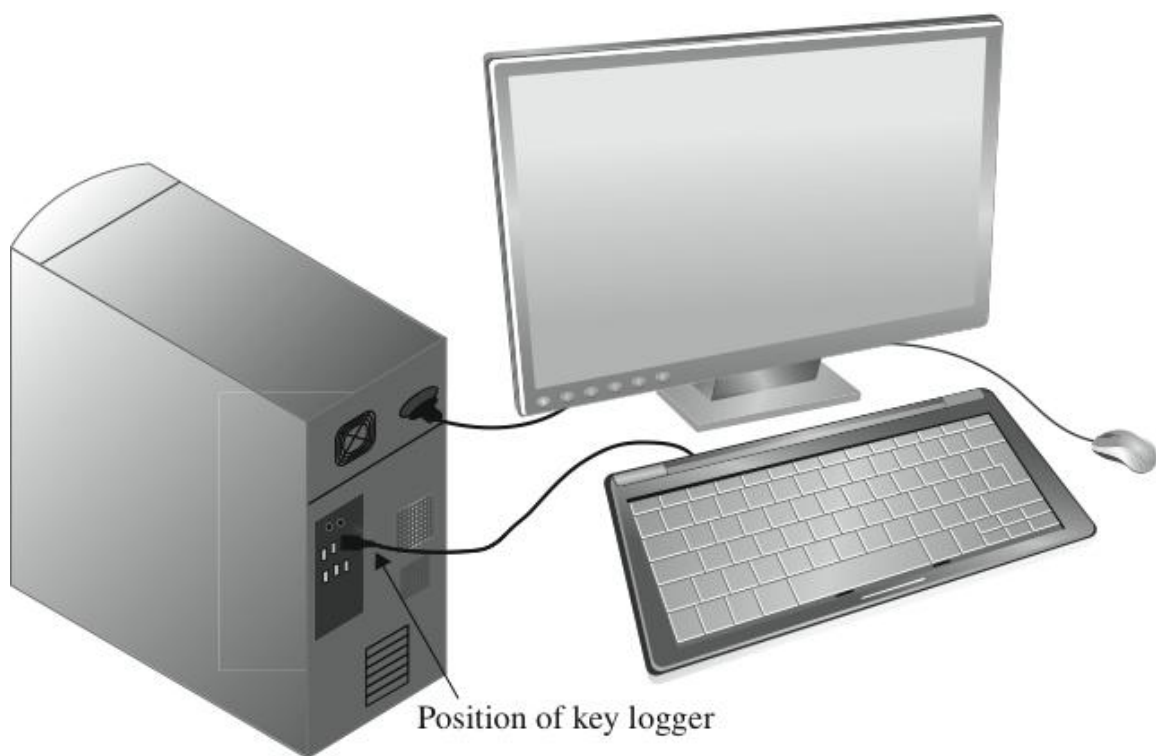
Ennél vannak összetettebb módszerek is, amelyek igényelnek bizonyos fokú képzettséget és felszereléseket is, ezek közül mutatnék be párat. Gyakran előfordul, hogy valaki hajszal méretű kamerával próbálja meg kifigyelni jelszavunkat. Bár észrevenni nehéz, a fent említett kéztakarásos módszerrel ugyanúgy védekezhetünk ellene. Ennél sokkal nehezebb dolgunk van, ha valaki egy álpanelt helyez a valódi felé, így a beütött jelszavunkat kétszeresen is érzékelik, az egyik esetben sajnos elküldve a kódot illetékteleneknek. Hatásos módszer lehet a védekezésre, ha észleljük, hogy a terminál megváltozott, furcsa alakja van, domború, esetleg a gombok másak, ebben az esetben egyből jelezni kell a rendellenességet a szakértőknek.



Ezen kívül létezik egy még hatásosabb módszer, ami ellen lényegében esélytelen védekezni. Amikor beütünk egy számkódot, az ujjunk által megérintett gombokon hő keletkezik, így valamilyen szinten nyoma marad a terminálon. Megfelelő hő érzékelő kamera segítségével meg lehet állapítani milyen gombokat nyomott be az előttünk használó személy. Amennyiben hagyományos négy számjegyű PIN kódról beszélünk, ismerve a négy beütött számjegyet, 24 számkód lehetséges. Feltételezve, hogy 3 helytelen megadás után biztonsági riasztást vonhat maga után, napi két próbálkozással számolva, átlagosan 6, legfeljebb 12 nap után át lehet jutni a beléptetési ponton. Arról nem is beszélve, hogy kézmozdulatok megfigyelésével a számok nem, de megadás sorrendje (fentről lefelé, balról jobbra, stb..) könnyen megfigyelhető még takarás mellett is, így a hő képpel együtt akár elsőre is bejuthat egy illetéktelen.



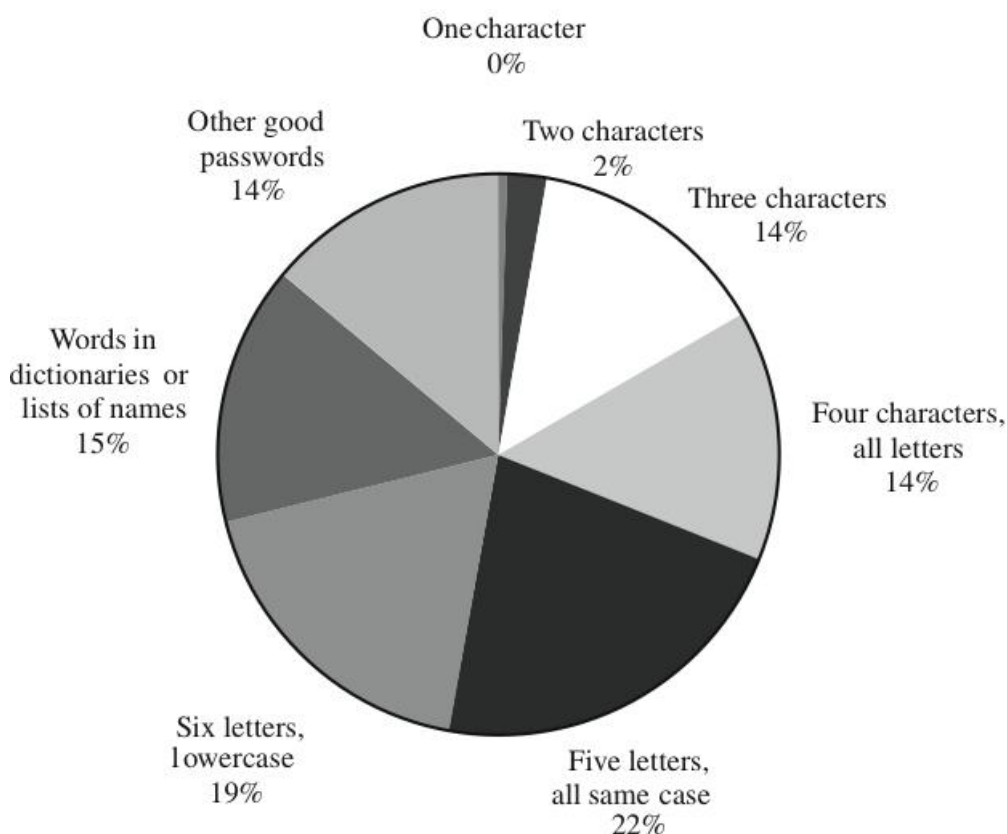
terminálokon kívül megoldható a beléptetés komplex jelszavak használatával is. Ebben az esetben nagyobb biztonságot nyújt, hiszen a lehetséges jelszó, sokkal több karakterből állhat, ráadásul nem korlátozódik csak számokra. Ilyenkor általában számítógépeket használnak a jelszó megadáshoz és többnyire felhasználónévvel kombinálják. Az előnyeikhez hozzátartozik, hogy a számítógépet használhatjuk másra is, akár a beléptetéssel kapcsolatban (információlekérés, naplózás), akár általánosan is. Viszont hátrányai közé tartozik, hogy a számítógép biztonsága könnyen kompromittálható ún. keylogger-ek alkalmazásával. Ezek lehetnek software-es vagy hardware-es megoldások. Első esetben egy rosszindulatú program formájában, utóbbi esetben pedig egy eszközként. A programot úgy kell elképzelni, mint egy kártékony vírust, mely tudtukon kívül, figyeli a leütött billentyűket és ezt az adatot továbbítja egy rossz szándékú illetőnek. Amennyiben nem programot, hanem eszközt használnak, azt szinte észrevehetetlenül rejtik el a számítógépen, valahol a billentyűzet érintkezésénél.



A továbbiakban szeretném pár szóval említeni a jelszavak biztonságát. Minden felhasználónak, aki bármilyen jelszót birtokol (legyen szó beléptetésről vagy általánosan), tudatosan kell megválasztania azt, személyesen felel érte, hogy megbízható legyen. Egy jelszóval kapcsolatban alapvető követelmények:

- Legalább 4 karakterből álljon
- Tartalmazzon vegyesen betűt, számot, egyéb karaktert
- Tartalmazzon vegyesen kis és nagy betűket
- Értelmes szót ne lehessen kiolvasni belőle
- Dátumot, évszámot, életkor ne lehessen kiolvasni belőle

Az ilyen kritériumok alapvetőek, ezek nélkül találgatással esetlegesen meg lehet fejteni a jelszavunkat. Nagyon gyakori példa, hogy valaki egy számára fontos dátumot használ jelszóként, amelyet egy *social engineering* eljárással könnyen kideríthet egy rosszakarató (nem kell nagyra gondolni, könnyen elképzelhető, hogy közösségi oldalakon megtalálható információról van szó...). Amennyiben jelszavunk komplex, a találgatásos módszer ellen kellő védelmet nyújt. Sajnos a támadó részéről, ilyenkor jön képbe a *brute force* módszer, amely nyers erővel próbálja végig a lehetséges jelszavakat. Nyilván ez időt és energiát vesz igénybe, így időben észrevehető, ha valaki ilyesmivel próbálkozik. Amennyiben odafigyelünk, esetleg őrzést alkalmazunk, illetve hálózatunkat és védjük kellőképp, egy megfelelő jelszó jelentősen erősíti beléptetésünk védelmét.



Összességében elmondható, véleményem szerint, hogy a számkódos, illetve egyéb jelszavas megoldások önmagukban nem nyújtanak megfelelő védelmet a beléptetés biztosítására. A biztonság egyéb területein is felmerülnek hasonló hiányosságok, ezért törekedni kell mindenhol a komplex megoldásokra. Bankok esetében például, egy ATM terminálnál a kártya chip vagy mágnes részét is le kell olvasni a PIN kód megadása előtt, és együttesen biztosítanak egy megfelelő, de korántsem kijátszhatatlan védelmet. Megint csak nem hagyományos értelemben vett beléptetési téma, de például az internetbankok esetében egyre elterjedtebb az jelszó megadása mellett az SMS-ben kapott kód megadása is, így egy birtokunkban lévő tanúsítvány (előre megadott telefonszámú SIM kártya birtoklása) megléte is feltétele a beléptetés biztosítására. Ez jó példa lehet beléptetés kiépítésénél, bár gyakorlatiasabb megoldás egy valamilyen kártya és mellette a számkód alkalmazása (természetesen még mindig nem nagy objektumok beléptetésénél) a nagyobb biztonság elérése érdekében.



3.2.2. Birtoklás alapú elektronikus beléptető rendszer

Ebben a témában a leggyakrabban előforduló módszer a valamilyen kártya segítségével történő belépés, így én is ezek biztonságával fogok foglalkozni.

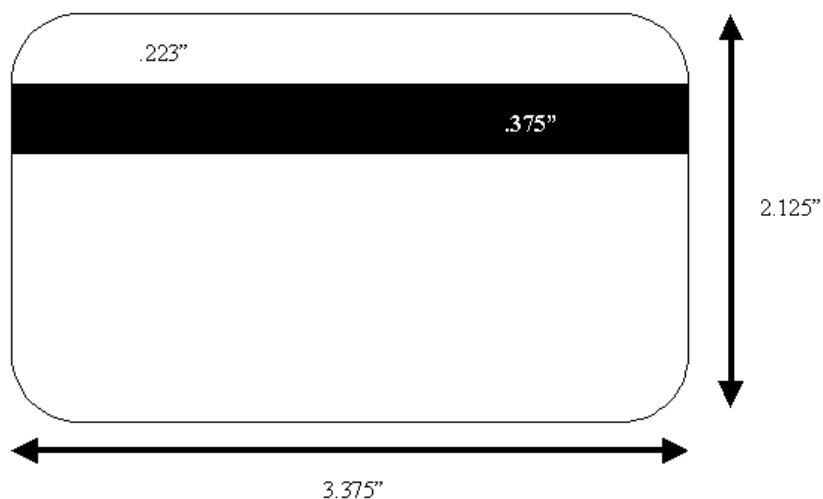
Legelőször is szeretném bemutatni a különböző elérhető kártyákat:

- Lyukkártya
- Vonalkódos kártya
- Chipkártya
- Mágneses kártya
- *Proximity* kártya (közelítő vagy RFID kártya)

Úgy vélem, hogy az elsővel már nem érdemes foglalkozni, mert nincsen már használatban, illetve nem is nyújtana elégséges biztonságot. A vonalkódos megoldás gyakorlati alkalmazásának vannak előnyei, hiszen könnyen előállítható, akár laminált papír alapú kártya is megfelelően működik, olvasó is könnyen kezelhető, nem véletlen, hogy a boltokban elterjedt módszer. Ellenben biztonsági szempontból több kivetnivalót is von maga után, legfőképp, hogy könnyen lehet lekopírozni őket. Ha megvan a kívánt vonalkód minta, elég akár egy hagyományos papírlapra kinyomtatni, és máris készítettünk egy egyszeri belépőt. A minta megszerzéséhez az illetéktelennek nincs más dolga, mint lefényképezni, ami a mai mikro-méretű kamerákkal egyáltalán nem jelent kihívást. Ilyen rendszert akkor érdemes alkalmazni, amikor a jogosultság megszerzése nem igényel különösebb kiváltságokat, és a beléptetés a különböző jogosultak közötti megkülönböztetést szolgálja, hiszen relatíve alacsony költségvetésű megoldás. Erre jó példa az egyetemünkön működő könyvtárban használt vonalkódos kártya, hiszen bárki beléphet a könyvtárba, a lényeg, hogy tudják, kinek a nevén vannak a kiadott könyvek. Nehezen tudnám elképzelni, hogy bárkiben is felmerülhet, hogy hamisítson magának egy egyetemi beléptető kártyát..

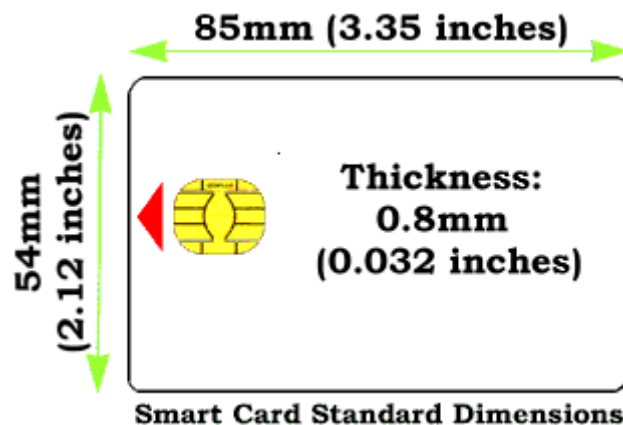


A mágneskártya technológiája a második világháború idején született és a 60-as években fejlődött ki, így nem újkeltű a téma. A dolog működésének elve, hogy a csíkban elhelyezkedő részecskék mágneses pólusát változtatjuk, ezáltal adatot lehet benne tárolni (akár jogosultság tanúsítványát). Mára már elérte azt a szintet, hogy potom pénzekért bárki rendelhet magának, előállítási költsége minimális. Bár egy mágneses kártya megléte önmagában nem elegendő, azt be is kell állítani úgy, hogy átjussunk vele a beléptetési ponton, de mindenesetre egy jogosulatlanak megkönnyíti a dolgot. Manapság a mágneses kártya nem jelent kellő mértékű biztonságot, ezt jól bizonyítja az a tény is, hogy az Egyesült Államokban a mágneses bankkártyákkal kapcsoltban rengeteg csalás és visszaélés történt. Európában, így idehaza is, a bankkártyák ezért a chip és a jelszóhasználat kettős biztonságát alkalmazzák (a mágneses kártyával egyetemben).



A chipkártyák (más néven okos kártyák), napjaink egyik legelterjedtebb és biztonságosabb kártya típusa. Működési elve egy kisméretű integrált áramkörön (IC) alapul, amelyben tároljuk az adatot (tanúsítványt), természetesen megfelelő rejtjelezéssel, amit egy olvasóval elő lehet hívni. Manapság rendkívül népszerű, a technológiát mellesleg a mindenki telefonjában ott rejlő SIM kártyák esetében is használják. Előállítási költsége valamivel drágább, mint a mágneses kártyáé, de nem ez adja a biztonságát. Egy chipkártyát nehéz feltörni, hiába is jutunk hozzá egyhez, és feltételezzük, hogy van hozzá egy olvasónk is. Ahhoz, hogy valaki hozzáférjen a benne tárolt adatokhoz, fel kell törnie a rejtjelezést, ami nem egy mindennapi feladat. Vannak különböző módszerek, mind informatikai, mind elektronikai, amivel meg lehet próbálni kijátszani a rendszert. Ha például megfelelően pontos mérőműszerekkel rendelkezünk, megpróbálhatjuk lemérni a feszültséget és az eltelt időt a titkosítás során, ami enged következtetni a rejtjelezés tulajdonságaira. Felmerülhet esetleg a

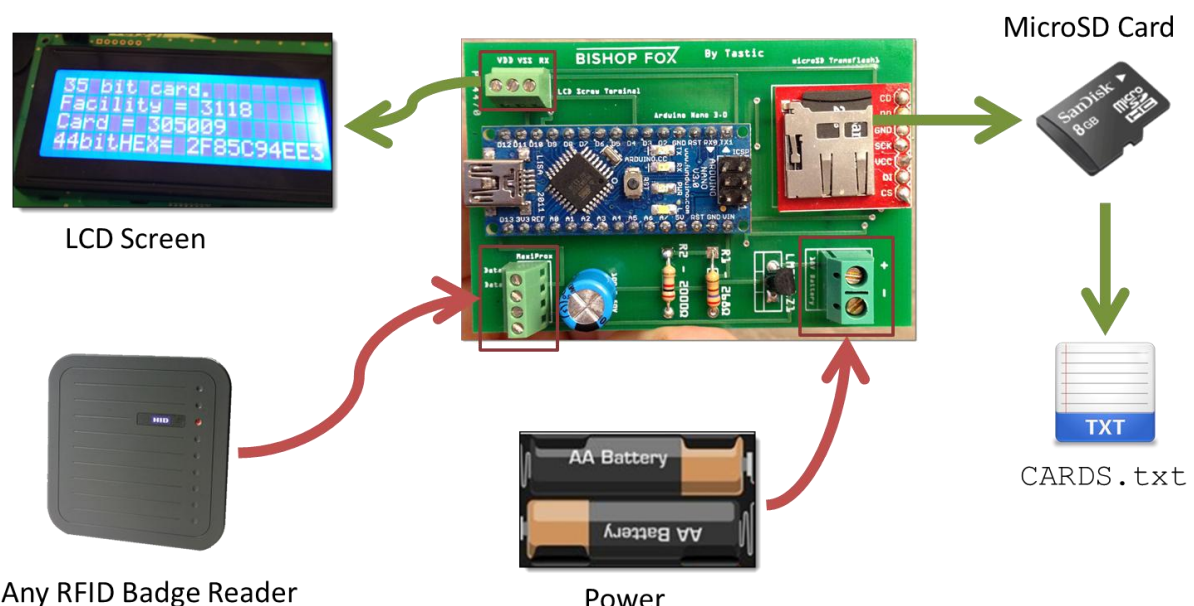
rövidzár, vagy különböző *brute force* támadások lehetősége is. Ha a biztonság alapelveig nyúlunk vissza elmondható, hogy mint minden más eszköz és módszer, ez sem nyújt teljes védelmet, nem feltörhetetlen. Ettől függetlenül elmondható, hogy napjainkban elfogadható mértékű biztonságot nyújt. A leggyakrabban felmerülő kockázat itt is a személyi tényező. A legegyszerűbb visszaélés a módszerrel szemben, ha fizikailag ellopják valakinek a chipkártyáját és felhasználják, akár a beléptetésnél is. Ezért is fontos az, amit már említettem korábban, és amire a bankkártyák is jó példák, hogy ilyen kártyák használata mellett más beléptetési módszer alkalmazása is szükséges (célszerű összekötni egy PIN kód ismerettel).



Végül marad a beléptetés terén leginkább elterjedt kártya, amit egyes szakirodalmak közelítő kártyaként fordítottak, ami sokat elmond a működéséről is. Az alapelve az elektromágneses indukció. Egy ilyen kártyában egy többszörösen összetekert vezeték található, egy kisméretű integrált áramkörrel (chip) összekötve.



A leolvasó egység rádió sugarakat bocsájt ki, ilyenkor az összetekert vezeték, mint antenna működik, és a rádió mezőjének energiáját felhasználva, úgymond „aktiválja” a chipet, ami a benne tárolt adatot, szintén vezeték nélkül visszasugározza a leolvasónak, amely aztán a kapott információ alapján eldönti, hogy a kártya tulajdonosa jogosult-e vagy sem a belépésre. Mindez egy pillanat alatt zajlik le, és leggyakrabban egy jellegzetes hang, illetve többnyire zöld fény jelzi a belépés jogosultságát. Gyakorlatiasság szempontjából ez a megoldás bizonyul az egyik legjobbnak, hiszen a kártyát nem kell az olvasóba behelyezni, így lényegesen meggyorsítja a beléptetést. Biztonsági szempontból érdemes más módszerrel egyidejűleg használni, a lopások és visszaélések elkerülése végett. A gyors beléptetés fenntartása érdekében, jelszavak használata helyett élőerős módszerrel együtt is megoldható, ahol az őrség külső szempontok alapján (nem, kor, magasság, bőr/haj szín, stb..) tudja ellenőrizni a belépőt, hogy ő valóban a jogosult személy-e (ez történik, példának okáért, egyetemi *campus*-unk beléptetése esetében is..). Van viszont a lopáson kívül másik támadási felülete, amely ellen védekezni is nehezebb. Kihasználva, hogy a hagyományos kártyákkal ellentétben a *prox* kártyák vezeték nélküliek, megoldható az „aktivizálásuk” anélkül, hogy akár tudomást szereznénk róla. Hiszen mágneses- vagy chipkártyák esetében át kell húzni, vagy be kell helyezni egy leolvasóba, amit ha tudunkon kívül történik, észlelni fogunk, ha másból nem is, de a kártya hiányából. Ha viszont feltételezzük, hogy valaki rendelkezik egy olyan eszközzel, amely a megfelelő jeleket sugározza és olvassa a kártya által visszaküldött jeleket, akkor máris hozzájutott a kártyánkon tárolt adatokhoz. Persze a gyakorlati megvalósítása összetettebb, mint ahogy most pár mondatban leírtam, de mint a zártörés esetében, lelkes amatőrök is hozzáfoghatnak. Az internet telis tele van különböző megoldással, hogyan kell építeni és működtetni ilyen leolvasó eszközöket, elérhetők tervrajzok, beszerezhetők a szükséges alkatrészek, elemek, és rengeteg oktató videót is találhatunk.



Amennyiben valaki megszerzi a kártyában tárolt adatokat, beléptetés esetében a tanúsítványt, akkor rendelkezni fog a jogosultságunkkal is, innentől kezdve elő tud állítani úgynevezett klón kártyát (*proximity* kártyák ára párszáz Ft körül mozog), és biztosítva van a beléptetése. Az adatok leolvasásához nem kell nagydologra gondolni, valaki elsétál mellettünk egy válltáskával, ami pár centiméteres közelségbe kerül a zsebünkben lévő kártyához és meg is szerzi az adatot (a kártyán tárolt kód kisméretű, 26-37 bit közötti). Ha pedig egy zsúfolt tömegközlekedési eszközön utazunk, a támadónak még könnyebb a dolga. A legtöbb beléptetés céljából használt *prox* kártya nem tartalmaz titkosítást, ezért is van kiemelten könnyű dolga a támadónak. Szakértők szerint az Egyesült Államokban a beléptetési rendszerek 70-80% *proximity* kártyás alapú, vélhetően a gyakorlati hasznossága végett, és mégis belátható, hogy óriási biztonsági rést hordoz magában. Érdekességként biztonsági szempontból idevágó téma a bankok által kiadott úgynevezett *paypass* (*paywave*, *expresspay*) kártyák. Ezek tulajdonsága, hogy a *prox* kártyához hasonlóan csak a leolvasó közelébe kell helyezni és kész is a tranzakció. Biztonsági okokból van egy limit, ami fölötti vásárlás esetén, a PIN kód megadása is szükséges, ez hazánkban 5000Ft-ot jelent. Ezt a rossz szándékú támadók ki is használják, főként a fent említett tömegközlekedési eszközön végigsétálva, egy hordozható terminállal, és máris 4000 forintokkal károsítják meg a gyanútlan utazókat. Persze a gyakorlatban ez is kissé összetettebb, de a veszély valós. A védekezés egyik lehetséges formája, a külföldön elterjedtebb és kapható úgynevezett blokkoló tárcák, amibe ha belehelyezzük a kártyát, azt mindegy árnyékolja, és nem engedi „aktiválni”.



Másik megoldás lehet, ha csak akkor tartjuk magunknál a kártyát, mikor tudjuk, hogy szükségünk lesz rá és használni fogjuk. További védelmet jelenthet, ha a kártyát nem a nyakunkon lógva hordjuk, hanem a táskánk mélyén, illetve ha kerüljük a zsúfoltabb helyeket (bevásárló központok, tömegközlekedés). Összességében úgy vélem, hogy a *proximity* kártyák a fent említett okok miatt nem nyújtanak kellő biztonságot. Használata csakis más módszerekkel együtt ajánlott, lehetőleg jelszavas beléptetéssel egybekötve.

3.2.3. Biometrikus azonosítás

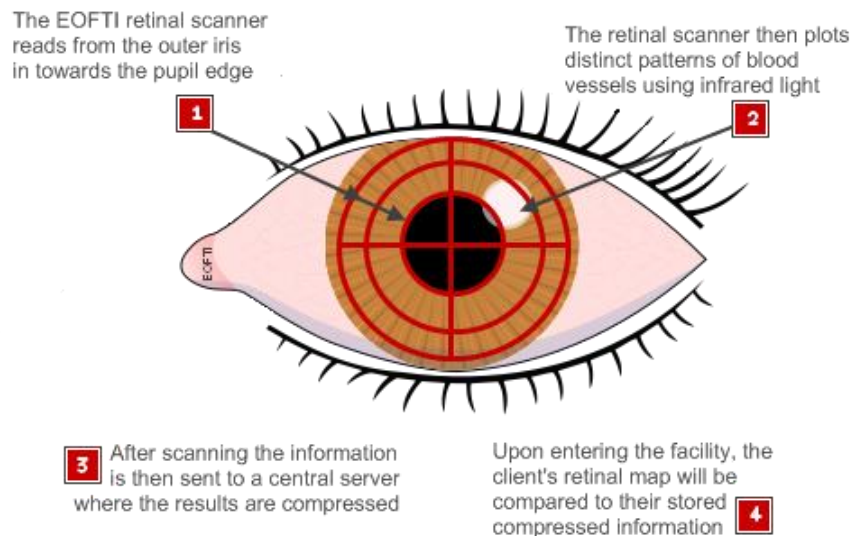
Az ezen az elven működő rendszerek lényege, hogy a belépni szándékozó egyén személyét vizsgáljuk, hogy megállapítsuk jogosultságát. A biometrikus azonosítást egyébként máshol is használják, leginkább a rendőrségi nyomozások esetében. Az alapelve, hogy minden ember rendelkezik olyan tulajdonságokkal, melyek csakis rá jellemzőek. Ezek elemzésével egyértelműen azonosítható bárki, amivel elméletben ideális lenne egy tökéletes beléptető rendszer kiépítéséhez. Gyakorlatban azonban felmerülnek olyan problémák, amik miatt ez a rendszer sem számít tökéletesnek.

Biometrikus azonosítás legelterjedtebb formái:

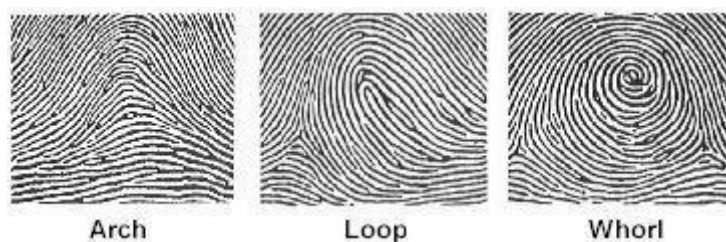
- Retina vizsgálat
- Ujjlenyomat vizsgálat
- Tenyér vizsgálat
- Kézírás ellenőrzés
- DNS vizsgálat

Elsőként a retina (írisz) ellenőrzésről ejtenék pár szót. A szemünkbe vért szállító többszázezer ércsatorna elhelyezkedése annyira komplex és összetett, hogy személyenként eltérő, ezáltal annak vizsgálatával egyértelmű lehet az azonosítás. Egyik hátránya, hogy egyes betegségek módosíthatják a retinánkat (pl. cukorbetegség), így nem tekinthető olyan biztos jellemzőnek, mint a DNS, vagy az ujjlenyomat. Előnye viszont, hogy nagyon gyorsan végrehajtható a vizsgálat, pillanatok alatt azonosítható valaki. Magas anyagköltsége miatt, csak a nagy biztonságot igénylő szervezetek beléptetésénél (FBI, CIA, NASA, stb..) elterjedt a használatunk. Kijátszásuk nem lehetetlen, viszonylag olcsón előállítható olyan kontaktlencse, amely módosítja egy adott személy íriszét annyira, hogy ne ismerje fel egy rendszer. A beléptetés szempontjából ez semmi jelentőséggel nem bír, hisz egy támadó célja az lenne, hogy valaki más retináját reprodukálja és így jusson be. Erre a megoldásra irányulnak kutatások, de több akadályba is ütköztek. Egyik megoldás elméletben, ha egy közeli és elképesztően jó minőségű képet készítenek valaki szeméről (elég elvont helyzet), majd rendkívül jó minőségben kinyomtatják, akkor van rá esély, hogy átjut vele az ellenőrzésen. Ellenben többnyire az ilyen rendszerek nemcsak egy képet készítenek és elemzik a retinát, hanem többféle világítást alkalmaznak, több szögből is, amelyeket a papírra nyomtatott tinta másképp ver vissza, mint az emberi szem. Illetve, ha valaki ily módon túl is jut, amennyiben van élőerős védelem, az nyomban kiszúrja a visszaélést és intézkedik az ügyben.

Összességében úgy gondolom, hogy egy retina ellenőrző beléptető rendszer kellően nagymértékű biztonságot nyújt, ám érdemes figyelembe venni a magas költségeit, illetve javasolt más módszerekkel kombináltan használni.



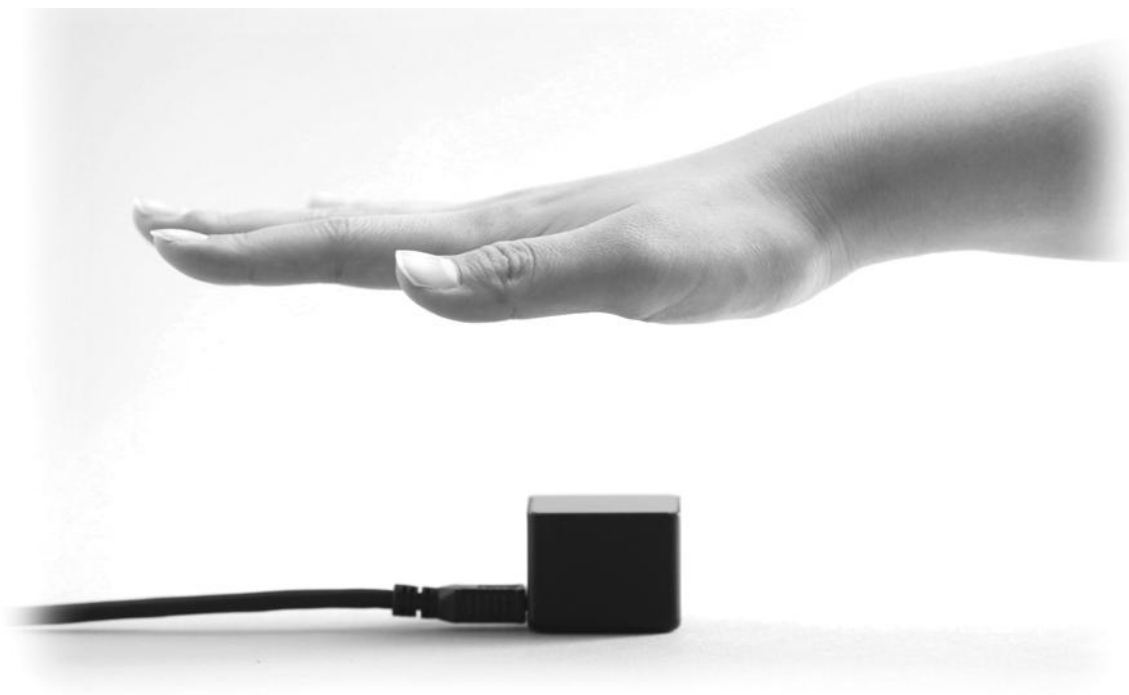
Az ujjlenyomat vizsgálat egy sokkal elterjedtebb és nem csak a beléptetésnél használt módszer, mely lehetővé teszi az ember ujjhegyén lévő minták elemzéséből megállapítani az illető személyazonosságát. Ennek két gyakorlatban elterjedt módszere létezik: optikai és ellenállás alapú. Az első esetben egy jó minőségű és kivilágított fotót készítünk az ember ujjáról és a képet digitalizálva kezdjük meg az elemzést. A másik esetben a felületen, hasonlóan, mint az érintőképernyők működési elvénél, az ujjunk áramvezető tulajdonsága végett megjelenik az ujjlenyomatunk digitális képe, ezt vizsgáljuk. Általában az utóbbit használják, mivel megbízhatóbb (nem hátrány a piszkos ujj és nem játszható ki egy másik fotóval). Amennyiben megvan a kép, egy számítógépes rendszer elemzi a mintákat az ujjlenyomatunkban (*boltív, hurok, örvény* minták) és ezek alapján összevetik az adatbázist egyezéssel.



Bár közeli rokonoknak lehet hasonló, de nincs két ember, akinek teljesen azonos az ujjlenyomata, így elméletben 100%-ig megbízható módszer az azonosításra. Sajnos a gyakorlatban vannak felmerülő problémák a módszerrel kapcsolatban: a digitális technológia ejtethet hibákat, például az FBI által használt IAFIS ujjlenyomat azonosító rendszer is csak 98%-ban számít megbízhatónak. Továbbá egy japán egyetemi tanár, Tsutomu Matsumoto, előállított egy *gumi* ujjlenyomatot, ami a nevét a gumimacihoz hasonló anyaga miatt kapta. Az illető egy tanulmányban bemutatta, hogy állítható elő könnyedén ilyen *gumi* ujjlenyomat, mik a tulajdonságai, hogyan képes vele a rendszert kijátszani. Ez a tanulmánya egyébként bárki számára ingyenes elérhető a világhálón. Természetesen a korábban említett fotós, vagy a fenti *gumi* ujjlenyomatos módszerek ellen könnyen védekezhetünk élőerős beléptetés alkalmazásával. Összességében elmondható, hogy megfelelő mértékű biztonságot tud nyújtani, ráadásul ma már nem számít drága csúcstechnológiának (példa okáért a legújabb iPhone készülékek beépített digitális ujjlenyomat olvasóval árulják).



Az ujjlenyomat olvasáshoz hasonló a tenyér vizsgálata, amely szakértők szerint nagyobb biztonsággal működik, és nem játszható ki a *gumi* ujjlenyomat módszerrel. A működése visszavezet a retinához, ahol szintén mindenkinél egyedi módon elhelyezkedő vérerek vizsgálatával azonosítható egy ember. Ár szempontjából viszont olcsóbb a retina ellenőrzőnél, illetve használatához nem is kell megérinteni a terminált, nem kell közel hajolni szkenneréhez, így kifejezetten higiénikus, „emberbarát” módszernek számít.



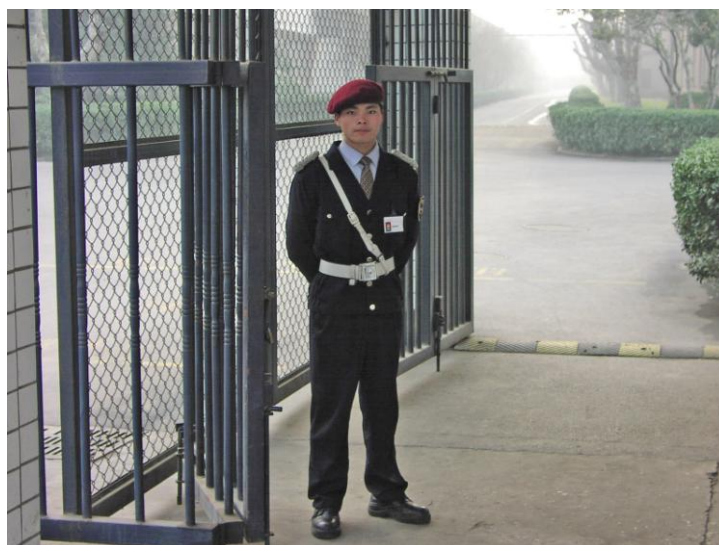
A kézírás elemzése az azonosításon túlmenően egy önálló tudományág is (grafológia), amiről külön könyvek is íródtak, ellenben a beléptetésnél ezt a módszert nem használják, így dolgozatomban nem térnék ki rá. A DNS vizsgálat szintén egyfajta azonosítás, de hosszú várakozási ideje és nagy anyagköltségei miatt beléptetésnél nem, csak orvostudományban és kriminológiában használják, így most erre sem térnék ki.

3.3. Élőerős beléptetés

Akár biztonságról beszélünk általánosan, akár kifejezetten beléptetési rendszerekről, már az idők kezdete óta létezik az élőerős védelem fogalma. Erre a történelem folyamán több kifejezést is használtak, manapság a személyőr, vagyonőr, fegyveres biztonsági őr elnevezések a legelterjedtebbek. Az őrsegek, őrszolgálatok elterjedtek mind a civil mind a katonai életben is. Rengeteg vállalkozás foglalkozik őrzés-védelem szolgáltatás nyújtásával. Örökkel találkozhat az ember mindenfelé, nagyobb bevásárlóközpontokban, pénzügyintézetekben, repülőtereken. Az őrök feladata elsődlegesen egy adott objektum, tárgy, vagy személy őrzése, védelme, de fontos szerepet játszanak a beléptetési rendszerek működtetésében is, a továbbiakban ezt szeretném bemutatni.

Elsőként szeretném bemutatni az élőerős védelem típusait:

- Fegyveres őr
- Portás
- Kutyás őr
- Alkalmi őr
- Rendőrség
- Őrző-védő cég
- Gondnok
- Lakó
- Járókelő



Jól látható, hogy az elvárt és ismert őrségeken kívül vannak rendhagyóak is. A rendőrség például ritkán végzi egy konkrét objektum őrzését, még inkább annak beléptetési rendszerét (hacsak nem egy rendőrségi intézmény esetében), viszont bűncselekmény, vagy annak gyanúja esetén bármikor kiértésíthető, így a védelem szerves részét képezi. Egy járőrelőt, vagy lakót megint csak nem gondolnánk a védelem részének, mindazonáltal jogtalan belépéseket, behatolásokat, esetleges betöréseket képes észlelni és bejelenteni, illetve jelenléte is hozzájárul a biztonság fenntartásához.

Az első és véleményem szerint legfontosabb szerepe az őrzést végző személynek a figyelés. Az illető személy jelenléte már eleve elrettentően hathat, így védelem szempontjából ez rendkívül előnyös. Itt említeném meg esetlegesen egy portás szerepét, akinek nincsen fegyverhasználati képzettsége, vagy különösebb biztonsági ismeretei, ellenben egy esetleges jogtalan behatolást ugyanúgy tud jelezni, illetve segíti a beléptetés zavartalan működését. Ezen felül, egy őr nemcsak odafigyel a rend és a szabályok betartására, hanem adott esetben képes meg is állítani egy esetleges illetéktelen belépőt.

Ha egy adott beléptetés csak egyfajta módszerrel történik, a korábban említett támadások valamelyikével többféleképpen is kijátszható a védelem. Ám amennyiben rendelkezünk élőerős védelemmel, akkor értelemszerűen a behatolónak az őrséget is ki kell játszania valamilyen formában, különben az őr feltartóztatja a jogtalan belépését. Amennyiben valahol forgókapus beléptetési rendszert használnak, különösen fontos az őrség jelenléte, hiszen a kapu nem jelent valós fizikai védelmet, rendeltetése az illetéktelen behatoló feltartóztatása, amíg az őr intézkedik.

Az őrség gyakorlati alkalmazása a beléptetés tekintetében túlmutathat az egyszerű jelenlétén és megfigyelésén is. A személyi védelem használható igazoltatásos beléptetésre. Ennek hátránya, hogy lassítja a folyamatot, hiszen egyenként kell igazoltatnia a belépésre váró személyeket, hogy jogosultak-e. Előnye viszont, hogy míg egy kulcsot, vagy egy kártyát ellophat egy illetéktelen személy, és ily módon belépést nyerhet, ám valaki személyazonosságát nem lehet „ellopni”. Az ilyen fajta beléptetést nem célszerű nagyobb intézmények esetében használni, mert feltorlódást okozhat, hiszen ugyanazok az emberek beléptetése lezajlik napi szinten kétszer. Ellenben egyszeri rendezvények szervezésekor kifejezetten előnyös az igazoltatásos beléptetési rendszer alkalmazása.

3.3.1. Személyi tényező gyenge pontjai

Dolgozatomban a beléptetési biztonság elemeit vizsgálgatva igyekszem azok támadhatóságára is kitérni, így az élőerős védelem esetében is szeretném ezt bemutatni.

Ha ebben a témában kell a sebezhetőségről szót ejteni, mindjárt azzal kezdeném, hogy a legnagyobb rizikó faktor minden védelemben az emberi tényező. Egyelőre még nem értünk el olyan technológiát, ami nem igényelne emberi közreműködést, még ha csak időszakosan és részlegesen is (karbantartás, beüzemelés, irányítás, ellenőrzés, stb..), ezért elmondható, hogy a védelem minden aspektusának része az emberi tényező. Ez hatványozottan igaz, ha egy őrségről beszélünk, ahol maga az ember jelenti a biztonságot. Mielőtt rátérek a potenciális támadási felületeket, fontos külön csoportba csoportosítani őket.

Elsőként az olyan sebezhetőségekkel foglalkozom melyek nem szándékosak és többnyire nem kiszámíthatóak, és kár szempontjából a kisebb mértékűek. Ilyen esetekben főként emberi mulasztás következtében sérül a védelem. Egy beléptető rendszer kiépítésénél figyelembe kell venni ennek lehetőségét, és intézkedéseket elkövetni ennek megelőzése érdekében. Fontos, hogy amennyiben őrséget alkalmazunk beléptetésnél, részletes biztonsági szabályzatot kell írni, melynek a folytonos betartását rendszeres időközönként ellenőrizni kell. Emellett oda kell figyelni, hogy megfelelően válasszuk ki az alkalmazni szánt személyeket, részletesen vizsgáljuk meg az előéletüket, kezdetben pedig csak próbaidőben lássanak el őrséget. Végül pedig célszerű alkalmazni őrségparancsnokot, akinek feladata a beléptetési ellenőrzésén és működtetésén túl az őrség megfelelő állapotának fenntartása. Amikor a beléptetésünket építjük ki, fontos odafigyelni, hogy olyan cégeket, lakatosmestereket, biztonság technikusokat, informatikusokat alkalmazzunk, amelyek megbízhatók, megfelelő tanúsítvánnyal rendelkeznek, a nemzetközi szabványoknak megfelelnek. Amennyiben a fentieknek megfelelően járunk el, kiküszöbölhetők, de legalábbis leredukálható a gondatlanságból elkövetett hibák, károk, mulasztások mértéke.

A személyi tényezőn alapuló sebezhetőség nagyobb és egyben ártalmasabb kategóriája a szándékos károkozás. A leggyakrabban előforduló esetek:

- Szabotázs
- Lopás
- Csalás
- Sikasztás

- Zsarolás
- Titoksértés
- Ipari kémkedés
- Terrorizmus

Felmerülhet a kérdés, hogy mi vesz rá egy adott alkalmazottat, hogy megkárosítsa az őt alkalmazó szervezetet? Első és legfontosabb ok a vagyonszerzés. Ez lehet önálló módon végrehajtott (lopás, sikkasztás), vagy külső tényező által ösztönzött (szabotázs, ipari kémkedés). Előfordul továbbá, hogy valamilyen személyes titkát kihasználva zsarolással rávegyék a károkozásra. Végül pedig elképzelhető, hogy személyes meggyőződés alapján, netán alul motiváltság vagy épp személyes sérelem miatt szándékosan károsítja a szervezetet.

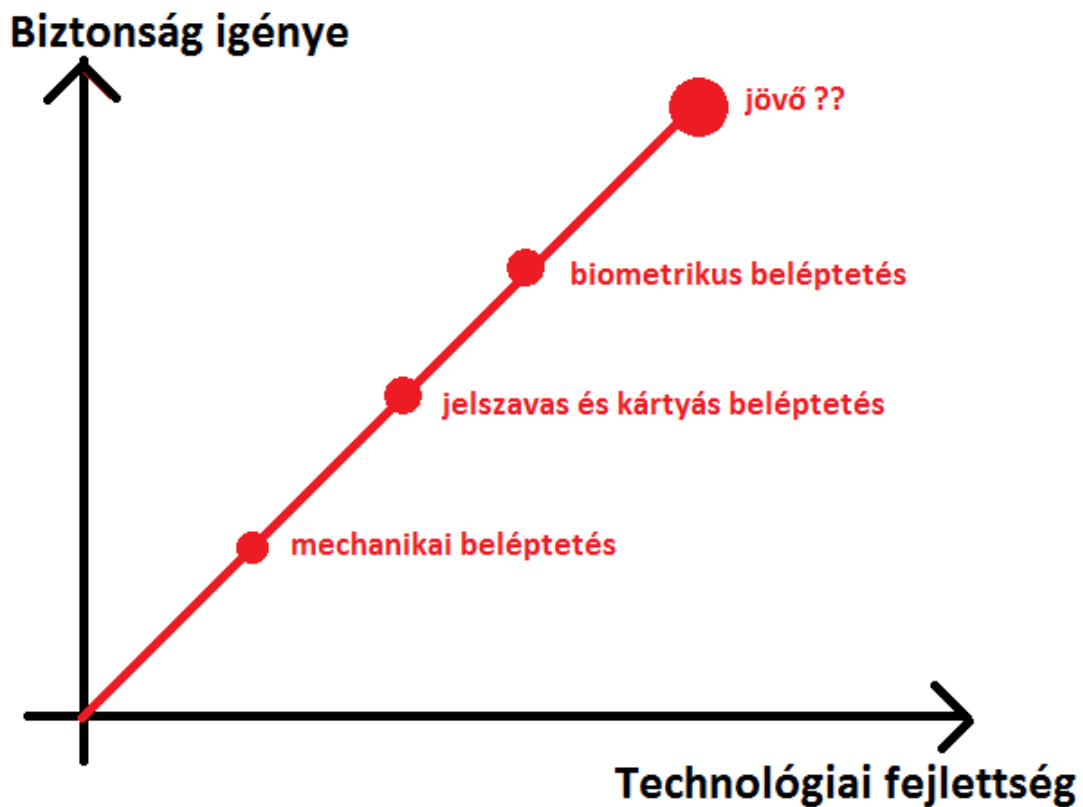


4. Összefoglalás

Dolgozatom végéhez érve eljutottam odáig, hogy levonjam a végső következtetéseket, tanulságokat, mérlegeljem az elért eredményeket.

A választott témám a beléptetési rendszerek (*access control systems*) volt, amelynek a biztonsági felépítését vizsgáltam. Igyekeztem a védelem minden aspektusát nézni, legfőképp olyan rendszerekre kitérni, amik a gyakorlatban használatosak, előfordulnak, találkozhatunk velük a mindennapokban is. Amit fontosnak tartottam, hogy mindig kitértem a védelem megtámadására, hogy hogyan kell rést ütni a védelembe, milyen gyakori módszerek fordulnak elő. A beléptetés minden eleménél megvizsgáltam az előnyöket és hátrányokat, majd a felmerülő szükségletek alapján mutattam be, mikor, milyen érdemes használni. Úgy vélem az általános bemutatáson kívül kitértem arra is, hogy miként kell védelem szempontjából kiépíteni egy adott objektum beléptetését. Igyekeztem összegzéseim több forrásból összegyűjteni, gyakorlati tudásokat is leírni a lexikálisak mellett. A konklúziókat nehéz lenne egybe foglalni, hiszen úgy vélem, dolgozatom minden egyes részénél végeztem kisebb összefoglalásokat az adott részegységről. Amennyiben komplex beléptető rendszer kiépítése a célunk megfelelő védelemmel, hisz lényegében ez dolgozatom témája, akkor figyelembe véve egy adott objektum költségvetését, fizikai tulajdonságait, kockázatelemzését, az általam felsoroltak közül (és azok kombinációiból) kiválasztható a megfelelő beléptetési rendszer.

A dolgozatom zárásaként szeretnék kitérni a téma jövőjére néhány mondatban. A beléptetési rendszerek fejlődése egyértelműen összefügg a technológiával és az általuk nyújtott biztonsággal. Mikor megjelent az elektromosság, és a hagyományos mechanikai módszerek nem nyújtottak kellő mértékű biztonságot, gyökeres változások léptek be a beléptetési rendszerek tekintetében. Úgy vélem, hogy hasonló elő fog még fordulni (akár többször is) a történelem folyamán. Jelenleg az mondható el, hogy a mechanikus beléptetések rendszere lehanyatlóban van, sokszor már leginkább pszichológiai hatásukra alapozunk, biztonságuk ritkán éri el a megfelelő szintet. Az olyan elektronikus beléptető rendszerek melyek valamilyen tulajdonban lévő tárgyra (kártyák), vagy tudásra (jelszó) alapulnak, kellő mértékű biztonságot tudnak nyújtani és ezek a legelterjedtebbek. Az olyan intézmények, objektumok, melyek kiemelkedő biztonságot igényelnek, és rendelkeznek kellő mennyiségű anyagi forrással, egyre inkább áttérnek a biometrikus beléptetésre. Ez is jól mutatja, hogy a technológiai fejlődés és a biztonság szükséglet növekedése együttesen okozza a változásokat.



Az élőrős védelem mindig is jelen volt a beléptetésnél, valamilyen formában, és úgy vélem ez a jövőben se lesz másként. Ami változás megfigyelhető, az inkább az emberek mennyiségénél látszódik, hiszen amíg a középkorban külön őrségeket szerveztek egy-egy kapu védelmére, ma már egy biztonsági őr kamerák segítségével több tucat beléptetési pontot is ellenőrizhet egyszerre, a jövőben meg az arányok valószínűleg még inkább eltolódnak. Dolgozatom legvégén azt tudom csak elmondani, hogy a beléptetés a történelem folyamán végig szerves része volt életünket, és úgy vélem lesz is mindaddig, amíg van a világon magántulajdon. Ennek elsődleges célja a védelem, így ennek vizsgálata mindig is idő- és szükségszerű, gyakorlati haszna pedig megkérdőjelezhetetlen. Zárásként Benjamin Franklin-től, az Egyesült Államok egyik alapítójától idéznék: „*Distrust and caution are the parents of security*” („bizalmatlanság és óvatosság a biztonság szülei.”)

5. Források

Internetes források:

- <http://www.nzeldes.com/Miscellany/images/Curiosities05.jpg>
- <http://jerkingthetrigger.com/wp-content/uploads/2012/11/SerePick-Titan-7-Flats.jpg>
- http://img.photobucket.com/albums/v611/101_aristotle/lockpicktemplate.jpg
- <http://en.wikipedia.org/wiki/Security>
- http://en.wikipedia.org/wiki/Access_control
- http://en.wikipedia.org/wiki/Physical_security
- http://en.wikipedia.org/wiki/Access_control
- http://en.wikipedia.org/wiki/Lock_%28device%29
- <http://www.theamazingking.com/images/locks/spp-tension.jpg>
- <http://www.uobd2.net/upload/pro/pick-gun-brockhage-downward-european-locks-door.jpg>
- <http://www.wrc.noaa.gov/wrso/posters/cx-0000-018.jpg>
- <http://static5.businessinsider.com/image/4d25cedb49e2ae6a09030000/this-atm-keyboard-will-steal-your-card-pin-and-youll-never-notice-it.jpg>
- <http://cdni.wired.co.uk/620x413/or/PIN.png>
- <http://www.magicaonline.com/hello-barcode-small.JPG>
- http://en.wikipedia.org/wiki/Magnetic_stripe_card
- <http://www.npr.org/blogs/alltechconsidered/2013/12/19/255558139/outdated-magnetic-strips-how-u-s-credit-card-security-lags>
- http://www.cherrycorp.com/english/keyboards/faqs/FAQs_files/image001.gif
- http://en.wikipedia.org/wiki/Smart_card
- <https://media.blackhat.com/us-13/US-13-Brown-RFID-Hacking-Live-Free-or-RFID-Hard-Slides.pdf>
- <http://www.proxclone.com/>
- http://www.bishopfox.com/wp-content/uploads/2013/08/Tastic_RFID_-_PCB_InputsOutputsv2.png
- http://www.eofti.com/images/retinal_scan.png
- http://en.wikipedia.org/wiki/Fingerprint_recognition

- <http://cryptome.org/gummy.htm>
- <http://affinis.in/prod/images/stories/virtuemart/product/fingerprint-lock.jpg>
- http://photos1.blogger.com/blogger/3259/1468/1600/pattern_types1.jpg
- <http://www.fujitsu.com/us/services/biometrics/palm-vein/pac.html>
- <http://sleepzine.com/wp-content/uploads/2007/08/sleeping-guard.jpg>
- http://upload.wikimedia.org/wikipedia/commons/f/f7/Private_factory_guard.jpg
- http://en.wikipedia.org/wiki/Social_engineering_%28security%29
- <http://en.wikipedia.org/wiki/Phishing>
- <http://www.d00med.net/uploads/0d832c77559a2070a766f899e7efb783.png>
- <http://www.porticor.com/wp-content/uploads/2012/03/weak-link-300x225.jpg>
- http://ace.imageg.net/graphics/product_images/pACE3-990695enh-z8.jpg

Nyomtatott irodalom:

- Kerekes János et al.: Információ, Biztonság. Budapest, CEDIT, 1997. ISBN 9638180307
- Muha Lajos és Bodlaki Ákos: Az informatikai biztonság. Budapest, PRO-SEC Kft., 2003. ISBN 9638602260
- Farkas Péter [konzulens Kiss Sándor]: Beléptetés, azonosítás, biometria azonosítás. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Vegyi-, Katasztrófavédelmi és Védelmi Igazgatási tanszék, 2006.
- Robert Newman: Security and Access Control Using Biometric Technologies. Boston, Course Technology, 2010. ISBN 9781435441057
- Christopher Hadnagy: Social Engineering: The Art of Human Hacking. Indianapolis, Wiley Publishing, 2011. ISBN 9780470639535
- Charles P. Pfleeger és Shari Lawrence Pfleeger: Analyzing Computer Security. Pearson Education Inc, 2012. ISBN 0132789469