HADMÉRNÖK

VI. évfolyam 1. szám - 2011. március

Bunyitai Ákos
bunyitai.akos@gmail.com

A MA ÉS A HOLNAP BELÉPTETŐ RENDSZEREINEK AUTOMATIKUS SZEMÉLYAZONOSÍTÓ ELJÁRÁSAI BIZTONSÁGTECHNIKAI SZEMPONTBÓL

Absztrakt

E tanulmány röviden összefoglalja és összehasonlítja azokat a kiforrott, széles körben alkalmazott és elfogadott személyazonosítási eljárásokat, amelyek kiinduló pontjai lehetnek a jövő beléptető rendszereinek. Tárgyalja az információ-, a tárgy- és a biometria alapú módszerek főbb jellemzőit. Célja a bemutatás – logikus rendszerezésen és rövid magyarázatokon keresztül – a téma iránt érdeklődők számára. Terjedelmi okok miatt nem célja azonban a beléptető rendszerekről átfogó ismeretekkel rendelkezők tudásszomjának oltása.

This article gives a brief summary of well known, widely used and user friendly identification methods, which can be the basis of the future's access control systems. It is about the main specifics of information-, object- and biometry based methods. The purpose is demonstration via logical structure and short explanation. It is for inquirers, not for access control system's experts, because of this length.

Kulcsszavak: *beléptető, személyazonosítás, kód, RFID, biometria ~ access control system, identification, code, RFID, biometry*

BEVEZETÉS

Napjainkban minden jelentős objektumnál elvárás, hogy vagyonvédelmének részeként egy olyan rendszer kerüljön kiépítésre, melynek fő célja a belépési jogosultság ellenőrzése (és az áteresztés megvalósítása mechanikai vagy elektromechanikai berendezések segítségével). Az ellenőrzés megfelelően gyors és megbízható kell legyen, egyértelműen és minden kétséget kizáróan ki kell szűrnie a belépésre jogosultak körét, nem gátolhatja mozgásukat és a nap 24 órájában működőképes kell maradnia. Az ilyen feladatok elvégzésére jöttek létre a beléptető rendszerek. A továbbiakban be kívánjuk mutatni a napjainkban leginkább előremutató(nak látszó) személybeléptető rendszerek főbb típusait, a személyazonosítás módja szerint csoportosítva.

A tanulmány célja egy közérthető, rövid áttekintő összefoglalása és összehasonlítása a beléptető rendszereknek biztonságtechnikai szempontból. Nem célja azonban az elavultabb, sérülékenyebb, illetve a személyazonosításra kevésbé használatos rendszerek bemutatása.

1. FOGALMAK MEGHATÁROZÁSA

Az alábbiakban a tanulmányban előforduló legfontosabb fogalmak kerülnek definiálásra, a rövidebb magyarázatot igénylőket az előfordulás helyén magyarázzuk.

Beléptető rendszer: „Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését." „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!"[5]

Automatikus: emberi beavatkozást nem igényel, pl.: nem automatikus, ha belépéskor az őr összehasonlít egy mentett és egy – a belépéskor rögzített – kamereképet a belépőről.

Azonosítás: személy vagy tárgy azonosságának megállapítása vagy kizárása.[6]

Személyazonosítás: az az eljárás, mely során egyértelműen megállapítható az egyén kiléte, vagyis, hogy valóban az-e, akinek kiadja magát.

Biometrikus azonosítás: a személyazonosítás egyik fajtája, az ember egyénenként eltérő mérhető biológiai jegyein, élettani vagy viselkedési jellemzőin (biometria) alapuló azonosítási eljárás.

2. RÖVIDEN A BELÉPTETŐ RENDSZEREKRŐL

2.1. A beléptető rendszer fő részei

- *Olvasó(k)* feladata, hogy az azonosításra alkalmas adatokat szolgáltassa a rendszer felé.

- *Vezérlő(k)* feladata, hogy az olvasóról beérkező adatok alapján eldöntse, hogy az adott személy az adott időpontban adott irányban jogosult-e az áthaladásra, működtesse, felügyelje az APAS-t (ld. később), naplózás.

- *Felügyeleti rendszer (pl.: PC-n futó felügyeleti szoftver):* feladata a rendszer ellenőrzése, a vezérlő egységek felprogramozása és a jogosultságok eldöntése, események rögzítése, visszakeresése, listázása.

- *Áthaladást szabályzó eszközök és érzékelőik* (a szakirodalomban az *APAS* rövidítés használatos az angol *Access Point Actuators and Sensors* meghatározásból) feladata, hogy kizárólag az arra jogosultak belépését tegye lehetővé (jogosulatlan személy be/ki lépésének akadályozása mechanikus vagy elektromechanikus eszközökkel), szingularizáció (egy azonosítás, egy áthaladás) és a gátló-szerkezet állapotának (nyitott, zárt, stb.) megállapítása. Pl.: forgókereszt, forgóvilla, gyorskapu, mágneszár, stb. érzékelőik működését a továbbiakban nem vizsgáljuk.

2.2. Online és Offline rendszerstruktúra

- *Online*-nak nevezhetünk egy beléptető rendszert, ha folyamatos a kapcsolata a felügyeleti rendszerrel.

- *Offline*-nak nevezhetünk egy beléptető rendszert, ha nincs folyamatos kapcsolata a felügyeleti rendszerrel, vagyis nem online. Ekkor a jogosultságokat a vezérlő egységhez kapcsolódva (pl.: PDA segítségével) változtathatjuk meg és így érhetjük el az eseménynaplót is.

2.3. Fail safe – fail secure: az áthaladást szabályozó eszköz működése szempontjából lehet életvédelmi (*fail safe*) vagy vagyonvédelmi (*fail secure*). Életvédelmi akkor, ha tápkimaradáskor az eszköz állapota nyitott, vagyis szabaddá válik a menekülési út. (Ld. 9/2008. ÖTM rendelet az Országos Tűzvédelmi Szabályzat kiadásáról menekülési utakra vonatkozó előírásait!) Vagyonvédelmi akkor, ha tápkimaradás esetén az állapota reteszelt.

2.4. Antipassback jelentése: belépési azonosító (kódkulcs) áthaladás utáni visszaadásának megakadályozása. Ez kiküszöböli a kártya átadhatóságából adódó problémák egy részét. Az antipassback fajtái: logikai (nem engedélyez egymás után azonos irányú mozgást), időzített (bizonyos időn belül nem engedélyezi az újbóli áthaladást), területi ellenőrzött (csak a rendszer által nyilvántartott helyről engedélyezi az áthaladást). Lehetséges a fentiek kombinációja is, pl.: logikai időzített.[7]

2.5. A beléptetés folyamata: azonosítás (személy, gépjármű, stb.), belépési jogosultság eldöntése, APAS működtetése, áthaladás, visszazárás. A beléptető további funkciói az események naplózása, rendszerfelügyelet, stb.

2.6. Két féle azonosítási módot különböztethetünk meg algoritmus szerint: pozitív és negatív kiválasztáson alapuló eljárást.

- Pozitív kiválasztásnak nevezzük, ha a rendszer a belépő személytől kapott információkat csak az adatbázisban hozzá rendelt adatokkal veti össze („csakugyan Ő az?”).

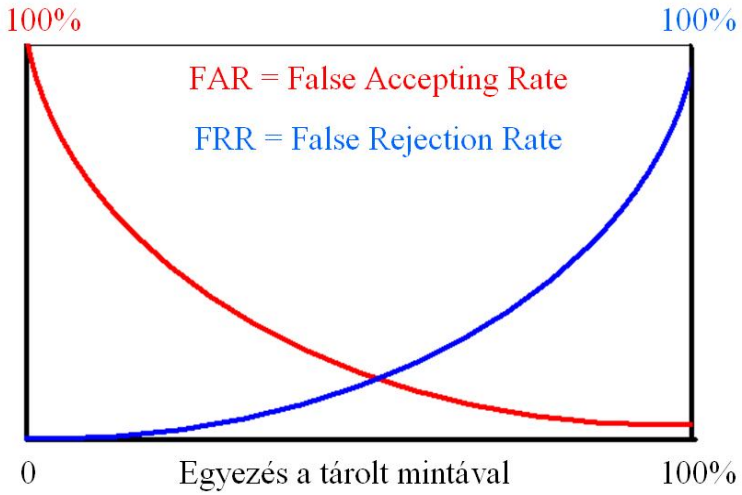
- Negatív kiválasztásnak nevezzük, ha a felhasználótól a belépéskor kapott információkat a rendszer a teljes adatbázisban keresi („ugyan ki lehet ez?”).

Könnyen belátható, hogy a pozitív kiválasztás sokkal gyorsabb – mivel nem kell a teljes adatbázist vizsgálni – hátránya azonban, hogy meg kell oldani a belépő adatainak előzetes kiválasztását (pl.: user ID).

2.7. A FAR, FRR és FTER mutatók

FAR (*False Accepting Rate*): hamis elfogadási hányad megmutatja, hogy az azonosítás milyen arányban ismert fel jogosulatlan felhasználót jogosultként.

FRR (*False Rejecting Rate*): hamis elutasítási hányad megmutatja, hogy az azonosítás milyen arányban utasít el jogosult felhasználót.



1. ábra. A hamis elfogadás és hamis elutasítás kapcsolata adott rendszerben (szimbolikus ábra).

Természetesen biztonságtechnikai szempontból a hamis elfogadás (FAR) veszélyesebb, hiszen belépésre jogosulatlan személyt engedett be a rendszer.

FTER (*Failure To Enroll Rate*): a biometrikus azonosítóknál fellépő adatfelvételi hiba mértéke megmutatja, hogy a minták milyen arányát nem tudja rögzíteni.

A továbbiakban – követve a szakirodalmi gyakorlatot – az angolszász (FAR, FRR és FTER) rövidítéseket alkalmazzuk.

3. SZEMÉLYAZONOSÍTÁSI MÓDSZEREK

A személy kilétének megállapítására többféle eljárást dolgoztak ki, ezeket 3 fő csoportba sorolhatjuk:

- *tudás (információ) alapú,*
- *birtokolt tárgy alapú,*
- *biometrikus tulajdonság alapú azonosítás.*

„Egy beléptető rendszer biztonsága a felismerés osztályozásán és a jogosultság osztályozásán alapul.”[8]

Az azonosítás biztonságának fokozásának érdekében célszerű a fentiek kombinálása. Az MSZ-EN 50133:2006 négy felismerési osztályt határoz meg: *0.* azonosítás nélkül, *1.* a felhasználó által ismert információn alapuló, *2.* azonosító tárgyon vagy biometrián alapuló, *3.* azonosító tárgyon vagy biometrikus azonosítón túl információt is szükséges az azonosításhoz. Azonosító tárgy és biometria kombinációja szintén ehhez a felismerési osztályhoz tartozik.

A programozhatóság védelmében „a különböző lehetséges kódok száma és a jogosult személyek száma közötti arány legalább 1000:1 legyen” és „a különböző kód változatok száma legalább 10.000 legyen”. A 2. és e fölötti felismerési osztály esetén legalább 10^6 db eltérő felismerési kód kezelhetőségére van szükség, FAR<0,01% és FRR<1%. A „jelkulccsal

vagy biometriával kapcsolatban használt személyes kód esetén" minimum 10.000-ret kell tudnia kezelni a rendszernek.[8]

A szabvány által javasolt minimális követelmények ma már nem tekinthetők célkitűzésnek egy rendszer tervezésekor, példaként vessük össze a fent említett FAR<0,01% (10^4:1) értéket a 4. fejezet összehasonlító táblázatában közölt FAR értékekkel! Láthatjuk, hogy a rendelkezésre álló technika és az igények messze túlszárnyalják ezt.

Amennyiben a beléptető rendszer valamely része egy behatolás-jelző rendszer részét képezi, ennek a résznek a behatolás-jelzési szabványok vonatkozó követelményeit is ki kell elégítenie. Kockázatfokozatok alapján meghatározott eltérő számú minimális kódvariáció vagy fizikai kulcs javasolt. Megkülönböztethető: alacsony, alacsony és közepes közötti, közepes és magas közötti és magas kockázat (Grade 1-4). Így alacsony kockázat esetén minimum 1.000 eltérő kódot vagy minimum 300 fizikai kulcsot; magas kockázat esetén minimum 1.000.000 kódot vagy 100.000 fizikai kulcsot kell tudni kezelni a rendszernek. Fizikai kulcs értsd: azonosító tárgy. A pontos meghatározások és értékek megtalálhatók a vonatkozó szabványban.[9]

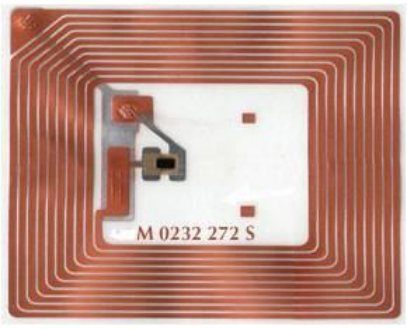
A szabványok külön nem emelik ki, de előfordulhat, hogy a rendszer biztonságának fokozása érdekében a nyitáshoz/záráshoz egynél több személy jelenlétének szükségességét írjuk elő.

3.1. Azonosítás felhasználó által ismert információ alapján

Jellemzően a numerikus PIN (személyes azonosítószám, *Personal Identification Number*) kód (általában 4, 6, 8 jegyű decimális szám), illetve meghatározott hosszúságú alfanumerikus jelsorozat (minimum 5 karakter hosszú). A vagyonvédelmi rendszerek általában nem tudnak különleges karaktereket, ékezetes karaktereket kezelni, kis-és nagybetűket megkülönböztetni. A 4 digit hosszúságú numerikus kód variációnak száma $V_n^{k,i} = n^k$ képlet alapján 10^4. Könnyen belátható, hogy a 6 digit hosszúságú kód variációinak száma 100-szorosa, a 8 digitesé 10.000-szerese a 4 digitesének. Az alfanumerikus karakterekből álló jelszavak variációs számánál az angol ABC 26 betűjét és a tíz számot alapul véve, 5 karakteres jelszóból $(26+10)^5$ = 60.466.176 féle létezhet.

3.2. Azonosítás birtokolt tárgy alapján

Jellemzően a rádiófrekvenciás azonosító eszköz (RFID, *Radio-Frequency IDentification*).



2. ábra. Egy RFID tag belseje.

Felépítése igen egyszerű, egy műanyag tokban antenna és egy mikrochip helyezkedik el. (ld. 2. ábra)

Csoportosításuk:

- Működési frekvencia szerint
    - 125 kHz
    - 13,56 MHz
    - 430 MHz
    - 862-956 MHz (UHF)
    - 2,45 GHz
    - stb.

    } szabad felhasználású frekvenciák
- Olvasási távolság szerint [5]
    - Contactless <5cm
    - Proximity 5-50cm
    - Hands free 0,5-2m
    - Long range >2m
- Energiaellátás módja szerint
    - Passzív
    - Aktív
    - Szemi-passzív (BAP, *Battery Assisted Passive*)
- Végezhető művelet szerint
    - Gyárilag programozott
    - Egyszer írható
    - Átírható
    - Írható/olvasható

*Működésük*ben eltérnek a passzív, aktív és szemi-passzív típusok. A *passzív* kártyák olvasása úgy történik, hogy a kártyát az olvasóhoz közelítve, belépve annak elektromágneses erőterébe, a benne lévő antennában feszültség indukálódik, amely biztosítja a kommunikációhoz és a belső chip működéséhez szükséges energiát. Az *aktív* tag amint detektálja az olvasó erőterét, saját energiaforrásból sugároz, így nagyobb olvasási távolság érhető el. A *szemi-passzív* tag a saját működését belső energiaforrásból biztosítja, a kommunikációhoz viszont az olvasó által sugárzott jelet használja (csak reflektál).[11]

Zavarérzékenység: a nagy méretű fém tárgyak vagy azonos frekvencián működő eszközök közelsége zavart okozhatnak az olvasásban.

Olvasási karakterisztika, irányítottság: az olvasónak az a tulajdonsága, hogy mely térrészből képes az azonosító olvasására. Alapvetően a működési frekvencia határozza meg. A hosszú hullámú olvasók körkörösen olvasnak, a mikrohullámúak erősen irányítottak. A telepítéskor számolni kell az olvasók egymásra hatásával.

Átolvasás: az a jelenség, amikor az egymás közelében levő olvasók olvasási terei átfedik egymást. Ilyenkor előfordulhat, hogy nem (csak) az az olvasó érzékel, melynél az azonosítót használni akarják (pl. a vékony fal két oldalán felszerelt olvasóból a túloldali érzékel, és emiatt hibás lesz a mozgásirány). [12]

Anti-collision: az olvasónak az a tulajdonsága, hogy egyidejűleg több, az olvasási terében található azonosítóval tud kommunikálni. Ahogyan nő az olvasási távolság, úgy nő a valószínűsége annak, hogy egyszerre több azonosító kerül az olvasó RF terébe. E helyzetek kezelésére többféle eljárást dolgoztak ki, ezt hívjuk „anti-collision”-nek (anti-ütközés).

Azonosító kártyák biztonsága: alapvetően 4-féle típus különböztethető meg adat-és információvédelem szempontjából. Ezek lehetnek [13]:

- Nyílt (open): egyszerű fix kód, olvasható és értelmezhető (vagy strukturálatlan) adattartalom. Megjegyzés: kötelességünknek érezzük felhívni a figyelmet arra, hogy az egyszerű fix kódos RFID eszközök másolása és hamisítása ma már nem jelent problémát.

- Kódolt (encoded): olvasható, nem értelmezhető, de másolható.

- Adathozzáférés védett (password protected): jelszóval elérhető, önmagában másolhatatlan. Megjegyzés: egy olvasó és hozzá tartozó kártya birtokában visszafejthető.

- Titkosított (encrypted): jelenleg a legbiztonságosabb, a használatos algoritmusokat ld. később!

A fentiekből látszik, hogy a XXI. században az RFID eszközök másolásvédelmében egyre inkább előtérbe kerülnek az informatikából ismert adat- és információvédelmi eljárások. Alkalmazható szimmetrikus kulcsú algoritmus (a titkosításhoz és a visszafejtéshez ugyanazt a kulcsot használja). Az algoritmus paraméteréül 112 bites kulcs (3-DES) szolgálhat. Használható továbbá nyílt kulcsú algoritmus is, pl.: RSA. A tanulmánynak a DES, 3-DES, AES, stb. adattitkosítási szabványok tárgyalása azonban nem célja.[14][15] Megjegyzendő, hogy az RFID technológia és az informatika összekapcsolásával előállhat olyan probléma, hogy egy RFID kártyán lévő számítógépes vírus támadja meg az informatikai rendszert pl.: SQL beszúrás (SQL injection) technika.[16]

Az azonosító eszközzel szemben támasztott követelmények: személyhez köthető legyen, másolás és hamisítás ellen védve legyen, hordozza az adott beléptető rendszer és az eszköz tulajdonosára jellemző információkat, kis méret, könnyű kezelhetőség, sorozatban gyártható legyen, a környezeti behatásokat adatvesztés nélkül viselje el, legyen esztétikus és olcsó.[20]

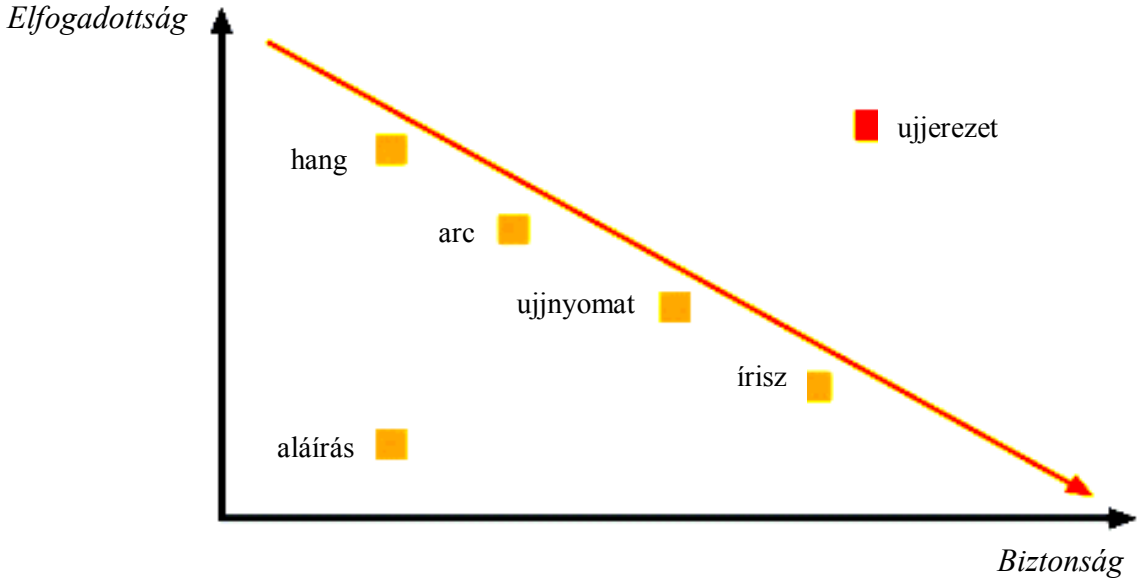
A rádiófrekvenciás azonosító eszköz ma már elérhető kis méretben is (ld. 3. ábra), ezeket állatokba vagy emberekbe ültetve alkalmazzák. Az Amerikai Egyesült Államokban jelenleg a VeriChip az egyetlen, amit emberi RFID implantátumként lehet használni, ezért a

VeriChip fogalommá vált. A technológia ellen tiltakoznak a jogvédők, azzal érvelve, hogy az RFID chipen lévő információk (személyes adatok, egészségügyi adatok, stb.) jogosulatlan kezekbe kerülhetnek vagy akár a kormány használhatja a szabadságjogok megtépázására, ezért hívják a technológiát Orwellinek (George Orwell 1984. című regényében leírt társadalom alapján). Tiltakozik továbbá több vallási aktivista, párhuzamot vonva a Bibliából ismeretes Sátán Jelével. A VeriChip támogatói a könnyű és kényelmes kezelhetőség mellet érvelnek, az adatlopásra azt válaszolják, hogy a chipben csak egy 16 digites kód található. Az RFID implantátum egészségügyi hatásait még vizsgálják.[21]

3. ábra. Egy RFID implantátum nagyságának viszonyítása egy rizsszemhez.

3.3. Azonosítás személyes tulajdonság alapján

Jellemzően a biometrián alapuló személyazonosító berendezések. Ezek lehetnek: ujjnyomat-, tenyérnyomat-, kézgeometria-, tenyérerezet-, ujjerezet-, írisz-, retina-, testhőkép-, DNS-, hang-, írás azonosítók, arcfelismerők, stb.



4. ábra. A biometrikus azonosítási módszerek elhelyezkedése a felhasználók és a biztonság szemszögéből.

A fentiekből kiemelendőnek tartjuk az ujjnyomat- és írisz azonosítókat – a széles körű elfogadottságot, kiforrottságot, elterjedtséget és biztonságtechnikai jellemzőiket (kombinációk száma, FAR, hamisíthatóság, stb.) figyelembe véve – ezek a módszerek látszanak leginkább elterjedni. A továbbiakban ezeket tárgyaljuk.

- *Ujjnyomat-azonosítás:* Francis Galton óta tudjuk és alkalmazzuk, hogy ujjunkon lévő bőr gyűrődéseiből (fodorszálak) kialakult mintázat egyedi és életünk során nem változik. Ez a mintázat – az ujjnyomat – 18 hetes korban alakul ki és a későbbiekben csak a kéz méretbeli változásait követi. Megjegyzendő, hogy az égés, vágás, kopás, marás, stb. során esetlegesen értékelhetetlenné vált mintázat legkésőbb 14-40 napon belül regenerálódik (kivéve, ha mély a sérülés, ekkor viszont egyedi heg képződik). Az ujjnyomat-típusok lehetnek: boltozat, hurok vagy örvény mintájúak, azonosításhoz a jellegzetes pontjait vizsgáljuk. Ilyen jellegzetes pontok: elágazás, végződés, kereszteződés, sziget, horog, híd, stb. Egy ujjnyomaton megközelítőleg 100 jellegzetes pont található. A legtöbb ország 12 (Magyarország 10) sajátossági pont egyezését egyértelmű személyazonosításnak tekint. 12 sajátossági pont és azok egymáshoz viszonyított helyzetének ismétlődése – Osterburg számításai szerint – $1:1{,}25*10^{20}$ valószínűségű.[6]

  Ujjnyomat-azonosításkor a berendezés vizsgálja, hogy az ujj élő-e, ez legegyszerűbben az ujjbegy hőmérsékletének és/vagy felületi nedvességének mérésével végezhető.[24]

  Az ujjnyomat-azonosítók képrögzítőinek főbb típusai és működésük röviden:

  - Optikai: az ujjat egy LED világítja meg, a képződött kép egy prizmán és egy lencserendszeren jut a CMOS vagy CCD érzékelőhöz.
  - Kapacitív: a fodorszálak és a bőrredők közti eltérő kapacitást detektálja.
  - Nyomásérzékelős: a szenzor alatt piezo-elektromos nyomásérzékelő mátrix található, ami detektálja a fodorszálakat.
  - Hőérzékelős: a redők és a völgyek közti hőmérséklet-különbségek mérésén alapszik.
  - Ultrahangos: ultrahangot sugároz az ujjra, a visszaverődő hullámokból alkotja a képet.

5. ábra. A Suprema BioEntry Plus ujjnyomat-azonosító (és RFID olvasó) használata laborkörülmények közt.

Megjegyzés: hangsúlyozni kívánjuk, hogy az ujjnyomat-azonosítók általában nem daktiloszkópok, belőlük az eredeti ujjnyomat nem visszaállítható és a megbízhatóságuk sem azonos.

- *Írisz-azonosítás:* John G. Doughman 400 különböző azonosítási pontot mutatott ki a szem szivárványhártyáján és az Ő nevéhez fűződik az az (írisz egyedi mintázatát leíró és kódoló) algoritmus, amely minden írisz-azonosító működésének alapja. „A vizsgálat a szivárványhártya látható (pl. rajzolat), valamint láthatatlan (pl. infravörös) tulajdonságain alapul. Az elsődleges látható paraméter a trabekuláris hálózat, amely az írisz sugaras mintázatát adja. Ez a rajzolat az embrionális fejlődés 8. hónapjában alakul ki és többet nem változik az ember élete során. További jellegzetességek a körök, az árkok, vagy a korona. Az infravörös leolvasás révén a retinahártya láthatatlan erezetéről készíthető felvétel.”[24]

  Írisz-azonosításkor a berendezés vizsgálja, hogy a szem élő-e, ez legegyszerűbben a pupillareflex vizsgálatával és/vagy a szem hőmérsékletének mérésével végezhető.

4. A SZEMÉLYAZONOSÍTÓ ELJÁRÁSOK ÖSSZEHASONLÍTÁSA

Az összehasonlító táblázatban (1. sz. táblázat) szereplő típuspéldák a tanulmányaimból ismertek közül kerültek kiválasztásra. Természetesen más gyártók termékei jobb tulajdonságokkal rendelkezhetnek. Pl.: GK Technology 6161T Fingerprint System FAR$\leq 10^6$:1.[28]

Azonosítási módszer	*Összehasonlítási szempont*		**Kombinációk száma**	**FAR**	**Hamisíthatóság, ellophatóság**	**Olvasási távolság**	**Hátrány**
INFORMÁCIÓ	**4**	**digites numerikus**	10^4	felhasználók száma/kombinációk száma	"leleshető"	-	leleshető, elfelejthető, átadható
	6		10^6				
	8		10^8				
	5 karakteres alfanumerikus		$\sim 6*10^7$				
TÁRGY	**RFID**		10^{12}	felhasználók száma/kombinációk száma	magas biztonságú kódolt kártyák esetén minimális a kiolvasás esélye	típusonként változó	ellopható (maga a tárgy), átadható
BIOMETRIA	**ujjnyomat (Suprema BioEntry+)**		Az egyezés valószínűsége $1:1{,}25*10^{20}$.	10^6:1 (10^5:1)	A védelmi funkciók miatt gyakorlatilag lehetetlen (élő-élettelen szövet megkülönböztetése).	-	Az emberek ~3%-ának nincs értékelhető ujjnyomata.
	írisz (Panasonic BM-ET330)		Az egyezés valószínűsége $1:10^{78}$, a Föld népessége $\sim 10^{10}$.	10^7:1 ($1{,}2*10^6$:1)		30-40 cm	széles körben nem elfogadott, relatíve lassú (1,5-10 s egy azonosítás)

1. táblázat. A személyazonosító eljárások összehasonlítása.

ÖSSZEFOGLALÁS

A személyazonosító eljárások összehasonlításából megtudhattuk, hogy kizárólag a biometrián alapuló módszerek azonosítják egyértelműen a személyt, a másik két módszer a személy által ismert információt vagy az általa birtokolt tárgyat azonosítja. Ezek átadhatóak, elfelejthetők/elveszthetők, leleshetők/ellophatóak, stb. E hátrányukkal szemben áll az alacsony ár, a kiforrott, elfogadott és elterjedt technológia mellett megannyi más jellemző, melyek megléte nem feltétlenül egyértelmű a biometrikus azonosítóknál.

A jövő beléptető rendszereitől elvárható a magas fokú épületfelügyeleti, tűz-és vagyonvédelmi integráltság az alrendszerek autonómiájának megőrzése mellett (riasztórendszer, kamerarendszer, beléptető rendszer, épületfelügyeleti rendszer, tűzjelző rendszer); gyors, könnyű kezelhetőség és áttekinthetőség nagyméretű saját kijelzőn és/vagy számítógépen (térképes megjelenítés, ikonos kezelés, stb.); többféle kommunikációs csatorna; magas fokú testreszabhatóság; bővíthetőség különféle gyártmányú termékekkel. A fentieken túl előtérbe kell, hogy kerüljön a felhasználói elfogadottság és használhatóság, a vonatkozó jogszabályok betartása mellett.

Felhasznált irodalom

[1] Dr. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései c. PhD értekezés, 2.3. Beléptető rendszerek p.22-26., 5.2. Behatolás-jelző és beléptető rendszerek integrációja p.98., 2009.

[2] Cserép Attila – Jelics Miklós – Herwerth Miklós – Ercse Sándor – Kákonyi Gyula –Kaló József – Kerekes János – Regős Viktor – Gonda Béla – Szilágyi Szilárd – Csengeri Péter – Breyer Gábor – Cseh András: Vagyonvédelmi Nagykönyv, második kiadás, CEDIT Kft, Budapest, 1997.

[3] Dr. Guttengeber Ádám – Dr. Szili László – Cserhalmi Ferencné – Dr. Szűcs György – Móró Lajos- Dunai Kovács Béla: Személy-és vagyonőrök, biztonságtechnikai szakemberek tankönyve, PRO-SEC Kft, Budapest, 1997.

[4] Allaga Gyula- Avar Gábor – Melis Zoltán – Dr. Nádor György – Rónai Tibor – Sárkány Márta: Kártyás rendszerek, PRÍM kiadó.

[5] Filkorn József: Beléptető rendszerek c. előadás, 2009.

[6] Wikipédia, a szabad enciklopédia, 2011.01.03.

Azonosítás
http://hu.wikipedia.org/wiki/Azonosítás_(kriminalisztika)

RFID
http://en.wikipedia.org/wiki/Radio-frequency_identification

VeriChip
http://en.wikipedia.org/wiki/VeriChip

FDA
http://en.wikipedia.org/wiki/Food_and_Drug_Administration

Francis Galton

http://hu.wikipedia.org/wiki/Francis_Galton

Daktiloszkópia
http://hu.wikipedia.org/wiki/Daktiloszkópia

Írisz-azonosítás
http://en.wikipedia.org/wiki/Iris_recognition

[7] Filkorn József: Beléptető rendszerek c. előadás, 2011.

[8] MSZ-EN 50133-1:2006 Riasztórendszerek. Beléptető rendszerek biztonságtechnikai alkalmazásokhoz, 1. rész: Rendszerkövetelmények

[9] MSZ-EN 50131-1:2006 Riasztórendszerek. Behatolásjelző rendszerek, 1. rész: Általános követelmények

[10] Renke Bienert: RFID Chips Greet the Future, Elektor Electronics, September 2006, p.14-18.

[11] Filkorn József: HYPERX előadás, 2002.

[12] Filkorn József: Beléptető rendszerek tervezése előadás, 2009.

[13] Filkorn József: Beléptető rendszerek karbantartása, SZVMSZK konferencia, 2007.

[14] Pálffy Zoltán: RFID és biztonság – 2010, Detektor Plusz 2010/5-6, p.45.

[15] Amdrew S. Tanenbaum: Számítógép hálózatok, 8. fejezet Hálózati biztonság, Panem Kiadó, 2003.

[16] RFID Viruses and Worms, 2011.01.05.
Melanie R. Rieback – Patrick N. D. Simpson – Bruno Cripso – Andrew S. Tanenbaum: Is Your Cat Infected with a Computer Virus?, Vrije Universiteit Amsterdam, Department of Computer Science
http://www.rfidvirus.org/papers/percom.06.pdf

[17] RFID Journal
http://www.rfidjournal.com/

[18] SecurityOrigo - Központban a biztonság
www.securityorigo.eu

[19] Seawing biztonsági beléptető rendszerek, 2010. 12. 10.
http://www.seawing.hu/belepteto_rendszer

[20] Pricz László: Beléptető rendszerek fejlődése a kezdetektől napjainkig, alkalmazási lehetőségeik bemutatása c. szakdolgozat, Gábor Dénes Főiskola, 2006.

[21] How Stuff Works: How RFID Works, 2011.01.03.
http://electronics.howstuffworks.com/search.php?terms=rfid

RFID Criticism, 2011.01.03.
http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid7.htm

[22] National Science and Technology Council: The National Biometrics Challenge, USA, 2006.
http://www.biometrics.gov/nstc/pubs/biochallengedoc.pdf

[23] Hitachi VeinID Technology, 2011.01.08.
http://www.hitachi.com.sg/veinid/solutions/

[24] Dr. Kovács Tibor: Biometrikus azonosító eszközök jegyzet, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2010.

[25] Suprema BioEntry Plus ujjnyomat azonosító, 2011.01.06.
http://www.supremainc.com/eng/product/fs_31.php?mark=13

[26] Suprema BioEntry Operation Manual v. 2.0, 2006.

[27] Panasonic BM-ET330 írisz azonosító, 2011.01.06.
ftp://ftp.panasonic.com/pub/Panasonic/cctv/SpecSheets/BM-ET330.pdf

[28] GK Technology, 2011.01.08.
http://gktechnology.in/pdf/eBroucher.pdf

Képek jegyzéke