

Beléptető rendszerek biometrikus támogatással

Dr.Fialka György PhD.

c.egyetemi docens

SZVMSZK elnöke

A beléptető rendszerek szerepe

- A védett területek megbízható, beléptetés szabályozásának eszköze.
- Kiválasztása, működtetése alapjai
- A szeparálást meghatározó szabályozás szerepe
- A közel és távoli hozzáférés kérdései
- A megbízható azonosítás meghatározó elemei
- Létszám, idő, tárolás, adatvédelem
- A működtetés buktatói (fizikai korlátok, tárolási, környezeti, megbízhatósági, stb.)

A beléptetési azonosítás lehetőségei

- Személyes felügyelettel
- Beléptetési kódok alkalmazása
- Azonosító kártyák (Speciálistól a mágnesesig)
- Aktív elemek alkalmazása
- Biometrikus érzékelők alkalmazásával

A biometriai azonosítási módszerek alapfeltételei

- Az ember magában hordja a teljesen egyedi, nem hamisítható Kódját ami tetszőleges hosszúságú karakterrel igény szerinti azonosítást tesz lehetővé
- egyedi (csak arra a személyre jellemző),
- állandó (pl. a korral nem változik),
- mérhető (adattá konvertálható),
- gyors (néhány másodperc alatt eredményt szolgáltat),
- elfogadott (higiénikus felvételi-ellenőrzési eljárás),
- megbízható (kevésbé sérülékeny, csekély számú támadási ponttal rendelkezik).

A biometria által nyújtott azonosítási lehetőségek

- **Egyedi azonosításra alkalmas adatok**

aláírás,

arckép,

ujjlenyomat, ujjnyomat, ujjnyom,

talplenyomat,

hangtónus,

DNS genotípus,

fehérvérsejt antigén,

kézgeometria,

kézerezet, ujjerezet (érhálózat),

arc (2D, 3D),

kéz, csukló,

szem retinájának vagy íriszének mintázata, stb.

Az alkalmazás általános feltételei

- Az alkalmazott módszer környezet tűrése
- Az ellenőrzés időtartama
- Az azonosítás megbízhatósága
- Az ellenőrzési módszer törvényessége
- Az alkalmazott eszközök ára
- Egészségügyi megfelelés

A biometriai érzékelők alkalmazása

- A mérési folyamat mechanizmusa a következő:
 - A szenzor, detektor rögzíti a szükséges biometriai mintát az adott személytől.
 - A teljes mintából a program kiemeli a jellegzetes (azonosításra alkalmas) jegyeket.
 - Az algoritmus ezt az adatbázisban található mintaelemekkel összeveti és kiértékeli.
 - Ez alapján azonosítási választ generál (egyeznek - nem egyeznek, „Go - No go” típusú azonosítás).

Gyakorlati megoldások tenyér és ujjérhálózati scannerek



Gyakorlati megoldások Irisz azonosítás



Ujjnyomat scannerek



Gyakorlati alkalmazás egy ATM-nél



A biometrikus azonosítók kiválasztási szempontjai

- **Általánosság, univerzalitás:** a felhasználói csoport minden egyes tagja rendelkezik-e a mért jellemzővel.
- **Egyediség:** előfordulhat-e az az eset (milyen gyakran), hogy több felhasználó is ugyanazzal a jellemzővel rendelkezik.
- **Maradandóság:** változik-e idővel az adott paraméter.
- **Eltulajdoníthatóság:** mennyire másolható, eltulajdonítható az adott biológiai, biometriai jellemző (külső vagy belső paramétereket mérünk-e).
- **Teljesítmény:** a biometrikus adat beolvasása után milyen gyorsan képes a módszer a válaszadásra.
- **Elfogadottság:** a felhasználó részéről mennyire elfogadható módszer (szükséges-e közvetlen kontakt az eszközzel az adatfelvételhez).
- **Megtéveszthetőség:** mennyire megtéveszthető az adott biometrikus módszer (idegen, hamis minták bevitele egy adott rendszerbe).

A biometria adatvédelmi kérdései személyes adatokra vonatkozóan

- A rögzített adatok további felhasználása
- A rögzítés módja, tárolási kérdései
- Az eredeti adat/személy reprodukálhatósága /HASH kódolás/
- A távol azonosítás adatforgalmi megoldásai
- Kombinált lehetőségek

**Köszönöm a megtisztelő
figyelmüket!**