

Biometrija v Time&Space

Biometrija postaja glavna tehnologija za identifikacijo, avtentikacijo, avtorizacijo in kontrolo pristopa, saj odpravlja pomembne omejitve klasičnih metod, kot so na primer ključi in gesla. Omejitve lahko najbolj povzamemo, če osvetlimo naslednje tri primere.

Težave s ključi

Pod imenom »ključ« razumemo moderne verzije ključev, kot so RFID značke, pametne ID kartice, USB ključi in podobni fizični žetoni. Ne glede na to, kako napreden je ključ, ga vedno spremlja ena pomanjkljivost: ker gre za predmet, ga lahko izgubimo ali nam ga ukradejo. Hramba ključa zahteva posebno skrb. Ključ lahko tudi posodimo in ne razkriva uporabnikove identitete, zato ni zaupanja vreden način identifikacije.

Težave z gesli

Stoletja dolgo so ljudje zaradi težav s ključi raje uporabljali gesla. Z geslom elegantno rešimo problem izgube ali kraje, a tudi geslo ni brez napak. Ker gre za podatek, ga lahko pozabimo ali komu razkrijemo. Če gesla ne varujemo kot skrivnost, nam nič ne koristi. Grozijo mu različne nevarnosti, kot so prisluškovanje, prevare, grožnje, izsiljevanje ali celo preprosto ugibanje.



Težave s ključi in gesli

Varnost lahko zagotovo izboljšamo s kombinacijo ključa in gesla. Najbolj poznan primer so kartice ATM (kreditne kartice s PIN kodo). A kot lahko vidimo iz nešteti zlorab kreditnih kartic, je tudi takšna kombinacija varnostnih mehanizmov pogosto ogrožena. Žal niti ključi niti gesla niti kombinacija obojega ne morejo zagotoviti ustrezne stopnje varnosti in udobja.

Biometrična identifikacija temelji na prepoznavi značilnosti, ki so lastne vsakemu posamezniku. S tem odstira popolnoma novo raven zanesljivosti in učinkovitosti. Dve glavni prednosti biometrije sta neposredno povezani s šibkimi točkami ključev in gesel: prednost udobja in prednost varnosti.

Prednost udobja

Biometrična identifikacija odpravlja potrebo po ključih (ali karticah) in pomnjenju gesel.



Prednost varnosti

Biometrična identifikacija odpravlja tveganje za nepooblaščen dostop z izposojenimi, pozabljenimi ali ukradenimi ključi (ali karticami) in zlorabljenimi gesli.

Na splošno velja, da biometrijo povezujemo z visoko stopnjo varnosti. Praktične prednosti lažje uporabe pa še vedno pogosto spregledamo. Prednost uporabe prstnega odtisa za kontrolo pristopa je precej očitna. Poleg tega, da zagotavlja višjo stopnjo varnosti, tudi odpravlja potrebo po karticah in geslih.

Registracija s prstnim odtisom ni le bolj prijazna od registracije s kartico, temveč tudi preprečuje, da bi »štemplali« sodelavce, kot se je pogosto dogajalo pri klasičnih registracijskih terminalih.

Biometrična identifikacija je še vedno precej nova in hitro razvijajoča se tehnologija, zato se še spopada z nekaterimi izzivi. Pogosto se zgodi, da nova rešitev pride na trg, preden je res pripravljena za uporabo. Včasih je problematično tudi, da od biometrične identifikacije pričakujemo 100 % zanesljivost. To seveda ni možno; vedno obstaja možnost napak, četudi zelo majhna.

V nekaterih kulturah je lahko uporaba biometrične identifikacije problematična. V osrednjem delu Evrope so ljudje na primer zelo zadržani glede identifikacije s prstnim odtisom. Verjetno v njej vidijo povezavo z nekdanjimi totalitarnimi sistemi. Čeprav se zdijo takšni pomisleki povsem iracionalni, jih moramo upoštevati. EU zagovarja »previdno« in »nadzorovano« uporabo biometrije. **Zakonodaja v EU se med državami precej razlikuje – od zelo liberalnih (na primer Združeno kraljestvo) do zelo omejenih (na primer Slovenija).**

Pretirano omejevanje biometrične identifikacije je zagotovo izziv. V Sloveniji uporaba biometrije za registracijo delovnega časa ni dovoljena. To se nanaša na vse vrste biometričnih podatkov (prepoznavna obraza, prstni odtis, prepoznavna žilnega sistema itd.) in vse načine uporabe, vključno z uporabo predloge na kartici, ki je splošno poznana kot metoda, ki najbolj ščiti zasebnost. V Sloveniji uporabo »biometričnih ukrepov« odobri Informacijski pooblaščenec, kadar je to dokazano nujno za doseganje varnosti.



Špicin Time&Space

Sistem Time&Space že več kot dve desetletji podpira biometrično tehnologijo. V tem času je Špica postala glavni dobavitelj biometričnih rešitev v regiji in ima nameščeno največjo bazo. Naše sisteme za identifikacijo preko prstnega odtisa uporablja že več kot 100.000 uporabnikov.

Špica uporablja biometrične čitalnike vodilnih svetovnih proizvajalcev biometričnih rešitev. V partnerstvu s podjetjem Morpho (www.morpho.com) omogočamo integracijo z njihovim sistemom za branje prstnih odtisov in 3D prepoznavo obraza. Specializirane in vladne biometrične rešitve implementiramo tudi v sodelovanju z drugimi proizvajalci.



Identifikacija ali verifikacija

Biometrični čitalniki običajno preverjajo ujemanje dejanskega biometričnega vzorca osebe, ki se želi registrirati, s shranjenimi vzorci (t. i. predlogami) vseh kandidatov, ki uporabljajo biometrijo. Ta metoda se imenuje čista identifikacija oz. »ujemanje ena-proti-mnogo«.

Z zmanjševanjem števila kandidatov do enega samega se bistveno zviša hitrost in izboljša natančnost identifikacije. V tem primeru govorimo o verifikaciji oz. »ujemanju ena-proti-ena«.

Metodo ujemanja ena-proti-ena je veliko lažje vpeljati, poleg tega niso vsi biometrični čitalniki dovolj natančni za identifikacijo ena-proti-mnogo. Zlasti to velja pri velikem številu kandidatov. V okoljih z nekaj sto ali nekaj tisoč kandidati je izbira ustreznih čitalnikov lahko zelo omejena.

Time&Space nudi podporo tako za identifikacijo (ena-proti-mnogo) kot verifikacijo (ena-proti-ena). Vendar veljajo nekatere omejitve zaradi razlik med napravami in proizvajalci.

Prstni odtis

Identifikacija ali verifikacija s prstnim odtisom je klasična biometrična tehnologija in zaradi zrelosti rešitve ter cenovno dostopnih čitalnikov tudi najpogosteje uporabljena.

Špicine rešitve za kontrolo pristopa vključujejo zunanje čitalnike prstnih odtisov, bodisi samostojne ali povezane v mrežo dostopnih terminalov. Beleženje delovnega časa se izvaja s čitalniki, ki imajo vgrajen bralnik prstnih odtisov.



Prepoznavna šarenice

Identifikacija s prepoznavo šarenice se je zaradi visoke natančnosti in tudi visoke cene običajno uporabljala v okoljih z zelo visokimi varnostnimi standardi, na primer za dostop do trezorjev, arhivov z občutljivimi informacijami, vojaških objektov ipd.

Ker cene te tehnologije padajo, se identifikacija s prepoznavo šarenice širi v območja z nižjimi varnostnimi standardi in na področje registracije delovnega časa.

Prepoznavna šarenice je še vedno ena najbolj natančnih identifikacijskih metod, zato lahko upravičeno pričakujemo, da se bo njena prisotnost še bolj utrdila predvsem na področjih, kjer ima zanesljivost prednost pred stroški ali udobjem.



Prepoznavna obraza

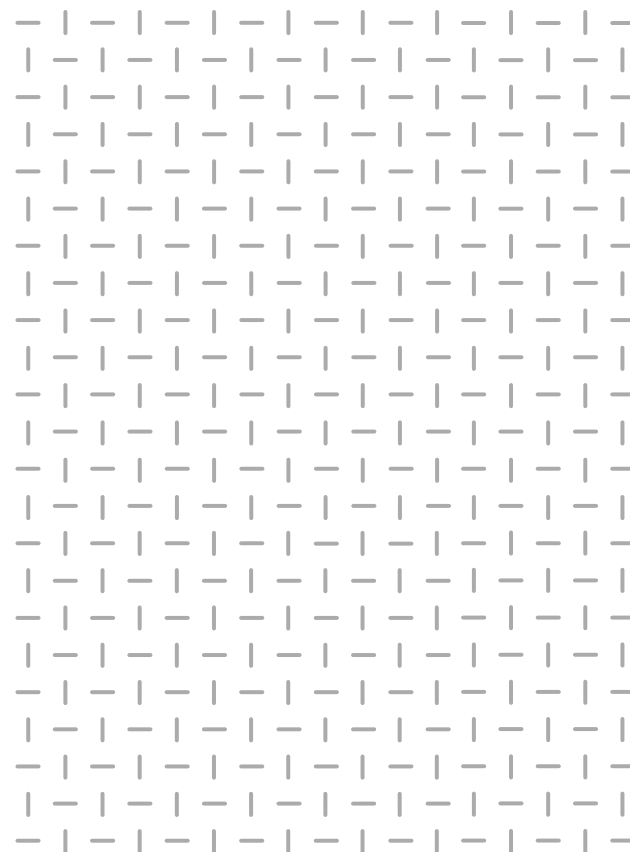
Obstaja več različnih načinov in oblik prepoznave obraza. Vendar do nedavnega tehnologija prepoznave obraza še ni bila dovolj dovršena, da bi jo lahko uporabljali za kontrolo pristopa ali beleženje delovnega časa.

Spremembo na tem področju je prinesel razvoj 3D prepoznave obraza, pravi prodor pa je ta tehnologija doživela, ko smo za preverjanje ujemanja presegli uporabo fotografij in 2D vzorcev. 3D prepoznavna obraza vključuje različne napredne tehnologije, kot so stereoskopske slike, površinsko oblikovanje, uporaba infrardečega valovanja in laserja.

Rezultat je uspešna odprava največjih ovir, s katerimi smo se soočali pri 2D čitalnikih:

- manjša občutljivost na naklon kamere, obraza ni treba postaviti popolnoma natančno,
- manjša občutljivost glede pričeske in brade, oblačil (šal, kapa) ali celo očal,
- manjša odvisnost od svetlobe, lahko se jih uporablja celo v popolni temi,
- veliko težje je goljufati, saj so veliko bolj natančni in napredni.

Vision Access proizvajalca Morpho odlikujeta hitrost in zanesljivost delovanja, kar je bilo dokazano tudi v praksi. Najpogosteje se uporablja v okoljih, kjer je nujna zanesljiva in diskretna kontrola pristopa, na primer v bankah, zavarovalnicah, poslovnih stavbah in na letališčih. Običajno se uporablja v kombinaciji z avtomatskimi vrati ali vrtljivimi križi, ki zagotavljajo nemoten pretok ljudi in enostaven pregled nad dogajanjem.



Upravljanje predlog

Biometrična identifikacija temelji na primerjavi dejanskega vzorca osebe, ki se želi registrirati, in shranjenimi vzorci, imenovanimi biometrične »predloge«. Predloge moramo zbrati, preden začnemo z uporabo sistema, zato vsak biometrični sistem potrebuje sistem za upravljanje predlog.

V večjih sistemih z veliko čitalniki in uporabniki je upravljanje predlog lahko zajeten, a pogosto tudi podcenjen izziv.

Upravljanja predlog se lahko lotimo na dva načina z dvema različnima strategijama shranjevanja predlog. Prvi temelji na centraliziranem upravljanju predlog, shranjenih v pomnilniku podatkovne baze.

Druga rešitev se imenuje »template-on-card« (TOC) – predloga na kartici. Deluje v obratni smeri kot prva metoda in za shranjevanje predlog uporablja pametne ID kartice. Predloge so shranjene na kartici, ki jo hrani uporabnik, in ne krožijo med drugimi uporabniki, zato je ta metoda bolj primerna za okolja, kjer je varnost pereč problem.

Metoda TOC ne deluje brez kartic, zato je za sisteme, kjer se uporabljajo le biometrični čitalniki, edina možnost uporaba centraliziranega upravljanja.

Tako metoda TOC kot centralizirano upravljanje imata svoje prednosti in slabosti, zato je pri izbiri prave rešitve treba upoštevati veliko različnih faktorjev.

Time&Space podpira oba načina upravljanja predlog. V enem sistemu lahko celo uporabljate kombinacijo obeh metod.



spica

TIME  SPACE