Pretnje biometrijskim sistemima i pretnje od njih

BRANKICA POPOVIĆ, DRAGAN RANĐELOVIĆ
Kriminalističko policijska akademija,
Beograd, Srbija

Stručni rad
UDC:621.398:654.94:615.478.6=861

Postoji veliki interes za korišćenje biometrike u širokom spektru aplikacija za identifikaciju zbog toga što oni imaju niz prednosti u odnosu na druge sisteme za proveru autentičnosti. Međutim sa aspekta sigurnosti nužno je ukazati na mogućnosti biometrijskih sistema i odrediti stepen njihove ugroženosti od različitih vrsta napada. Takođe je potrebno razmotriti moguće pretnje i neželjene posledice upotrebe biometrijskih sistema uz poseban naglasak na problem ugrožavanja privatnosti pri neodgovarajućem korišćenju ovih sistema.

Ključne reči: *biometrika, identifikacija, automatizovani sistemi, pretnje*

1. UVOD

U sadašnjoj, informatičkoj, epohi razvoja ljudskog društva autentifikacija ličnosti je nužno potreban proces jer postojanje Inerneta kao globalne računarske mreže koja se svakim danom sve više širi kao i sve šira automatizacija raznih poslova i usluga zahteva pouzdane metode za utvrđivanje i proveru identiteta. Tako se prosečan stanovnik naše planete dnevno identifikuje više od desetak puta prilikom korišćenja računara, kreditnih i platnih kartica kao i raznih drugih automatskih terminala zbog korišćenja različitih usluga, prilikom raznih bezbedonosnih kontrola kretanja i dr.[1].

U eri masovnog korišćenja računara taj proces identifikacije izgleda jednostavan ali nije tako lak kao što se čini. Identifikacija ličnosti treba da bude brza, pouzdana, jeftina, i u velikom broju slučajeva društveno prihvatljiva što je sve zajedno jako teško ispuniti.

U oblasti sigurnosti poznata su 3 različita načina za proveru autentičnosti:

- Nešto što znaš (*knowledge*) – šifra, lični identifikacioni broj(PIN), neka lična informacija koja se lako pamti (npr. mesto rođenja i sl.);
- Nešto što imaš (*possesion*) – razne vrste kartica (npr. "pametne" i sl.);
- Nešto što jesi– *biometrika* (neka fiziološka ili karakteristika ponašanja, poznate i pod imenom biometrijski potpis ili ključ).

Adresa autora: Kriminalističko policijska akademija, Beograd – Zemun, Cara Dušana 196

Rad primljen: 02. 02. 2009.

Primeri biometrijskih karakteristika koje se danas ispituju ili koriste su: otisci prstiju, geometrija šake, izged lica, oko, glas, potpis, DNK, itd [2,3,4].

Biometrika je oblast prepuna kontroverzi jer može da pozitivno identifikuje osobu i time spreči čitav niz prevara vezanih za identitet, ali ona može i da, bez dozvole subjekta, prati postupke osobe i poveže lične informacije iz različitih izvora, što je napad na privatnost. Njeno korišćenje je potencijalno moćno sredstvo u rukama jakih korporacija pa i vlada pojedinih država, kao i njihovih različitih agencija, da kontrolišu pojedince a time i društvo u celini. Sve napred navedeno ukazuje na potrebu proučavanja kako mogućih pretnji za njihov siguran rad tako i pretnje koje biometrijski sistemi mogu svojim delovanjem i samim svojim postojanjem da čine ljudima.

U ovom radu ćemo se prvo upoznati sa osnovama biometrijskih sistema sa posebnim osvrtom na njihovu tačnost. Zatim ćemo prikazati moguće tačke napada na biometrijske sisteme i pretnje karakteristične samo za ove sisteme, ali i dati koji su odgovori na njih. U posebnom odeljku su pobrojane moguće pretnje ljudima od strane biometrijskih sistema a posebno je objašnjen uticaj na privatnost ljudi kao bitna pretpostavka za širu upotrebu biometrijskih sistema.

2. BIOMETRIJSKI SISTEMI

2.1 Osobine

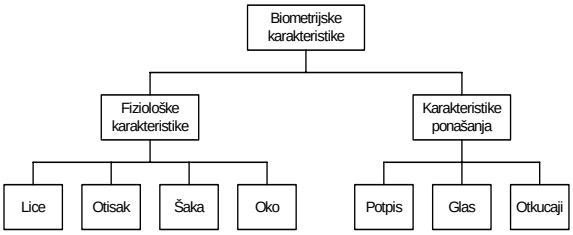
Termin biometrika potiče od grčkih reči *bios* i *metrikos* (*bios*-„život" i *metrikos*-„mera") i odnosi se na jedinstvene biološke karakteristike (fizičke, fiziološke ili karakteristike ponašanja) pojedinca. One se mogu koristiti za proveru autentičnosti i utvrđivanje

identiteta, a pogodne su za primenu u automatizovanim sistemima [1].

Da bi se biološke mere mogle klasifikovati kao biometrijske moraju zadovoljiti uslove:

1. *Univerzalnost* – svaka osoba mora imati ovu karakteristiku;
2. *Jedinstvenost* – karakteristika je različita za svakog člana populacije;
3. *Nepromenljivost* – karakteristika ne sme da se menja tokom vremena i pri različitim uslovima prikupljanja;
4. *Kolektibilnost* – karakteristika mora biti prikupljiva i kvantitativno merljiva [4].

Primeri biometrijskih karakteristika koje se danas koriste u automatskim sistemima (lice, šaka, oko, otisak prsta, potpis, glas, obrazac kucanja) prikazani su na slici 1.



Slika 1 - Podela biometrijskih sistema po poreklu karakteristika

Naravno pri odabiru biometrijskog sistema koji se koristi za utvrđivanje identiteta mora se voditi računa i o sledećim faktorima:

- *pouzdanost* – odnosi se na tačnost, brzinu, kao i na faktore koji mogu uticati na rad sistema;
- *prihvatljivost*– označava stepen spremnosti ljudi da prihvate korišćenje ovog sistema u svakodnevnom radu;
- *otpornost* – koliko je sistem otporan na potencijalno krivotvorenje i napade.

tako da različiti biometrijski sistemi u različitoj meri ispunjavaju gore pobrojane uslove.

U tabeli 1. data je percepcija ispunjavanja gore pobrojanih uslova kod različitih biometrijskih sistema pri čemu su V, S i N oznake za visoko, srednje i nisko ispunjavanje pojedinačnog faktora (uslova) respektivno.

A. ***Verifikacija*** – vrši se kada neka osoba tvrdi da ima neki identitet (u tradicionalnim sistemima to se radi sa lozinkom, ID karticom i sl.); sistem potvrđuje ili odbija identitet upoređivanjem prezentovane biometrijske karakteristike sa šablonom (*template*) prethodno sačuvanim u bazi i izvodi se poređenje jedan–prema–jedan (one–to–one comparasion). Ovo je takozvano '***pozitivno prepoznavanje***' čiji je cilj da se spreči da više ljudi koristi isti identitet.

B. ***Identifikacija*** – sistem mora da izvrši prepoznavanje osobe tako što će uporediti njene biometrijske karakteristike sa svim šablonima sačuvanim u bazi da bi našao najveće poklapanje. Tom prilikom se izvodi jedan–prema–mnogo (one–to–many) poređenja i ovo se naziva '***negativno prepoznavanje***' gde sistem može utvrditi da li je osoba ono što implicitno tvrdi da nija. Cilj je da se spreči da jedna osoba koristi više identiteta.

Tabela 1 - Pregled biometrijskih tehnologija sa merom ispunjavajna pojedinih faktora

Biometrika	univerzalnost	Jedinstvenost	nepromenljivost	kolektibilnost	Pozdanost	prihvatljivost	otpornost
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	S
Geometrija šake	S	S	S	V	S	S	S
Iris	V	V	V	S	V	N	V
Retina	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N

Biometrijski sistem generalno posmatrano ima dva režima rada:

C. ***Verifikacija*** – vrši se kada neka osoba tvrdi da ima neki identitet (u tradicionalnim sistemima to se radi sa lozinkom, ID karticom i sl.); sistem potvrđuje ili odbija identitet upoređivanjem prezentovane biometrijske karakteristike sa šablonom (*template*) prethodno sačuvanim u bazi i izvodi se poređenje jedan–prema–jedan (one–to–one comparasion). Ovo je takozvano '***pozitivno prepoznavanje***' čiji je cilj da se spreči da više ljudi koristi isti identitet.

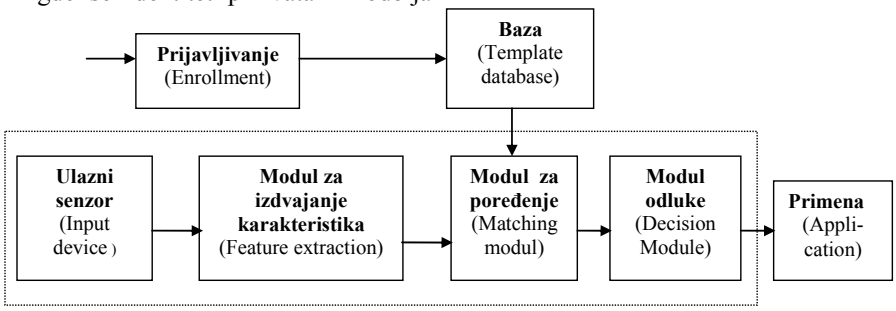
D. ***Identifikacija*** – sistem mora da izvrši prepoznavanje osobe tako što će uporediti njene biometrijske karakteristike sa svim šablonima sačuvanim u bazi da bi našao najveće poklapanje. Tom prilikom se izvodi jedan–prema–mnogo (one–to–many) poređenja i ovo se naziva '***negativno prepoznavanje***' gde sistem može utvrditi da li je osoba ono što implicitno tvrdi da nija. Cilj je da se spreči da jedna osoba koristi više identiteta.

Potrebno je naglasiti da se metode *possesion and knowledge* mogu koristiti samo za verifikaciju, dok se za identifikaciju tj.negativno prepoznavanje jedino može koristiti biometrika.

Svaki biometrijski sistem ima četri modula kako je to dato na slici 2 [5]:

1. *ulazni uređaj-senzor* (sensor module) – koji uzima i digitalizuje biometrijsku karakteristiku (npr. skener za otiske prstiju, digitalna kamera za lice, itd.);
2. *modul za izdvajanje karakteristika* (feature extraction module) – koji obrađuje digitalizovan podatak radi izdvajanja karakteristika koje ga čine jedinstvenim i koje se mogu smestiti u šablon (*template*) (npr. izdvajanje minucija iz slike otiska);
3. *modul za poređenje* (matching module) – gde se porede izdvojene karakteristike sa podacima iz šablona sačuvanog u bazi;
4. *modul za donošenje odluke* (decision-making module) – gde se identitet prihvata ili odbija (verifikacija), ili utvrđuje na osnovu skora poređenja (identifikacija).

Svakako da i peti modul tj. *baza* (template database) mora postojati u strukturi jednog biometrijskog sistema i to je mesto gde se čuvaju šabloni uzeti od osobe u postupku prijavljivanja (*registracija – enrollment*). Sama baza može biti centralna ili lokalna u odnosu na mesto gde se koristi ili može biti mobilna ako je na uređaju koji korisnik nosi sa sobom (smartcard i sl.) ali može biti i kombinacija bilo koje dve ili čak sve tri baze podataka. Takođe se ti podaci mogu čuvati tako da se mogu koristiti samo za tu aplikaciju i organizaciju, ili za više njih.



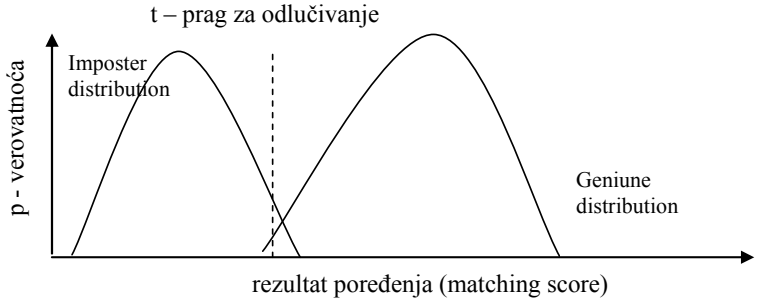
Slika 2 - Blok dijagram biometrijskog sistema

2.2 Tačnost biometrijskih sistema

Kao izlazni rezultat biometrijski sistemi daju stepen podudaranja (*matching score*) ulaznog podatka sa šablonom sačuvanim u bazi. Dva uzorka iste biometrike od iste osobe mogu da se razlikuju u zavisnosti od uslova i vremena njihovog uzimanja, pa se nemože očekivati njihovo apsolutno poklapanje. Sa većim stepenom podudaranja uzoraka sistem je sigurniji da dva biometrijska uzorka dolaze od iste osobe. Generalno, odluku sistema definiše neka granica (prag) koju korisnik postavlja u skladu sa konkretnom aplikacijom biometrijskog sistema.

Rezultati dobijeni od poređenja parova uzoraka različitih osoba, kao i oni dobijeni od poređenja uzoraka iste osobe daju nam raspodele koje se zovu '*impostor distribution*' i '*genuine distribution*', i prikazane su na slici 3.

Očigledno je da se u jednom delu te raspodele preklapaju. Prilikom projektovanja biometrijskog sistema granica (prag) odlučivanja se projektuje u skladu sa specifičnim zahtevima aplikacije [6].



Slika 3 - Uticaj praga na performanse (tačnost) biometrijskog sistema

Tačnost biometrijskih sistema može se odrediti preko dve specifične promenljive a to su:

- **FAR** (false accept rate) – lažno prihvatanje, gde se biometrijske karakteristike od dve različite osobe prihvataju kao da su iste
- **FRR** (false reject rate) - lažno odbijanje, gde se biometrijske karakteristike od iste osobe ne prihvataju tj. smatraju se uzorcima različitih osoba

Smanjivanjem jednog faktora (greške) povećavamo drugi. Kako uspostaviti najbolji odnos zavisi

od konkretne primene sistema i od toga gde ćemo postaviti prag za odlučivanje. Naime ako se želi maksimalna sigurnost da samo stvarno autorizovani korisnici prolaze kroz sistem, čak i po cenu da se ponekad i odbije autorizovani korisnik onda se smanjuje FAR po cenu povećanja FRR. Ovo je u slučajevima zaštite raznih sigurnosnih sistema. Sa druge strane za neke komercijalne aplikacije odbijanje autorizovanog korisnika može naneti velike štete, pa se tu smanjuje FRR na račun povećanja FAR (tabelu 2) [7].

Tabela 2 - Pregled biometrijskih tehnologija sa stanjem tačnosti

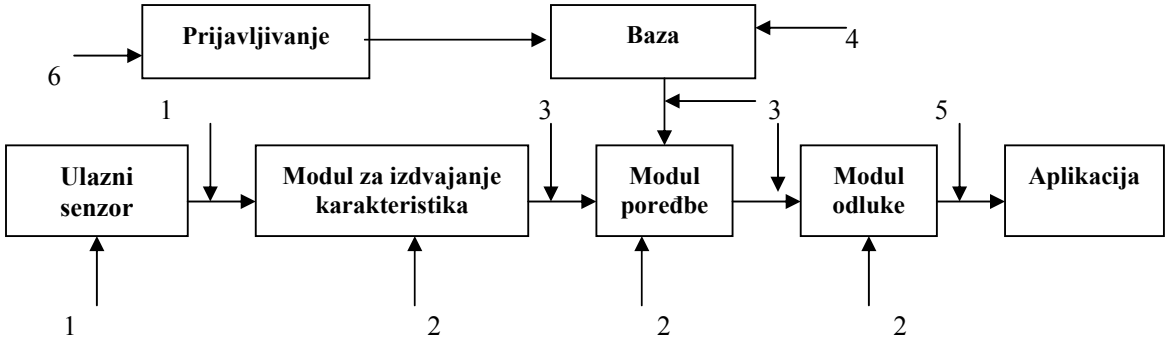
Biometrika	FAR	FRR	Komentar
Lice	1%	10%	Promenljivo osvetljenje, unutra/spolja
Otisak prsta	2%	2%	Rotacija i preterana distorzija kože
Geometrija šake	2%	0.1%	Sa prstenjem i neprikladnim postavljanjem
Iris	0.94%	0.99%	Unutrašnje okruženje
Retina	0.0001%	0.2%	Najbolji uslovi
Glas	2%	10%	Text independent, multilingual

3. PRETNJE BIOMETRIJSKOM SISTEMU

3.1 Vrste pretnji

Slabe tačke postoje u svakom sistemu, a na slici 4 prikazane su slabe tačke biometrijskih sistema [8]:

1. Prezentovanje lažne biometrike može biti dvojako:
   - Lažno predstavljanje tj. falsifikovanje podatka koji se stavlja pred senzor (*impersonation*);
   - predstavljanje prethodno ukradenog biometrijskog podatka čime se zaobilazi senzor (tzv. *replay* napad);
2. Trojanski konj pretnja je takođe dvojaka:
   - modul za izdvajanje karakteristika može biti tako napadnut da proizvede unapred definisan set karakteristika (u nekom trenutku i pod određenim uslovima) i njima zameni karakteristike ulaznog signala;
   - napad na moduo za poređenje je takav da se lažno proizvede visok ili nizak skor poređenja što direktno utiče na modul za donošenje odluka, kao i na sam moduo za donošenje odluka gde se postiže generisanje željene odluke;
3. Pretnja napadom na komunikacione kanale čiji je cilj da se presretnu karakteristike i to pre modula za poređenje, i odmah po izlasku iz tog modula radi promene istih;
4. Pretnja napadom na bazu gde se čuvaju šabloni uzeti u postupku registracije i to je pretnja neautorizovane modifikacije jednog ili više šablona, čime se može postići lažno predstavljanje ili uskraćivanje korisniku nekih mogućnosti;
5. Vrlo važna je pretnja gde se može promeniti odluka poslednjeg modula a u skladu sa kojom se ponaša aplikacija;
6. Često zanemarena pretnja sigurnosti, koja je i izuzetno važna, je pretnja prilikom postupka registracije. Svaki neautorizovani pristup ovom procesu može da prouzrokuje ozbiljne posledice po sigurnost. Naime registrovanjem lažnih korisnika mogu se pravom korisniku promeniti podaci, tako da je i nadgledanje procesa registracije od velikog značaja za sigurnost rada celog biometrijskog sistema.



Slika 4 - Vrste napada na određene tačke biometrijskog sistema

Ukoliko napadač ima vremena i mogućnosti (što je slučaj u udaljenim nenadgledanim aplikacijama) da generiše i pruži sistemu veći broj šablona u pitanju je klasičan napad silom (*brute-force-attack*) koji je karakterističan za sisteme zaštićene šiframa. U slučaju biometrijskog sistema ovakvi napadi su retki zbog teškog generisanja biometrijskih šablona. Koliko je sistem zaštićen od ovakvih napada direktno zavisi od

projektovanih grešaka FAR i FRR. Tako sistem projektovan sa FAR od 0,001% ima verovatnoću da bude prevaren u proseku 1 od 100000 pokušaja, što odgovara sigurnosti koja se ima sa šifrom od 5 znakova [4]. Neuporedivo je pri tom teže generisati 100000 biometrijskih šablona od klasične šifre od 5 znakova (u pogledu korištenih resursa i vremena).

3.2. Specifične pretnje

Pretnja koja je karakteristična samo za biometrijske sisteme je napad tzv. lažnom biometrikom (*fake biometrics*).

1) *Impersonation* napadi su slučaj kad se senzoru predstavlja lažna biometrika. Npr. lažni prst, falsifikuje se potpis ili se na licu ima maska. Najnezaštićenije na ovu vrstu napada su lice i glas, ali su u praksi poznati slučajevi gde je sistem prevaren lažnim otiskom, pa čak i okom.

2) *Replay* napadi su u stvari lažno prijavljivanje prethodno dobijenih (ukradenih) pravih biometrijskih karakteristika i dobijenih šablona, pri čemu se zaobilazi senzor.

Razvijaju se različiti metodi za sprečavanje ovakvih napada i to od kriptografije, zatim izazov-odgovor (*challenge/response*) sistem kojim se obezbeđuje prisustvo osobe u trenutku davanja biometrijskih podataka, pa do istovremenog korišćenja više biometrijskih karakteristika u multimodalnim biometrijskim sistemima.

Pravljena su istraživanja sa ciljem da se utvrdi koliko su postojeći biometrijski sistemi osetljivi na ovakav vid napada. Tako su prijavljeni u praksi provereni razni vidovi 'krađe identiteta' [9]:

- Lice – eksperimenti su pokazali da snimak lica (bez znanja subjekta koji je u pokretu) ako se stavi ispred kamere za prepoznavanje često ima za posledicu prihvatanje identiteta;
- Otisak – Matsumoto je sa grupom svojih saradnika dokazao da model otiska napravljen od silikona i želatina, a na osnovu pravog ili latentnog otiska skinutog recimo sa čaše, kod komercijalnih sistema za prepoznavanje preko otisaka u 80% slučajeva ima za posledicu prihvatanje identiteta. Takođe je pokazao da se relativno lako mogu prevariti i dodatni sistemi koji proveravaju 'živost' podatka [10];
- Iris – u Nemačkoj je takođe uspešno prevaren sistem za identifikaciju preko irisa tako što je korišćena odštampana slika ljudskog oka

U biometrijskim sistemima se javlja specifičan problem koji se ne pojavljuje u sistemima koji koriste *knowledge&possesion* metode. To je zamena kompromitovane biometrike. Krađa identiteta u slučaju biometrijskih sistema ima nesagledive posledice. Naime ako se desi da vam neko ukrade karticu ili lozinku, jednostavno ćete poništiti istu i dobiti drugu koja je različita. Ali ukoliko je iz bilo kog razloga biometrika kompromitovana onda je to zauvek. Naime čovek poseduje ograničen broj biometrijskih podataka (jedno lice, 10 prstiju, 2 oka...). Još ako je biometrijski podatak korišćen u više različitih aplikacija, to znači da su svi ti podaci dostupni onome ko je došao u posed biometrijske karakteristike.

Mora se naglasiti da krađa identiteta (ili zloupotreba biometrijskih podataka) ne mora biti delo pojedinca. Naime korporacije mogu koristiti biometrijske podatke radi uskraćivanja određenih prava bivšim radnicima, ili onima koji su već registrovani u policijskim biometrijskim bazama i sl. Vladine agencije mogu koristiti ove podatke radi uskraćivanja prava i sloboda licima za koje to smatraju potrebnim npr. traženim teroristima (čak i mimo zakonskih propisa).

4. PRETNJE BIOMETRIJSKIH SISTEMA

4.1 Vrste pretnji

Kao i kod upotrebe mnogih drugih zanimljivih i snažnih informacionih tehnologija, postoji zabrinutost od mogućih pretnji ljudima zloupotrebom biometrijskih sistema. Ta zabrinutost izazvana je činjenicom da je jednom u bazu skladišten otisak prsta ili druga biometrijska karakteristika postala izvor moguće kompromitacije za ceo život, jer kada je taj podatak zloupotrebljen korisnik ne može učiniti ništa jer ne može promeniti svoj otisak prstiju t.j. neku drugu svoju biometrijsku karakteristiku.

Neke važnije pretnje biometrijskih sistema ljudima su:

- Nezaštićenost informacija zbog standardizacije biometrijskih senzora

Razni senzori (razni proizvođači hardvera), generišu različite biometrijske rezultate i vIt is very difficult to create standard on identical encryption paths.eoma je teško stvoriti standard za tako različito kodirane izlazne rezlultate. Biometrijski standard se može dobiti samo ako ti izlazi budu neskriveni kako bi se uklonila na svakom pojedinačno biometrijskom senzoru od proizvođača ugrađena sopstvena zaštita tj. enkripcija. Te tako nezaštićene informacije predstavljaju ozbiljnu opasnost za privatnost prava.

- Marketing biometrijskih proizvoda

Uprkos potvrde sve većeg prisustva komercijalno dostupnih biometrijskih senzora, mnoge kompanije marketinški promovišu zamenjive biometrijske proiz-

vode (posebno na nivou potrošačkih proizvoda) radije nego što promovišu dodatke za lozinke, pri čemu propisi o oglašavanju i izradi biometrijskih proizvoda uglavnom ne postoje. Krajnji korisnici moraju se osloniti na objavljene test podatake i druga istraživanja koja pokazuju da ti proizvodi zadovoljavaju određene standarde performansi, a koje su verovatno najbolji rad pod optimalnim uslovima. Sa druge strane relativna otpornost te biometrike je mala i može da bude poražena kroz izmene i reverzni inženjering.

- Sociološka zabrinutost

Sve šira upotreba biometrijskih sistema u različitim privatnim firmama ali i javnim i državnim institucijama neminovno će povećati zabrinutost građana zbog npr.:

- upotrebe nehigijenskih biometrijskih senzora koji su tako potencijalno škodljivi po korisnike,
- brige za zloupotrebu ličnih informacija, npr. od strane vlade kako bi se utvrdile potencijalno loše osobine u ljudima zarad globalne kontrole populacije.

- Velika cena biometrijskog osiguranja

Kada lopovi ne mogu da dobiju pristup osiguranim svojstvima, oni loveći čekaju i napadaju na vlasnike pristupa. Ako je pristup osiguran sa biometrijskim sistemima, potencijalno je moguće da je cena osiguranja viša od osigurane imovine tj. Pristupnih svojstava.

4.2 Pretnja privatnosti

Privatnost tumačimo mogućnošću da živimo slobodni bilo kog uticaja, da ostanemo autonomni i da sami kontrolišemo pristup ličnim podacima [4]. Danas se biometrijski sistemi koriste u svim oblastima života, od finansijskih, medicinskih, poslova komunikacija pa do različitih poslova osiguranja, zaštite, vladinih agencija, kriminalistike i forenzike.

Mnogi su razlozi otpora pojedinca upotrebi ovih sistema. Tako neke biometrike (otisak, lice, DNK) nose negativnu konotaciju upotrebe u kriminalistici. Druge se opet kulturološki doživljavaju nedostojnim čoveka. Religiozni aspekt se takođe ne sme zanemariti gde se spominje "znak zveri" i citira Otkrovenje 13:16-17 Kod problema privatnosti razmatramo 3 aspekta:

1. nenamerno proširivanje funkcionalnog delokruga biometrijskih sistema – pošto su biometrijske karakteristike u suštini biološke mogu se iz njih dobiti i dodatne informacije (npr. medicinske) koje se mogu iskoristiti za diskriminaciju pojedinca ili grupa;
2. nenamerno proširivanje aplikativnog polja rada – dolazi do neželjene identifikacije u slučajevima kada osoba zakonski koristi drugi identitet (zbog bezbednosti i sl.); štaviše mogu se povezati informacije vezane za ponašanje, navike i sklonosti pojedinca dobijene iz više različitih aplikacija čime se postiže značajna moć nad njim;
3. skriveno prepoznavanje – biometrijske karakteristike nisu tajne, moguće ih je dobiti bez saglasnosti osobe. Ona je samim tim uskraćena za privatnost i anonimnost na koju imaju pravo.

Ili ako ovo sistematizujemo dobićemo da biometrika ugrožava:

- *privatnost osobe* – u odnosu na način na koji se zahteva uzimanje biometrijskih podataka;
- *privatnost ličnih podataka* – koji se takođe zahtevaju prilikom registracije; sakupljanjem i razmenom podataka daje se mogućnost potpune kontrole nad populacijom čiji se biometrijski podaci imaju;
- *privatnost slobodnog ponašanja* – pošto se uz pomoć biometrike mogu pratiti radnje i ponašanje osobe, organizacije mogu praćenjem ponašanja da pokušaju da spreče neželjene akcije. Međutim mogu i da dele ove informacije sa drugima npr. radi odgovarajućeg nastupa na tržištu, ili sa vladinim organizacijama i sl.
- *nemogućnost anonimnosti i prijavljivanje pod pseudonimom*. Predstavlja jako oružje za razne agencije i vlade ali i neiscrpni izvor mogućih zloupotreba od istih;

Tu je i problem crnog tržišta baza biometrijskih podataka. Tako bi se slike irisa mogle koristiti za analizu u medicini (*iridologija*), pa se može zamisliti koliko bi ovakva baza mogla vredeti nekim kompanijama ili npr. osiguravajućim društvima.

Oni koji se zalažu za privatnost ističu potrebu da biometrijska baza bude decentralizovana, još bolje i da je nema tj. da svaki uzeti uzorak kao šablon bude sačuvan na kartici koja je u isključivom posedu pojedinca koji je biometrijski podatak i dao. Naravno tu se javlja problem zamene ukradene ili oštećene kartice, ali se određena razmišljanja u ovom pravcu moraju ozbiljno uzeti u obzir [11].

Možemo reći da su biometrijske tehnologije stvorile okruženje u kojem razne vladine agencije i korporacije mogu da steknu enormnu moć nad pojedincem. Prihvatanje "imperativa tehnologije", dopušta mogućnosti velikih zloupotreba sa nesagledivim posledicama po privatnost. Mora se zato prvo urediti oblast korišćenja biometrike na sledeći način:

- tehnološka regulativa koje će se pridržavati svi proizvođači biometrijske opreme;
- zakonska regulativa koja će na novi način urediti ovu oblast;
- moratorijum na uvođenje biometrijske tehnologije dok se ne regulišu uslovi i zaštiti privatnost pojedinca.

4. ZAKLJUČAK

Najslabija sigurnosna tačka svakog sistema je autentifikacija korisnika. Biometrika je donela izuzetan napredak u ovoj oblasti ali i ovi sistemi imaju svoje mogućnosti limitirane ograničenjima koja se manifestuju određenim implikacijama po sigurnost. Postoji veliki broj pretnji koje takođe utiču na sigurnost biometrijskih sistema, kao i veliki broj pretnji od delovanja i postojanja tih sistema od kojih je najvažnija pretnja ljudima njihov uticaj na privatnost. Donošenje zakonskih propisa u ovoj oblasti, definisanje standarda i pravila ponašanja mogu delimično umanjiti ove sumnje. Međutim činjenica da je biometrika jedinstveni i univerzalni identifikator koji i bez saglasnosti subjekta može povezati njegove različite lične podatke, kao i mogućnost namernog zaobilaženja zakonskih regulativa (delimično suspendovanje ljudskih prava i sloboda u SAD-u posle napada 11.09.2001 godine tzv. *Patriot Act I i II*) nalažu detaljnu analizu i odeđivanje oblasti stvarne potrebe njenog korišćenja, kao i primene dodatnih tehnika radi sprečavanja mogućih zloupotreba.

LITERATURA

[1] Miller, B., IEEE Spectrum, 31(2), p. 22-30, 1994.

[2] Phillips J., McCabe R., Chellappa R., In Proc. 9th Eur. Signal Proc. Conf. EUSIPCO-98, I, p.1-8, Rhodes, Greece, 1998.

[3] Popović B., Popović M., Zbornik radova sa savetovanja Mesto i Uloga Policije u Prevenciji Kriminaliteta, p.518-532, Beograd, 2002.

[4] Prabhakar S., Pankanti S., Jain K., IEEE Security & Privacy Magazine, 1(2), p. 33-42, 2003.

[5] Ross A., Jain K., Patt. Recogn. Letters, 24, p. 2115-2125, 2003.

[6] Bolle R.M., Connell J.H., Ratha N.K., Patt. Recognition, 35, p. 2727-2738, 2002

[7] Wikipedija, Web page , http://en.wikipedia.org/wiki/Biometrics#Danger_to_owners_of_secured_items

[8] Ratha K., Connell H., Bolle M., Patt. Recogn. Letters, 24, p. 2105-2113, 2003.

[9] Forte D., Computer Fraud & Security, 10, p. 12-14, 2003

[10] Matsumoto T., Matsumoto H., Yamada K., Hoshino S., In Proceedings of SPIE, 4677, p. 275-289, San Jose, USA, 2002

[11] Tomko G., In Privacy Laws & Business 9th Privacy Commissioners/Data Protection Authorities Workshop, Spain, 1998 available at www.dss.state.ct.us/digital/tomko.htm.

SUMMARY

THREATS TO BIOMETRIC SYSTEMS AND THE THREATS THEY CAN CAUSE

There is a great interest in use of biometric identification systems in wide area of application since they have some advantages over other systems for authenticity check. Nevertheless it is necessary to emphasis their limitations regarding security on the occasion of different sources of attacks. Also it is important to consider possible threats of biometrics systems on the people as result of their implementation, especially it is necessary to notice the endanger of privacy aspect in inadequate use of biometric systems.

Key words: *biometrics, identification, possibilities, threats*