Univerza v Ljubljani

Fakulteta za računalništvo in informatiko

Podiplomski študij

INFORMACIJSKI SISTEMI IN ODLOČANJE

Biometrija in pametne kartice

seminarska naloga pri predmetu

Kriptografija in računalniška varnost

Vigor Baša

vigor.basa@uni-lj.si

Kazalo vsebine

1 Uvod

V zadnje čase pojem računalniške varnosti pridobiva vse večji pomen. To je predvsem zaradi opravljanja vse večjega deleža poslovanja preko interneta, kot tudi zaradi vse večjega števila različnih elektronskih naprav, ki jim se za njihovo aktivacijo moramo identificirati se, oz. vnesti kodo.

Pri tem si človek mora zapomniti veliko število različnih gesel in ključev za kriptosisteme kar predstavlja ne majhen problem. Rešitev leži v uporabi pametnih kartic, ki lahko v sebi hranijo vse potrebne podatke za različne naprave. Ta podatke (gesla, ključe, ...) je na nek način potrebno aktivirati, oz. moramo se predstaviti pametni kartici, ki potem dovoli uporabo potrebnega ključa. Kartici se lahko predstavimo s pomočjo PIN-a, kratkega gesla si ga lažje zapomnimo, kot tudi s pomočjo biometrije.

2 Biometrija

Tehnologija biometrične avtentikacije, kar pomeni uporabo fizičnih lastnosti ali vedenja posameznika z namenom potrjevanja njegove identitete, se že dolgo let uporablja v okoljih kjer je zahtevana visoka varnost. Njena uporaba v kontekstu informacijske varnosti, kjer imamo senzorje zraven posameznih delovnih postaj ali prenosnikov, je razmeroma nov pojav, ki je omogočen predvsem zaradi znižanja cen opreme za biometrijo. Biometrija se lahko uporablja tudi v zelo lokalnem kontekstu, na primer za aktivacijo podpisov na pametnih karticah.

2.1 Kaj je biometrija

Biometrija pomeni avtentikacijo osebe s pomočjo njenih biometričnih karakteristik. Biometrija za avtentikacijo uporablja osebne fiziološke značilnosti ali značilnosti obnašanja. Te značilnosti imajo prednosti, saj jih je težko ukrasti ali kopirati.

Biometrične lastnosti lahko posnamemo na različne načine. Različne procedure merijo način tipkanja, geometrijo prstov, proporcionalno dolžino prstov ali geometrijo rok. Nadaljnje možnosti so analiza glasu, obraza, dinamika podpisa ter registracija vzorca retine (očesne mrežnice), šarenice ali genskega koda (DNS), kot tudi registracija prstnih odtisov.

V praksi se biometrične lastnosti delijo na pasivne in aktivne lastnosti:

- **Pasivne lastnosti:** obraz, retina, šarenica, prstni odtis, uho, geometrija roke, vzorec žil na zadnjem delu glave in vonj.
- **Aktivne lastnosti:** podpis, lastnosti pisanja, glasa in govora, lastnosti tipkanja po tipkovnici, geste in mimika pri govoru.

Vse te možnosti lahko nastopajo tudi v kombinacijah. Tipična kombinacija lastnosti je na primer registracija obraza in dinamika obraza pri govoru kombinirana s identifikacijo glasu.

Biometrična lastnost mora omogočati specifične kakovosti, da jo lahko uporabimo kot biometrično proceduro:

- **Jasnost** – lastnost mora biti edinstvenega pomena, to pomeni, da je dovolj raznolika ko jo uporabimo na različnih osebah.
- **Trajnost** – lastnost se z leti lahko le minimalno spremeni. Te minimalne spremembe morajo biti nadomeščene s prilagodljivimi biometričnimi procedurami. Obstajati mora

varnostni sistem za primer možnosti izgube ali neuporabnosti določene biometrične lastnosti.

- **Razširjenost lastnosti** – ena od lastnosti mora obstajati v celi množici potencialnih uporabnikov, toda vedno obstajajo manjše skupine v populaciji, ki določene lastnosti ne kažejo. Na primer, zelo malo ljudi ima nerazločno strukturo prstnih odtisov. Nekatere lastnosti niso primerne za določene skupine uporabnikov (npr. slepi, nemi). V takih primerih morajo obstajati alternativne procedure.

Vsaka biometrična lastnost ponuja možnost dodatnih informacij. Npr. pri primerjanju prstnih odtisov lahko gledamo prstne odtise več prstov in v različnem zaporedju. Podobno pri glasovni identifikaciji poleg same identifikacije glasa lahko uporabimo dodatno geslo, ki ga uporabnik izgovori.

Pri biometriji ločimo dva postopka:

- Verifikacija - proces avtentikacije v katerem biometrični sistem primerja zajeto biometrijo posameznika s tisto shranjeno na šabloni (1:1)
- Identifikacija - proces v katerem biometrični sistem identificira osebo z izvajanjem ena - proti-več iskanja med celotno registrirano populacijo.

2.2 Uporabniška sprejemljivost.

Naslednja pomembna stvar pri biometričnih postopkih je sprejemljivost pri uporabnikih. Pri tem imamo naslednje aspekte:

- Udobnost – pomembno vlogo igrajo čas v normalnih in posebnih (zavrnitev zaradi napake) primerih, enostavnost uporabe, čas za registracijo, frekvenca za nujno osveževanje vzorcev in podobno.
- Zaupnost/Transparentnost – uporabnik mora razumeti postopek in biti pripravljen na sodelovanje. Prednost imajo primeri, ko je procedura podobna že obstoječim postopkom.
- Nadlegovanje – napake zaradi higiene ali poseganje v privatni prostor posameznika (npr. skeniranje očesne mrežnice) lahko povzročijo manjšo sprejemljivost.
- Strahovi pred uporabo (npr. strah skeniranja retine), predsodki do registracije in uporabe

2.3 Napake

Najbolj pomembne napake v zvezi z biometrijo so napačen sprejem ali napačna zavrnitev.

- Verjetnost napačnega sprejema (FAR – *false acceptance rate*) je verjetnost sprejema neavtorizirane osebe zaradi podobnih biometričnih lastnosti.
- Verjetnost napačne zavrnitve (FRR – *false rejection rate*) je verjetnost zavrnitve avtorizirane osebe zaradi prestroge zahteve po identičnosti karakteristik.

Verjetnost napačnega sprejema in napačne zavrnitve mora biti speljana v sprejemljivo razmerje glede na zahtevano stopnjo varnosti.

2.4 Primerjava biometričnih procedur

Predstavljeni kriteriji uporabniške sprejemljivosti, edinstvenosti, konstantnosti in razširjenosti lastnosti kot tudi tehnični in finančni kriteriji morajo biti postavljeni v razmerje glede na zahtevan nivo varnosti. Tabela 1 prikazuje povzetek iz poročila o biometričnih procedurah (Morgan Keegan & Co – Januar 2001 [1]).

Rang	**Natančnost**	**Prijazna uporaba**	**Cena**	**Skupaj**
1	DNA	Glas	Glas	**Prstni odtis**
2	Šarenica	Obraz	Podpis	Glas
3	Retina	Podpis	**Prstni odtis**	
4	**Prstni odtis**	**Prstni odtis**	Obraz	
5	Obraz	Šarenica	Šarenica	
6	Podpis	Retina	Retina	
7	Glas	DNA	DNA	

Tabela 1: Natančnost, udobnost in cena biometričnih procedur

- Najbolj varna tehnika je genetska koda – DNS. Pomanjkljivost je njena nepraktičnost za vsakdanjo, pogosto uporabo. Uporabna je predvsem v kriminologiji.

- Identifikacija šarenice ponuja visok nivo varnosti, sorazmerno s tem pa zahteva napredno tehnologijo ter se ponavadi uporablja za aplikacije, ki zahtevajo visoko varnost. Enako velja za identifikacijo očesne mrežnice.
- Za vsakdanjo poslovno uporabo je tehnologija prstnih odtisov najboljši kompromis med varnostjo, enostavnostjo in ceno uporabe.

2.5 Tehnike biometrije

2.5.1 Prstni odtisi

Tehnika prstnih odtisov uporablja vzorce, ki jih najdemo na prstnih konicah. Obstaja veliko načinov za verifikacijo prstnih odtisov. Nekatere lahko odkrijejo ali je predstavljen pravi prst, druge pa tega ne zmorejo.

Število različnih naprav za prstne odtise je večje kot pri vsaki drugi tehniki biometrije. Z znižanjem cene takih naprav se tehnika prstnih odtisov uveljavlja na širšem področju uporabe.

Identifikacija s pomočjo prstnih odtisov je dobra izbira za notranje/zaprte sisteme, kjer uporabnikom lahko podamo ustrezno razlago in uvajanje in kjer sistem deluje v kontroliranem okolju. Ne bo presenetilo, če se bo kontrola dostopa do aplikacij opravljala izključno s prstnimi odtisi zaradi razmeroma nizke cene, majhne velikosti naprave ter enostavne integracije z delovnimi postajami. [2]

2.5.2 Geometrija roke

Geometrija roke vključuje merjenje in analiziranje oblike roke. Ta biometrična tehnika ponuja dobro razmerje karakteristike izvedbe in je razmeroma enostavna za uporabo. Uporabna je v primerih, ko imamo veliko uporabnikov ali uporabniki do sistema ne dostopajo pogosto in so zato manj disciplinirani pri dostopu.

Natančnost je lahko zelo visoka, če želimo. Organizacije uporabljajo bralce geometrij roke v različnih scenarijih. Posebej popularni so v beleženju prisotnosti. Geometrija roke, zaradi enostavnosti integracije v druge sisteme in procese ter enostavnosti uporabe, velikokrat predstavlja prvi korak za veliko biometričnih projektov. [2]

2.5.3 Retina

Biometrija retine, ali očesne mrežnice, vključuje analizo plasti krvnih žilic v ozadju očesa. To je uveljavljena tehnologija, ki s pomočjo slabe svetlobe, ki gre skozi optiko, skenira enotne vzorce retine. Skeniranje retine je lahko zelo natančno, od uporabnika pa zahteva gledanje v napravo in fokusiranje v dano točko. To ni preveč udobno če ima uporabnik očala ali je zaskrbljen zaradi gledanja v bralno napravo. Skeniranje retine zaradi teh razlogov ni navdušeno sprejeto čeprav tehnologija sama zase dobro deluje. [2]

2.5.4 Šarenica

Biometrija, ki temelji na šarenici analizira vzorce, ki se nahajajo v barvnem prstanu okoli zenice. Skeniranje šarenice je brez dvoma manj vsiljivo kot skeniranje retine. Uporablja standardne kamere in ne zahteva direktni kontakt z napravo. Z tehniko skeniranja šarenice lahko dosežemo nadpovprečno zanesljivost. Tehnika deluje tudi preko očal, lahko pa jo uporabimo tudi za identifikacijo. Enostavnost uporabe ter integracija s sistemom nista bila pozitivni strani naprav za skeniranje šarenice, toda na trg prihajajo nove naprave od katerih pričakujemo napredek na tem področju. [2]

2.5.5 Obraz

Razpoznavanje obraza analizira karakteristike obraza. Tehnika potrebuje digitalno kamero za izdelavo obrazne slike uporabnika, ki ga avtoriziramo. Tehnika potrebuje dodatne periferne naprave, ki niso standardne za osebne računalnike ter kot taka ni primerna za omrežno avtorizacijo. Primeri uporabe so v igralnicah kjer se kreirajo podatkovne baze obrazov, ki pomagajo varnostnem osebju za hitro odkrivanj nevarnih gostov. [2]

2.5.6 Podpis

Verifikacija podpisa analizira način kako uporabnik podpiše svoje ime. Pomemben je končni izgled podpisa kot tudi druge lastnosti (hitrost, pritisk), ki jih skeneri za podpise, vsaj zaenkrat, ne obvladujejo v zadostni meri. Verifikacija podpisa, za razliko od drugih biometričnih tehnik, predstavlja dopolnitev standardnega podpisovanja. Ljudje so vajeni podpisovanja kot verifikacije identitete in v biometriji podpisovanja ne vidijo nič nenavadnega. [2]

2.5.7 Glas

Pri avtentikaciji glasu algoritem pretvarja glas v tekst. Biometrija glasu ima največ potenciala za razvoj, ker ne zahteva novo strojno opremo, saj večina osebnih računalnikov vsebuje mikrofon. Slaba kakovost in hrup v prostoru nekoliko vplivajo na verifikacijo. Programska oprema za avtentikacijo glasu potrebuje dodatne izboljšave. Predpostavlja se, da bo ta tehnologija postala dodatek biometriji prstnih odtisov. Veliko ljudi verjame, da je biometrija prstnih odtisov veliko bolj zanesljiv način avtentikacije ter bo zaradi tega biometrija glasu verjetno predstavljala zamenjavo za PIN- e, uporabniška imena ali gesla. [2]

2.6 Možnosti uporabe biometrije

Varnostni sistemi uporabljajo biometrijo za dva glavna namena - za identifikacijo in za verifikacijo uporabnikov. Identifikacija je bolj zahtevna zato, ker mora sistem preiskati celotno bazo uporabnikov, da bi zadel uporabnika. Katero tehniko biometrije uporablja varnostni sistem je odvisno od tega, kaj sistem ščiti in proti komu poskuša zaščititi.

Danes se biometrija uporablja večinoma za fizično varnost pri kontroli dostopa do varnih lokacij. Taka zvrst kontrole je zelo uporabna na mestih z veliko uporabnikov kot so Olimpijske igre, letališča, kjer se za pogoste uporabnike uporablja skeniranje šarenice, vselitveni urad v ZDA, kjer za manj rizične in pogoste potnike uporabljajo skeniranje roke in podobno.

S padcem cene biometričnih naprav se je biometrija začela vse bolj uveljavljati tudi v kontroli virtualnega dostopa. V e-poslovanju se uporablja kombinacija biometrije in pametnih kartic za boljšo avtentikacijo uporabnika na drugem koncu.

Ena izmed bolj aktualnih področij raziskovanja je uporaba biometrije za skriti nadzor. Z uporabo tehnologij za razpoznavanje obraza in telesa se poskušajo narediti sistemi za avtomatično simultano identifikacijo več posameznikov znotraj množice kar po zelo uporabno na letališčih, vhodih v stavbe, igralnicah in podobno. Pri tem je glavna težava v tem, da morajo sistemi delovati neodvisno od drže uporabnika, zornega kota ali razdalje od detektorja.

3 Pametna kartica

Pametna kartica je plastična kartica velikosti navadne kreditne kartice z vgrajenim mikroprocesorjem in RAM/ROM spominom, tako da poleg spominskih sposobnosti vsebuje tudi računske sposobnosti. Takšna neodvisnost omogoča pametnim karticam zaščito proti napadom zato, ker ni odvisna od zunanjih pripomočkov. Zaradi teh lastnosti pametne kartice se pogosto uporabljajo v različnih aplikacijah, ki zahtevajo visoko varnostno zaščito in avtentikacijo.

Pametna kartica se je v svetu prvič pojavila leta 1979, vendar se takrat ni uveljavila zaradi previsokih stroškov, povezanih z njeno proizvodnjo. Razvoj računalniške tehnologije je omogočil, da je cena povprečne pametne kartice padla z deset dolarjev na približno dva evra danes. Ob nadaljnji množični proizvodnji bo samo še padala, vendar cene magnetne kartice verjetno še dolgo ne bo dosegla.

Izumitelj pametne kartice (Roland Moreno) se je osredotočil na finančne storitve kot poglavitno smer pri razvoju in razširitvi uporabe pametnih kartic. Pametne kartice naj bi postale vodilni instrument za prenos in razširitev elektronskega poslovanja zaradi lastnosti, kot sta varnost in sposobnost hranjenja podatkov. Kljub temu je bilo uvajanje pametnih kartic na finančno področje dokaj počasno, saj danes pametne kartice za finančne transakcije predstavljajo majhen del skupnega trga, na katerem se uporabljajo.

Nekateri izmed možnih načinov uporabe čip kartice so:

- plačilno sredstvo; pri zamenjavi z običajnimi plačilnimi sredstvi se čip kartica pojavlja kot elektronska čekovna knjižica, elektronski potovalni ček, elektronska denarnica in podobno,
- dvig gotovine na bančnih avtomatih,
- avtorizacija dostopov,
- kot elektronski podpis za preverjanje identitete, verodostojnosti in pooblastil prejemnika in pošiljatelja v sistemu elektronske izmenjave podatkov.
- osebna izkaznica
- telefonske plačilne kartice
- prepustnice (za parkirišča, avtoceste, itd)
- nosilke pomembnih zdravstvenih informacij
- kartice za GSM aparate

Razlog, da so trije kartični operaterji (Europay, Mastercard, Visa) v letu 1995 začeli uvajati plačilne kartice s čipom, je preprost. Magnetni trak na plačilnih karticah se uporablja že približno 30 let in omogoča hranjenje le nekaj številk in besed, pa še te je možno brisati in spreminjati. Informacije na magnetni kartici so slabo zaščitene, saj je možno enostavno prekopirati zapis s kartice na drugo kartico.

Čip kartice so pred zlorabami bolje zaščitene, lahko zberejo več informacij ter omogočajo varnejše poslovanje bankam in uporabnikom.

Za izdajatelja in uporabnika pametnih kartic je zelo pomembna zaščita podatkov na njej. Zlorabe preprečuje trojni sistem preverjanja. Prvi je ta, da kartica preveri, ali je terminal, preko katerega poteka plačilo, originalen. Drugi je ta, da terminal preveri pravilnost kartice. Nazadnje se preveri identifikacija imetnika kartice (ali je imetnik kartice tudi njen lastnik), in sicer z uporabo PIN kode. Po nekaj nepravilnih poskusih vnosa identifikacijske številke se kartica sama zaklene. Do zlorabe pametne kartice lahko vseeno pride, če pride do kraje identifikacijske številke, zato se pojavljajo drugačne oblike zaščite. Gre za biometrične tehnike, na primer primerjave prstnih odtisov, geometrije rok, očesne mrežice ali podpisov. Bralna naprava preveri, če je biometrični podatek na kartici enak temu, kar pokaže uporabnik. Dodatna zaščita je kodiranje informacij, ki potujejo od terminalov do centrale. Samo pooblaščen računalniški sistem, opremljen z ustreznim šifrantom, lahko bere podatke z originalne kartice.

Tehnologija pametne kartice je dovolj zapletena, da močno zmanjša možnost prevare. Vse je odvisno od zmogljivosti čipa in dovršenosti šifriranja (kripto procesorja), tako da boljših pametnih kartic ni mogoče kopirati. Veliko trenutnih modelov pametnih kartic ima vgrajen kripto-procesor ter lahko neodvisno računajo digitalne podpise. Na tak način uporabnikov privatni ključ nikoli ne zapusti sigurno okolje pametne kartice.

Pametne kartice postajajo vse bolj pomembne v našem vsakdanjem življenju. Uporabljajo se za prenos občutljivih podatkov o uporabnikih. V zvezi z varnostjo je veliko argumentov za in veliko argumentov proti uporabi pametnih kartic za shranjevanje takih informacij. Ti argumenti so bili vedno vzrok sporov in razprav.

4 Biometrija v povezavi s pametnimi karticami

4.1 Opis tehnologije

PIN in gesla niso varni, lahko se odkrijejo, prenesejo in pozabijo. Napadi na gesla so najbolj pogosti napadi na informacijsko varnost in tudi najbolj enostavni. Biometrične lastnosti v povezavi s pametnimi karticami pomagajo pri reševanju teh pomanjkljivosti. V primerjavi z različnimi metodami za deblokiranje pametnih kartic, procedura prstnih odtisov zagotavlja najbolj uporabno in ekonomično rešitev, ki ponuja ustrezno stopnjo varnosti.

V tem primeru prstni odtis, ki ga ni možno pozabiti in je enoten, zamenjuje PIN. Uporabnikov tajni ključ, ki je skrit na pametni kartici se lahko aktivira samo s pomočjo posebne in takojšnje biometrične identifikacije prvotnega uporabnika.

Uporaba biometrije poleg boljše varnosti ponuja tudi nekatere druge prednosti, ki lahko olajšajo njen sprejem:

- Uporabniku ni potrebno izmišljevanje gesla, ki ga je težko zapomniti. Bolj nenavadno geslo je bolj varno toda težje si ga je zapomniti.
- Biometrična avtentikacija je hitrejša in enostavnejša od ostalih primerljivih alternativ.
- Ena prijava omogoča eno avtentikacijo in s tem zamenjuje več PIN-ov in gesel. Uporabniku ni potrebno pomnjenje množice gesel za kup aplikacij.

Biometrija ne more funkcionirati brez kriptografije in je lahko samo komplementarna metoda za PIN/geslo. Iz biometričnih lastnosti, ki vsebujejo odstopanja, se ne more izpeljati kriptografski ključ, ki vsebuje precizne matematične izračune in ne dovoljuje odstopanja. Na primer, prstni odtis zaradi variacij temperature in počutja uporabnika kaže manjše razlike, ki jih moramo upoštevati pri preverjanju. Ostanki umazanije in praha na prstu bralni napravi tudi povzročajo motnje.

Takojšnja avtentikacija s pomočjo biometrije je varna dokler ni v porazdeljenem okolju. Vedno mora obstajati zapis za primerjavo identifikacije. Ta zapis mora biti shranjen v primerni oblasti (banka, računalniški sistem delodajalca). Kakorkoli, v takem primeru, lahko vsaka oseba, ki vsebuje ustrezni vzorec biometrije, zlorabi to z namenom predstavljanja pod drugo identiteto.

4.2 Primerjava različnih vrst pametnih kartic

4.2.1 Geslo/PIN baza

Najbolj enostaven primer povezave pametnih kartic in biometrije je tako imenovana Geslo/PIN baza. Najbolj enostaven in univerzalen način za povezavo biometrije in digitalnih podpisov je naslednja procedura: Uporabnik se identificira ciljnem sistemu z biometrično lastnostjo. Aplikacija primerja izmerjeno vrednost s shranjeno vrednostjo (šablono) v bazi. Če obe vrednosti ustrezajo, se PIN iz baze, ki ustreza šabloni, deblokira – lahko je daljši in bolj kompleksen od PINa, ki bi si ga uporabnik moral zapomniti. Ta PIN urabimo za prijavo na uporabnikovo napravo za podpisovanje (pametna kartica, datoteka s ključem). Za uporabnika izgleda, da prijava poteka s pomočjo biometrije, v bistvu pa poteka po ovinkih s pomočjo PINa. Ta postopek ima prednosti in slabosti.

Prednosti Geslo/PIN baze:

- Uporabniku ni potrebno pomnjenje gesla za svojo pametno kartico (podpisovalno napravo) in ga tudi ne more pozabiti.
- Pametne kartice ne morajo biti prirejene za biometrijo in se lahko uporabljajo brez modifikacij. Biometrična prijava je realizirana okoli njih.

Pomanjkljivosti Geslo/PIN baze:

- Avtentikacija na pametno kartico še vedno poteka s pomočjo PINa. Če nekdo drug pozna PIN, oseba lahko prevzame podpis brez potrebe po biometrični avtentikaciji.
- Če uporabnik pozna PIN lahko prenese pametno kartico drugim osebam, ki potem lahko uporabijo podpis. Uporabniku tako ni več garantirana varnost.
- Glavna pomanjkljivost je ta, da je PIN za podpisovalno napravo shranjen v bazi in ne samo pri uporabniku. Če napadalcu uspe prebrati celo bazo ali če posluša komunikacijo med bazo in uporabnikom lahko pridobi PIN in ga uporabi za uporabnikovo pametno kartico.
- PIN ne more biti zašifriran ker se iz biometrije ne more določiti jasen ključ. Ponavadi se uporablja programsko fiksiran ključ, ki ponuja majhno varnost.
- Če napadalcu uspe postaviti svojo šablono odtisa na mesto avtoriziranega uporabnika, se lahko drugič prijavi z njegovo pametno kartico.

4.2.2 Primerjanje na kartici (MOC - Match-On-Card)

Primerjanje na kartici je razmeroma nov postopek, ki odpravlja prejšnje pomanjkljivosti. Namesto PINa je na kartici shranjena biometrična šablona. Za aktivacijo podpisa s podpisovalne naprave se na napravo namesto PINa pošilja trenutni sken biometrične lastnosti. Namesto primerjanja PINa znak po znak procesor na napravi, s pomočjo primerjalnega algoritma, primerja trenutni sken s shranjeno šablono. Razen večje kompleksnosti komparativnega algoritma je procedura skoraj identična prijavi s pomočjo PINa.

Pametne kartice s takimi lastnostmi so dostopne od konca leta 2000. Prve aplikacije za to tehnologijo so bile dostopne od 2. četrtletja 2001. Tehnologija prstnih odtisov je danes priljubljena biometrična procedura. Čeprav je ta metoda sorazmerno primerna za kombinacijo biometrije in kriptografije še obstajajo nekatere specifične prednosti in pomanjkljivosti.

Prednosti MOC

- Resnična prijava s pomočjo biometrične lastnosti (ni več PINa).
- Vse se opravlja na kartici (hranjenje šablone in primerjava). Ni več potrebna posebna baza za šablone in PINe. Tako odpade veliko možnih točk za napade. Inštalacija in administracija programske opreme je enostavnejša, ker takih baz ni potrebno inštalirati in replicirati.
- Podprta je uporabnikova mobilnost. Vsi podatki za avtentikacijo so shranjeni na uporabnikovi kartici. Podpisovanje se lahko opravlja brez povezave na strežnik šablon, kar obenem predstavlja tudi pomanjkljivost saj kartice ni možno preklicati.
- Veliko uporabnikov ni zadovoljno, da se njihovi biometrični podatki hranijo na centralni podatkovni bazi. Z MOC ta zaskrbljenost odpade. Uporabnik vse podatke nosi s seboj, podatki pa se ne morejo prebrati s kartice in tako možni napadi odpadejo.

Pomanjkljivosti MOC

- MOC ni primeren za čiste programske rešitve, ki uporabljajo datoteke ključev namesto pametnih kartic.
- Namesto PINa se v kartico pošiljajo biometrični podatki. Primerjalni algoritem je bolj kompleksen toda to še vedno ostanejo vhodni podatki, podobni dolgemu PINu, ki jih lahko rekonstruiramo ali prestrežemo in jih pošljemo namesto originalnega skena.
- MOC ni še standardiziran. Trenutno ne morejo vse pametne kartice podpirati MOC.

- Ni vsaka biometrična procedura primerna za MOC. Na razpolago imamo malo prostora za šablono, za primerjavo je potreben zahtevnejši algoritem toda ne sme trajati predolgo (približno eno sekundo). Tehnologija prstnih odtisov je zato najbolj primerna za MOC.

Izboljšana varianta MOC kartice ima vgrajen skener za prstni odtis na sami kartici. S tem rešimo pomembno pomanjkljivost navadne MOC kartice – možnost prestreganja podatkov, ki potujejo med kartico in zunanjo napravo za branje prstnih odtisov. Velika prednost skeniranja na sami kartici je tudi večja kompatibilnost z obstoječo IT, ki je ni potrebno prilagajati za uporabo biometrije.

5 Zaključek

Veliko podjetij za svoje poslovne procese išče višjo varnost kot jo ponujajo gesla. Začetek akcije s pomembnimi posledicami mora biti jasno in dokazljivo pripisan avtorizirani osebi tako, da se tudi kritični poslovni procesi lahko izvajajo po elektronski poti.

Enostavnost uporabe v povezavi z varnostnimi funkcijami je pomemben faktor za njihov uspeh. S pomočjo biometrično kompatibilnih terminalih za pametne kartice se poveča udobnost uporaba, vzporedno s tem se veliko poveča tudi stopnja varnosti. Stroški administracije se znižajo, odpadejo tudi težave s pozabljanjem gesel.

Prihodnost biometrije se kaže predvsem v kombinirani uporabi z drugimi tehnikami identifikacije in verifikacije, kakor smo to videli na primeru uporabe biometrije in pametnih kartic.

6 Seznam uporabljenih virov

1. Pohlmann, Robert: Forget About PINs, Business Briefing: Global Infosecurity, 2002.
2. Liu Simon, Silverman Mark: A Practical Guide to Biometric Security Technology.
3. Lisimaque, Gilles: Workshop on ID Cards, Carnegie Mellon University, 2001.
4. Pankanti, Sharath; Prabhakar, Salil; Jain Anil K.: On the Individuality of Fingerprints, 2001.
5. Chan, Siu-cheung Charles; An Overview of Smart Card Security,1997.
6. UK Government Biometrics Working Group, Biometric Device Protection Profile (BDPP), 2001.
7. Aufreiterm Richard: Biometrics and Cryptography – Match On Card Paves the Way to Convenient Security, Ultimaco, 2001.
8. Kent, Stephen: Biometrics & System Security, Communications and multimedia security conference - Portorož, 2002
9. Jurišić, Aleksander; Tonejc, Jernej:Pametne kartice in varnost, Monitor, junij 2001