

ИЗАЗОВИ ВЕЗАНИ ЗА ПРИВАТНОСТ И БЕЗБЕДНОСТ ПРИЛИКОМ УПОТРЕБЕ БИОМЕТРИКЕ

Бранкица Поповић¹, Драган Ранђеловић¹, Милош Банђур²

¹ Криминалистичко-полицијска академија, Цара Душана 196, Београд

brankica.popovic@kpa.edu.rs, dragan.randjelovic@kpa.edu.rs

² Факултет техничких наука, Кнеза Милоша 7, Косовска Митровица, bandjo@ptt.rs

Апстракт: Употреба информационих и комуникационих технологија у свим аспектима живота и рада, одлика је савременог друштва. Поред несумњивих могућности унапређивања наших активности, ова технологија, нажалост, доноси и нове изазове са аспекта безбедности података којима располаже, а поготово са аспекта заштите приватности појединца. Биометрика, као водећа технологија управљања идентитетом, генерално се доживљава као технологија која је противник приватности. Због изузетне важности тог аспекта, спроводе се интензивна истраживања и као једно од могућих решења предлаже се комбиновање биометрике са криптолошким механизмима. У овом раду приказане су могућности али и слабе тачке биометријских система, као и начин на који комбинација са криптолошким техникама може унапредити њихов рад са становишта оба споменута аспекта, безбедност и приватност. Посебно је објашњена нова технологија названа Биометријска Енкрипција.

Кључне речи: биометријски системи, криптологија, заштита података, приватност

1. УВОД

Изузетан напредак у информационој и комуникационој технологији (ИЦТ¹) довео је до чињенице да се све више пословних активности не могу замислити без употребе рачунара, рачунарских мрежа, мобилних уређаја и комуникација. Штавише, њихова употреба се не ограничава само на пословни домен, већ све већу улогу имају и на приватни аспект појединца укључујући забаву, склапање пријатељства, развијање личних склоности и талената, образовање и сл. Ова технологија је такође омогућила сакупљање, чување и добијање огромне количине информација (међу којима су и они најосетљивији - лични), као рутински и више не тако скуп процес, чак и без знања или дозволе појединца. За њих су изузетно заинтересовани државни и комерцијални (пословни) сектор. Први под синтагмом заштите грађана (укључујући методе скривеног надгледања и контролисања) и борбе против тероризма, а други због несумњивих могућности управљања тржиштем. Међутим, оваква доступност података неминовно

¹ ИЦТ – *Information and communications technologies*: термин покрива широки спектар сервиса, апликација, технологија, опреме и софтвера неопходних да би се та технологија могла користити.

подстиче сумњу у њихову правилну и закониту употребу. Наиме, са развојем технолошке и геополитичке ситуације, прикупљање, продаја или размена личних² (приватних) информација постала је уносан посао којим се баве многе компаније. Ту су укључени и тзв. 'невини подаци' (*Innocent data*), као подаци који можда не изгледају као лични али то постају обзиром на начин на који се користе.

Јасно је да се са појавом сваке нове технологије јављају и непланиране могућности и нежељене последице њеног коришћења. Једна од највише разматраних нежељених последица, тј. промена која је изазвала највећи степен забринутости у друштву последњих година, је губитак приватности, као и опасност да се последично дозволи и могући губитак људских права и слобода, пре свих права на анонимност. Наиме, идентитет није више заснован само на физичким документима. Он се данас за појединца успоставља комбиновањем различитих делова личних информација (*Personally Identifiable Information–PII*) од биографских података, физичких докумената до биометријских карактеристика.

Обзиром да нове технологије захтевају специфичне мере ради обезбеђивања корисникова права на приватност, марта 2006 Европски Парламент је усвојио Директиву о чувању података произведених или обрађених путем јавно доступних сервиса електронске комуникације или кроз јавне комуникационе мреже, тако што је допунио Директиву 2002/58/ЕС о приватности електронске комуникације [1]. Она садржи одредбе које су кључне за гарантовање да корисници могу веровати сервисима и технологији коју користе у електронској комуникацији. У њој се дефинишу категорије података који се чувају, временски оквир као и начела којих се треба придржавати у области безбедности података, пре свега:

- аутентичност (*Authentication*) –потврда прокламованог идентитета ентитета или корисника. Одговарајући методи аутентификације су неопходни за многе апликације и сервисе укључујући *online* трансакције, контролу приступа подацима и сервисима и др. Аутентификација мора да укључи могућност анонимности, пошто многи сервиси не захтевају идентитет корисника, већ само поуздану потврду одређеног критеријума (тзв анонимна уверења-*anonymous credentials*);
- приватност (*Privacy*) где под заштитом приватност подразумевамо елиминисање ризика (или смањење на прихватљив ниво) да један субјект користи туђе информације а да за то нема овлашћење.

Провера аутентичности може се обавити уз ослонац на верификацију [2]:

1. нечега што субјекат **ЗНА** (*knowledge* – нпр. ПИН број или лозинка);
2. нечега што субјекат **ИМА** (поседује) (*possession* – нпр. сигурносна идентификациона картица);
3. нечему што субјекат **ЈЕСТЕ** (*biometrics* - биометрика заснована на физичким или карактеристикама понашања).

² 'лична информација' (*Personal Information*) је свака информација која се може искористити да идентификује особу.

Све већа примена биометријских система, као тренутно најпоузданије технологије утврђивања идентитета, убрзала је истраживања научне заједнице, али и заинтересованог невладиног сектора, колико су они отпорни на различите претње³ и ризике⁴ којима могу бити изложени. Анализиране су и рањивости⁵ које за последицу могу имати неповратну компромитацију личних информација (пре свега биометријских) као и негативан утицај на приватност појединца. Ради заштите података у тим системима анализирана је могућност примене проверених криптолошких техника, као и развој нових, прилагођених употреби са биометријским подацима.

У раду ће бити објашњене могућности биометријских система као и њихове комбинације са одговарајућим криптолошким техникама ради побољшања заштите безбедности личних информација као и права на приватност појединца.

2. БИОМЕТРИЈСКИ СИСТЕМИ

Биометрика мери јединствене биолошке карактеристике (физиолошке и/или карактеристике понашања) појединца које се користе за проверу и утврђивање идентитета. Биометрика се већ сада (са правом или не) сматра кључним фактором у апликацијама где се захтева повећана сигурност. Развијени су и у употреби системи који се заснивају на следећим биометријским карактеристикама [3]: лице, глас, отисак прста, геометрија шаке, око, вене, потпис, динамика куцања и др.

Биометријски системи могу се користити у широком спектру апликација које захтевају поуздану аутентификацију корисника као што је приказано у Табели 1. До недавно се аутентификација у државном сектору доминантно заснивала на системима заснованим на поседовању (*possession*), а комерцијални сектор на системима заснованим на знању (*knowledge*), али се то великом брзином мења у корист биометријских система.

Табела 1. Решења за аутентификацију која укључују биометрику

Форензика (FORENSIC)	Државни (владин) сектор (GOVERNMENT)	Комерцијални сектор (COMMERCIAL)
Идентификација лешева	Национална ИД документа	АТМ и кредитне картице
Криминалистичке истраге	Возачке дозволе, регистровање гласача	Контрола приступа, логовање на рачунар
Утврђивање очинства	Дистрибуција социјалне помоћи	Мобилни телефони, ПДА
Случајеви несталих особа	Гранични прелази, контрола пасоша	Е-трговина, Интернет, е- банкарство, е-учење

Сви биометријски системи имају две фазе: фазу уписивања, и продукциону фазу. У првој фази, један или више биометријских узорака узимају се од особе (нпр. отисак

³ Претња (*Threat*) представља потенцијални нежељени догађаја (инцидент)

⁴ Ризик (*Risk*) представља процењену вероватноћу да ће се претња остварити

⁵ Рањивост (*Vulnerability*) представља слабост која може бити искоришћена за реализацију претње. Обично су последица лошег пројектовања, имплементације или загађења софтвера

прста, слика лица и др.). Из тих узорака се затим издваја биометријски шаблон⁶ који се чува у систему за касније коришћење. У продукционој фази особа даје биометријску карактеристику коју биометријски систем пореди са претходно сачуваним шаблоном ради утврђивања подударности истих. У зависности од степена подударности систем ‘прихвата’ или ‘одбија’ особу. Говори се о степену подударности из разлога што се шаблон добијен из тада презентоване биометријске карактеристике скоро сигурно разликује од сачуваног шаблона (различити сензори, притисак на сензор, микроклима, повреде и сл.) тако да никада немамо 100% подударање.

Биометријски систем генерално посматрано има два режима рада:

1. **Верификација** (неки овај поступак називају Аутентификацијом) – подразумева 1-према-1 поређење (1:1) тј. пореди предочену биометрику са сачуваним шаблоном те исте особе. Шаблон може бити сачуван у централизованој бази, на уређају или на картици коју ће носити особа. Ово је такозвано ‘**позитивно препознавање**’ чији је циљ да се спречи да више људи користи исти идентитет.
2. **Идентификација** – подразумева 1-према-много (1:N) поређење, где се презентована биометрика пореди са свим шаблонима сачуваним у бази (која мора бити централизована) ради утврђивања идентитета. Ово се назива ‘**негативно препознавање**’ где систем може утврдити да ли је особа оно што имплицитно тврди да није. Циљ је да се спречи да једна особа користи више идентитета.

Рецимо и да постоји изузетан отпор на међународној сцени употреби великих централизованих биометријских база у идентификационим системима⁷, због могућих последица по приватност појединца, о чему ће касније бити више речи.

Да би се могао квалификовати рад биометријских система установљен је скуп мера. Тако се тачност биометријских система може одредити преко две специфичне променљиве:

- **FAR** (*false acception rate*) - лажно прихватање, где се биометријске карактеристике од две различите особе прихватају као да су исте;
- **FRR** (*false rejection rate*) - лажно одбијање, где се биометријске карактеристике од исте особе не прихватају тј. сматрају се узорцима различитих особа.

Смањивањем једне грешке повећавамо другу. Како успоставити најбољи однос зависи од конкретне примене система. Величине за FRR/FAR које представљају произвођачи биометријских система често су непоуздане. Независна истраживања су показала⁸ да је за већину биометријских система, FRR у опсегу од 0.1% до 20%, што

⁶ Шаблон је уствари дигитална редуцирана структура биометријске карактеристике особе. Нпр. код отиска прста та структура најчешће подразумева број, положај и тип минуција (детаља) издвојених из слике отиска.

⁷ International Data Protection Commissioners, “Resolution on the use of biometrics in passports, identity cards and travel documents,” Montreux (September 2005), vidi na www.edps.europa.eu/legislation/05-09-16_resolution_biometrics_EN.pdf

⁸ International Fingerprint Verification Competitions FVC2000/2008

значи да ће легитимни корисник бити одбијен просечно једном у 1000 покушаја (односно 1 у 5 покушаја). FAR варира од 1 у 100 (апликације где се не захтева велика сигурност), до 1 у 10,000,000 (апликације где се захтева изузетно велика сигурност).

Следеће важне карактеристике биометријског система су брзина (систем мора да донесе тачну одлуку у реалном времену), и безбедност (систем мора бити отпоран на различите видове напада).

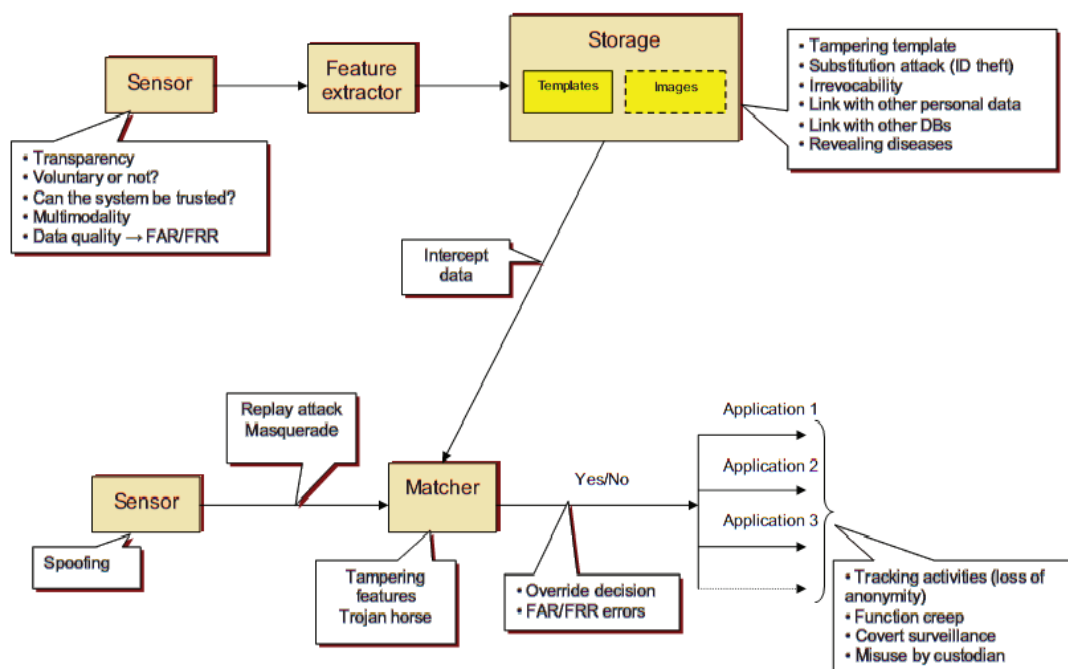
Значи, при одабиру биометријског система у обзир се морају узети следећи фактори:

- *поузданост* – односи се на тачност, брзину, као и на факторе који могу утицати на рад система;
- *безбедност* – колико је систем отпоран на потенцијално кривотворење и нападе и
- *прихватљивост* – означава степен спремности људи да прихвате коришћење овог система у свакодневном раду и *цена* – колико кошта увођење и експлоатација система;

Тренутно је немогуће оптимизовати сва три наведена фактора тј. имплементација биометрике је за сада компромис оптимизовања једног или у најбољем случају дава горе наведена фактора.

3. БЕЗБЕДНОСНИ АСПЕКТ БИОМЕТРИЈСКИХ СИСТЕМА

Као и у другим системима, тако и биометријски системи нису апсолутно сигурни од напада или превара (*foolproof*) и имају своје слабе тачке које су приказане на Слици 1.



Слика 1. Врсте напада на одређене тачке биометријског система (модификовано из [4])

Могући су различити напади [5, 6, 7] који укључују и:

- превару лажном биометриком представљеном сензору (*spoofing*);
- превару убацивањем претходно снимљеног података (*Replay attacks*) и маскирањем (*Masquerade attack*) [8];
- Замену биометрике у бази где се чува (*Substitution attack*);
- Фалсификовање карактеристика (*Tampering*);
- Промену одлуке модула за поређење (*Overriding Yes/No response*) и др.

Познати су и документовани различити случајеви преваре биометријских система лажном биометриком [9] и кад су у питању комерцијално доступни системи засновани на отисцима напади су имали успеха од 67–100%. Такође је забележено да је у Куала Лумпуру банда одсекла прст власнику кола како би могла да га покрене и украде⁹.

Развијају се различити методи за спречавање оваквих напада на биометријске системе који укључују криптографију, затим изазов-одговор (*challenge/response*) систем којим се обезбеђује присуство особе у тренутку давања биометријских података, *aliveness detection*¹⁰, мултимодалне биометријске системе и др.

Највећи проблем биометријских система је тај што биометрика није тајна [10] (нпр. отиске прстију свакодневно остављамо на свему што дотакнемо). Једанпут компромитована биометрика то остаје заувек, јер исту неможемо поништити или заменити.

Срушен је и мит који су пласирали продавци биометријских система да се биометријски податак не може реконструисати из сачуваног биометријског шаблона [11]. Неколико аутора је показало да је, под условом да се зна скор поређења две биометријске карактеристике, могуће извршити сасвим добру процену непознатог податка у бази регистрованих корисника [12] и то на основу шаблона отиска прста [8, 13] или лица [14].

Имајући све горе наведено у виду приликом избора мера заштите биометријских шаблона мора се обезбедити :

- Различитост (*Diversity*): заштићени шаблон треба да онемогући узајамну претрагу кроз више различитих база (*cross-matching*);
- Могућност поништења (*Revocability*): треба да је могуће поништити компромитовани шаблон;
- Могућност обнове (*Renewability*): добити нови шаблон из исте биометрике;

⁹ “Finger chopped off to beat car security”- <http://www.newscientist.com/channel/mech-tech/mg18624943.600>

¹⁰ Поступак провере да ли приложена биометрика потиче од стварне особе која се налази поред сензора у тренутку аутентификације

- Сигурност (*Security*): треба да буде изузетно тешко, ако не и немогуће, добити изворну биометрику из њеног шаблона;
- Перформансе (*Performance*): имплементирани заштитне мере не би смеле да деградирају перформансе система.

4. БИОМЕТРИЈСКИ СИСТЕМИ И ЗАШТИТА ПРИВАТНОСТИ

Широка размера употребе биометријских података многе наводи на помисао да је у питању покушај завере светске владе у сенци да прикупи огромну количину ‘корисних’ података који би омогућили инфраструктуру за глобално (скривено?) надгледање људске популације. Чак и ако то није сасвим тачно због дискутабилних перформанси биометријских система у случају великих база, и даље остаје отворено питање угрожавања приватности.

Сам коцепт приватности подразумева:

- приватност везану за доношење одлука (*Decisional privacy*): слобода појединца да прави приватне изборе без неприличних уплитања (мешања) споља;
- просторну приватност (*Spatial privacy*): слобода да се буде сам, без контакта са другим људима и без надгледања (*monitoring agents*¹¹);
- приватност везана за намере (*Intentional privacy*);
- приватност информација (*Information privacy*): слобода појединца да ограничи приступ одређеним личним информацијама.

Злоупотреба биометријских система може се извршити кроз:

- Непотребно/неовлашћено прикупљање биометријских података, без корисникове дозволе, знања или без одређене намене;
- Неовлашћену употребу биометријских података у сврхе за које није била намењена;
- Неовлашћено откривање и дистрибуција биометријске информације без корисникове дозволе;
- Употребу јединственог идентификатора (*Unique identifier*): биометрика се несме користити као универзални идентификатор пошто може обезбедити повезивење података из различитих база.

Присутан је и страх корисника од проширивање функционалног делокруга биометријских система, пошто су биометријске карактеристике у суштини биолошке и из њих се могу добити и додатне информације које се могу искористити за дискриминацију појединца или група. Тако су годинама проучаване различите корелације између шаблона папиларних линија и одговарајућих болести: деменције¹²,

¹¹ Intelligent Software Agents – ISA, чине софтвер и/или хардвер који извршавају задатак за корисника али уз његово минимално учешће. Програм се извршава на рачунару или у мрежи и за то време прикупља, обрађује, складишти и дистрибуира податке. Неки од тих података могу бити осетљиви лични подаци или то постају у комбинацији са другим прикупљеним подацима о појединцу.

¹² *vidi Arch Neurol.* 1986 Jul;43(7):665-8., Fingerprint pattern differences in early- and late-onset primary degenerative dementia., Seltzer B, Sherwin,

психолошких карактеристика¹³ чак и хомосексуалности¹⁴. Позната је и обавештајна активност омогућена употребом биометрике (*Biometrics Enabled Intelligence–BEI*)¹⁵.

Како би се обезбедила што је могуће већа таштита приватности имплементација биометријских система мора се заснивати пре свега на законским основама. Закон даје основне принципе о којима морају водити рачуна и они који креирају политику заштите као и инжињери. Ти се принципи називају *Fair Information Practices* и дефинисани су још 1980 год. од стране *OECD (Organization for Economic Co-operation and Development)* као смернице за заштиту приватности приликом руковања личним подацима¹⁶. Осам дефинисних принципа су:

1. Принцип ограничења прикупљања (*Collection limitation principle*): прикупљање личних података требало би да се спроводи законитим средствима и када је год то применљиво, уз знање и сагласност индивидуе;
2. Принцип квалитета података (*Data quality principle*): лични подаци требало би да буду релевантни, тачни, потпуни и ажурни за предвиђену намену;
3. Принцип спецификације сврхе (*Purpose specification principle*): мора се дефинисати у које се сврхе скупљају подаци и то пре него скупљање започне.
4. Принцип ограничења употребе (*Use limitation principle*): лични подаци неби требало да буду доступни у друге сврхе осим оних за које је појединац дао сагласност или које су предвиђене законом;
5. Принцип заштите сигурности (*Security safeguards principle*): лични подаци требало би да буду заштићени од сигурносних ризика као што су неовлашћено обелодањивање, употреба, измена, уништење или губитак;
6. Принцип отворености (*Openness principle*): циљ истраживања, главна сврха употребе личних података, као и правила и пракса које се односе на њихову заштиту, као и идентитет особе која контролише те податке требало би да буду јавни;
7. Принцип индивидуалног учешћа (*Individual Participation principle*): појединац треба да има право да: сазна од контролора података да ли је неки податак који се односи на њега сачуван као и да оспори те податке и затражи њихово брисање, исправку или допуну;
8. Принцип одговорности (*Accountability principle*): контролор података треба да је одговоран за придржавање мера које подржавају наведене принципе;

http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=pubmed&dopt=Abstract&list_uids=3729743

¹³ [vidi http://www.edcampbell.com/PalmD-History.htm](http://www.edcampbell.com/PalmD-History.htm)

¹⁴ Finger Length Helps Predict Test Exam Results, Homosexuality, Cancer, Musical Ability and Aggressive Personality -- Study Shows <http://www.viewzone.com/fingers.html>

¹⁵ обавештајна информација повезана са и/или добијена из биометријског податка, која повезује одређену особу непознатог идентитета са местом, активношћу, уређајем, догађајем, делом или оружјем. На тај се начин омогућава циљано претраживање као и шема кретања.

¹⁶ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Поред ових смерница, заштиту приватности можемо постићи ако користимо одговарајуће технологије¹⁷ (тзв. *Privacy Enhancing Technologies–PET*¹⁸). Оне омогућавају појединцу да управља својим идентитетом и личним идентификационим информацијама (*personally-identifiable information–PII*) на начин да се заштити приватност. Ово укључује средства или системе за:

- Анонимност или могућност коришћења псеудонима;
- Сигурно управљање лозинкама и другим средствима аутентификације;
- Ограничену могућност праћења и надгледања;
- Дозвољава корисницима да селективно обелодани своје приватне информације другима при чему испољава максималну контролу над тим подацима када су једанпут обелодањени.

У том процесу значајно место заузимају криптолошки механизми. Популарност криптографије резултат је њене способности да гарантује аутентификацију, интегритет, поверљивост и непорицање у свим разменама података и комуникацијама у информатичком друштву. Међутим чак и концепт *PKI (Public Key Infrastructure)*¹⁹ има неколико битних, већ годинама познатих, сигурносних проблема²⁰ који су предмет интензивног разматрања [15]. Они настају углавном због: коришћења машина опште намене за потписивање (*general purpose machines for signing* – када може бити компромитован приватни кључ); због слабости концепта поверења у хијерархијским системима (ко коме верује за шта); због међусобне повезаности са другим системима (*interoperability*²¹). Проблем је додатно усложњен ограниченом ваљаношћу пара кључева, нпр. одрицање код уговора потписаних на дуге стазе или код дигиталних архива.

Са друге стране, традиционални сертификати *PKI* садрже информације о њиховом власнику. Сваки дигитални сертификат може се јединствено повезати са особом којој је издат (или до уређаја у који је инкорпориран) и може се пратити аутоматски док се креће кроз систем. Имајући то у виду можемо рећи да дигитални сертификати не нуде више приватности него нпр. јединствен матични број грађана (ЈМБГ) или број кредитне картице. Последице, дигитални сертификати могу се злоупотребити да онемогуће његовог власника да користи ресурсе на које има право, или да блокира његову комуникацију у реалном времену²² и то је још једна слабост постојеће *PKI* имплементације.

¹⁷ Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies COM(2007) 228 final

¹⁸ Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II). Vol. I - www.ipc.on.ca/index.asp?layid=86&fid1=329, Vol. II - www.ipc.on.ca/images/Resources/anoni-v2.pdf

¹⁹ инфраструктура система са јавним кључевима односи се на систем и процесе који се користе за издавање и руковање асиметричних кључева и дигиталних сертификата

²⁰ Више на <http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt>

²¹ Дефиниција: 'Способност размене и коришћења података' wordnet.princeton.edu/perl/webwn или 'Способност система, јединица или снага да обезбеде податке, информације, материјале и услуге и да приме (прихвате) исте од других система, јединица или снага као и да их користе и да омогући да сви заједно ефективно раде' (DoDD 5000.1) www.acq.osd.mil/osjtf/termsdef.html

²² Нпр. Црна листа сертификата може се уградити у Интернет рутере

5. КОМБИНОВАЊЕ БИОМЕТРИКЕ И КРИПТОЛОШКИХ АЛГОРИТАМА

Обзиром на изузетне могућности, али и ограничења која се имају при употреби две тренутно најнапредније технологије (биометријски системи и криптолошки механизми) јасно је зашто се кренуло правцем истраживања могућности њиховог повезивања.

Типичан приступ за заштиту биометријских информација прати главни правац истраживања у области безбедности који подразумева: криптовање биометријских података помоћу стандардних криптолошких механизма (шифрирање, стегнографија и техника воденог печата) [16, 17], што побољшава свеукупну безбедност система, али нажалост оставља и даље отвореним многа питања везана за приватност²³. Иако се може применити већина стандардних техника, постоје и неке које су специфичне рецимо за отиске прстију. Тако су Соутар и Томко [18] разматрали практични систем приватног (сличног *DES*) шифровања заснованог на Фуријеовој трансформацији слике отиска прста. Коришћење невидљивих водених печата може обезбедити администратору биометријске базе, да су све слике у бази аутентичне и да их није нико неовлашћено мењао [19] и то у случајевима када је неопходна визуелна инспекција без потребе да се енкриптује кодирана информација. Такве слике се не користе у поступцима издвајања карактеристика или упоређивање и тако се обезбеђује смањење ризика од неовлашћеног убацивања лажних записа у базу.

У случају преноса биометријских карактеристика преко несигурних линија једно од предложених решења је употреба стеганографије и водених печата. Наиме биометријске карактеристике се могу сакрити у некој слици домаћину, у којој би локације пиксела биле модификоване у зависности од тајног кључа. Такође је предложено да, за мултибиометријски систем, тајни кључ који је сакривен у слици отиска може бити лице корисника [16]. Предлаже се и метода коришћења два кључа, један за криптовање биометријског шаблона пре уграђивања садржаја (*before embedding*), што овај метод чини сигурнијим, и други кључ за убацивање воденог печата што метод чини робуснијим [20]. Метод не захтева оригинални биометријски податак за издвајање убаченог печата, и може да обезбеди високу тачност издвојеног садржаја и у случају различитог шума и изобличења.

Највећи изазов при коришћењу биометријских система је чињеница да једном компромитован биометријски шаблон остаје заувек компромитован [10]. Као могуће решење понуђена је тзв. *cancelable biometrics* техника [6] где је уведен концепт биометријских шаблона специфичних (различитих) за апликацију и који се у случају компромитације могу поништити.

Док се криптолошки механизми често и успешно користе за заштиту биометријских података, улога биометрике у побољшању криптографије (нпр. за управљање кључевима) није баш тако јасна. Конвенционалне криптографске технике користе кључеве за шифровање који су у суштини довољно дугачки низови бита (обично 128

²³ ISO/IEC WD 24745, "Biometric Template Protection":
www.nia.din.de/sixcms/media.php/1377/SC27N4997rev1_SD7_Catalog_Proj&Stand_May2006.htm?backend_call=true#24745; www.incits.org/tc_home/CS1/2007docs/cs1070006.pdf

бита или више) које је немогуће запамтити. Стога се кључ генерише, након неколико корака, из лозинке или ПИН-а који се могу запамтити и зато се сматра да је управљање лозинкама (и последично кључевима) најслабија тачка сваког криптосистема. Са друге стране биометрика даје појединцу јединствену карактеристику која му је увек доступна без потребе да је памти, па је логично питање да ли се она може искористити као криптографски кључ? Нажалост, одговор је негативан пошто су биометријске слике и шаблони променљиве природе, тј. сваки нови узорак исте биометрике увек је другачији, а конвенционалне криптографске технике не толеришу грешку ни у једном биту.

Приликом разматрања да ли биометрика може да побољша *PKI* треба направити разлику између:

1. Употребе биометрике за ослобађање кључа (*Key release*)– Криптографски кључ се чува заједно са биометријским шаблоном, после успешног поређења кључ се ослобађа. У овом случају се захтева чување шаблона. Има производа²⁴ који чувају криптографски кључ у такозваном систему од поверења (*Digital Signal Processor – DSP*). Кључ се ослобађа након успешне биометријске верификације и тада улази у конвенционални криптосистем. Биометријски шаблон или слика је такође негде сачуван, често у криптованој форми, тако да је и даље актуелна већина питања везана за сигурност и приватност;
2. Употребе биометрике за додељивање кључа (*Key binding*) – Кључ је додељен биометријском шаблону на начин да су оба недоступна нападачу, после успешног поређења кључ се ослобађа. Овде се не захтева чување шаблона;
3. Употреба биометрике за генерисање кључа (*Key generation*) – Кључ се добија из биометријског податка, али је у овом случају тешко генерисати шаблоне са високом ентропијом и високом стабилношћу кључа.

Пошто се због своје варијабилности биометријска слика или шаблон не може (још увек) сам за себе узети као криптографски кључ, поставља се питање да ли се може из ње, конзистентно, издвојити релативно мали број бита (нпр. 128)? Или да ли је могуће доделити (везати) 128 битни кључ биометријској информацији, тако да се може конзистентно обновити (*regenerate*)? Одговор на прво питање је још увек проблематичан, док је одговор на друго питање покренуо целу једну нову област истраживања, названу Биометријска Енкрипција (БЕ, други термини: биометријски криптосистеми, приватни шаблони, биометријски кључ, биометријски потпис, и др.)[21]. Такви системи се могу користити у широком спектру апликација [22, 23]. Један од препознатих проблема код њиховог коришћења је недовољна корелисаност биометријских шаблона. Наиме, узорковање истог биометријског сигнала у различитим временским тренуцима (чак и када се ради са истим сензором, а да не причамо о различитим) доводи до малих разлика у биометријском шаблону, и практично онемогућава примену стандардне једносмерне криптографске функције, јер након њихове примене излази неће бити ни слични један другом, тј. хаш вредност је комплетно другачија. Софистициран начин да се произведу довољно усаглашени (корелисани) шаблони је да се изврши модификација биометријске слике како је предложио Adler [24].

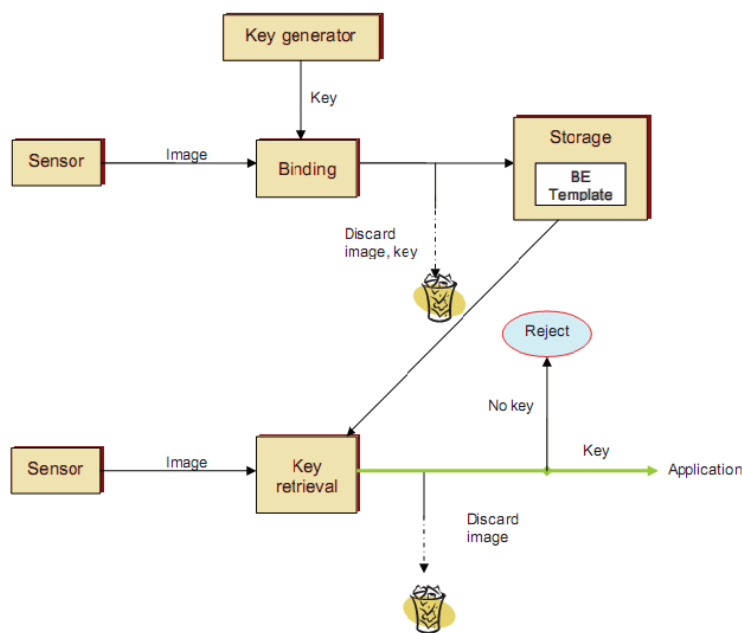
²⁴ www.ceelox.com; www.sequiam.com; www.lacie.com/products/product.htm?id=10166

5.1. БИОМЕТРИЈСКА ЕНКРИПЦИЈА

Биометријска енкрипција (БЕ) је процес који поуздано повезује (додељује) ПИН или криптографски кључ биометрици, тако да се ни кључ ни биометрика немогу обновити (успоставити) из сачуваног шаблона. Кључ се поново креира (*re-create*) само ако је тачна биометрика презентована за верификацију.

Дигитални кључ (лозинка, ПИН, и сл.) се произвољно генерише при уписивању тако да је чак ни корисник не зна. Кључ је комплетно независан од биометрике, и може се увек променити или ажурирати. Након узимања биометријског узорка, БЕ алгоритам сигурно и конзистентно (доследно) повезује кључ са биометриком да би се креирао заштићени БЕ шаблон, који се такође назива “приватни шаблон”. У суштини, кључ је енкриптован са биометриком. На крају уписивања (*enrolment*), и кључ и биометрика се одбацују (не чувају се).

Приликом верификације, корисник презентује ‘свеж’ биометријски узорак, који ће, када се примени на легитимни БЕ шаблон, омогућити БЕ алгоритму да успостави исти кључ/лозинку. Другим речима биометрика служи као кључ за дешифровање. БЕ алгоритми су тако осмишљени да урачунају прихватљиве варијације биометријских узорака. Ово је fuzzy шема енкрипције/декрипције, пошто је биометријски узорак другачији сваки пут када се узоркује, за разлику од кључа за криптовање у конвенционалним криптографским техникама. Велики је технолошки изазов направити овакав систем функционалним. Блок шема биометријског система енкрипције приказан је на Слици 2. Након добијања дигиталног кључа, једна од могућих примена је рецимо у *PKI* за генерисање пара кључева (јавни/приватни).



Слика 2. Шема функционисања Биометријске Енкрипције (модификовано из [4])

БЕ технологија има огроман потенцијал да побољша приватност и безбедност. Неки од кључних предности ове технологије су:

1. НЕМА чувања биометријске слике или шаблона— минимизација података који се прикупљају;
2. Вишеструки/поништливи идентификатори – БЕ омогућава појединцу да користи једну биометрику за више различитих налога и сврха без страха да ће они међусобно бити повезани том биометриком односно њеним шаблоном;
3. Побољшана сигурност аутентификације:
 - Нема напада заменом (*substitution attack*): Нападач не може креирати свој шаблон пошто незна дигитлни кључ и друге податке који су коришћени за креирање легитимног шаблона;
 - Нема мењања (*tampering*): Пошто се издвојене карактеристике не чувају, нападач нема могућности да их мења;
 - Нема напада прерушавањем (*masquerade attack*): БЕ обезбеђује ефикасну заштиту за системе удаљене аутентификације;
 - Нема напада Тројанским коњем (*Trojan horse attacks*): БЕ алгоритам на користи систем скора (нумерички резултат поређења) да би донео одлуку, већ само успоставља (или не) кључ. Зато нападач нема могућност да превари систем тако што би убацио висок скор поређења;
 - Нема преписивања коначне одлуке биометријског система Да/Не: Излаз БЕ алгоритма је 128-бит (или дужи) дигитални кључ, насупрот бинарне одлуке Да/Не.

Најбољи резултати код тестираних биометрика има се код дужице (*iris*) ($FRR=0.47\%$, $FAR=0$) при генерисању 140-битног кључа. Ово су занемарљиво веће грешке него код обичног биометријског система који користи дужицу. Код употребе отиска прста има се приметљива деградација у тачности у односу на класичан АФИС²⁵ што је разумљиво пошто је слика отиска прста више подложна дисторзији и другим факторима који смањују тачност. Системи препознавање преко лица су значајно побољшали своју тачност последњих година. Philips Research су направили први БЕ систем који ради са лицем као биометријском карактеристиком. Публиковане грешке су $FRR=3.5\%$ за базу са малим варијабилитетом међу сликама, до $FRR=35\%$ где је у бази велики варијабилитет. $FAR=0$ у оба случаја. Дужина коришћеног кључа је 58 бита што је довољно за замену лозинке. Систем су назвали privIDTM, и део је EU 3D Face пројекта (WP2.5)²⁶.

Иако биометријски системи енкрипције нису широко распрострањени и још су у фази истраживања²⁷, они нуде неке погодности за многе апликације [23]. Највећа предност је можда за мобилне апликације нпр. за мобилне телефоне, лаптоп рачунаре,

²⁵ Automatic Fingerprint Identification System

²⁶ www.3Dface.org Пробни рад на аеродрому у Salzburg-u

²⁷ Turbine (TrUsted Revocable Biometric IdeNtitiEs), www.turbine-project.org биометријска енкрипција заснована на отисцима прстију

или за биометријска идентификациона документа. Друга важна примена је за контролу приступа дигиталним подацима, са нагласком на очувању *copyright* права. Коначно, биометријска енкрипција ће помоћи при разматрању питања приватности са аспекта коришћења биометријске технологије [21, 23, 25].

6. ЗАКЉУЧАК

Налазимо се у добу када је практично постало немогуће не користити информационо комуникациону технологију у неком аспекту живота и рада. При томе је проблем поузданог утврђивања идентитета увео на велика врата употребу биометријских система, а да се при томе није довољно водило рачуна о могућим нежељеним последицама које прате увођење сваке нове технологије.

Како неможемо рећи да постоји систем који је немогуће преварити, а обзиром на изузетан значај који имају информације (поготово личне и приватне) које круже у тзв. дигиталном свету, разумљива је бојазан да те информације могу бити злоупотребљене. Постоји и додатна опасност од компромитације биометријских података пошто су они по својој природи јединствени идентификатор који се не може поништити или заменити, а помоћу којих је могуће повезати личне информације из различитих база и апликација. Сама употреба биометријских система представља опасност по приватност појединца, пошто онемогућава анонимност.

Зато се истражује могућност комбиновања биометријских система и криптолошких техника ради обезбеђивања највећег могућег степена безбедности података, али и заштите приватности. Технологија Биометријске Енкрипције је област у којој истраживања дају значајне резултате, развијају се разни прототипи чак и комерцијалне апликације. БЕ је пример технологије која у себе инкорпорира основне принципе заштите података и приватности, више него било које друго биометријско решење.

ЛИТЕРАТУРА

1. Adler A., 'Sample images can be independently restored from face recognition templates', in Proc.Can.Conf. Elec.Comp.Eng., pp.1163–1166, 2003
2. Adler A., 'Vulnerabilities in biometric encryption systems', in Proceedings Audio-andVideo-based Biometric PersonAuthentication (AVBPA2005),RyeBrook,NewYork. LNCS, vol. 3546, pp.1100–1109. Springer,Berlin, 2005
3. Cavoukian Ann, Stoianov Alex,'Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy', IPC Publication, 2007 <http://www.ipc.on.ca/images/Resources/bio-encryp.pdf>
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Changes made by Directive 2006/24/EC

5. Feng J., Jain A.K., 'FM Model based Fingerprint Reconstruction from Minutiae Template', in Proceedings ICB 09, LNCS: Advances in Biometrics, Vol. 5558/2009, pp. 544–553, 2009
6. Gunsel B., Uludag U., and Tekalp A.M., 'Robust Watermarking of Fingerprint Images', Pattern Recognition, Vol 35(12), pp. 2739–2748, 2002
7. Hill C.J., 'Risk of masquerade arising from the storage of biometrics', B.S. Thesis, Australian national University, 2001 <http://chris.fornax.net/biometrics.html>
8. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF>
9. <http://www.giac.org/resources/whitepaper/access/2.php>
10. Jain A.K., Bolle R., and Pankanti S. (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic. New York, 1999
11. Jain A.K., Uludag U., 'Hiding Biometric Data', IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol 25(11), pp. 1494–1498, 2003
12. Mallow Chrisopher, 'Authentication Methods and Techinques', SANS Institute, 2007
13. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S., 'Impact of Artificial Gummy Fingers on Fingerprint Systems', in Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275–89, 2002
14. Muhammad Khurram Khan, Jiashu Zhang, and Lei Tian, 'Protecting Biometric Data for Personal Identification', in S.Z. Li et al. (Eds.): Sinobiometrics 2004, LNCS 3338, pp. 629–638, 2004.
15. Prabhakar S., Pankanti S., Jain A.K., 'Biometric Recognition: Security and Privacy Concerns', IEEE Security & Privacy Magazine, Vol. 1, No.2, pp. 33–42, 2003
16. Rainer Plaga, 'Biometric keys: suitable use cases and achievable information content', Int. J. Inf. Secur., vol. 8, pp. 447–454, 2009
17. Ratha N.K, Connell J., Bolle R., 'Enhancing Security and Privacy in Biometrics-based Authentication Systems', IBM Systems Journal, Vol.40, No. 3, pp. 614–634, 2001
18. Schneier B, Ellison C., 'Ten Risk of PKI: What You' re Not Being Told About Public Key Infrastructure', Computer Security Journal, vol. 16 no. 1, pp.1–7, 2000
<http://www.schneier.com/paper-pki.pdf>
19. Schneier B., 'Inside Risks: The Uses and Abuses of Biometrics', Communications of the ACM, vol. 42, pp. 136, Aug. 1999
20. Soutar C. and Tomko G.J., 'Secure Private key generation Using a Fingerprint', in Proc. CardTech/SecurTech Conf., vol 1, pp. 245–252, 1996
21. Soutar C., Gilroy R., Stoianov A., 'Biometric System Performance and Security' in Conf. IEEE Auto. Identification Advanced Technol., 1999
http://www.bioscrypt.com/assets/security_soutar.pdf

22. Soutar C., Roberge D., Stoianov A., Gilroy R., Vijaya Kumar B.V.K., 'Biometric EncryptionTM using image processing', in Proceedings of SPIE, vol. 3314, pp. 178–188, 2009 <http://www.bioscrypt.com>
23. Tomko G., 'Privacy Implications of Biometrics - A Solution in Biometric Encryption', in 8th Ann. Conf. Computers, Freedom and Privacy, Austin, TX, USA, 1998
24. Uludag U., 'Finger minutiae attack system', in Proc. Biometrics Conference, Washington, D.C. USA, Sept. 2004
25. Uludag U., Pankanti S., Prabhakar S., Jain A.K., 'Biometric Cryptosystems: Issues and Challenges', in Proc. IEEE 92, pp. 948–960, 2004
26. Yeung M., Pankanti S., 'Verification Watermarks on Fingerprint Recognition and Retrieval', Journal of Electronic Imaging, vol. 9, no. 4, pp. 468–476, 2000
27. Поповић Бранкица, Ранђеловић Драган, 'Претње биометријским системима и претње од њих', ТЕХНИКА- Електротехника, 58 (1), стр.7–13, 2009

Popović Brankica¹, Randelović Dragan¹, Bandur Miloš²

¹Academy of Criminalistic and Police Studies, Cara Dušana 196, Belgrade, Serbia

brankica.popovic@kpa.edu.rs, dragan.randjelovic@kpa.edu.rs

² Faculty of Technical Sciences, Kneza Miloša 7, K. Mitrovica, Serbia, bandjo@ptt.rs

PRIVACY AND SECURITY CHALLENGES IN DEPLOYING BIOMETRICS

Abstract: Rapid progress of ICT and biometric technologies and their expanded use is the characteristic of modern society, but they are raising specific concerns concerning personal data protection and privacy. Today biometric is not regarded as Privacy-Enhancing Technology. There are intensive researches in area of combining biometrics and cryptology where are expected to gain more privacy friendly solutions for identity management systems. In this paper some possibilities and vulnerabilities of biometric systems are shown, as well as the mechanisms (cryptographic) which can enhance their performance regarding privacy and security aspect. New technology named Biometric Encryption is described.

Keywords: Biometric Systems, Encryption, Data protection, Privacy