UDC: 004.4:621.39 Info M: str. 48-54

SVEOBUHVATNI PREGLED I KOMPARACIJA SAVREMENIH KORISNIČKIH AUTENTIFIKACIONIH METODA ZA MOBILNE UREĐAJE
A COMPREHENSIVE OVERVIEW AND COMPARISON OF CONTEMPORARY USER AUTHENTICATION METHODS FOR MOBILE DEVICES

Dragan Korać
(University of Belgrade, korac@teol.net)

REZIME: Tokom proteklih nekoliko godina, snažni razvoj mobilnih tehnologija uslovio je stvaranje novih izazova u pogledu autentifikacionih metoda namijenjenih za mobilne uređaje. Perfomanse, pristupačnost i sposobnost konekcije mobilnih uređaja u različitim komunikacionim kanalima stvorili su uslove za primjenu različitih oblika mobilnih autentifikacionih metoda. Međutim, uvidom u dostupnu literaturu može se zaključiti da je ovo istraživačko polje ne dovoljno istraženo po dubini odnosno da ne postoji rad koji obezbjeđuje sveobuhvatni pregled, klasifikaciju i komparaciju savremenih korisničkih autentifikacionih metoda namjenjenih za mobilne uređaje. Stoga, ovaj rad daje sveobuhvatni pregled, klasifikaciju i komparaciju savremenih mobilnih autentifikacija zasnovanih na ključnim korisničkim parametrima kao što su zaštita, upotrebljivost i privatnost. Njihove prednosti i nedostaci su detaljno naglašene. Na osnovu izvršene komparativne analize mobilnih autentifikacionih metoda nekoliko važnih izazova je identifikovano. Jedan od njih je da do sada ne postoji "najbolji" šablon za mobilne autentifikacije. Takođe, ovaj rad daje prijedlog razvoja novog alata u savremenim korisničkim autentifikacionim metodama namjenjenim za mobilne uređaje. Takav alat može biti upotrebljen za stvaranje "najboljeg" šablona kao i za procjenjivanje i dizajniranje mobilnih autentifikacionih rješenja. Na kraju, u cilju pomoći razvoja jake mobilne autentifikacije predložen je i alternativni prijedlog jake mobilne autentifikacije kao adekvatan odgovor na buduće autentifikacione izazove.
KLJUČNE REČI: mobilni uređaj, savremene mobilne autentifikacije, jaka autentifikacija i biometrija
ABSTRACT: Over the past few years, the strength development mobile technologies are creating new challenges with regards to mobile authentication methods. Performance, availability and ability of mobile devices to connect to different communication channels have created conditions for applying various forms of the mobile authentication methods. However, from available literature can be concluded that this is research field immature and insufficiently explored in depth respectively that there is no paper which provides a comprehensive overview, classification and comparison of contemporary user authentication methods intended for mobile devices. Therefore, this paper gives a comprehensive overview, classification and comparison of contemporary mobile authentication basad on the key users parameters such as security, usability and privacy. Their advantages and disadvantages are emphasised in detail. On basis of performed comparative analysis of mobile authentication methods several important authentication challenges are identified. One of these is that there is no "the best" template for mobile authentication so far. Also, this paper gives proposal the development a new tool in contemporary user authentication methods intended for mobile devices. Such tool can be used for making "the best" template as wel as for evaluating and designing mobile authentication solutions. Finally, in order to help develop strong mobile authentication, this paper suggests an alternative proposition which would enable the development of strong mobile authentication as an adequate answer for future authentication challenges.
KEY WORDS: mobile device, contemporary mobile authentication, strong authentication and biometrics.

1. UVOD

Trend ubrzanog tehnološkog progresa mobilnih tehnologija uslovio je da su mobilni uređaji postali neodvojivi dio ljudskog života. Oni danas predstavljaju suštinske multifunkcionalne alate koji su postali mnogo više od pukog sredstva za komunikaciju. U svijetu povećane interkonekcije, rapidno je povećano uzjamno međudejstvo između uređaja i ljudi [1]. Mobilni uređaji su popularnost i atraktivnost stekli u posljednjoj deceniji zahvaljujući ogromnom razvoju u polju bežičnih mreža i softverskih i hardverskih kapaciteta. Sa eksponencijalnim tehnološkim razvojem mobilni uređaji (mobile phones, personal digital assistants – PDA, etc.) su oplemenjeni sa mnogim funkcijama koje korisniku pružaju neslućene mogućnosti. Sa povećanjem novih funkcija mobilni uređaji zahtijevaju i potrebu za većom zaštitom posebno za aplikacije u postupcima plaćanja [2] ili osjetljivih informacija [3]. Perfomanse mobilnih telefona u vidu moćnog procesora i malih dimenzija učinili su ga "džepnim" komjuterom prihvatljivim i primjenjivim u mnogim privatnim i poslovnim aplikacijama. Ipak, vrijednost pohranjenih informacija na mobilnim uređajima je nemjerljiva u poređenju sa vrijednošću samog mobilnog uređaja.

Posebno, poslednjih nekoliko godina sa razvojem novih smart tehnologija mobilni uređaji sve više svojim karakteristikama i funkcijama podsjećaju na personalne računare – PC, ali u aspektu sigurnosti i zaštite informacija značajno zaostaju u odnosu na PC [4, 5]. Da bi se obezbijedila adekvatna zaštita personalnih informacija u mobilnom autentifikacionom području neophodno je sagledati sve relevantne faktore koji se javljaju u tim procesima. Jedan od osnovnih i učestalih faktora je taj što su tradicionalni mobilni autentifikacioni mehanizmi fokusirani isključivo na zaštitni interes definisan u polju zaštitnog inženjeringa. To podrazumijeva da je često visok nivo zaštite, kao ključni faktor, preporučen i primijenjen bez ozbiljnih korisničkih razmatranja i uzimanja u obzir korisničkih potreba. Takođe, potrebno je posebno razmotriti adekvatno mobilno autentifikaciono rješenje iz perspektive upotrebljivosti i skalabilnosti jer su one daleko najvažnije, važnije čak i od jakih autentifikacija podržanih kriptografskim i biometrijskim ključevima. Time se istinski postavlja pitanje korisničke upotrebljivosti u takvom mobilnom autentifikacionom okruženju. Faktor upotrebljivosti u mobilnom autentifikacionom rješenju je suštinski, važniji čak i od jakih mobilnih autentifikacija podržanih kriptografskim i biometrijskim ključevima. Pored faktora zaštite i upotrebljivosti

važnu ulogu prilikom razvoja odgrovarajućeg mobilnog autentifikacionog rješanja ima i faktor privatnosti. Upravo, u ovom radu su prema pomenutim izdiferenciranim ključnim faktorima izvršena komparacija mobilnih autentifikacionih tehnologija. U važnim djelatnostima kao što je bankarstvo potrebna su jaka mobilna autentifikaciona rješenja koja nije moguće realizovati ako nisu sistematično i argumentovano sagledane pojedinačne metode autentifikacije.

Kratki pregled ovog rada je sljedeći: sekcija dva opisuje definicije i prethodne radove. Sekcija tri opisuje savremene autentifikacione metode na mobilnim uređajima kao i njihove prednosti i nedostatke. Sekcija četiri daje komparaciju i buduća istraživanja. Na kraju, sekcija pet daje zaključke.

2. DEFINICIJE I PRETHODNI RADOVI

Kada govorimo o autentifikacionim metodama, korisno je dati neke osnovne definicije u pogledu ove teme. Prije svega, neophodno je istaći da procesu autentifikacije prethodi proces identifikacije [6]. Drugim rječima, proces autentifikacije logički nastupa po završetku procesa identifikacije. Radi se o potpuno dva različita, međusobno zavisna procesa koja idu u paru. Međutim, fokus ovog rada je na autentifikaciji kao primarnom procesu.

Prisutne su različitosti u definicijama i terminološkim odnosima pojmova autentifikacije, verifikacije i validacije. Dybkaer u radu [7] se bavi sa terminološkim poređenjem pojma i koncepta verifikacija i validacije. Takođe, Cofta u radu [8] navodi process verifikacije identiteta kao zbunjujući poznatu autentifikaciju, koja je dizajnirana da poveća pouzdanje u povezivanju između različitih identiteta. Može se zaključiti da pomenuti pojmovi suštinski predstavljaju sinonime koji daju odgovor na pitanje "Jesam li ja koji treba da budem?" [9].

U dostupnoj literature ne postoji univerzalna definicija pojma jaka autentifikacija. U ovom radu jaka autentifikacija je definisana kao složena autentifikacija koja podrazumijeva upotrebu najmanje dva ili više osnovnih autentifikacionih faktora (slika 1). Ako su u procesu jake mobilne autentifikacije upotrebljena dva/tri autentifikaciona faktora govorimo o dvostrukoj/trostrukoj, tj.višefaktorskoj autentifikaciji. U mobilnom autentifikacionom pristupu procesom jake mobilne autentifikacije ostvaruje se sinergijski pristup. Svaki od pojedinačnih faktora pri integraciji jake autentifikacije zadržava svoj izvorni oblik dodajući jedan novi nivo zaštite. Moć takvog autentifikacionog mobilnog mehanizma onemogućava napadaču pristup osjetljivim informacijama ako nije prošao sve nivoe odnosno sakupio sve potrebne kredencijale.

Slika 1. – *Jaki metod autentifikacije na mobilnom uređaju*

Brojni prethodni radovi su dali pregled različitih biometrijskih autentifikacija [10], [11], [12], [**13**], [14], i neki od njih Vapen, et al., u radu [14] ukazuju da ne postoji komparacija autentifikacionih metoda napravljena posebno za mobilne uređaje. Njihovi istraživački programi su naglasili važnost različitih komparacija autentifikacionih metoda zasnovanih na biometrijskim tehnikama, gdje je fokusiranje na posebna pitanja ili potraga na problem iz određene perspective. Na primjer Clarke and Furnell su u radu [10] predstavili rezultate poređenja perfomansi biometrijskih tehnika koji *The UK National Physical Laboratory* je vodio. Na osnovu prezentovanih rezultata moguće je zaključiti da su poređenje uradili na nekoliko biometrijskih tehnika čija je primjenjivost razmatrana prema mobilnim uređajima. Prema Sheeba, et al., u radu [13] daje se komparacija parametara za različite biometrijske tehnologije. Takođe, u radu [15] autori su dali opšti pregled mobilnih autentifikacija opisanog u manje detalja. Danas su u upotrebi brojna pojedinačna autentifikaciona rješenja sa kojim se ne postiže visok nivo zaštite identiteta i osjetljivih informacija. Svaki od pojedinačnih autentifikacionih rješenja ima, kako određene prednosti, tako i značajne nedostatke koji mogu biti neatraktivni za većinu servis provajdera – SP.

U ovom radu su izdiferencirani nedostaci i prednosti pojedinačnih tehnologija i metoda ključni za sagledavanje i razvoj jakih autentifikacionih rješenja. Međutim, u dostupnoj literature mi nismo dosada uspjeli pronaći bilo koju komparaciju savremenih autentifikacionih metoda namjenjenih za mobilne uređaje. Doprinosi ovog rada je taj što mi dajemo sveobuhvatni pregled i komparaciju savremenih korisničkih autentifikacionih metoda za mobilne uređaje zasnovane na percepciji autora. Stoga, glavni problem u ovom radu je usmjeren na opisivanje, pregled i poređenje metoda autentifikacije na mobilnim uređajima koji čine osnovu jakog metoda mobilne autentifikacije. Sa adekvatnim opisom i pregledom pojedinačnih metoda autentifikacije moguće je izvršiti pravilnu procjenu koji postojeći autentifikacioni mehanizmi mogu biti primjenjivi za integraciju u novo jako autentifikaciono rješenje zasnovano na mobilnim uređajima. Drugi doprinosi ovog rada uključuju i prijedlog izrade alata u savremenim korisničkim autentifikacionim metodama namjenjenim za mobilne uređaje sa kojim bi bilo moguće stvoriti "najbolji" šablon, i izvršiti procijenu i dizajniranje mobilnih autentifikacionih rješenja.

3. SAVREMENE AUTENTIFIKACIONE METODE NA MOBILNIM UREĐAJIMA

Poslednjih godina sa razvojem smart mobilnih tehnologija omogućena je primjena gotovo svih autentifikacionih tehnologija koje su do skora smatrane privilegovanim samo za autentifikaciju putem tradicionalnih PC. Autentifikacione metode na mobilnim uređajima su složene metode koje obuhvataju nekoliko naučnih oblasti obično podijeljenih u tri glavna područja: *na nečemu što znaš* – lozinka, *na nečemu što imaš – token*, i *na nečemu što jesi – biometrija*.

3.1. *Passcodes*

Passcodess je opšti termin koji uključuje personal identification numbers – PIN, alfanumerički password i druge grafičke lozinke [16].

Password je autentifikacioni metod koji se zasniva na ljudskim sposobnostima da zapamti određenu jedinstvenu kombinaciju alfanumeričkog ili grafičkog zapisa. Uzimajući u obzir ograničene ljudske sposobnosti pamćenja ovaj autentifikacioni metod u poređenju sa svim ostalim mobilnim autentifikacionim metodama se svrstava u najnesigurnije mehanizme. Svakako, da veća upotreba lozinki i sposobnost ljudskog pamćenja su ograničavajući faktori koji često korisnika iz praktičnih razloga naginju na upotrebu prostih lozinki. Takođe, korisnici koji imaju više naloga pribjegavaju korišćenju iste lozinke za višestruke naloge. Neophodno je istaći da i jake lozinke primoravaju korisnika na zapisivanje poput ljepljivog podsjetnika, koji lijepe na vidnim mjestima, a iste mogu biti kompromitovane ili izložene drugim metodama napada poput napadi rječnikom i napadi grubom silom ili iscrpljivanjem.

Brojni su dobro poznati nedostaci ovog mobilnog autentifikacionog metoda u kojem prednjači teška pamtljvost, česta upotrebljivost korišćenih lozinki, mogućnost inficiranja malicioznim programima mobilnih uređaja, poteškoće pri preciznom unosu lozinke na malom osjetljivom ekranu tastaure, ponavljajuće greške unosa mogu rezultirati zaključavanjem naloga koji zahtijevaju da bude resetovan bez odlaganja, unošenje brojeva i punktuacijskih znakova zahtjeva promjenu tastature i sl. Nasuprot nedostacima, jednostavnost, cijena (besplatne), praktičnost i pogodnost ovu nezgrapnu metodu svrstava u najčešće korišćenu autentifikacionu metodu na veb sajtovima. U slučaju kompromitovanja lozinke su zamjenljive i lake za resetovanje. Mnoge grafičke lozinke su predložene kao dio mobilnog autentifikacionog rješenja u kome se nastoji postići prevazilaženje nedostataka navedenih tekstualnih password-a. Prednosti ovog mobilnog autentifikacionog metoda u odnosu na PIN ili tekstualne lozinke što su mnogo lakše za pamćenje i ne prisiljavaju korisnika da ukucava lozinku na maloj tastaturi mobilnog uređaja. U dodatku, pristup upotrebe grafičkih lozinki mnoge korisnike čini zadovoljnim.

Personal identification number – PIN je autentifikacioni metod koji spadaju najčešće korišćene mobilne metode u postupku zaključavanja mobilnih uređaja. Predstavlja prvi i osnovni sloj zaštite personalnih informacije pohranjene na SIM (*engl.subscriber identity module*) kartici mobilnog uređaja. Opšta varijanta sastoji se najčešće iz 4-digitalna koda koja se unose putem tastature. Dužina od 4-digitalna koda spada u proste password-e koji predstavljaju lak plijen za napadi rječnikom i napadi grubom silom, ali koji su gotovo neupotrebljivi u ovom mobilnom autentifikacionom metodu. Naime, nekoliko pogrešnih pokušaja pristupa mobilnom uređaju uzrokovaće automatsko zaključavanje kartice čineći je potpuno beskorisnom. Prema Clarke, et al., trenutna upotreba autentifikacione metode zasnovan na PIN-u je problematičan, i oni u radu [10]. navode da je preko 83% je voljno da prihvati neki oblik od biometrijskih autentifikacija na svojim uređajima.

3.2. *Token*

U mobilnom autentifikacionom metodu token predstavlja sam mobilni uređaj. Ovaj metod obezbjeđuje viši nivo zaštite u odnosu na prethodni. Prednosti ovog metoda su što većina ljudi već posjeduje neki mobilni uređaj što značajno smanjenje cijenu proizvodnje i održavanja token uređaja. Token uređaji sami po sebi predstavljaju teret i za korisnika i za organizaciju, za razliku od mobilnog uređaja o kojem korisnik svakodnevno brine. Takođe, mobilni uređaj ima komunikacione i računarske sposobnosti koje dopuštaju autautomatizaciju autentifikacionih procesa, oslobađajući korisnika tog tereta, a postoje i dobri zaštitni mehanizmi izgrađeni na GSM sistemu koji mogu biti eksploatisani. Drugim rječima, prednosti su u tome što mobilni uređaji koriste višestruke komunikacione kanale čime se dodatno povećava nivo zaštita u autentifikacionom području. Na taj način napadač se primorava na potpunu kontrolu svih komunikacionih kanala prilikom izvršenja napada. Nasuprot prednostima, mane ovog metoda su visoka ranjivost prema krađi i česta pozajmljivanja i oštećenjima, kompromitovanja ili gubljenju kao i tehnička ograničenja u računanju, memoriji, vijeku baterije i mrežnim performansama.

Mobilni autentifikacioni metod zasnovan na tokenu javlja se u softverskom i hardverskom formatu. Hardverski token je mobilni uređaj koji putem SMS ostvaraju proces autentifikacije - *metoda one time password – OTP*. Na SIM kartici mobilnog uređaja – token (mobilni telefon) mogu biti pohranjeni kriptografski ili biometrijski ključevi. Softverski mobilni token zahtijeva od korisnika da na mobilnom uređaju instaliraju softver putem kojeg generiše lozinku za autentifikaciju – *metod OTP korišćenjem SMS.*

A one time pasword – OTP je dvostruki mobilni autentifikacioni metod koji korisnik generiše na mobilnom uređaju bez konekcije klijent – server. Mobilni uređaj djeluje kao token i koristi određene kredencijale stvarajući lokalni OTP. Da bi server djelovao sinhronizovano i izvršio komparaciju lozinki dostavljenih od strane klijenta neophodno je da isti posjeduje sve identifikatore kako bi mogao generisati istu lozinku. Lozinku klijent može podnijeti onlajn ili putem uređaja kao što je bankomat.

A one time pasword – OTP korišćenjem SMS je dvostruki mobilni autentifikacioni metod u kojem korisnik zahtijeva od servera da umjesto njega genriše vrijednost OTP. Ovaj metod zasniva se na principu da korisnik putem SMS poruke šalje serveru svoje kredencijale. Server provjerava sadržaj SMS poruke i ukoliko je potvrđena ispravnost, na bazi tih kredencijala generše OTP koji odmah putem poruke vraća korisniku. Svakako, korisniku se ostavlja dovoljno vremena za upotrebu OTP prije njenog isteka. Lozinka ovog tipa je prilično kratka, vremenski ograničena samo za jednu sesiju. Nedostaci ovog metoda su što imaju ograničenu entropiju, mogu biti opservirani ili presretnuti, ostaju validni samo kratki vremenski period [17], i zahtijevaju plaćanje SMS usluga kako za SP tako i za korisnke. Postoji nedostatak i u pogledu hardverskog ograničenja mobilnih telefona jer mnogi posebno stari mobilni telefoni ne podržavaju pokretanje više aplikacija u isto vrijeme. Prosto rečeno, mobilni telefon ne podržava istovremeno

slanje poruke i mogućnost da ima otvorenu aplikaciju veb pretraživača, što ukazuje da zatvoren veb pretraživač čini beskorisnim SMS. Najvažnije prednosti ovog metoda su dostupnost praktično za svakoga, nenarušavanje privatnosti i ne zahtijeva dodatni hardver ili instaliranje softvera čak i pri promjeni SIM kartice. Isto tako, ne zahtijeva primjenu novih tehnogija prije svega smart tehnologija. Veoma je jednostavan i lak za razumijevanje iz korisničke perspektive. Upotreba ovog autentifikacionog metoda je alternativa ukoliko server i klijent ne djeluju sinhronizovano. Primjena ovog autentifikacionog metoda je u mnogim sistemima (e-bankarstvu).

Mobilni sertifikat je mobilni autentifikacioni metod zasnovan na javnim ključevima infrastrukture – PKI i ključevima i sertifikatima pohranjenim na korisničkoj personalnoj SIM kartici. Sertifikat sadrži jedinstvene identifikatore broj socijalnog osiguranja sa personalnim detaljima ime, datum rođenja, pol, nacionalnost i slično. Funkcionisanje autentifikacionog metoda zasnovanog na mobilnim sertifikatima uslovljeno je poznavanjem korisnički broja mobilnog telefona od strane SP. Proces se zasniva da SP koji kada autentifikuje korisnika na osnovu unijetih kredencijala traži provjeru istog od strane operatora mobilnog telefona (sertifikatora autoriteta – CA). Po prijemu zahtjeva CA šalje autentifikacioni zahtijev prema korisniku radi utvrđivanja verifikacije korisničkog mobilnog telefona. Tada korisnik unosi PIN broj koji se zove SPIN koji otključava tajni ključ pohranjen na SIM kartici sa kojim korisnik potpisuje zahtijevni izazov. Na osnovu potpisa CA vrši provjeru da li zahtijevani izazov bio potpisan sa pravim tajnim ključem ili ne, i o tome obavještava SP. Prednosti ovog autentifikacionog metoda je taj što su lakše razumljivi iz korisničke perspektive, te omogućavaju upotrebu mobilnog sertifikata za vrijeme trajanja telefonskog poziva. Mana ovog autentifikacionog metoda je u cijeni jer zahtijevaju od učesnika u komunikacionom procesu (SP i korisnika) da plaćaju usluge servisa. Takođe, moguće je da servis bude upotrebljen isključivo mobilnim telefonom što dovodi do preblema nemogućnosti pokretanja više aplikacija u isto vrijeme koji karakterišu metod zasnovan na SMS – OTP.

Near field communication – NFC je tehnologija koji dopušta mobilnom telefonu funkciju kao što je čitač pametnih kartica. NFC je bežična komunikaciona tehnologija kratkog dometa zasnovana na radio frekventnoj identifikaciji – RFID. Sa NFC čipom mobilni telefoni mogu djelovati kao čitači, primjera radi kreditne kartice mogu biti upotrebljene putem mobilnog telefona. Prednosti ovog metoda je što mobilni uređaji mogu biti korišćeni za zamjenu fizičkih ključeva i bonus kartica. Posebna primjena ove tehnologije je u integrisanju sa biometrijskim metodama kao što je fingerprint. NFC tehnologija svojim pozitivnim stranama nadograđuje postojeće biometrijske tehnologije stvarajući sinergijski pristup. Sa druge strane, mane su prije svega u nedovoljnoj upotrebljivosti, zaštiti i privatnosti.

3.3. *Biometrija*

Svjedoci smo da posljednih godina biometrija snažno utire put u mobilnim autentifikacionim metodama. Ključni razlog za uvođenje biometrije u mobilne autentifikacione procese predstavlja zaštita [18]. Autentifikacioni metod zasnovan na biometriji obezbjeđuje najviši nivo zaštite, koji eliminiše nedostatke prethodnih metoda. Biometrijska autentifikacija je automatski metod prepoznavanja ličnosti koja koristi pojedinačne biometrijske crte poput fizioloških karakteristika kao što su iris, lice, otisak prsta, geometrija dlana, retina, vene, i druge fizičke karakteristike kao što su glas, potpis, dinamika kucanja i sl. Osnovna biometrijska svojstva korišćena u autentifikacionim procesima su univerzalnost, razlikovanje, trajnost, prikupljivost, učinkovitost, prihvatljivost i mogućnost zaobilaženja [Maltoni et al.,]. Razlikujemo unimodalni i multimodalni sistem. Unimodalni u procesu autentifikacije koristi jednu biometrijsku metodu, dok multimodalni koristi više biometrijskih metoda u autentifikacionim procesima. Unimodalni biometrijski sistemi, pored povoljnosti i jednostavnosti nisu savršeni i trpe nekoliko praktičnih problema poput neuniverzalnost, bučnost senzora, unutrašnja klasna varijacija, ograničeni stepeni slobode, neprihvatljiva stopa greške, pogreške pri upisu, i spuf napadi [12]. Savladavanje unimodalnih biometrijskih nedostataka postiže se primjenom multimodalnih biometrijskih tehnika. Prednosti biometrije u odnosu na sve druge metode su u brzini, jednostavnosti sistema i nivou pružene zaštite. Biometrija koristi kredencijale koji se ne mogu zamijeniti, ukrasti, zaboraviti ili izgubiti. Sa druge strane, glavni nedostatak biometrije ogleda se u pitanju privatnosti kao i njene nepromijenjivosti za fizički oštećena lica.

Fingerprint je autentifikacioni metod koji se zasniva na upoređivanju minutiae (grebenova, bifurkacija, ili ostrva na prstu) koje su stečene korišćenjem senzora čitača otiska prsta [19]. Otisak prsta je jedan od najpopularnih i prihvatljivih biometrijskih tipova [20]. Posebnu popularnost ovog metoda podigao je Apple sa izdavanjem novog modela smart telefona 5S koji po prvi put ima ugrađen čitač otiska prsta [21]. Ovaj inovativni čitač prsta koristi tehnologiju radio talasa koji detektuju subepidermalne slojeve korisničke kože, zahtijevajući "živi prst" korisnika u trenutku logovanja. Na ovaj način savladava se najveći nedostatak prethodnih metoda otiska prsta, a to je mogućnost kopiranja poput želatina ili nasilne amputacije prsta. Međutim, bitno je napomenuti da i inovativni čitač prsta ima određene nedostatke koji i pored svih navedenih prednosti ipak omogućavaju napadaču da izvrši kopiranje kredencijala. Prednosti ovog metoda su pouzdan rad, brzina, tačnost i čitljivost za 360-stepeni sa slikom dobrog kvaliteta. Najveći nedostatak ovog modela je u nakupljanju prašine i nečistoće i znoja kao i drugih tečnosti na dodirnim površinama mobilnog uređaja i prsta. Trenutna primjena je u korisničkom otključavanju mobilnog uređaja. Ovaj inovativni autentifikacioni metod je zamjena password-u.

Voice/Speech je mobilni autentifikacioni metod koji se isključivo oslanja na karakteristike glasa/govora. Ovakav metod zahtijeva da korisnik pri autentifikaciji izgovori neku frazu koje se upoređuju sa pohranjenim uzorkom. Mobilni atentifikacioni metod glasa usmjereni su na spoznaji ko govori, dok je prepoznavanje govora u velikoj mjeri usmjereno na prepoznavanju riječi odnosno fraza nezavisno ko govori [22]. Metoda

mobilne autentifikacije korišćenjem glasa analizira akustične karakteristike govornika kao što su ton i fonetika. Prednosti ovog metoda su u cijeni, prihvatljivosti i nenametljivosti za korisnika. Nedostatak ovakvog metoda je u podložnosti prevarama u vidu snimanja glasa legitimnog korisnika koji se kasnije može reprodukovati pri mobilnoj autentifikaciji. Takođe, nedostaci ovog metoda su u promjenjivosti korisničke boje glasa koja može biti uzrokovana objektivnim i neobjektivnim korisničkim problemima. Objektivni korisnički problemi su u vidu, bolesti, promuklosti, prehlade i raspoloženja korisnika (pjevanjem ili glasnim pričanjem). Neobjektivni korisniči problemi su bučnost pozadine, dob korisnika i promjenjivosti boje glasa u jutarnjim u odnosu na podnevne ili večernje sate. Poboljšanje verzije ovog metoda postiže se sa uvođenjem određene vrste pitanja za korisnika od strane sistema.

Face je mobilni autentifikacioni metod koji omogućava prepoznavanje ličnosti putem lica Zasniva se na opštom principu uzimanje korisničke slike lica posredstvom kamere mobilnog uređaja. Potom se vrši izdvajanje karakterističnih tačaka na licu i matrično poređenje sa ranije stečenim uzorkom pohranjenim u bazi podataka. Na osnovu tih poređenja odgovor može biti verifikujući ili odbijajući. Međutim, poput drugih mobilnih autentifikacionih metoda i ova metoda pokazuju određene nedostatke, prije svih u cijeni. U postupku uzimanje slike lica mnogo je faktora koji mogu uzrokovati nepodudarnost slike. Na primjer, odstupanja od pozicije uzimanja slike, ugla kamere pri snimanju, količine svijetlosti koja padne na lice, i promjena ugla gledanja u kameru i sl. Moguće zloupotrebe ove metode su u maskiranju lica [20], kao i problemima sa promijenjivosti lica uzrokovanim biološkim procesom starenja, nošenja brade ili naočara, promjena frizure, šminke izraza lica i brade. Stoga, 2D metode imaju visoku stopu jednakog udjela pogreške – EER (engl. *equal error rate*).

Iris je mobilni autentifikacioni metod veoma sličan licu, koji omogućava prepoznavanje ličnosti putem irisa. Iris biometrija koristi prezentovanje tekstualne podloge irisa kao sredstva da verifikuje identitet ličnosti [23]. Metod prepoznavanja irisa se zasniva na opštom principu uzimanje korisničke slike irisa posredstvom kamere mobilnog uređaja. Proces se zasniva na izdvajanju karakterističnih tačaka na irisu i matrično poređenje sa ranije stečenim uzorkom pohranjenim u bazi podataka. Na osnovu tih poređenja odgovor može biti verifikujući ili odbijajući. Zbog jedinstvenih karakteritika kao što su vremenski nepromjenjivost za svaku osobu, genetska ne zavisnost i brzine raspadanja nakon smrti, iris je gotovo nemoguće zloupotrijebiti. Nizak EER je svrstava među najbolje mobilne autentifikacione metode. Nedostatak ovog metoda je velika složenost matričnog algoritama, skupoća mobilnih uređaja koji zahtijevaju kameru izuzetno visoke rezolucije. Takođe, kao i kod metoda lica isti uzroci mogu uticati na nepodarnost irisa. Za razliku od autentifikacionog metoda zasnovan na prepoznavanju lica, ovaj metod zbog svoje složenosti spada u obećavajuću mobilnu autentifikacionu metodu.

Keystroke Dynamics je mobilni autentifikacioni metod zasnovan na korisničkom jedinstvenom načinu kucanja na tastaturi definisan vremenskom sekvencom. Prednosti ovog metoda su što istovremeno omogućava proces autentifikacije korisnika i kontinuirano prati dinamiku kucanja. Ovaj metod može biti klasifikovan kao statički ili kontinuirani [24]. Statički se odnosi na analizu dinamike kucanja izvršene u određenom vremenskom intervalu npr. proces logovanja, dok se kontinuirani odnosi na analizu kucanja izvršenu neprekidno za vrijeme cijele sesije, obezbijeđujući na taj način alat za otkrivanje zamjene korisnika nakon uspješnog logovanja [25]. Nedostaci ovog metoda su što dinamika kucanja predstavlja naučenu tehniku koja je promijenjivog karaktera i vrlo je nezgrapan zbog male tastature na mobilnom uređaju. Takođe, ovaj metod ima dodatni problem sa mobilnim uređajima koji posjeduju meki metod unosa poput osjetljivih ekrana.

Gait recognition je mobilni autentifikacioni metod koji dopušta automatsku verifikaciju identiteta ličnosti pri njegovom hodu. Javlja se u tri različita formata *Mashine Vision* [27], [26], *floor sensor* [28] i *wearable sensor* – WR [29]. Princip ovog metoda zasniva se da korisnik nosi oko struka, u džepu ili na cipelama pokretni snimajući senzor na osnovu kojeg se autentifikuje korisnik. WR može biti akcelerometar (mjeri akceleraciju), žiro senzor (mjeri rotaciju i broj stepeni po drugoj rotaciji), senzor sile (mjeri silu pri hodu) i tako dalje [28]. Glavna prednost ovog metoda je što omogućava nenametljivi autentifikacioni metod za mobilne uređaje koji već sadrže akcelerometar (poput mobilnih telefona, PDA i sl.) i popravlja daleko najgoru prepoznavajuću stopu. Mana ovog metoda je u cijeni nabavke senzora i nametljivosti za korisnik u vidu obaveznog nošenja senzora.

4. KOMPARACIJA I BUDUĆA ISTRAŽIVANJA

U Tabeli 1 komparativno su prikazane različite mobilne autentifikacione metode prema izdiferenciranim ključnim karakteristikama kao što su zaštita, upotrebljivost i privatnost.

Zaštita je prvi i najznačajni faktor u svim mobilnim autentifikacionim procesima, značajan kako za korisnika tako i za SP-e. Zaštita podrazumijeva skup metoda, tehnika i aktivnosti koje imaju za cilj viši nivo sigurnosti. Zaštita zahtijeva opsežan i integrisan mobilni autentifikacioni pristup, koji treba da podržava poslovne ciljeve ili misiju organizacije.

Upotrebljivost je faktor koji nije ništa manje važan od faktora zaštite. Podrazumijeva mobilnu autentifikaciju oblikovanu u razumljivoj formi za korisnika. Postizanjem dobre upotrebljivosti je posebno izazov za male mobilne uređaje. Veliki broj različitih mobilnih uređaja čije su sve operacije pomalo različite, čine ovo još više izazovnijim. Upotrebljivost čini autentifikacioni sistem jednostavnim i lakšim za upotrebu smanjujući barijere za usvajanje.

Privatnost je ograničavajući faktor u sprečavanju narušavanja korisničke autonomije i slobode u prihvatanju mobilnih autentifikacionih metoda.Obezbijeđivanje najvišeg nivoa privatnosti postiže se upotrebom anonimnosti i pseudonimnosti.

Neophodno je istaći da je organizacija ta koja određuje podobnost odabira nekog mobilnog autentifikacionog rješenja na osnovu balansiranja:

- cijene zaštite naspram vrijednosti imovine koju štite,
- vjerovatnoće naspram mogućnosti, i
- poslovne potrebe naspram zaštitnih potreba.

Svako odabrano mobilno autentifikaciono rješenje treba da odgovara misiji i ciljevima organizacije. Pojedinačne mobilne autentifikacione metode namjenjene za mobilne uređaje su naizgled vrlo jednostavno ali su suštinski veoma kompleksne. Kompleksnost se javlja pri stvaranju jakog mobilnog autentifikacionog mehanizma. Kao što je u uvodu i pomenuto ranije, ne postoji rad koji bi dao jedinstveno "najbolje" šablonsko rješenje u mobilnim autentifikacionim pristupima. Na osnovu analize gore pomenutih podataka, prikazanih u Tabeli 1, odgovor i daje objašnjenje zašto to i nije bilo moguće postići takav šablon u autentifikacionom pristupu. Prije svega, karakteristike autentifikacionih metoda imaju različite korisničke vrijednosti posmatrane prema različitim karakteristikama. Na primjer, ako se uporede metode PIN-a i biometrije (fingerprint) metode prema izdiferenciranim ključnim karakteristikama sa korisničkim prioritetima prikazanim u Tabeli 1, PIN obezbjeđuje nizak nivo zaštite sa visokim nivoom upotrebe i privatnosti, naspram biometrije (fingerprint) koja obezbjeđuje visok nivo zaštite i nizak nivo upotrebe i privatnosti.

Tabela 1 – Komparacija različitih mobilnih autentifikacionih metoda zasnovanih na percepciji autora.

Karakteristike				Zaštita	Upotreba	Privatnost
NEŠTO ŠTO ZNAŠ		PASSCODES	PIN	Nizak	Visok	Visok
			Lozinka	Nizak	Visok	Visok
NEŠTO ŠTO IMAŠ		TOKEN	OTP	Srednji	Srednji	Visok
			OTP korišćenjem SMS	Srednji	Srednji	Visok
		PKI	Mobilni sertifikat	Srednji	Nizak	Srednji
		RFID	Polje bliske komunikacije - NFC	Srednji	Nizak	Srednji
NEŠTO ŠTO JESI	BIOMETRIJA	FIZIOLOŠKE	Otisak prsta	Visok	Nizak	Nizak
			Lice	Visok	Nizak	Nizak
			Iris	Visok	Nizak	Nizak
		FIZIČKE	Glas/Govor	Visok	Srednji	Nizak
			Dinamika kucanja	Visok	Srednji	Nizak
			Prepoznavanje koraka	Visok	Srednji	Nizak

Zaključak je da u u takvom autentifikacionom pristupu korišćenjem pojedinačnih metoda ne postiže maksimum korisničkih prioriteta. Stoga, u praksi pri stvaranju bilo kog autentifikacionog rješenja, ove metode su korišćene u kombinaciji sa drugim autentifikacionim metodama. Takođe pri dizajniranju jakog mobilnog autentifikacionog rješenja, postoje i drugi problemi kao što su sposobnosti – različite fizičke i mentalne sposobnosti, potrebe, godine, i znanja. Za izgradnju budućeg "najboljeg" rješenja potrebno je imati pristup prema svim tim problemima koji će se holistički rješavati. Za takav holistički pristup neophodno je listu korisničkih prioriteta dodatno proširiti kako bi se na jedinstven način obuhvatili i svi drugi važni korisnički prioriteti kao što su cijena, kompleksnost i dostupnost. Takvi korisnički prioriteti kod korisnika na najdirektniji način utiču na prihvatanje određenog mobilnog autentifikacionog rješenja. Na primjer, neko autentifikacione rješenje i pored najbolje autentifikacione zaštite kod korisnika u slučaju visoke cijene ili kompleksnosti može da bude neprihvaćeno.

Za buduća istraživanja ovaj rad daje prijedlog izrade novog alata sa kojim bi se omogućilo stvaranje "najboljeg" šablona. Sa takvim alatom moglo bi se izvršiti procijenjivanje i dizajniranje autentifikacionih rješenja. Međutim, potrebno je uzeti u obzir da su u komparativnoj Tabeli 1 identifikovanim korisničkim prioritetima dodijeljene deskriptivne ocjene a za izradu predloženog alata potrebno je iste dovesti u određeni relacioni odnos sa numeričkim vrijednostima. Za realizaciju ovog zadatka neophodno je buduće istraživačke pravce usmjeriti ka uvođenju funkcije pripadnosti gdje se deskriptivne ocjene mogu matematički izraziti stepenom pripadnosti koji ima vrijednost iz jediničnog intervala [0,1]. Na ovaj način može se zaključiti da sa postizanjem konkretnih numeričkih vrijednosti nekog autentifikacionog rješenja je moguće postići i njegovo praktično vrijednovanje.

5. ZAKLJUČCI

U ovom radu je dat opis, pregled, klasifikacija i komparacija najčešće korišćenih autentifikacionih tehnologija namjenjenih za mobilne uređaje, ali i one za koje se u narednom periodu može očekivati veća primjena. Iz dostupnih preglednih radova obezbijeđeni su podaci koji ukazuju na ubrzani trend pomjeranja granica tehnologija sa povećanom popularnošću i atraktivnošću mobilnih smart uređaja u autentifikacionim pristupima. Kroz ovaj pregled i komparaciju autentifikacionih metoda namjenjenih za mobilne uređaje nekoliko je stvari zaključeno prije prihvatanja bilo kog mobilnog autentifikacionog metoda. Prvo, ne postoji jedinstvena mobilna autentifikaciona tehnologija koja bi istovremeno obezbijedila maksimalni nivo zaštite i bila opšteprihvatljiva za sve korisnike. Ukoliko jedna mobilna autentifikaciona tehnologija ima nedostatke u određenom pravcu, u drugoj koja se pojavi kao korektura, obavezno se javljaju problemi druge prirode. Nesumnjivo, da rješenje sa kojim bi se ublažili nedostaci pojedinačnih tehnologija zahtijeva primjenu jakih mobilnih autentifikacija tj. kombinovanje više različitih mobilnih tehnika. Drugo, na osnovu izvršene analize autentifikacionih rješenja prikazanih u komparacionoj tabeli potpuno se jasno uočava sva složenost i kompleksnost pojma mobilnih autentifikacionih metoda, kao i mogućnosti različitih autentifikacionih pristupa.

Na osnovu činjenica prezentovanih u radu moguće je predložiti optimalan, robusan i pouzdan mobilan autentifikacioni pristup zasnovan na integrisanoj primjeni ključnih tehnologija upotrebom SIM kartice i inovativnih fizioloških biometrijskih tehnologija. Snaga ovakvih predloženih rješenja treba da ima dubok pozitivan uticaj ne samo sa aspekta povećanja nivoa zaštite već i upotrebljivosti primijenjivog na veliki broj korisnika različitih sposobnosti, umijeća, znanja i vještina. Organizacije će biti u mogućnosti da bolje štite sisteme i imovinu obezbijeđujući korisnicima fleksibilna mobilna autentifikaciona rješenja u kojima se ne zahtijeva upotreba dodatnih hardvera. Ovakva rješenja namjenjena su za organizacije koje u svom funkcionisanju zahtijevaju primjenu visokog nivoa zaštite, na primjer e-bankarstvo.

Na kraju, ovaj rad ima za cilj da otvori novi set pitanja za buduća istraživanja u kojima bi se napravio iskorak prema stvaranju novog alata sa kojim bi se stvorili preduslovi za stvaranje najboljeg šablona u mobilnim autentifikacijama, i koji bi takođe mogao biti korišćen za procjene i dizajniranja mobilnih autentifikacionih rješenja.

REFERENCES

[1] Patil P.S., Nimbhorkar S.U.: A Survey on Location Based Authentication Protocols For Mobile Devices. International Journal of Computer Science and Network, Vol 2, Issue 1, pp. 44-47, 2013.

[2] Simić D.: Elektronski sistemi plaćanja i zaštita. INFO M, Časopis za informacione tehnologije i multimedijalne sisteme, Београд, Бр. 15-16/2005., стр. 27-31., 2005.

[3] Angulo J., Wästlund E., Gullberg P., Kling D., Tavemark D., Fischer-Hübner S.: [Short Paper] Understanding the user experience of secure mobile online transactions in realistic contexts of use.Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13, Washington, DC, 2012.

[4] Asher N.B., H.Sieger, A.B.Oved, N.Kirschnick, J.Meyer & S.Moller. On the need for different security methods on mobile phones.Mobile HCI, Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, 465-473, New York, NY, USA, 2011.

[5] Polla M. L., Martinelli F., & Sgandurra D.: A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials, Vol. 15, Issue 1, pp. 446 – 471, Canada, 2013

[6] Bogićević M, Milenković I., Simić D., "Identity Management – A Survey", Chapter 19 in Monograph Innovative Management and Firm Performance¸ pg. 370-384, Palgrave Macmillan, July 2014.

[7] Dybkaer Rene´. 'Verification' versus 'validation': a terminological comparison. Accredition and Quality Assurence. Vol. 16. Issue 2. pp. 105-108, Springer-Verlag, 2011.

[8] Cofta Piotr. Towards a beter citizen identification system. Identity in the Information Society Volume 1, Issue 1 , pp. 39-53, Springer Netherlands, 2008.

[9] Gafurov D., Helkala K., and Søndrol T.: Biometric gait authentication using accelerometer sensor. Journal of Computers, Vol.1, no.7, pp.51–59, 2006.

[10] Clarke N.L., Furnell S.M.: Advanced user authentication for mobile devices. Computers & Security, vol.26, pp.109-119, Elsevier Advanced Technology, 2007.

[11] Clarke N.L., Furnell S.M.: Authentication of users on mobile telephones - a survey of attitudes and practices. Computers & Security, vol. 24, no.7, pp. 519 – 527, Elsevier Advanced Technology, 2005.

[12] Sheeba T. & Bernard M.J.: Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein. International Journal of Computer Applications (0975 – 8887), Vol. 51, No. 5. pp. 55-60, Foundation of Computer Science, USA 2012.

[13] Coskun V., Ozdenizci B. & Ok K.: A Survey on Near Field Communication (NFC) Technology. Wireless Personal Communications, Volume 71, Issue 3, pp. 2259-2294, Springer US, 2013.

[14] Vapen Anna and Shahmehri Nahid: Security levels for Web Authentication using Mobile Phones. Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology. Series Volume 352. pp. 130-143, Springer Berlin Heidelberg, 2011.

[15] Korać, D., Simić, D.: A Survey of Authentication Methods on Mobile Devices. Proceedings of the 2013 international conference on ICT Conference and Exibition, Aranđelovac, InfoTech 2013.

[16] Wiedenbeck S., Waters J., Sobrado L., and Birget J.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on advanced visual interfaces, ACM, pp. 177–184, New York, NY, USA, 2006.

[17] Corella F., Lewison K., A Comprehensive Approach to Cryptographic and Biometric Authentication from a Mobile Perspective. 2013. http://pomcor.com/whitepapers/CryptographicAuthentication.pdf [pristupano u Jan. 2015.]

[18] Tao Qian & Veldhuis Raymond: Biometric Authentification System on Mobile Personal Devices. IEEE transaction on instrumentation and measurement. vol. 59 no. 4. pp. 763-773, 2010.

[19] Tulyakov S., Farooq F., Mansukhani P., and Govindaraju V.: Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters, Vol. 28, No. 16, pp.2427–2436, North-Holland, Elsevier, USA 2007.

[20] Bayly D., Castro M., Arakala A., Jeffers J., Horadam K.: Fractional biometrics: safeguarding privacy in biometric applications. International Journal of Information Security, Vol. 9, Issue 1, pp. 69-82, Springer, (2010).

[21] http://apple.com [pristupano u Jan. 2015.]

[22] Brunelli R. and Falavigna D.: Person identification using multiple cues. IEEE Transactions on pattern analysis and machine intelligence, Volume 17, Issue 10, pp. 955–966, Washington, DC, USA, 1995.

[23] Bowyer K.W., Baker S.E., Hentz A., Hollingsworth K., Peters T. & Flynn P.J.: Factorsthat degrade the match distribution in iris biometrics. Identity in the Information Society, Volume 2, Issue 3, pp. 327-343, Springer, 2009.

[24] Maiorana E., Campisi P., González-Carballo N., & Neri A.: Keystroke Dynamics Authentication for Mobile Phones. SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing, Pages 21-26, New York, NY, USA, 2011.

[25] Monrose F., and Rubin A. D.: Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, Vol. 16, No. 4, pp. 351–359, Elsevier, 2000.

[26] Han J. and Bhanu B.: Individual recognition using gait energy image. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no.2, pp. 316–322, USA, 2006.

[27] Liu Z. and Sarkar S.: Improved gait recognition by gait dynamics normalization. IEEETransactions on Pattern Analysis and Machine Intelligence, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 28, no. 6, pp. 863–876. USA, 2006.

[28] Derawi M. O., Nickely C., Bours P. and Busch C.: Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on Darmstadt, 2010.

[29] Jenkins J. and Ellis C. S.: Using ground reaction forces from gait analysis: Body mass as a weak biometric. Pervasive Computing, Fifth International Conference, PERVASIVE 2007,Toronto, Canada, pp. 251–267, Springer Berlin Heidelberg, 2007.

Mr Dragan Korać, Univerzitet u Beogradu – Fakultet organizacionih nauka, student doktorskih studija.
Kontakt: korac@teol.net
Oblasti interesovanja: sigurnost, zaštita podataka i računarskih sistema, informacioni sistemi, mobilne tehnologije i fazi logika.