



UNIVERZITET SINGIDUNUM

**-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Autentifikacioni sistemi sa predlogom sopstvenog rešenja (SRSA)

- Master rad -

Mentor:
Prof. dr. Mladen Veinović

Student:
Mihailo Mudrinić
Br. indeksa: 410068/2014

Autentifikacioni sistemi

Sažetak: U ovom radu razmatraće se različiti sistemi i metodi autentifikacije korisnika tj. utvrđivanja istinitosti njihovih tvrdnji o svom identitetu. Razmatraće se osnovni bezbedonosni problemi funkcionisanja ovih sistema kao i primena kriptografskih rešenja u cilju rešavanja takvih problema. Takođe na praktičnom primeru jednog sistema za dvo-faktorsku i dvostepenu autentifikaciju uvidećemo mogućnosti kao i mane sistema za ograničavanje pristupa i eventualne načine prevazilaženja nekih od tipičnih problema vezanih za ovakve sisteme.

Ključne reči: autentifikacioni sistemi, kriptografija, bezbednost autentifikacionih sistema

SADRŽAJ

1. Metodologija	1
1.1 Uvodne napomene	1
1.2 Predmet istraživanja	1
1.3 Hipoteza.....	1
1.4 Ciljevi istraživanja.....	2
1.5 Naučne metode	2
2. Uvod.....	3
3. Teorijska osnova.....	5
3.1 Pregled.....	9
3.2 Sistemi sa klasičnom autentifikacijom (Zna)	9
3.2.1 Lozinke i Entropija	13
3.3 Sistemi sa naprednom autentifikacijom (Posедуje).....	14
3.4 Sistemi sa biometrijskom autentifikacijom (Jeste).....	16
3.5 Multi-faktorski sistemi	19
4. Bezbedonosni problemi i rešenja	23
5. Sopstveno rešenje sistema autentifikacije (SRSA)	25
5.1 Dvo-faktorski režim.....	32
5.2 Problemi pri korišćenju	34
6. Zaključak.....	35
7. Literatura	37

1. Metodologija

1.1 Uvodne napomene

U ovom radu obuhvaćene su metodologije pravilnog i sigurnog funkcionisanja sistema autentifikacije kao i zaštite korisničkih podataka kojima se pristupa putem sistema sa ograničenim pristupom.

U današnjoj eri modernih tehnologija i sve većom potrebom za automatizacijom procesa i generalnom potrebom da se zadaci obavljaju što brže i na što prostiji i efikasniji način, javlja se potreba za metodama autentifikacije koji bi bili ne-intruzivni, laki za korišćenje i pre svega sigurni.

Ovaj rad će se baviti različitim metodama kojima se može omogućiti pristup sistemima sa ograničenim pristupom, kao i praktičnim primerima sistema sa ograničenim pristupom, prvenstveno sistemima sa dvo-faktorskom i dvostepenom zaštitom, ali takođe će biti predstavljeni i neki od tipičnih sistema iz ove oblasti. Između ostalog rad će se baviti različitim metodama kojima se može omogućiti pristup sistemima sa ograničenim pristupom, od konvencionalnih sistema koji se zasnivaju na korišćenju korisničkog imena i lozinke, preko sistema u kojima se koriste pametne kartice do sistema koji se zasnivaju na jedinstvenoj činjenici da je čovek kao jedinka jedinstven i da se ta jedinstvenost može iskoristiti u proveru njegovog identiteta i autorizaciji pristupa sistemima ili njihovim delovima. Jedinstveni problemi, rešenja i unikatnosti različitih metoda biće obrađeni u ovom radu.

1.2 Predmet istraživanja

Predmet ovog istraživanja su sigurnosni izazovi koji su inherentni za sisteme autentifikacije, kao i moguća rešenja ili saveti kojim se mogu preduprediti i izbeći problemi vezani za transport, proveru i skladištenje podataka ovakvih sistema. Obuhvaćeni su pojmovi autentifikacije, ugrožavanja bezbednosti sistema autentifikacije a samim tim i bezbednosti samih sistema sa ograničenim pristupom, kao i pojmovi kriptografije, i drugih tehnika i metoda koje se mogu iskoristiti u prevazilaženju izazova koji se mogu pojaviti.

1.3 Hipoteza

Funkcionisanje sistema autentifikacije se prvenstveno zasniva na činjenici da se podaci za pristup, korisnička imena, lozinke, pametne kartice ili biometrijski ključevi moraju izdati osobi kojoj se pristup omogućava. Ova činjenica za sobom povlači potrebu za skladištenje istih na sigurnim lokacijama, proveru integriteta podataka i proveru tačnosti, sigurnost komunikacionog kanala koji se koristi za prenos istih takođe predstavlja deo celokupne problematike.

Svaki korak, izdavanje, korišćenje, provera, transport i skladištenje podložni su napadima i mogućnostima neautorizovanog pristupa i krađe.

Da li postoji apsolutno siguran sistem autentifikacije?

1.4 Ciljevi istraživanja

Eksploracija prednosti i mana različitih tipova i metoda autentifikacije i definisanje bitnih pretnji za funkcionisanje takvih sistema i podataka koji se u njima koriste, definisanje i analiza mogućih rešenja.

Takođe jedan od ciljeva je i informisanje svih uključenih u funkcionisanje ovakvih sistema bilo da su to kreatori ili korisnici ovih sistema o mogućim pretnjama po bezbednost njihovih podataka kao i davanje smernica koje mogu pospešiti sigurnost ne samo njihovih podataka već i samog sistema u celini.

1.5 Naučne metode

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije.

Metoda deskripcije je korišćenja pri objašnjavanju osnovnih pojmova i sistema funkcionisanja.

U teorijskim segmentima su primenjene metode indukcije, dedukcije i analize, a u izvođenju zaključaka metode sinteze i generalizacije.

2. Uvod

Dvadeset i prvi vek predstavlja eru modernih komunikacija, brzog životnog stila i potreba za lakoćom komunikacije. On predstavlja eru računara koji prožimaju svaki aspekt današnjeg života. Računare srećemo kada ustanemo, dok smo u prevozu, dok radimo, dok se opuštamo i odmaramo, pa u nekim slučajevima čak i dok spavamo.

Povećanom upotrebom računara otvaraju nam se mogućnosti o kojima se nekada moglo samo sanjati. Internet je možda jedan od najbitnijih izuma prošlog veka koje je čovek u potpunosti prihvatio. Nekada su ljudi, studenti odlazili u biblioteke kako bi došli do potrebnog znanja, prolazeći mnogobrojne knjige, prevrtali mnogobrojne strane, čitali mnogobrojne pasuse, dok se danas svo to znanje može svesti na objekat površine obične kutije žvaka.

Ono za šta su nam nekada trebali dani, meseci pa i godine da pronađemo i shvatimo danas se može pronaći i asimilirati u prostoru od samo nekoliko minuta ili sati. Sa neverovatnom preciznošću možemo pronaći termine i članke vezane za temu koja nas zanima.

Pre svega Internet i razvoj računarske tehnologije omogućili su nam mnogo lagodniji život. Dobar deo stvari koje su nekada bile obavljane isključivo ljudskom rukom danas obavlja mašina. Roditelji danas mogu pratiti svaki pokret svojih mališana upotrebom daljinskih kamera, ne moraju čak biti ni na istoj lokaciji već sve mogu pratiti sa svog smartfon uređaja ili laptopa. Posao se danas može obavljati iz udobnosti svoje fotelje, hrana se može naručiti sa samo nekoliko pritisaka na tipke tastature. Banke su danas skoro u potpunosti digitalizovane i sa novcem se može manipulirati na daljinu. Sve u svemu postali smo svet zasnovan na digitalnim interakcijama.

Svi ovi primeri imaju jednu zajedničku osobinu, personalizovani su samo za nas, kada pristupate sajtu banke račun koji vidite je samo vaš (ukoliko niste osoba sa tamnijim intencijama ali o tome ćemo malo kasnije), sajt za naručivanje hrane zna vašu adresu i bez greške topao obrok nađe vaš prag. Svi ti sistemi zasnovani su na kontroli pristupa. Unutrašnjim stranicama možete pristupiti samo ako znate podatak koji je unikatan i pripada samo vama. U većini slučajeva taj podatak predstavlja kombinaciju korisničkog imena i lozinke. Ta mala kombinacija alfanumeričkih karaktera i specijalnih znakova je sve što vam je potrebno da pristupite servisima koji vam mogu olakšati svakodnevni život.

Kada unesete tu unikatnu kombinaciju i pritisnete dugme „Enter“ vi bivate transportovani u potpuno drugi svet, digitalni svet jedinstven i personalizovan samo za vas. Takvom svetu najčešće poznati su vaše ime, vaše prezime, adresa na kojoj stanujete, broj vašeg fiksnog telefona, vašeg mobilnog telefona, vaš datum rođenja i da ne nabrajamo dalje, sve u svemu većina informacija koje odlikuju i uobličavaju osobu koja vi jeste.

U ovom trenutku ćete se možda zapitati „Ali ti podaci predstavljaju mene kao individuu da li su oni sigurni? Živimo u dobu tehnike i tehnologije, da li oni mogu biti ukradeni i iskorišćeni u svrhe u koje ja ne bih želeo da se koriste?“. Kratak odgovor koji bismo dobili na ovakvo pitanje od većine kompanija koje se bave online uslugama bio bi „Da, podaci su sigurni i ne postoji mogućnost da oni budu ukradeni!“. Takav odgovor možda jeste tačan u nekim situacijama, ali su nas škorašnja iskustva sa upadima u velike kompanije kao što su Apple, Facebook, Ubisoft, Sony itd. naučila da su podaci sigurni samo onoliko koliko su sigurni sistemi na kojima se oni skladište. Dakle sa određenom dozom sigurnosti se može reći da termini „privatnost“ i „apsolutna sigurnost“ ne postoje u današnjoj eri modernih računara i računarskih sistema, barem ne u potpunom značenju tih izraza.

Zato se uporedo sa razvojem računarskih sistema moraju razvijati i sistemi za autentifikaciju, koji moraju sa velikom preciznošću znati ko pristupa sistemima koji oni štite ali takođe biti i otporni na upade i eventualne pokušaje korišćenja ukradenih podataka od strane neautorizovanih osoba. Zbog toga se sve češće u današnjim sistemima na internetu mogu videti augmentovani konvencionalni sistemi koji pored korisničkog imena i lozinke uključuju i dodatne korake potrebne za autentifikaciju, zatim sistemi koji se zasnivaju na upotrebi spoljašnjih uređaja koji omogućavaju pristup bez prethodnog poznavanja bilo kakvog podatka i na kraju sistemi koji se zasnivaju na korišćenju biometrijskih podataka pomoću kojih se dobija pristup zaštićenim sistemima.

U ovom radu prikazaćemo neke od ovih sistema, baviti se njihovim načinom funkcionisanja, prednostima i manama i smernicama koje mogu pospešiti sigurnost ovih sistema.

3. Teorijska osnova

U današnjoj eri računarstva i tehnologije omogućavaju da se sve veći deo naših života odvija *online*, na mreži. Usluge koje su nam potrebne, zadaci koji moraju da se završe pa i osnovne stvari kao što su kupovina i literatura predstavljaju svakodnevicu virtuelnog sveta.

Sve ove radnje moraju se obaviti sa određenom dozom „preciznosti“ i sigurnosti, neke više od drugih. Da bi se postigla ta preciznost sistemi koji pružaju takve usluge moraju utvrditi naš identitet tj. autentifikovati ko smo mi kako bi nam na osnovu toga omogućili pristup personalizovanim lokacijama i virtuelnim stranicama.

Sam čin autentifikacije može se obaviti na nekoliko načina:

- nečim što **znamo** (lozinka, PIN broj, odgovor na predefinisano pitanje itd.)
- nečim što **posедујemo** (pametna kartica, smartfon uređaj, *hardware*-ski/*software*-ski tokeni i sl.)
- nečim što **jesmo** - biometrijski parametri (otisak prsta, DNK, iris itd.)

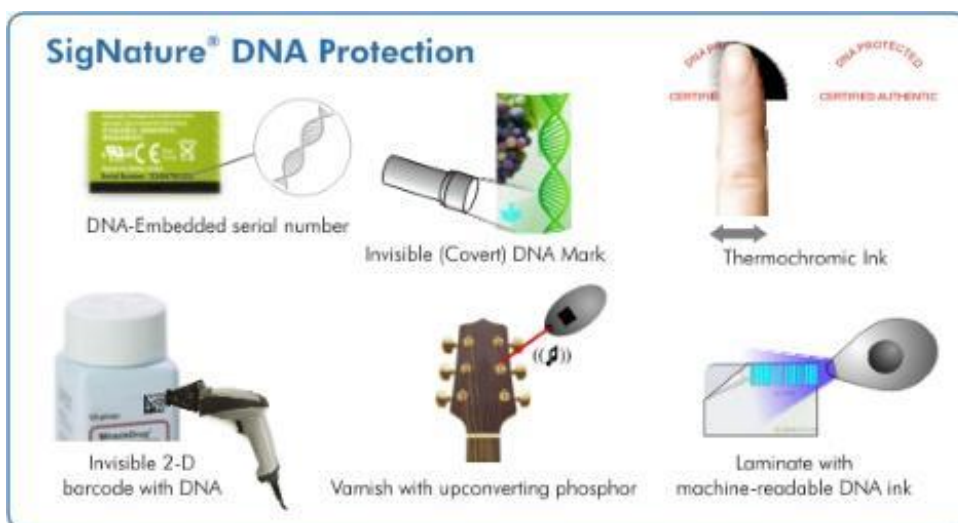
Username

Password

[Forgot your password?](#)

☐ Keep me logged in (for up to 30 days)

Log in



Osnovni koncepti u domenu bezbednosti komunikacija su:

- **Poverljivost** - obezbeđivanje tj. osiguranje da pristup podacima imaju samo ovlašćene osobe
- **Integritet** - obezbeđivanje celokupnosti podataka i zaštita istih od neautorizovane delimične ili celovite izmene.
- **Dostupnost** - osiguranje dostupnosti servisa autorizovanom korisniku.

Osvrnimo se prvo na nekoliko termina koji su integralni delovi celokupnog procesa.

Autentifikacija predstavlja proces pomoću koga se utvrđuje da li korisniku (osoba, mašina itd.) koji pristupa sistemu omogućiti pristup sistemu. Možemo je razložiti na lokalnu i udaljenu. Osnovna razlika između ova dva tipa je u tome što prilikom procesa udaljene autentifikacije dolazi do prenosa korisničkih podataka kroz komunikacioni kanal, dok se kod lokalne autentifikacije celokupan proces obavlja na lokalnom računaru pa samim tim se smanjuje mogućnost gubitka podataka ili njihove krađe.[1]

Udaljena **autentifikacija** unosi jedinstven problem u sferu komunikacija i slanju poruka na daljinu, prvenstveno zbog činjenice da takva komunikacija mora biti tajna. Tim problemom i njegovim rešenjima bave se **Kriptologija**, kao nauka o zaštiti podataka i **Kriptografija**, koja se bavi konstruisanjem i analizom protokola kojima se prevazilaze problemi nastali uticajem trećih osoba na komunikacioni kanal kojim podaci putuju.

Reč **kriptografija** (eng. *Cryptography*) nastala je od grčkih reči *kryptós*, što znači tajno, skriveno i reči *graphein*, što znači pisati. Osnovni cilj kriptografije je da obezbedi sigurnu komunikaciju i prenos podataka između dve ili više strana u uslovima kada se komunikacija mora obaviti nesigurnim kanalima ili kada tim kanalima mogu pristupiti ili u njih imati uvid treća osoba i očekuje se da zadovolji sledeće uslove:

- **Tajnost** – da obezbedi da uvid u podatke imaju samo ovlašćena lica.
- **Integritet** – da obezbedi integritet podatka, odnosno da onemogući neovlašćene izmene podataka, kao što su brisanje, zamena ili izmene na podacima.
- **Autentifikacija** – da obezbedi uzajamno identifikovanje svih strana i podataka u komunikaciji.
- **Neporecivost** – da onemogući negaciju preuzete obaveze ili izvršene radnje.

Inicijalne tehnike korišćene u kriptologiji postizale su ove uslove primenom partikularnih metoda šifrovanja čija je tajnost odnosno uspešnost u direktnoj sprezi sa njenom tajnošću načina generisanja šifrata odnosno nemogućnošću trećih osoba da saznaju princip stvaranja šifrata (*Scytale* i sl.)



1

Slika 1 - Scytale - Rani kriptografski uređaji

Vremenom se ipak pokazalo da takve metode nisu dovoljno bezbedne jer po otkrivanju principa generisanja šifrata takve metode postaju nebezbedne. Sa tim u vidu savremene metode šifrovanja zasnivaju se na primeni ključeva. Ključ predstavlja kombinaciju karaktera, čija dužina zavisi od metode koja se koristi, kojima se vrše određene izmene nad podacima koji se zaštićuju i tim činom se takvi podaci pretvaraju u nečitljivu kombinaciju karaktera za treća lica koja mogu prisluškivati naše kanale komunikacije i/ili imaju direktan pristup našim šifratima.

Ovakve metode imaju javno poznat kriptografski algoritam, što ne utiče na tajnost šifrata, već se ona postiže činjenicom da je za uspešno šifrovanje i dešifrovanje potreban ključ. Možemo razlikovati dva tipa kriptografskih algoritama:

- **Simetrične** - sa jednim tajnim ključem koji obe strane dele
- **Asimetrične** - sa parom ključeva, javnim i privatnim, gde je samo javni poznat ostalim učesnicima a privatni samo korisniku kome je dodeljen

Simetrični algoritmi zasnivaju se na kompletnoj tajnosti ključa jer se isti ključ koristi i za šifrovanje i za dešifrovanje, što za sobom povlači činjenicu da taj ključ mora biti poznat i strani koja poruku šalje i strani koja tu poruku prima, pa je stoga potrebno izvršiti bezbednu razmenu tog ključa pre slanja poruke i preporučljivo je istu izvršiti kanalom komunikacije koji nije isti kao kanal kojim se prenosi poruka.

¹ Izvor: <https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/Skytale.png/1024px-Skytale.png>

Ovi algoritmi se mogu podeliti na podgrupe i to na algoritme toka (*stream cipher*) (A5/1, A5/2, RC4 i dr.) i blokovske (*block cipher*) (DES, 3DES, RC5, RC6, IDEA i dr.).

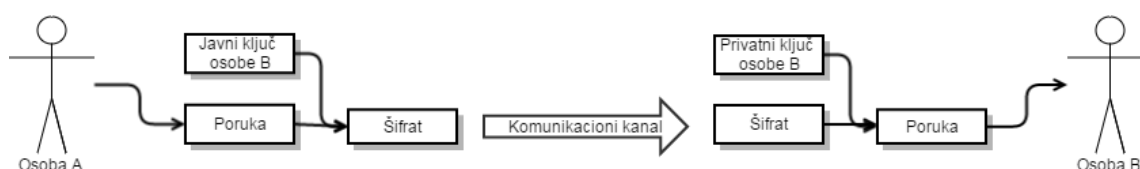


Simetrični kriptografski algoritam

Asimetrični algoritmi za razliku od simetričnih algoritama koriste par ključeva i to javni za šifrovanje i privatni za dešifrovanje. Glavna prednost im leži u činjenici da se sami javni ključevi mogu razmeniti i korišćenjem nesigurnih komunikacionih kanala.

Zasnivaju se na upotrebi jednosmernih funkcija enkripcije kod kojih je praktično nemoguće doći do originalnog otvorenog teksta i/ili privatnog ključa ukoliko se poznaje samo šifrat tj. krajnji rezultat enkripcije i javni ključ (javni ključ predstavlja, kao što i ime sugeriš, javni podatak poznat ne samo krajnjem korisniku već i celoj zajednici).

Osnovna razlika tj. nedostatak ovih algoritama predstavlja brzina generisanja šifrata i nisu toliko pogodni za enkripciju tj. šifrovanje velike količine podataka. Takođe se moraju rešiti i problemi međusobne autentifikacije. RSA, DSA predstavljaju neke od glavnih predstavnika ove grupe algoritama za šifrovanje.



Asimetrični kriptografski algoritam

Moderna kriptografska rešenja uglavnom koriste kombinaciju simetričnih i asimetričnih algoritama, tako što se asimetrični algoritmi koriste pri inicijalnoj razmeni simetričnih ključeva koji se nadalje koriste za šifrovanje tj. dešifrovanje.

Moramo pomenuti i kriptografske heš (*hash*) funkcije koje predstavljaju jednosmerne funkcije koje ulazni podatak promenljive dužine sažimaju i pretvaraju u podatak fiksne veličine (*hash*) kod kog male promene u sadržaju ulaznog podatka dovode do velikih promena izlaznog podatka. Samim tim ovakve funkcije se koriste za osiguranje integriteta poruke, tj. osiguravaju da je dobijena poruka identična originalnoj, neporecivosti i autentifikaciju. Neke od heš funkcija su MD5, SHA-1, SHA-256 itd.

3.1 Pregled

Autentifikacija se kao proces utvrđivanja istinitosti nečije tvrdnje o svom identitetu, može se grubo podeliti na tri tipa:

- Autentifikaciju nečim što korisnik **zna** kao što su na primer korisnička šifra i korisničko ime
- Autentifikaciju nečim što korisnik **posедује** kao što su pametna kartica, smartfon uređaj i sl.
- Autentifikacija nečim što korisnik jeste kao što su otisak prsta, iris, glas i sl.

3.2 Sistemi sa klasičnom autentifikacijom (Zna)

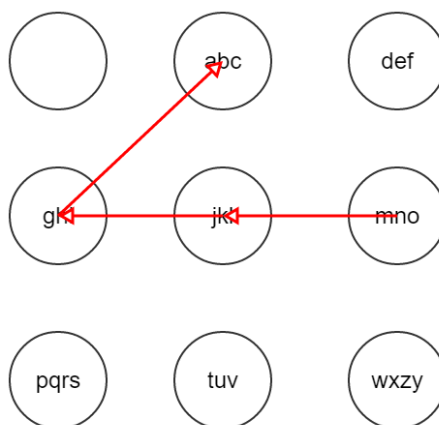
Sistemi klasične autentifikacije, koji predstavljaju i najrasprostranjeniji vid autentifikacije, zasnivaju se na nečemu što korisnik zna i predstavlja osnovni tip autentifikacije, bilo da je ona lokalnog ili udaljenog karaktera. Predstavljaju sisteme sa ograničenim pristupom kome se pristupa upotrebom para podataka, koji predstavlja kombinaciju korisničkog imena ili e-mail adrese i korisničke šifre ali može se svesti i na poznavanje samo jednog kompleksnijeg podatka *passphrase*, PIN broja ili izazov / odgovor kombinacija.

Modernija verzija ovog pristupa problematici autentifikacije predstavlja pristup sistemu upotrebom PIN koda, tipično 4 karaktera alfanumeričkog tipa mada je dužina varijabilna. Ovaj vid autentifikacije prvobitno se pojavio na mobilnim uređajima ali je ubrzo, zbog svoje jednostavnosti i lakoće korišćenja postao popularan i na drugim uređajima, što možemo videti na novijim multi platformskim operativnim sistemima gde jedan PIN kod može poslužiti kao medijum za autentifikaciju na više od jednog uređaja.



Slika 2 - Primeri PIN koda i autentifikacije šablonom

Jedna od zanimljivih varijacija ovog sistema predstavlja autentifikaciju pomoću unapred definisanog i zapamćenog *pattern*-a tj. šablona proizvoljne kompleksnosti. Ovakav šablon se unosi na podlozi veoma sličnoj numeričkoj tastaturi koja podseća na tastaturu mobilnih telefona. Prednost ove metode je u tome što se sam šablon može pamtititi kao kompleksiji niz karaktera, kombinacije slova i brojeva ili kao cela rečenica. Na primer ako bi smo uzeli rečenicu „Mihailo“, šablon bi izgledao ovako:



Slika 3 - Šablon reči Mihailo

Moderna era računarstva i razvoj Interneta su nam omogućili da veliki deo klasičnog života prebacimo u virtuelni svet. Evolucija našeg načina života za sobom povlači i evoluciju načina na koji svoj identitet dokazujemo pred drugima. Na primer ukoliko bismo hteli da koristimo web stranicu za kupovinu kao što su na primer Amazon ili Ebay moramo prvo pristupiti njihovim stranicama za registraciju gde unosimo svoje lične podatke kao što su ime prezime, adresa stanovanja, broj kreditne kartice, e-mail adresu, korisničko ime i lozinku. Nakon potvrde našeg identiteta putem e-mail-a ili mobilnog telefona možemo pristupiti stranici na kojoj unosimo prethodno odabrano korisničko ime i lozinku i na taj način nam se omogućava dalji pristup zaštićenim stranicama za kupovinu. Ovo je jedan od ustaljenih procesa autentifikacije nečim što korisnik zna i predstavlja *defacto* standard za potvrđivanje identiteta.

Sigurnost ovakvih sistema je u direktnoj sprezi sa tajnošću podatka ili kombinacije podataka koji se koriste u procesu autentifikacije, što znači da su ovakvi sistemi onoliko sigurni koliko su sigurni ti podaci. Podatak se mora zaštititi na tri osnovne lokacije, na samom izvoru, u toku komunikacije i na odredištu tj. serveru ili sistemu kom se zahteva pristup.

Zaštita podataka na izvoru svodi se na sugerisanje nivoa kompleksnosti kao i definisanju praga kompleksnosti koji ovakvi podaci moraju da zadovoljavaju. U istraživanju iz 2014 SplashData² je objavio listu 25 najpopularnijih korisničkih lozinki i među prvima se mogu naći lozinke kao što su 123456, password, qwerty i sl. Sa nivoom razvoja no kom se danas nalaze računari i tehnologija uopšte razbijanje ovakvih šifri više ne predstavlja preveliki izazov pa se shodno tome mora podići svest o tome da korisničke lozinke koje koristimo moraju biti kompleksnije (kombinacija velikih i malih slova, brojeva i specijalnih karaktera).

U sferi interneta, stranice na kojima se unose korisnička imena i lozinke uglavnom se zaštićuju HTTPS protokolom koji osigurava sigurnu komunikaciju između korisnika i servera na kom se stranica i autentifikacioni sistem nalaze. Korisnički podaci se takođe mogu haširati (*hash*) korišćenjem md5 *hash* funkcije pre samog slanja, na klijentskoj strani, u cilju dodatne sigurnosti i tako transportovati do odredišta. U sistemima koji koriste SSL/HTTPS ovo je preporučljivo uraditi ali nije obavezno dok u sistemima koji koriste klasičan HTTP ova operacija bi bila veoma poželjna jer je HTTP protokol podložan prisluškivanju.

S' obzirom na rastući trend upada na sisteme i krađu privatnih podataka koji uključuju korisnička imena i lozinke, zaštita podataka na odredištu odnosno serveru predstavlja glavni front zaštite korisničkih podataka. Korisnička lozinka je podatak koji ima najvećeg uticaja na ishod uspešnog/neuspešnog pokušaja autentifikacije, jer ona uglavnom predstavlja tajnu komponentu iz kombinacije korisničko ime/lozinka. Ona se uglavnom skladišti u vidu posoljene vrednosti (*salt*) u kome se originalnoj šifri koju korisnik definiše dodaje nasumična kombinacija karaktera koja se zatim hešira i kao takva sa *salt*-om skladišti u bazi podataka, ovde se takođe mogu naći i varijacije u vidu heširanja šifre pre kombinacije sa *salt*-om i sl. Ovim se osiguravamo da i ukoliko dođe do proboja u sistem i krađe podataka, napadač ne dobije direktan pristup korisničkim lozinkama u otvorenom obliku.

Konvencionalni sistemi iako najzastupljeniji predstavljaju i najnesigurniji vid autentifikacije tj. odobravanja pristupa sistemima sa ograničenim pristupom. Tehnologija napreduje nezaustavljivom brzinom, personalni računari postaju sposobniji u pogledu količine podataka koje mogu da obrade pa zaoblazanje ovakvih sistema u vidu *brute-force* i *dictionary* napada više ne predstavljaju samo zamisao već se sa malo vremena i snalažljivosti mogu sprovesti u stvarnost. Problem ovakvih sistema a prvenstveno sistema koji koriste korisničko ime i lozinku predstavlja tendencija samih korisnika da istu kombinaciju koriste na više različitih udaljenih servisa. Tako da napadač ima veoma veliku šansu da otkrivanjem jedne kombinacije otkrije i druge ili da mu to barem olakša otkrivanje drugih kombinacija.[6][7]

² <http://splashdata.com/press/worst-passwords-of-2014.htm>

Osnovni problem leži u teškoći pamćenja kombinacija i dugih lozinki za koje se vrlo često zahteva korišćenje specijalnih interpunkcijskih karaktera, velikih i malih slova i sl. Primer ovakve lozinke bio bi „Sup3r@m&m“ (super at m and m – kao Mihailo Mudrinic) .

Iako jačina lozinke nije propisana zakonima Internet zajednica preporučuje sledeće u vezi sa ovom problematikom:

- Ukoliko je moguće treba koristiti lozinke dužine od 12 do 24 karaktera
- Ukoliko je moguće poželjno je koristiti specijalne karaktere, mala i velika slova i brojeve.
- Preporučljivo je koristiti nasumične šifre.
- Ne treba koristiti identičnu lozinku na više od jednog servisa (npr. e-mail lozinka bi trebala biti različita od lozinke na socijalnim mrežama i sl.)
- Treba izbegavati ponavljanje karaktera, šablonskih reči i tipičnih reči koje se često koriste u svakodnevnom govoru, datuma ili brojevnih šablona koji imaju neki značaj, imena ljubimaca i sl.
- Za lozinke ne treba koristiti informacije koje su javno dostupne i koje se mogu povezati sa korisnikom.

Iako ovi sistemi možda predstavljaju najstariji oblik kompjuterske autentifikacije oni i dalje u većini slučajeva čine osnovu drugim sistemima bez obzira na tip autentifikacije koji se pruža na samom tom sistemu. Tako da je krucijalno posmatrati i ući u samu srž ovih sistema i osnovnu stvar na koju se on oslanja a to su lozinke.

3.2.1 Lozinke i Entropija

Sigurne lozinke predstavljaju osnovu dobrog sistema. Iako se na njih ne sme osloniti u potpunosti one predstavljaju polazni korak koji se koristi u većini današnjih sistema.

Mera sigurnosti lozinke se u većini slučajeva posmatra kroz vrednost entropije te lozinke. Što je veća entropija to je i lozinka bolja odnosno teže ju je otkriti. Na primer za otkrivanje lozinke čija je entropija 17 bita potrebno je 2^{17} pokušaja odnosno 2^{17} predstavlja maksimalan broj mogućnosti koje ta entropija može da predstavi.

Entropija, u Teoriji informacija, predstavlja meru neodređenosti sistema ili promenljive za koju se posmatra. Ovaj termin je u Teoriju informacija prvi uveo Klod Šenon (Claude Shannon), po njemu Entropija predstavlja količinu informacije sadržane u poruci.[2]

U dokumentu organizacije **IETF** (*The Internet Engineering Task Force*) preporučuje se korišćenje lozinke čija je entropija barem 29, za normalne sisteme dok se za sigurnije sisteme preporučuje korišćenje lozinke sa entropijom 128 i više.[10]

Vrednosti entropije za neke od tipičnih grupa karaktera ASCII formata koji su u upotrebi :

	Skup karaktera	Broj karaktera	Entropija
Arapski brojevi	0-9	10	3.322 bita
Heksadecimalni karakteri	0-9, A-F	16	4.000 bita
Velika ili mala slova alfabet	a-z ili A-Z	26	4.700 bita
Velika ili mala slova i brojevi	a-z ili A-Z, 0-9	36	5.170 bita
Velika i mala slova	a-z, A-Z	52	5.700 bita
Velika i mala slova i brojevi	a-z, A-Z, 0-9	62	5.954 bita
Svi vidljivi ASCII karakteri		95	6.570 bita
Proširena ASCII lista		218	7.768 bita

1 - Tabela vrednosti entropije

3.3 Sistemi sa naprednom autentifikacijom (Posедује)

Pored klasičnog sistema upotrebe korisničke lozinke kao sredstva utvrđivanja tačnosti nečije tvrdnje imamo sistem koji se u svojoj osnovi zasniva na korišćenju spoljašnjeg uređaja u cilju autentifikacije pred sistemom. Osnovna mana prethodnog sistema koji se zasniva na poznavanju nečega leži u činjenici da nešto što korisnik zna može biti zaboravljeno ili biti dovoljno jednostavno da se može lako zapamtiti ali sa druge strane nedovoljno sigurno da se ne može saznati.

Sistemi autentifikacije koji se zasnivaju na nečemu što korisnik poseduje u svojoj osnovi sadrže pametan uređaj koji se uglavnom koristi u sprezi sa nečim što korisnik zna na primer PIN broj.

Primeri ovakvih sistema su:

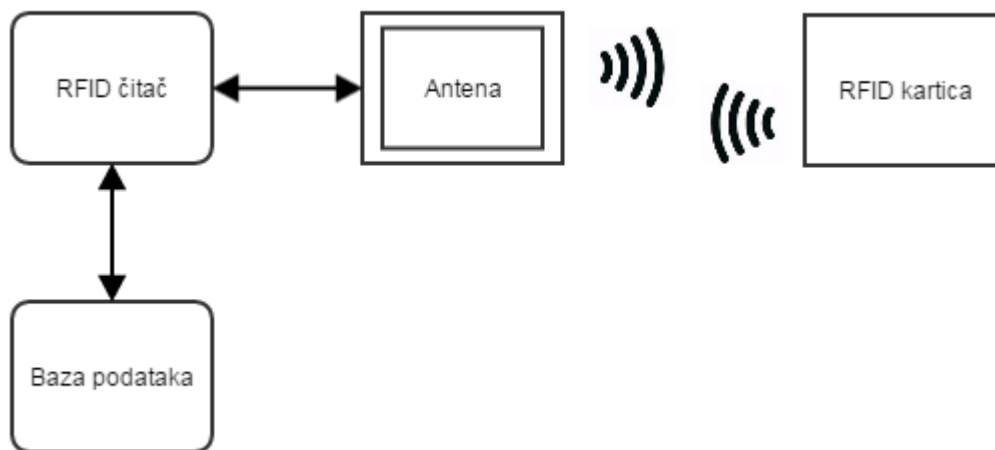
- Kreditne kartice
- RFID kartice
- Kriptografski kalkulatori ili tzv. smart kartice

Kreditne kartice se zasnivaju na magnetnoj traci na kojoj se nalaze snimljeni podaci. Ove kartice se koriste u sprezi sa PIN (*Personal Identification Number*) što pruža zaštitu od krađe jer se bez kombinacije oba podataka kartica ne može koristiti.

Osnovna mana ovih kartica je lakoća kopiranja same kartice i velika dostupnost uređaja pomoću koga se one mogu kopirati. PIN broj se uglavnom snima korišćenjem uređaja tzv. *Skimmer*-a ili minijaturnih kamera koje se postavljaju u blizini numeričkih tastatura koje služe za unošenje PIN broja. PIN kao kratak podatak je takođe podložan napadima pogađanjem pa banke sa tim u vidu ograničavaju broj pokušaja pri unosu.

RFID kartice predstavljaju bez-kontaktne kartice koje u sebi sadrže integrisana kola. Ovakve kartice tj. ovakav metod autentifikacije je u širokoj upotrebi kao deo personalnih dokumenata kao što su biometrijski pasoši, personalne identifikacione kartice i sl. One se takođe mogu koristiti i kao metode identifikacije ljudi, životinja i produkata. Veliki prodajni lanci se okreću ovakvom vidu označavanja (*tag*) svojih proizvoda.

RFID kartice mogu biti aktivnog i pasivnog karaktera. Pasivne kartice se aktiviraju samo u blizini čitača i koriste energiju radio talasa kako bi dale odgovor na zahtev čitača. Aktivne kartice imaju sopstveno napajanje i konstantno šalju podatke dozvoljavajući svima koji su u dometu a imaju odgovarajući čitač, da pristupe podacima.

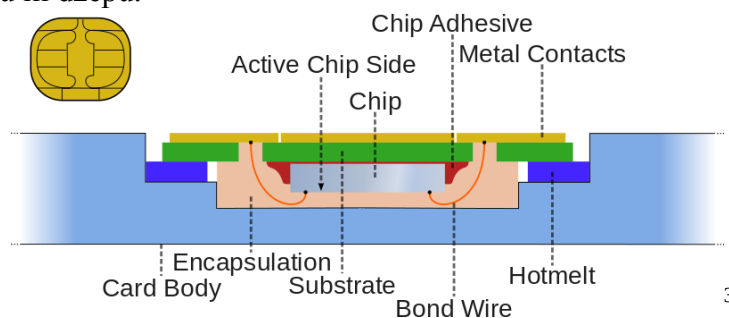


Slika 4 - RFID - princip funkcionisanja

Smart kartice ili kriptografski kalkulatori predstavljaju kartice/uređaje koji vrše neki vid kriptografske kalkulacije/obrade. Vrlo često će takve kartice imati memoriju i/ili će biti zaštićene PIN kodom. Ranjivost današnjih pametnih kartica predstavlja metoda analize energije odnosno grafova električne aktivnosti preko nekog perioda vremena.

Kartice ovog tipa se koriste u raznim oblastima, finansijskoj u vidu kreditnih kartica (bez magnetne trake), SIM kartica u mobilnim telefonima, zdravstvenih kartica, *single sign-on* ID kartica ili jedinstveno logovanje na sve sisteme koje kartica pokriva bez potrebe za dodatnim logovanjem na drugi sistem pri promeni.

Ovakve kartice uglavnom služe za autentifikovanje identiteta, i koriste PKI sistem (*Public Key Infrastructure*), na kartici se nalazi digitalni sertifikat izdan od strane PKI provajdera i ostale relevantne informacije. Iako se ovakve kartice smatraju najsigurnijim oblikom skladištenja privatnih informacija i uređajem koji povećava privatnost podatka to nije uvek slučaj jer se npr. bezkontaktnim smart karticama može pristupiti bez znanja korisnika koji takve kartice obično drže u novčaniku ili džepu.



Slika 5 - Primer Smart kartice sa čipom

³ http://en.wikipedia.org/wiki/File:Smartcard_chip_structure_and_packaging_EN.svg

Podgrupa ovakvih uređaja predstavljaju i posebni hardverski uređaj u vidu *token* uređaja koji se uglavnom zasnivaju na jednokratnim šiframa koje se menjaju u nekom vremenskom intervalu kreirana upotrebom one-time pad ili nekog drugog kriptografskom algoritma. Da bi ovakav uređaj funkcionisao on mora biti sinhronizovan sa udaljenim serverom koji pripada sistemu na kome se vrši autentifikacija.



Slika 6 - Primer Token sistema

3.4 Sistemi sa biometrijskom autentifikacijom (Jeste)

Sigurna autentifikacija predstavlja nešto čemu se teži u današnjoj eri modernih tehnologija i sve većih mogućnosti kompjuterskih sistema.

Klasični vidovi autentifikacije postaju sve nesigurniji, prvenstveno sistemi sa korisničkim imenima i lozinkama. Prema istraživanju Microsoft-a iz 2007. godine prosečan korisnik održava u proseku 25 različitih naloga na internetu i pri tome koristi svega 6.5 različite kombinacije autentifikacionih podataka. Ako na ovo dodamo podatak iz 2013. godine po kome je trojici eksperata u razbijanju kodiranih podataka trebalo svega sat vremena da probiju listu i postignu rezultat od ~ 90% pronađenih lozinki.

Sve ovo nas navodi na jednu nepobitnu činjenicu a to je da jedan od tri osnovne metode autentifikacije, ono što **znamo**, više nije dovoljan da nam obezbedi sigurnost da je osoba koja se loguje na sistem zapravo osoba koja bi smela da se loguje i pristupi sistemu.

Biometrija i sistemi autentifikacije bazirani na biometrijskim podacima daju jedno od rešenja koje je veoma teško kompromitovati i zaobići. U većini slučajeva gotovo nemoguće.

Biometrijska autentifikacija smatra se najsigurnijim rešenjem, kada se sagleda problematika autentifikacije kao vida utvrđivanja tačnosti tvrđenja o identitetu, ili barem kao rešenje koje je najzaštićenije od pokušaja krivotvorenja.

Biometrijski sistemi se zasnivaju na proveru određenih parametara koje osoba čiji se identitet potvrđuje poseduje. Ti parametri su: otisak prsta, oko (iris, mrežnjača), lice, dlan, uvo, DNK i miris.

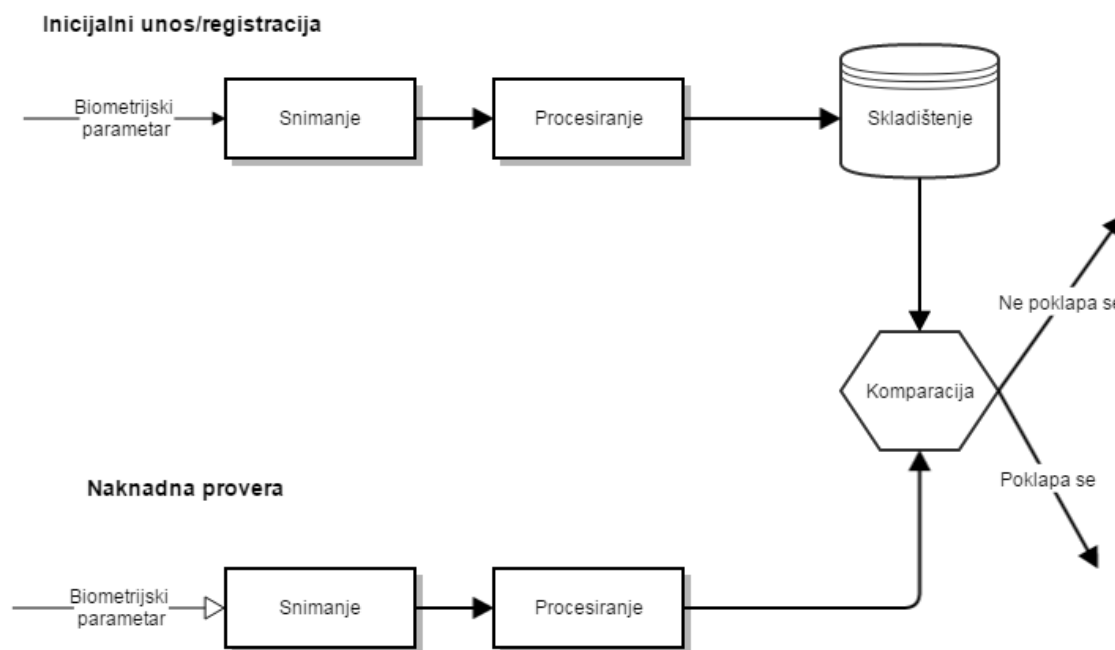
Skeniranje oka (Iris, Mrežnjača) - Jedan od verovatno najpopularnijih metoda prisutnih u današnjem dobu (što u realnosti što u fikciji). Možemo razlikovati dva pod tipa, a to su skeniranje retine i skeniranje irisa, odnosno zenice oka. Ovaj vid autentifikacije se odlikuje velikom preciznošću ali se ređe koristi jer su uređaji potrebni za ovakav sistem veoma skupi i teže dostupni.

Skeniranje otiska - Otisak predstavlja unikatnu kombinaciju ispupčenja i udubljena na prstima svih osoba i nepostoje dva ista otiska čak ni kod identičnih blizanaca. Ovaj način autentifikacije predstavlja najjeftiniji i najdotupniji oblik biometrijske autentifikacije i u širokoj je upotrebi.

Skeniranje dlana ruke - predstavlja skeniranje geometrije ruke ili dlana, dimenzija i ugla individualnih prstiju.

Prepoznavanje glasa - predstavlja metod kojim se na osnovu prethodno zabeležene sekvence korisnikovog glasa upoređuje trenutna sekvenca i odnosa se odnosno ograničava se pristup podatku ili sistemu.

Prepoznavanje lica - predstavlja metod koji se zasniva na korišćenju unikatnih odlika lica kao što su razmak između očiju, lokacije nosa, i generalnog oblika lica a osnovu kojih se vrši potvrđivanje nečijeg identiteta.



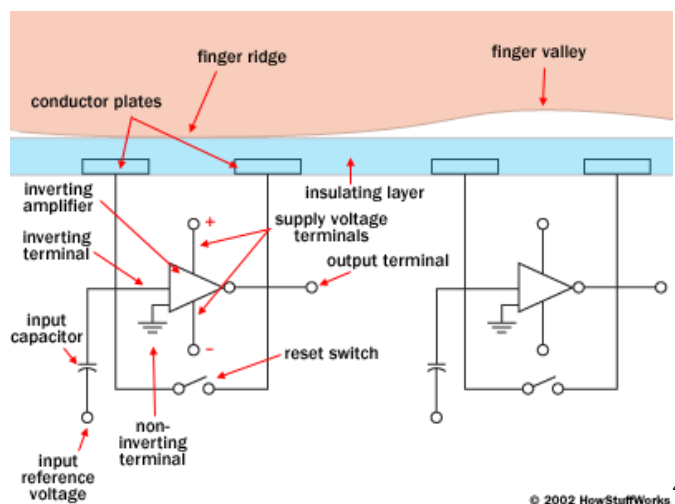
Slika 7 - Proces biometrijske autentifikacije

Proces biometrijske autentifikacije započinje se procesom inicijalnog skeniranja biometrijskog podatka i pravljenje šablona (*template*). Biometrijski podatak iris, otisak i sl se prvo skenira pomoću biometrijskog skenera, zatim se takav podatak procesira, izdvajaju se jedinstveni parametri biometrijskog podatka i stvara se šablon. Šablon se u daljem procesu skladišti u bazu podataka ili smart karticu ili bilo koji drugi medij koji se može koristiti za kasnije upoređivanje. Po završetku sistem dobija mogućnost provere identiteta tj. u mogućnosti je da autentifikuje osobu i potvrdi njen identitet.[3]

Biometrijski sistemi autentifikacije se sve češće mogu videti kao vidovi autentifikacije pri korišćenju personalnih uređaja, tablet računara i pametnih telefona, ali i kao vidovi autorizacije plaćanja robe i usluga.

Tipičan primer možemo pronaći u skeneru otiska prsta koji se danas može naći u mnogim modelima pametnih telefona. Postoje dva principa na kojima se baziraju ovi skeneri a to su:

- **Elektro-optički** – upotrebom jake svetlosti osvetljavaju se izbočine i udubljenja na prstu i tako formira slika samog otiska
- **Kapacitivni** – upotrebom minijaturnih provodnih pločica beleže se tačke koje provode elektricitet (izbočine) i tačke koje ne provode elektricitet (udubljenja) i na taj način se pravi *template* tj. šablon otiska.



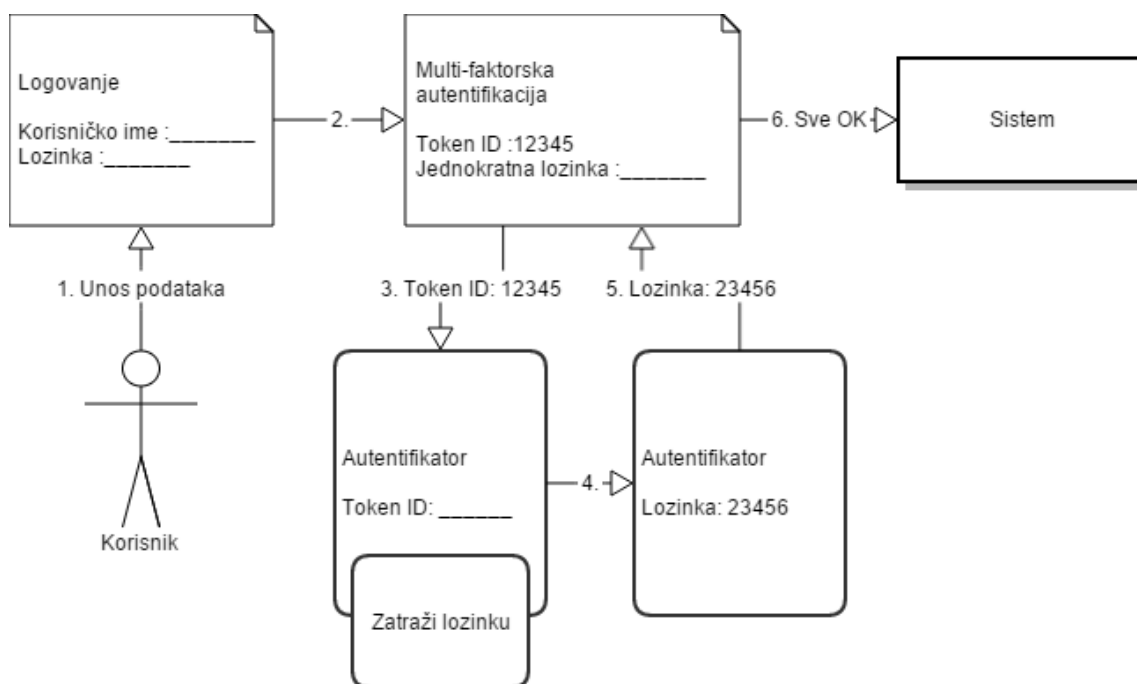
Slika 8 - Kapacitivni skener otiska prsta

⁴ Kapacitivni skener otiska prsta - <http://computer.howstuffworks.com/fingerprint-scanner3.htm>

3.5 Multi-faktorski sistemi

Multi faktorski sistemi predstavljaju jedinstvenu kombinaciju dva ili više niža metoda autentifikacije[5] tj. korišćenjem neke kombinacije metoda/faktora, nečega što korisnik poseduje i zna, nečega što jeste i zna ili kombinacije sve tri metode i kombinovanjem jednog ili više parametara iz svake metode. Ovo naravno nije novi koncept jer se može iskusiti svaki put pri podizanju novca na bankomatu koji zahteva fizičku kreditnu karticu i PIN broj kako bi dozvolio pristup bankovnom računu i omogućio podizanje novca.[9]

Tipičan primer ovakvog vida kombinovanja autentifikacionih sistema bio bi sistem u kome se pri inicijalnom zahtevu za autentifikacijom od korisnika zatraži kombinacija korisničkog imena i lozinke, a u drugom, tj. po uspešnom prolasku prvog koraka, od korisnika traži drugi sigurnosni podatak u obliku jednokratne lozinke koja može trajati od 10 - 30 sekundi (u slučaju mobilnih autentifikatora) ili više časova u slučaju e-mail autentifikacije. Dakle u osnovi ovog sistema imamo nešto što znamo (korisničko ime i lozinka) i nešto što posedujemo (mobilni telefon / autentifikacioni token uređaj) ili pak opet nešto što znamo u vidu e-mail-a.



Slika 9 - Primer sistema za multi-faktorsku autentifikaciju

U medijima i na internetu možemo takođe videti instance gde osoba mora proći kroz više instanci biometrijske autentifikacije (skeniranje oka, otiska prsta, prepoznavanja glasa) i korišćenje podataka koje osoba zna (lozinka, odgovori na određena pitanja i sl.), ovakav proces koristi se u institucijama u kojima se pristup mora strogo ograničiti kao što su laboratorije u kojima se vrše istraživanja nuklearni objekti i slično.

Primena više od jednog metoda na ovakav način drastično smanjuje mogućnost krađe identiteta.

Sa svim ovim u vidu NIST (National Institute of Standards and Technology) Američki institut za standarde i tehnologiju definisao je vodič za sigurne protokole udaljene autentifikacije[4]. Ova preporuka odnosno vodič sastoji se od 5 oblasti:

- Inicijalno dokazivanje identiteta i registracija korisnika.
- Token u vidu kriptografskog ključa ili korisničke lozinke koji se koristi prilikom autentifikacije
- Tokeni i mehanizmi koji se koriste pri ostvarivanju komunikacije
- Protokoli kojima se ostvaruje komunikacija između korisnika i sistema
- Mehanizmi za slanje rezultata autentifikacije trećim licima ukoliko za tim postoji potreba.

U avgustu 2005. FFIEC [5] izdao je dodatnu publikaciju u kojoj se pod „pravim“ sistemom sa multi-faktorskom autentifikacijom smatra onaj sistem koji koristi tri faktora autentifikacije a ne samo više instanci ili varijacija istog faktora.

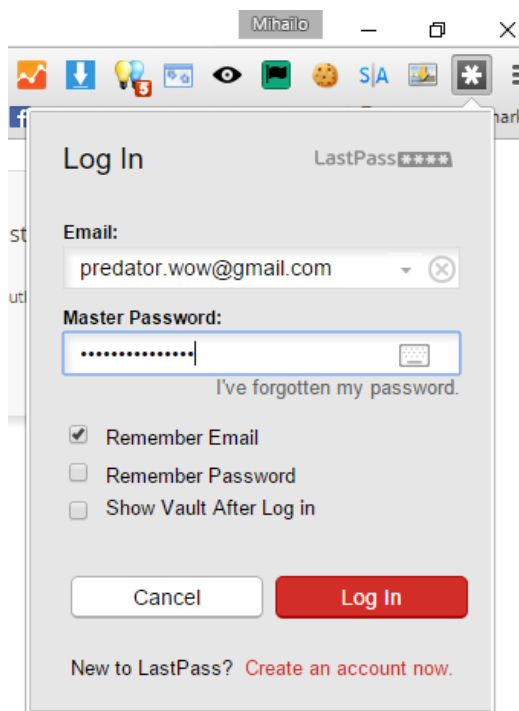
Jedan od popularnih stavova modernog doba predstavlja stav da je jedina sigurna lozinka ona lozinka koju ne možemo zapamtiti. Na prvi pogled ovakva izjava se može činiti čudnom ali lepota ovakvog načina razmišljanja leži u jednoj bitnoj činjenici a to je da se ovakvim načinom razmišljanja štitimo na više frontova i to:

- Šansa da koristimo istu lozinku na više sistema postaje infitezimalno mala
- Šansa da ovakvu lozinku nekome namerno ili nenamerno otkrijemo postaje skoro nemoguća
- Šansa da ovakvu lozinku neko napadne *dictionary* ili *brute-force* napadom i da je pritom otkrije postaje veoma mala, praktično nemoguća.

Ali sa druge strane, „Kako je moguće koristiti ovakve lozinke ako ih neznamo?“

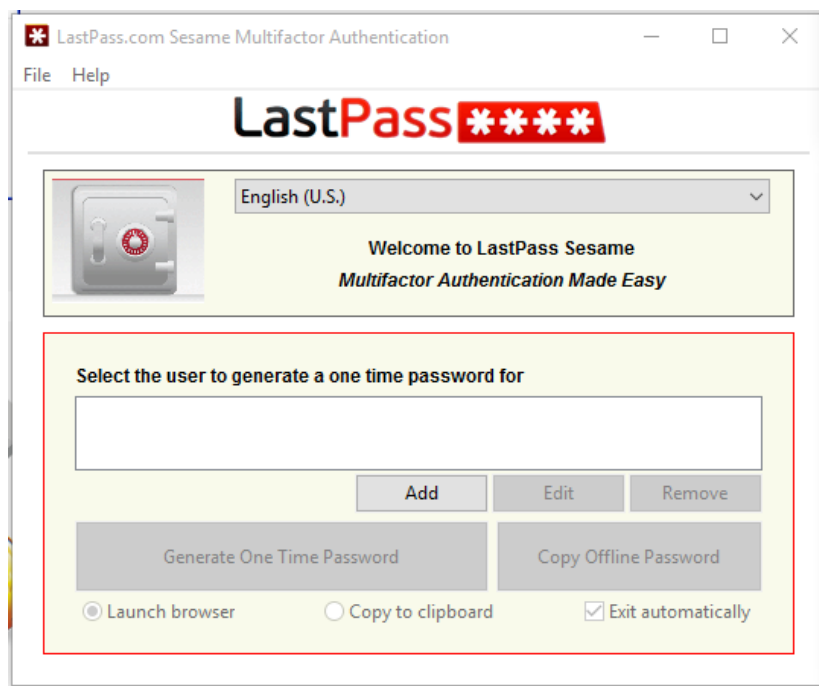
Postoje mnoga softverska rešenja koja nam ovo omogućavaju a koja se takođe mogu svrstati u domen multi-faktorskih sistema.

Tipičan predstavnik ove grupe predstavlja sistem *LastPass* u kombinaciji sa alatom *Sesame*



Slika 10 - Last Pass master login u okviru browser-a

Ova aplikacija se drži principa da je najbolja lozinka ona koju ni mi sami ne znamo. Ova aplikacija zahteva definisanje *Master Password*-a tj. glavne lozinke koja nam omogućava pristup sefu sa ostalim lozinkama. Po definisanju glavne lozinke sve ostale lozinke se mogu kreirati unutar same aplikacije po nasumičnom principu koji je u skladu sa preporukama najmerodavnijih tela u ovoj oblasti (*NIST* publikacija 800-63 **Error! Reference source not found.**, Microsoft, Google i sl.) .



Slika 11 - Last Pass Sesame - platforma za kreiranje ključa za multi - faktorski režim rada

U kombinaciji sa aplikacijom *Sesame* ovo rešenje se transformiše u pravo multi-faktorsko rešenje za autentifikaciju korišćenjem nečega što znamo, u ovom slučaju glavne lozinke i nečega što posedujemo, tj. USB ključa koji se dobija instalacijom ove aplikacije na USB uređaj. Ovakav vid autentifikacije zahteva postojanje i ispravnost oba faktora kako bi dobio pristup sefu sa lozinkama i kako bi se omogućio pristup i korišćenje lozinki za ostale servise.

4. Bezbedonosni problemi i rešenja

Svi tipovi sistema za autentifikaciju zasnivaju se na istoj osnovi, a to je da se podatak koji se proverava, a čijom se autentičnošću dalje garantuje identitet osobe koja ulazi u proces autentifikacije, mora prethodno biti uskladišten na nekom medijumu pogodnom za sistem u kom se vrši ovaj proces (baza podataka, smart kartica i sl.).

Skladištenje se može vršiti u potpunosti tj. celokupan podatak se može čuvati u okviru medija u izvornom obliku, ili izmenjenom obliku kao što je na primer slučaj sa korisničkim lozinkama, može se vršiti u vidu šablona (*template*) što je tipično za sisteme koji se baziraju na biometriji. Takođe se oni mogu skladištiti u kriptografski obrađenom obliku zaštićeni dodatnim nivoom sigurnosti u obliku PIN broja što je slučaj kod smart kartica.

Skladištenje predstavlja jedan od najtipičnijih tačaka u kojima se događaju ugrožavanja privatnosti odnosno u kojima se događa krađa podataka. U prethodnom periodu imali smo mnogobrojne slučajeve upada u sisteme velikih kompanija kao što su Valve Steam, Ubisoft, Ebay, JP Morgan Chase, Adobe i sl. U ovakvim upadima ukredeni su milioni privatnih podataka kao što su imena, adrese, heširane lozinke i brojevi kreditnih kartica i time je ugrožena privatnost miliona osoba.

Pored skladišta podataka tajnost podatka ugrožena je tokom njegovog puta od izvorišta do njegove destinacije kao i na samom izvorištu.

Kada govorimo o autentifikaciji pred udaljenim sistemom tipičan proces svodi se na čitanje podatka ukucavanjem od strane korisnika ili korišćenjem odgovarajućeg čitača, i prenosa istog kroz komunikacioni kanal. Iako skladište podatka odnosno mesto gde on postoji duži vremenski period treća lica mogu odlučiti da podatak presretnu na samom izvorištu ili u toku njegovog puta ka udaljenom sistemu.

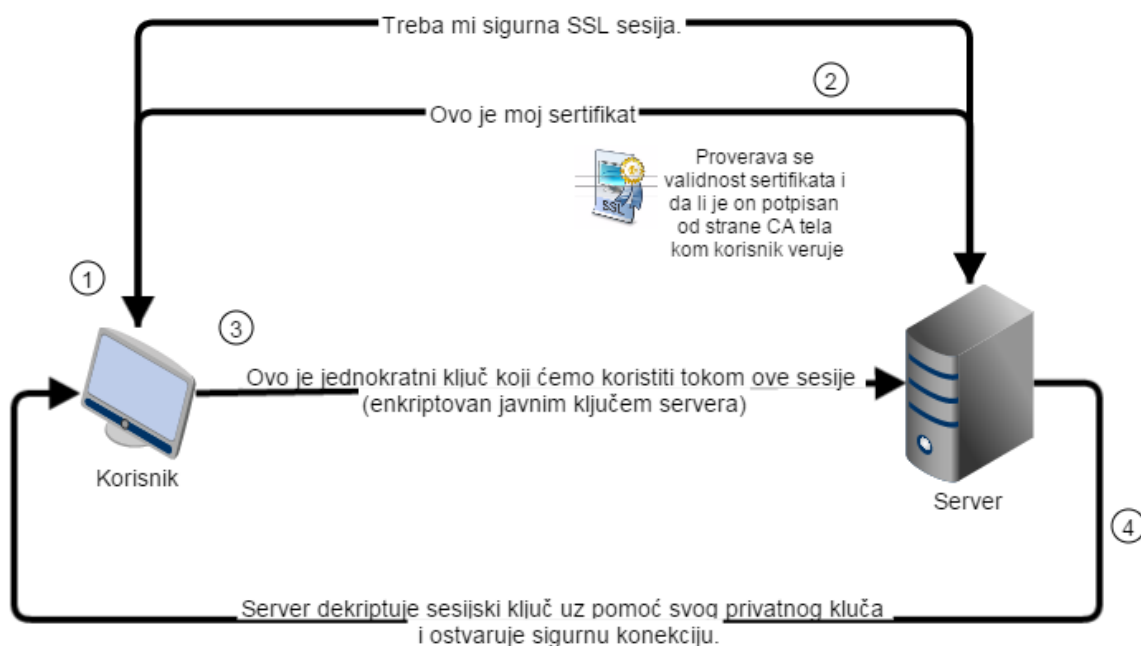
Sa rapidnim razvojem tehnologije i njenom sve lakšom globalnom dostupnošću, podaci korisnika postaju sve ugroženiji pa konvencionalni metodi zaštite podataka više nisu dovoljni.

Potreba tipičnog korisnika za upotrebom autentifikacije raste ubrzanim tempom jer se broj servisa koji se iz svakodnevnog života sele u digitalni svet povećava. Knjižare, prodavnice, biblioteke, fakulteti pa i državni organi i organi uprave imaju svoje digitalne odnosno web servise preko kojih možemo naručiti različite usluge ili proizvode, učiti, raditi. Svaki od tih sistema zahteva neki vid autentifikacije identiteta što je u većini slučajeva predstavlja korisnička lozinka. Ukoliko želimo da osiguramo bezbednost naših ličnih podataka ta lozinka bi trebala biti drugačija na svakom od sistema koji koristimo jer bi u suprotnom poznavanje jedne lozinke trećim licima dozvolilo upad na ostale sisteme koje koristimo.

Kompleksnost lozinki takođe mora biti na većem nivou jer proste lozinke koje se na primer sastoje od datuma rođenja ili imena ljubimaca, koje se inače lako pamte, najlakše pronalaze upotrebom „*rainbow*“ tabela ili pomoću *dictionary* napada. sve ove činjenice nas dovode u situaciju da pored velike količine lozinki dolazi moramo pamtiti i sve kompleksnije lozinke, što ultimativno dovodi do toga da korisnici bivaju prinuđeni da koriste aplikacije koje raspolažu njihovim lozinkama.

Kako bi se donekle zaobišao ovaj problem veliki sistemi počeli su sa uvođenjem dvo-faktorskih ili multifaktorskih sistema autentifikacije. Koji se zasnivaju na korišćenju jednostavnijih tokena (lozinki) ali preko dva ili više nivoa.

Komunikacioni kanali su vrlo često ranjivi na napade prisluškivanjem, i na primeru interneta to prisluškivanje se može obaviti na bilo kom kraju konekcije pa čak i bez fizičke prisutnosti osobe koja obavlja prisluškivanje. Iz tog razloga komunikacije preko nezaštićenih kanala vršiti se upotrebom TLS/SSL tj. HTTPS protokola.



Princip ostvarivanja sigurne SSL konekcije

HTTPS protokol u većini slučajeva eliminiše mogućnost prisluškivanja kanala i krađe podataka u toku transporta ali kao i svaki drugi sistem ni on nije savršen. 2014 godine otkriven je ozbiljan sigurnosni propust „*Heartbleed*⁵“ u popularnoj kriptografskoj biblioteci OpenSSL koja je upućenim napadačima omogućavao čitanje podataka na serveru koji koristi ovu biblioteku. Iako se u veoma kratkom roku pojavila ispravka koja je ovaj problem eliminisala, i dalje postoje sistemi koji koriste prethodne verzije biblioteka i samim tim su ranjivi ali i sama činjenica da je ovakav propust postojao navodi na razmišljanje koliko još ovakvih propusta postoji a nisu još uvek objavljeni?

⁵ <http://heartbleed.com/>

5. Sopstveno rešenje sistema autentifikacije (SRSA)

Na polju autentifikacionih sistema u današnje vreme ne postoji mnogo inovacija koje se mogu uvesti, a koje bi poboljšale način funkcionisanja sistema ili ga učinile sigurnijim. Uputstva i smernice za kreiranje, opsluživanje i korišćenje ovakvih i sličnih sistema mogu se naći u velikom broju publikacije različitih svetskih tehnoloških giganta, vladinih i nevladinih organizacija koje se bave ovom tematikom. Jedna od ovakvih organizacija je i NIST koja je u svojoj publikaciji 800-63 (800-63-1 i 800-63-2), iz avgusta 2013. god. pod nazivom „*Electronic Authentication Guideline*“ odnosno „Smernice za elektronske sistem autentifikacije“ dala set predloga za izradu sigurnih rešenja ovakvih sistema.

Ovaj sistem će obuhvatiti autentifikaciju na sam sistem, zaštitu odnosno osiguranje sigurnosti lozinke, kao i dvo-stepenim i dvo-faktorskim režimom rada koji pored konvencionalnog metoda, nečega što korisnik za koristi i nešto što korisnik poseduje i dodaje dodatni nivo zaštite putem zahteva za dodatnom autentifikacijom pred sistemom iz više izvora.

Pored klasičnog načina pristupa sistemu sa ograničenim pristupom korisnik mora uneti i dodatnu one-time / jednokratnu lozinku koju dobija putem svog e-mail naloga i koja predstavlja dodatni nivo osiguranja da sistemu pristupa baš ona osoba kojoj je taj pristup namenjen. Ovakva jednokratna lozinka ima ograničen vek trajanja čiji raspon može biti od svega nekoliko minuta do maksimalno 24 sata u zavisnosti od toga kakva aplikacija se nalazi iza autentifikacionog sistema.

Ovakav vid zaštite može se primeniti i u slučajevima kada se određenom uređaju dozvoljava i neograničen pristup sistemu u okviru jedne sesije odnosno korisnik se ne mora dodatno autentifikovati pred sistemom u narednom periodu u toku jedne sesije, tj. do trenutka dok se neki od parametara veze ne promeni u vidu IP adrese, mac adrese ili sl.

Pored jednokratne lozinke korisnik se može odlučiti da u iste svrhe iskoristi i mobilnu aplikaciju za Android operativni sistem koja mu u realnom vremenu pruža istu uslugu, odnosno na ekranu mobilnog uređaja korisnik dobija jednokratnu lozinku koju treba uneti u roku ne većem od 30 sekundi mada tipično ovakve aplikacije imaju prozor validnosti od 10 – 15 sekundi. Nakon čega lozinka postaje ne-validna i ne može se više iskoristiti već se mora uneti nova. Zbog manjeg perioda validnosti ovo takođe predstavlja i daleko sigurniji izbor jer u velikoj meri smanjuje broj dostupnih opcija nekome ko želi da dobije pristup korisnikovim podacima bez njegovog znanja i odobrenja.

Prednost mobilne aplikacije u odnosu na e-mail verziju jeste u činjenici da mobilni uređaj predstavlja nešto što korisnik fizički ima i poseduje, za razliku od e-mail sandučića koji predstavlja virtuelnu svojinu u *cloud*-u.

Ovaj sistem je baziran na programskom jeziku *PHP*, podlogu sistema predstavlja *CodeIgniter* framework, interaktivnost sa korisnikom postiže se skripting jezikom JavaScript, za baze podataka tj. komponentu za skladištenje podataka sistem se oslanja na MySQL kao server baza podataka, MyISAM i InnoDB koriste se kao *storage engine*-i.

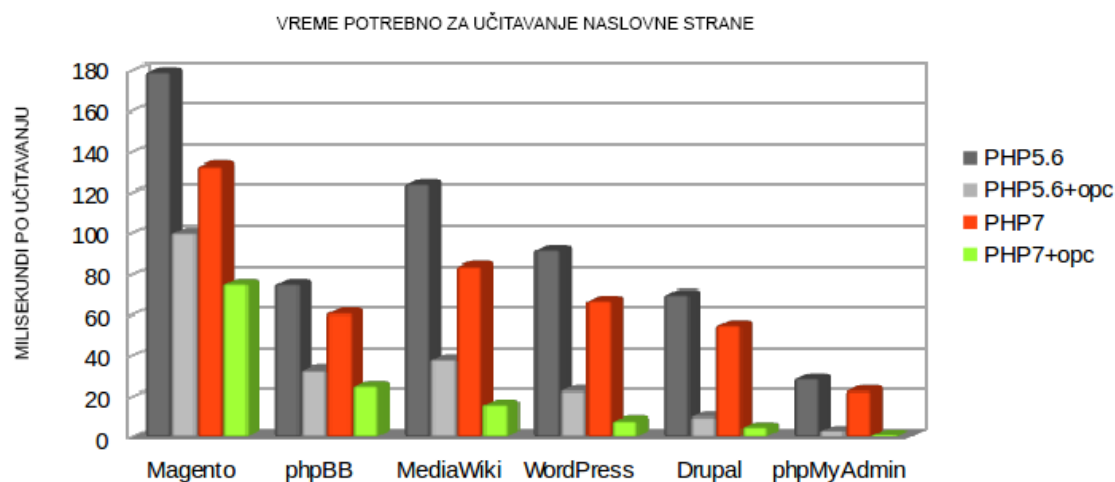
Za mobilnu aplikaciju koristi se *PhoneGap* framework za lakšu manipulaciju sadržajem, pored *PhoneGap* sistema koristi se i Android SDK (*Software Development Kit* – set alata, funkcija i biblioteka koje se koriste za razvoj i implementaciju različitih funkcionalnosti i proširivanje mogućnosti aplikacija) kroz Eclipse IDE (*Integrated Development Environment* – integrisano razvojno okruženje) alat.

PHP predstavlja jedan od najpopularnijih programskih jezika čija je osnovna namena web odnosno internet programiranje. Prema podacima iz 2015. godine. **PHP** se koristi na 81.3% internet prezentacija i aplikacija za koje je ta informacija dostupna[7].

Od inicijalnog pojavljivanja 1994. god. PHP je svojom opštom dostupnošću, i u velikoj meri jednostavnošću i lakoćom učenja tj. obuke novih programera osvojio svetsku scenu tehnologija u kojima se izrađuju web prezentacije i web aplikacije. Tokom godina ovaj programski jezik prošao je kroz velike transformacije ali je duh i osnovna ideja ovog programskog jezika zadržana a to je da pruži mogućnosti C - olkog jezika široj grupi ljudi i samim tim omogućiti brži razvoj internet programiranja i pospeši kvalitet.

Trenutna aktuelna verzija je 5.6 koja je pored velikog broja malih unapređenja uvela Variadične funkcije (*Variadic functions*), koja pruža mogućnost prosleđivanja varijabilnog broja argumenata funkciji, za razliku od ranijih verzija u kojima je taj broj morao biti jasno definisan (izuzimajući naravno mogućnosti koje nudi funkcija *func_get_args*). Takođe je važno pomenuti da se u narednom periodu očekuje izlazak verzije 7.0 koja je po najnovijim testovima nudi daleko bolje performanse u odnosu na trenutnu verziju 5.6, u proseku dva do dva i po puta brži od trenutne verzije.[8]

UPOREDNE PERFORMANSE PHP 5.6 I 7.0

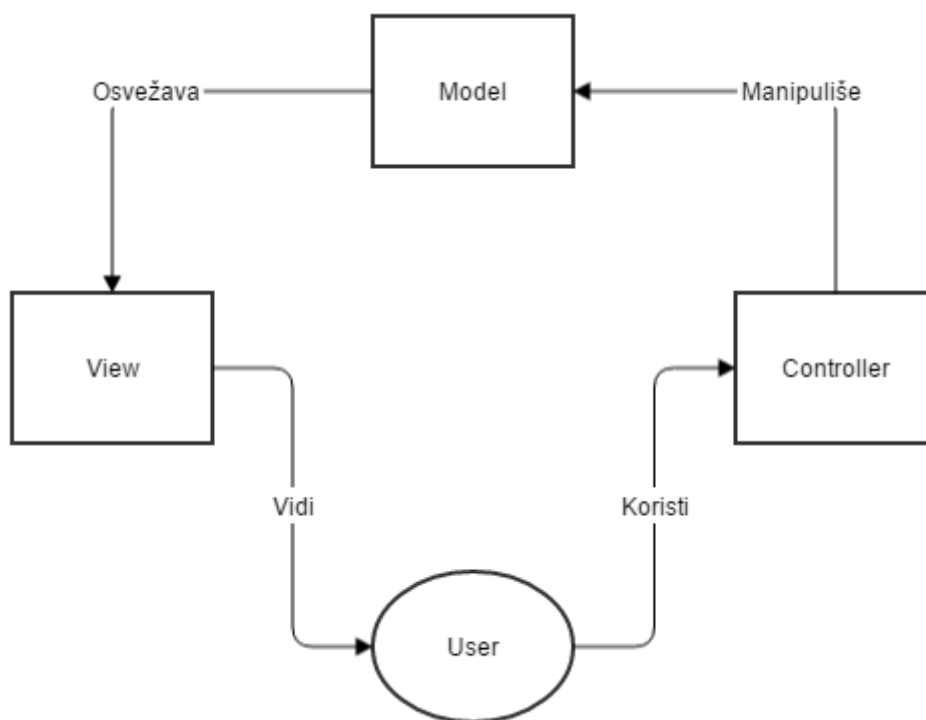


Slika 12 - Performanse PHP-a na različitim softverskim platformama

CodeIgniter (CI) predstavlja osnovu samog sistema u obliku *Framework* - a, koji predstavlja bazni set osnovnih klasa, klasnih metoda i pomoćnih funkcija. **CI** je baziran na MVC (Model – View - Controller) šablonu razvoja softvera. **Model** predstavlja komponentu koja služi za komunikaciju sa bazom podataka ili nekim drugim rešenjem za skladištenje podataka.

- **Model** predstavlja podatke i to predstavlja njegovu osnovnu funkcionalnost, pri čemu ne zavisi ni od **View**-a ni od **Controller**-a
- **View** služi za prikazivanje, odnosno vizuelizaciju, podataka dobijenih od modela i prosleđuje komande **Controller**-u.
- **Controller** obezbeđuje podatke **View**-u iz **Model**-a, i prihvata korisničke komande inicirane u **View**-u. On Zavisi i od **View**-a i od **Model**-a.

MVC se takođe ogleda i u određenoj dozi fleksibilnosti jer View i Controller mogu u nekim slučajevima biti ista stvar.



Slika 13 - MVC Šablon razvoja software-a

JavaScript (JS) – Ovaj programski jezik predstavlja interaktivnu komponentu sistema i proširuje mogućnosti **PHP** – a, koji prvenstveno služi za kreaciju statičkog sadržaja. **JS** uvodi interaktivnost između korisnika i sistema putem **AJAX** (Asinhroni JavaScript i XML) poziva. Na primer klikom na dugme Login u okviru sistema korisniku se prezentuje mali prozor u okviru trenutnog sadržaja u kome se unose korisnički podaci

koji se klikom na dugme Login šalju serveru na proveru. Celokupan proces se odvija na jednoj strani umesto na dve ili tri stranice što bi bio slučaj ukoliko bi se koristio samo **PHP**.

MySQL – predstavlja sistem za menadžment relacionim bazama podataka, i predstavlja osnovu sistema u pogledu skladištenja potrebnih podataka. U sistemu se koriste MyISAM i InnoDB *storage engine*-i. Razlog korišćenja dva tipa tabela leži u prednosti MyISAM tipa u pogledu brzine čitanja podataka korišćenjem SELECT komande dok je prednost InnoDB tipa u domenu upisivanja i osvežavanju podataka. Jedna od tipičnih i često korišćenih komandi u okviru bilo kog sistema jeste komanda SELECT COUNT(*) koja služi za brojanje redova po definisanom zahtevu i ograničenjima navedenim uz poziv, ovaj poziv najbolje ilustruje prednost MyISAM tipa jer se broj redova u okviru ovog kipa kešira tj. memoriše uz tabelu i index-e što nije slučaj kod InnoDB tipa.

PhoneGap – Predstavlja *framework* za izradu mobilnih aplikacija, i može se koristiti za izradu aplikacija za iOS, Android i Windows operative sisteme. On omogućava korišćenje HTML, CSS i JavaScript tehnologija u cilju pisanja osnove aplikacije koji se potom enkapsulira u nativni kod sistema za koji se aplikacija razvija. Ovaj framework takođe proširuje mogućnosti HTML-a i JavaScript-a i daje im mogućnosti korišćenja modula i specifičnih mogućnosti mobilnih sistema kao što su podaci žiroskopa, GPS i sl.

SRSA poštuje navedene preporuke tako da lozinke na ovom sistemu moraju ispunjavati minimum zahteva koji su definisani. Osnova sistema i dvo-stepeni režim rada

Rapidni razvoj tehnologije, i njena sve šira upotreba forsiraju transfer sve veće količine našeg dnevnog života „na mrežu“. Po podacima **ITU** (*International Telecommunication Union*) iz 2014. više od 70% korisnika u razvijenom svetu ima pristup internetu. Ovo uslovljava i pospešuje sve veći transfer dnevnih obaveza na Internet, kao što su posao, naručivanje gotove hrane i namirnica, kupovinu robe široke potrošnje, bilo šta što zamislite možete obaviti na Internetu.

Da bi ovo sve bilo moguće moraju postojati sistemi koji opslužuju prodavnice, restorane, velike prodajne lance. Svi ti sistemi na dnevnoj bazi rukovode, obrađuju i razmenjuju informacije međusobno. Te informacije su u većini slučajeva lične informacije poput imena, prezimena, adresa stanovanja, brojeva kreditnih kartica i sl. Neki od tih podataka se skladište u izvornom obliku, neki se šifruju dok se najosetljiviji podaci uopšte ne skladište ili je njihovo skladištenje strogo regulisano na međunarodnom nivou. Tipičan primer osetljivog podatka bio bi broj kreditne kartice čije je skladištenje i obrada regulisana PCI DSS (*Payment Card Industry Data Security Standard*) regulativom koja detaljno propisuje uslove, način i dostupnost istih.

Ali postoji jedna funkcionalnost ili deo sistema koji je zajednički za sve ove sisteme nezavisno od industrije u kojoj se koristi ili krajnje namene. Ovi sistemi su u većini slučajeva podeljeni na barem dva dela, deo koji je dostupan svima i deo koji je dostupan samo registrovanim članovima. Deo sistema dostupan samo registrovanim članovima zaštićen je sistemom za autentifikaciju korisnika koje tipično zahteva korisničko ime i lozinku kako bi se dozvolio pristup tome delu.

Iako na ovu temu postoji bezbroj varijacija i virtuelno je nemoguće ponuditi nešto što već nije iskorišćeno ili napravljeno. Sopstveno rešenje autentifikacionog sistema će ponuditi jednu od popularnih kombinacija.

Prvi modul omogućava zahteva od korisnika da po unošenju korisničkih podataka unese i dodatnu lozinku, koju mu sistem šalje na e-mail adresu definisanu u sistemu. Unošenjem ove dodatne lozinke korisnik dobija pristup samom sistemu i dozvoljava mu se dalji rad. Dodatna lozinka ima ograničeni vek trajanja i on na **SRSA** sistemu iznosi 24 sata mada se on može lako promeniti.

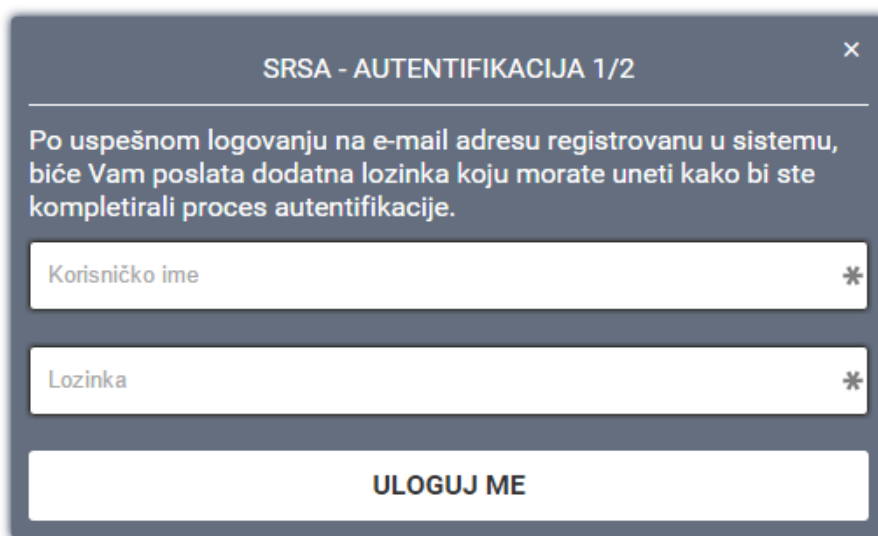
Ovo predstavlja osnovni način funkcionisanja sistema i ono što sam korisnik može da iskusi prilikom upotrebe. Cilj sistema je da na što bezbolniji način korisniku omogući sigurnost da sistemu može pristupiti samo on i nijedno drugo lice. Pored ovoga u samom sistemu postoje i dodatne operacije koje se događaju bez korisnikovog znanja ali u cilju poboljšanja njegove bezbednosti.

Sistem prilikom svakog zahteva za autentifikaciju beleži parametre koje u datom trenutku opisuju korisnika koji započinje proces, beleži se IP adresa korisnika, tip i verzija operativnog sistema uređaja sa kog se pristupa, vreme pristupa, URL stranice sa koje je korisnik došao na sistem (ukoliko postoji), tip i verziju pregledača koji se koristi, kolačiće ukoliko postoje. Po inicijalnom zahtevu korisniku stiže e-mail sa informacijom da je sa zabeležene IP adrese on ili neko drugi započeo proces autentifikacije i da klikom na pruženi link može da završi taj proces unošenjem navedene dodatne lozinke u roku od 24 sata. Klikom na link korisnik biva prosleđen na sistem i nudi mu se unos dodatne lozinke. Ukoliko je lozinka ispravna i još uvek validna korisniku se dozvoljava pristup sistemu.

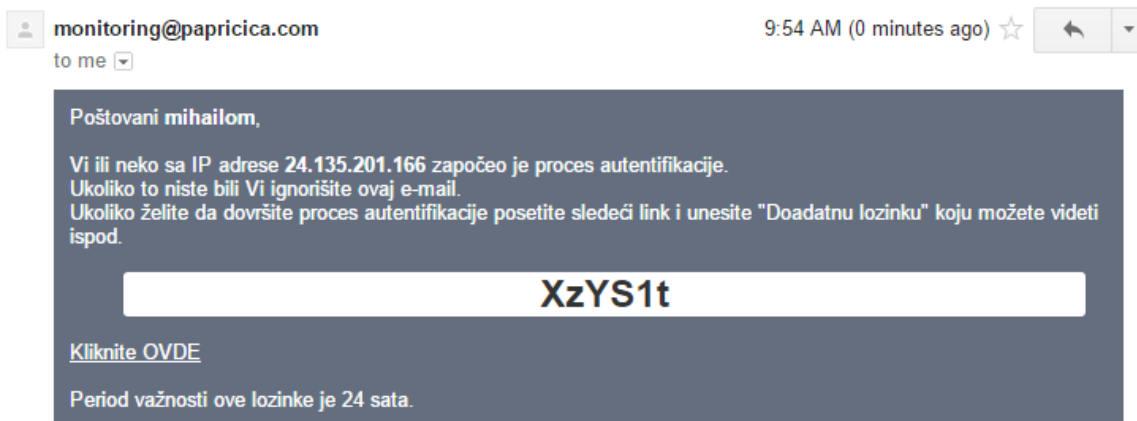
Prilikom klika na link sistem takođe beleži isti set podataka kao i u prvom koraku, kao još jedna sigurnosna predostrožnost.

Ovako zabeleženi podaci se mogu iskoristiti za eventualne forenzičke istrage u slučaju da se utvrdi da je sistem probijen i da osoba koja nema dozvolu da pristupi sistemu istu dozvolu dobila korišćenjem tuđeg naloga za koji je podatke dobila prevarom ili nekim drugim vidom (*phishing*, hakovanjem i sl.). Ovo predstavlja vid reaktivne forenzike koja se obavlja po prijavljenom slučaju.

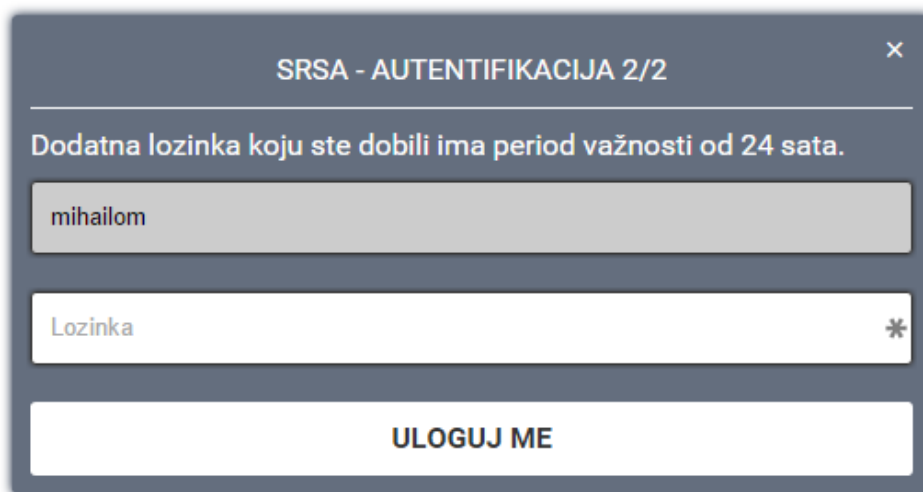
Ako sagledamo ove podatke proširenom kontekstu, odnosno ako ih posmatramo u različitim vremenskim periodima, možemo reagovati pro-aktivno i na primer na osnovu lokacije korisnika utvrditi da li postoji mogućnost da osoba koja pristupa sistemu u stvari nije osoba čiji se nalog koristi. Na primer ukoliko se prilikom jednog zahteva za autentifikaciji korisnik povezaao pomoću računara čija se IP adresa nalazi u Srbiji a sledeći dan ili sat se taj isti nalog koristi sa IP adrese u Kini, postoji velika verovatnoća da je u pitanju nedozvoljen pristup i takav pokušaj se može blokirati ili se korisniku može poslati dodatni e-mail zahtev za odobravanje takvog pokušaja.



Slika 14 - SRSA korak 1



Slika 15 - SRSA e-mail sa dodatnom lozinkom



SRSA - AUTENTIFIKACIJA 2/2

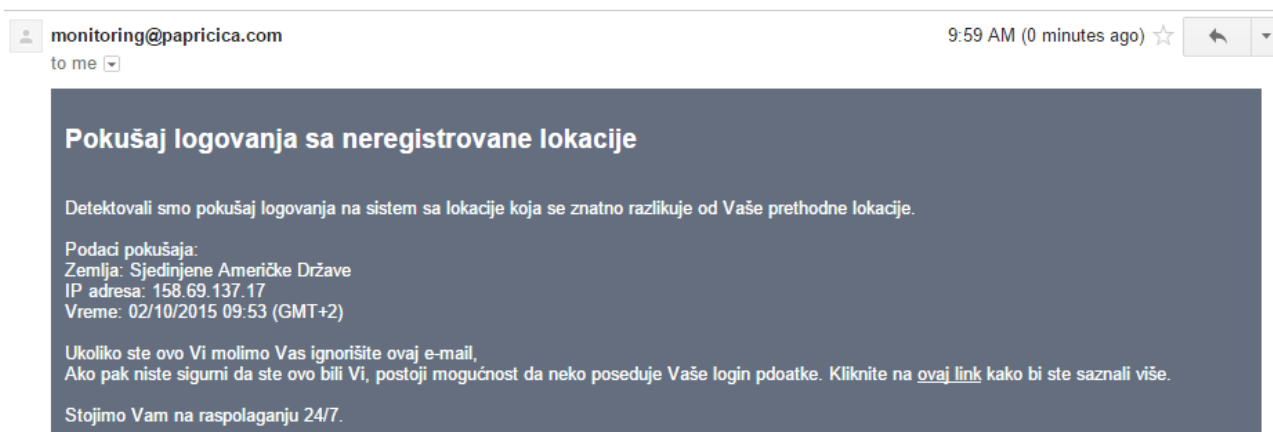
Dodatna lozinka koju ste dobili ima period važnosti od 24 sata.

mihailom

Lozinka *

ULOGUJ ME

Slika 16 - SRSA korak 2



Slika 17 - E-mail obaveštenje o pokušaju logovanja sa nepoznate lokacije

5.1 Dvo-faktorski režim

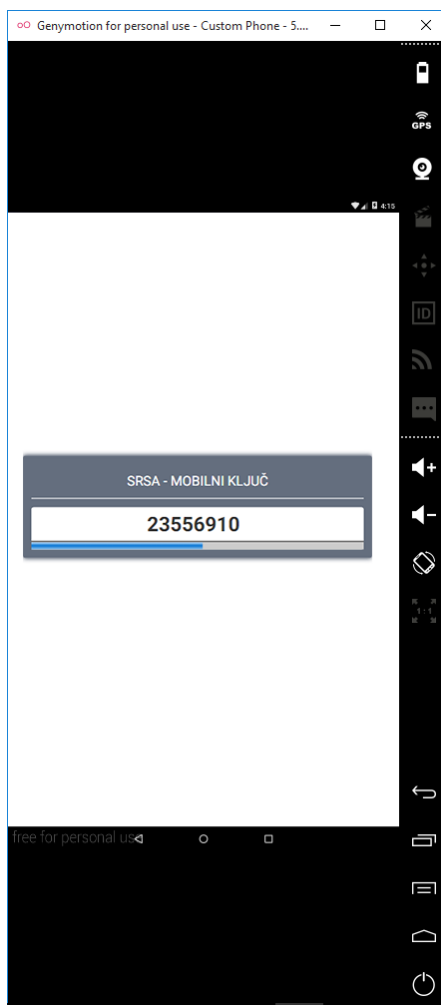
Prvi mod rada sistema dodaje dodatni nivo sigurnosti koji podiže nivo zaštite na celokupnom sistemu i dovoljan je za sisteme na kojima postoji potreba za povišenim nivoom sigurnosti ali gde nivo ne treba da bude previsok tj. informacije koje on sadrži nisu od preteranog značaja (npr. sistem ne sadrži brojeve kreditnih kartica, osetljiva dokumenta i sl.).

Za sisteme koji pak u sebi mogu sadržati ovakve osetljive informacije može se koristiti drugi režim rada sistema a to je mobilni autentifikator, aplikacija za *smartphone* uređaje bazirane na Android operativnom sistemu.

Po dolasku na sistem korisniku se nudi ekran za autentifikaciju, ukoliko nije već ulogovan na sistem. Unošenjem korisničkog imena i lozinke od korisnika se zahteva unošenje dodatnog numeričkog koda od osam cifara. Ulaskom u aplikaciju korisniku se na ekranu prikazuje kod koji on unosi na sistem. Životni vek ovog koda je znatno manji od životnog veka dodatne lozinke iz prethodnog režima, i iznosi 30 sekundi. Ukoliko korisnik unese odgovarajući kod koji je validan dozvoljava mu se pristup na sistem.

Kao i kod prethodnog režima i u ovom režimu se beleže dodatni podaci o korisniku koji se mogu iskoristiti pro-aktivno i reaktivno u slučaju da se dogodi ne autorizovani pristup ili krađa naloga.

Životni vek koda kao i skup karaktera i njihov broj dostupnih pri kreiranju samog koda može se menjati na sistemskom nivou.



Slika 18 - SRSA Mobilni autentifikator – prototip

SRSA - AUTENTIFIKACIJA 2/2

Ukucajte kod koji se prikaže na ekranu Vašeg mobilnog autentifikatora.

mihailom

Kod sa autentifikatora

*

ULOGUJ ME

Slika 19 - SRSA drugi korak - mobilna verzija

5.2 Problemi pri korišćenju

Kao i kod svakog sistema, u radu se mogu pojaviti problem pri korišćenju koji mogu ometi ili potpuno onemogućiti korišćenje.

Prvi i osnovni zahtev za korišćenje sistema jeste postojanje internet konekcije. Sa obzirom na to da u današnje vreme većina korisnika poseduje širokopojasnu internet konekciju koja se odlikuje velikim brzinama i takođe velikom stabilnošću, prvi režim rada u većini slučajeva nudi 99.9% stabilnosti (ali ograničenih realnom stabilnošću e-mail servisa kome pripada e-mail adresa pomoću koje se korisnik prijavio u sistem). Drugi režim se pak oslanja u većini slučajeva na mobilnu mrežu operatera mobilne telefonije na čijem se području korisnik nalazi i stabilnost te mreže može dovesti do povremenih problema pri korišćenju sistema, ali priroda kratkog životnog veka samog koda koji se koristi u ovom režimu osigurava da i ukoliko se greška dogodi ona ne dovede do nemogućnosti korišćenja sistema.

6. Zaključak

Internet predstavlja sadašnjost i budućnost. Razvoj interneta direktno je povezan sa ubrzanim razvojem tehnologije koja se sve više integriše sa našim svakodnevnim životom. Možemo slobodno reći da je današnji život nezamisliv bez upotrebe interneta i tehnologije.

Dvadeset prvi vek predstavlja eru tehnologije, rapidni razvoj nam omogućava daleko veću slobodu u svakodnevnom životu i olakšava međusobnu komunikaciju bez obzira na udaljenost participanata. Internet predstavlja medij koji omogućava većinu ovakvih olakšica i dolazimo u situaciju gde veći deo svetske populacije praktično živi i radi na njemu, Tu su socijalne mreže, različiti online servisi za dostavu i naručivanje robe, poslovi se obavljaju „na mreži“. Samim tim količina informacija i podataka, što slobodnih što privatnih, raste eksponencijalno iz momenta u momenat. Autentifikacioni sistemi predstavljaju vrata kroz koja se mora proći da bi se tim podacima ili uslugama pristupilo.

Tehnologija se može pronaći u svim periodima naše budne faze života, od trenutka kada ustanemo do trenutka kada krenemo na počinak okruženi smo pametnim uređajima, bilo da su to telefoni, televizori, računari. Rad od kuće poprima sve veći udeo u poslovnom okruženju, tele - konferencije na daljinu zamenjuju klasične sastanke u kancelariji. Sve u svemu možemo reći da imamo više slobode u svom dnevnom rasporedu.

Ali ovakav ubrzani razvoj takođe nosi i svoju cenu, moć procesora, skladišni prostor HDD uređaja, moć grafičkih procesora se eksponencijalno uvećala u proteklom periodu, što nas dovodi do problema sigurnosti na Internetu. Paralelino sa našim razvojem razvijaju se i osobe ili organizacije čiji je osnovni cilj monetarna dobit, i koje ništa neće zaustaviti da dostignu taj cilj.

Nekada su standardne lozinke bile sasvim dovoljna mera bezbednosti sistema kojima i danas pristupamo. 2002. internet sajt distributed.net je uspeo da izvrši probijanje 64-bitnog RC5 ključa, i za taj poduhvat koristili su preko 300.000 računara u različitim periodima, računari su bili sposobni da izvrše u proseku oko 12 milijardi provera po sekundi, ceo poduhvat trajao je 4 godine. Već 2011. pojavom jakih grafičkih procesora, običan personalni računar postaje sposoban da izvrši oko 2.8 milijardi provera po sekundi, dok računari napravljeni prvenstveno kao platforme za razbijanje šifara, mogu postići daleko veći broj provera.

Na hipotezu koju smo postavili „Da li postoji savršen sistem autentifikacije?“ može se odgovoriti na jednostavan način. Savršen ili idealan sistem za autentifikaciju ne postoji, jer takve sisteme kreira i osmišlja čovek dok je sa druge strane odnosno u ulozi napadača takođe čovek pa samim tim sve što se napravi može i da se razgradi i probije. Modifikacijom hipoteze u „Da li postoji dovoljno siguran sistem autentifikacije?“ dolazimo do hipoteze koju možemo potvrditi. Ukoliko pratimo sve vodiče i redovno osvežavamo naše sisteme, obaveštavamo korisnike o najnovijim trendovima u oblasti sigurnosti i edukujemo ih o istim, možemo postići zadovoljavajući nivo sigurnosti koji nam je potreban.

Sa svim ovim činjenicama u vidu, moramo unaprediti sisteme autentifikacije i zaštite, upotrebom više stepena autentifikacije. SRSA pokušava da upotrebom dva različita vida dodatne autentifikacije pospeši sigurnost sistema koji štiti i na taj način spreči eventualne upade u sistem i krađu podataka.

Ovaj sistem predstavlja osnovu i dobru podlogu za budući rad i izradu aplikacije za sigurno deljenje i transport fajlova različitog tipa. SRSA bi iza sebe štitio sistem na koji bi se postavljali fajlovi enkriptovani ključem korisnika, kod za dekripciju bi se potom mogao skinuti na eksterni uređaj, telefon, USB ili pametnu karticu, isključivo na uređaju sa koga se fajl postavlja. Potom bi se ključ mogao transportovati do odredišta na kome bi se kod mogao iskoristiti za pristup fajlu i njegovo dekriptovanje.

Budući rad obuhvatiće praktične primere upotrebe modernih metoda autentifikacije i pokazaće domete modernih tehnologija a sve u cilju da se poveća sigurnost autentifikacionog sistema i osigura sigurnost podataka zaštićenih iza ovakvih sistema.

7. Literatura

- [1] Veinović M., Adamović S., „**Kriptologija I: Osnove za analizu i sintezu šifarskih sistema**“, Univerzitet Singidunum, Beograd, 2013.
- [2] Milosavljević M., Adamović S., „**Osnovi teorije informacija i kodovanja**“, Univerzitet Singidunum, Beograd, 2013.
- [3] Jeroen Breebaart, Bian Yang, Ileana Buhan-Dulman, Christoph Busch, „**Biometric template protection: The need for open standards**“, Datenschutz und Datensicherheit - DuD, Vol. 33, No. 5. (1 May 2009), pp. 299-304.
- [4] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, „**Electronic Authentication Guideline**“, NIST Special Publication 800-63-2, 2013.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
- [5] FFIEC - Federal Financial Institutions Examination Council, „**Authentication in an Internet Banking Environment - FAQ**“
<http://www.federalreserve.gov/boarddocs/srletters/2006/sr0613a1.pdf>
- [6] Richard E. Smith, „**Authentication: From Passwords to Public Keys**“, Addison-Wesley Professional, Prvo izdanje, 11.11.2001.
- [7] Bidwell, Teri, „**Hack Proofing Your Identity in the Information Age**“. Syngress Publishing, 2002.
- [8] w3techs.com. „**Usage of server-side programming languages for websites**“
http://w3techs.com/technologies/overview/programming_language/all
- [9] SafeNet, „**Multi-factor Authentication Current Usage and Trends**“, WhitePaper, 2013.
- [10] IETF - The Internet Engineering Task Force, „**Randomness Requirements for Security**“ <https://tools.ietf.org/html/rfc4086>