Napredne metode autentifikacije u računalnim mrežama

Stanić, Maja

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

NAPREDNE METODE AUTENTIFIKACIJE U RAČUNALNIM MREŽAMA

Diplomski rad

Maja Stanić

Osijek, 2019.

Sadržaj:

1. UVOD

U današnje vrijeme sve više korisnika postaje aktivno na internetu za svoje osobne i profesionalne potrebe te se zbog toga internet brzo širi. Ali, zajedno s evolucijom umrežavanja i interneta rastu i moguće prijetnje na njemu samom. Budući da se nalazi na javnoj mreži, ozbiljne sigurnosne prijetnje mogu predstavljati izlaganje osobnih podataka pojedinaca, a također i dostupnost resursa kompanija ili vlade osobama koji ne bih trebali imati uvid u takve podatke.

Uz brzo rastući broj računalnih napada, sigurne računalne mreže postale su potreba svih organizacija. Iako stručnjaci i istraživači za kibernetičku sigurnost već duže vrijeme rade na sprečavanju neovlaštenog pristupa mrežama od malih do velikih poduzeća, broj računalnih napada se povećava iz dana u dan. Da bi održale privatnost, sigurnost i spriječili napade, brojne tvrtke i vlade poduzimaju mnoge sigurnosne mjere, ali je računalna sigurnost i dalje velika briga. Sigurnosti računalne mreže pridavalo se premalo pažnje s obzirom na primjenu i dostupnost tehnologije današnjoj populaciji. Rast broja programera od kojih mnogi nisu dovoljno obučeni po pitanju računalne sigurnosti svrstalo je ovo područje u veoma rizičnu djelatnost te ju čine sve ozbiljnijim problemom. Povećani broj incidenata ukazuje na važnost ovog područja i važnosti edukacije kako mladih koji se tek upoznaju s računalnim svijetom i tehnologijama, tako i iskusnih programera koji moraju držati korak s vremenom i sigurnosnim zahtjevima.

Prvi korak sigurnosnih provjera predstavlja proces autentifikacije i kao takav iznimno je važan za informacijsku sigurnost. Desetljećima se lozinka koristila za provjeru autentičnosti korisnika računala i u to vrijeme predstavljala je dovoljno dobru zaštitu, međutim sada se smatra preslabom metodom provjere i uvode se nove metode. Također, i danas se upotrebljavaju lozinke, ali u nešto drugačijem obliku. Koriste se lozinke s ograničenjem na minimalan broj znakova, teži se kombiniranju velikih i malih slova, brojeva te posebnih znakova, kako bi lozinka bila što teža za otkrivanje. Biometrija postaje jedna od najboljih sigurnosnih metoda budući da nijedna osoba ne dijeli iste fizičke osobine. Međutim, još uvijek nije dovoljno razvijena da postala cjenovno pristupačna za širu upotrebu. Kvalitetni biometrijski uređaji su veoma skupi te se iz tog razloga rjeđe koriste. Da bi se povećala sigurnost korisničkih podataka uvode se kombinacije više autentifikacijskih metoda što uvelike pomaže sprječavanju neovlaštenog pristupa podacima. Ako se pravilno implementira, višefaktorska provjera identiteta napadaču može znatno otežati krađu legitimnih vjerodajnica te onemogućiti daljnje zlonamjerne aktivnosti na mreži.

Zbog svoje učinkovitosti, višefaktorska provjera autentičnosti jedna je od najboljih metoda provjere korisničkih podataka.

U radu će biti objašnjeni osnovni sigurnosni zahtjevi i predstavljena moguća rješenja za ovaj tip problema. Za svako rješenje bit će predložena moguća praktična primjena. Pri implementaciji rješenja za ovu vrstu problema koristit će se dva besplatna poslužitelja, a to su Gluu i FreeRADIUS koji će biti objašnjeni u radu.

2. SEGMENTI PRIJAVE KORISNIKA

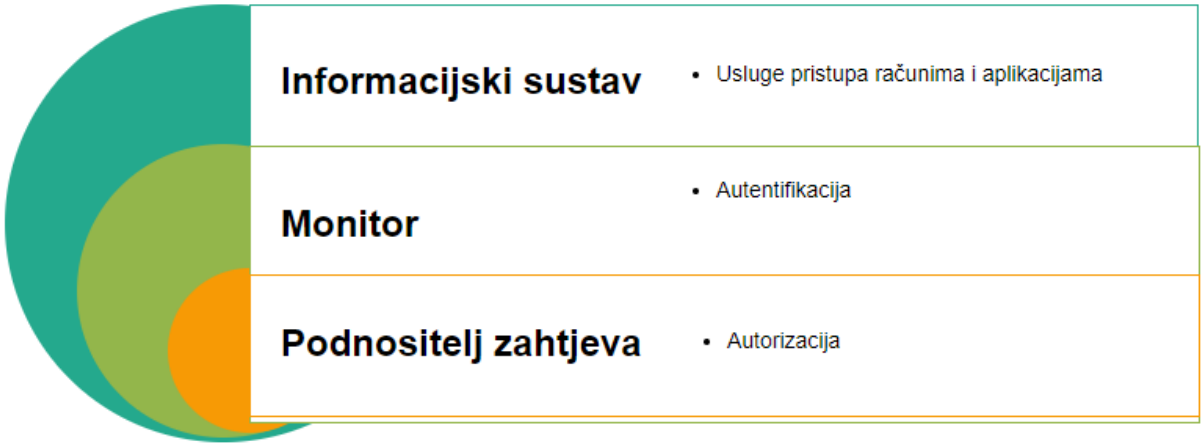
2.1. Identifikacija, autentifikacija i autorizacija

Identifikacija, autentifikacija i autorizacija su tri povezana sustava koji čine jezgru sigurnosti. Često postoji konfuzija između pojmova "identifikacije", "autentifikacije" i "autorizacije". Svaki od ovih pojmova zahtijeva korak upisa. U identifikaciji korisnik izjavljuje tko je on?. Sustavi provjere autentičnosti pružaju odgovore na pitanja: i tko je korisnik?, i je li korisnik stvarno taj koji se predstavlja da jeste? Autorizacija predstavlja ovlasti za svakog korisnika, čime se za svakog korisnika ograničavaju dostupni resursi kako ne bi došlo do zlouporabe ovlasti. U tablici 2.1. prikazana su značenja i metode autentifikacije i autorizacije.

Tablica 2.1. Pojašnjenje pojmova autentifikacije i autorizacije

	Autentifikacija	Autorizacija
Značenje	„Imaš li dopuštenje za pristup aplikaciji ?“	„ Imaš li dopuštenje za izmjenu aplikacije“?
Metode	Lozinka, dvofaktorska autentifikacija, multifaktorska autentifikacija, X509 certifikati, biometrijska autentifikacija, WebAuthN	Kontrola pristupa za URI, lista kontrola pristupa itd.

Proces autentifikacije podrazumijeva različite cjeline, slika 2.1.:



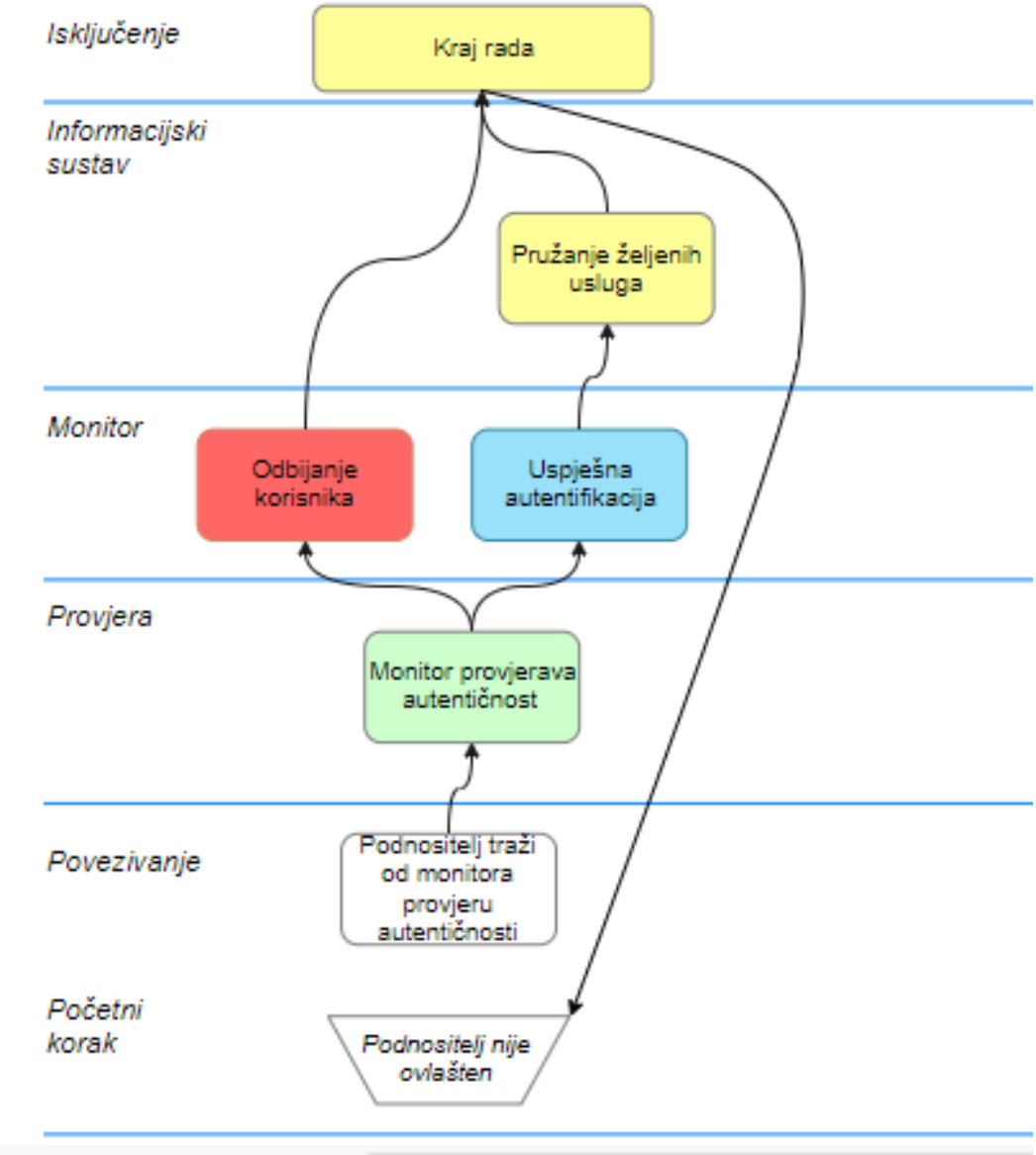
Slika 2.1. Razine autentifikacije

• Podnositelj zahtjeva je entitet koji autorizira sustav kako bi se koristio uslugama. To bi mogla biti osoba ili informacijski sustav (IS);

• Monitor je subjekt koji pruža uslugu provjere autentičnosti. Utvrđuje identitet podnositelja zahtjeva (ili ga odbija u slučaju pogrešne provjere autentičnosti) i provjerava može li se odobriti korištenje potrebne usluge;

• Informacijski sustav (IS) pruža usluge poput pristupa računu računala, aplikaciji itd.

Uobičajeni osnovni koraci za autentifikaciju su grafički prikazani na slici 2.2.



Slika 2.2. Osnovni autentifikacijski koraci

1. Početni korak: podnositelj zahtjeva nije ovlašten.

2. Korak povezivanja:podnositelj zahtijeva za IS upotrebu funkcije koja zahtijeva provjeru autentičnosti. Pita IS monitor za provjeru autentičnosti podnositelja zahtjeva.

3. Korak provjere : podnositelj zahtjeva je ovjeren i sesija je otvorena. IS pruža korisniku tražene funkcije.

4. Korak isključenja: korisnik se isključuje ili je povezan s monitorom i stanje se vraća na početni korak.

Ovaj se korak može pokrenuti u isteku aktivnog vremena za korisnika ili predugog trajanja zahtjeva. IS može zahtijevati različite razine provjere autentičnosti, na primjer, razinu za administratore i razinu za korisnike. U takvom sustavu nivo provjere autentičnosti mjeri se na skali [3]:

- razina 0 za neovlaštenog korisnika s najnižim pravima u sustavu;
- razina N za administratora s punim pravima;
- i jednu ili više razina između 0 i N.

IS može tražiti dodatnu autentifikaciju da bi IS prešao na višu razinu povjerenja za podnositelja zahtjeva. Sigurnost metode provjere autentičnosti ovisi o upotrebljivosti i prihvatljivosti. Ako je upotrebljivost loša, korisnici će brzo pronaći načine kako zaobići korake provjere autentičnosti što predstavlja prijetnju za sigurnost sustava.

Postupak provjere autentičnosti može se temeljiti na kombinaciji jednog ili više faktora provjere autentičnosti.

2.2. Autentifikacijski faktori

Četiri najvažnija faktora za provjeru autentičnosti su:

- Korisnik nešto zna: zaporka, PIN kod, djevojačko prezime majke, ime brata/sestre/prvog ljubimca itd. Faktor nešto što se zna je najčešći korišteni faktor i može biti lozinka ili jednostavan osobni identifikacijski broj (PIN). Međutim, to je i najlakše za razotkriti. Pri korištenju lozinki važno je koristiti jake lozinke. Snažna lozinka sadrži kombinaciju velikih i malih slova te posebnih znakova. U prošlosti su sigurnosni stručnjaci preporučivali da lozinke budu s najmanje osam znakova. Međutim, s povećanjem snage zaporki uobičajeno se preporučuju duže lozinke. Na primjer, mnoge organizacije zahtijevaju da lozinke administratora budu najmanje 15 znakova. Dulje se lozinke teže pamte, osim ako se ne postave u neku vrstu smislenog redoslijeda. Na primjer, fraza poput "Security brings success" može postati lozinka "S3curityBring$Succ3$$". Da se uočiti da svaka riječ započinje velikim slovom, svako malo slovo "s" mijenja se u $, a svako malo slovo "e" mijenja se u 3 i razmaci se uklanjaju. Lozinka se lakše pamti, ali je vrlo složena. Međutim, ako se korisnik mora prisjetiti duge lozinke bez ikakvog značenja, poput "8o%&hk =“mn", vjerojatnije je da će je zapisivati, slabeći sigurnost. Lozinke ne bi trebale sadržavati osobne podatke poput korisnikovog imena. Uz to, zaporka ne

bi trebala biti riječ koja se može naći u rječniku. Rječnik napada koristi bazu riječi sličnih rječniku, isprobavajući sve riječi u bazi podataka za podudaranje. Bitno je naglasiti da postoje napadači koji imaju pristup rječnicima na drugim jezicima. Drugim riječima, zaporka koja upotrebljava riječ s drugog jezika jednako je jednostavna za otkrivanje kao i lozinka koja se koristi na materinjem jeziku.

- Nešto što korisnik posjeduje: USB token, telefon, pametna kartica, softverski token, navigacijski kolačić itd. Pametna kartica je kartica veličine kreditne kartice koja ima ugrađeni certifikat koji se koristi za identifikaciju vlasnika. Korisnik može umetnuti karticu u čitač pametnih kartica radi provjere autentičnosti pojedinca. Pametne kartice uobičajeno se koriste s PIN-om koji omogućuje multifaktornu provjeru identiteta. Drugim riječima, korisnik mora imati nešto (pametnu karticu) i znati nešto (PIN). Token je ručni uređaj s LED-om koji prikazuje broj, a broj je sinkroniziran s autentifikacijskim poslužiteljem.
- Nešto što kvalificira korisnika: otisak prsta, fragment DNA, uzorak glasa, geometrija ruku,skeniranje mrežnice ili šarenice, rukopis i analiza glasa. Otisci prstiju i otisci ruku su danas najrasprostranjenija biometrijska metoda. Mnogi prijenosnici uključuju čitače otiska prsta, a čitači otisaka prstiju dostupni su i na USB uređajima. Otisci ruku upotrebljavaju se s mnogim zabavnim parkovima koji prodaju sezonske propusnice ili višednevne propusnice. Iako biometrija pruža najjaču provjeru autentičnosti, podložna je pogreškama. Lažna pogreška odbijanja, koja se također naziva pogreška tipa 1, događa se kada sustav lažno odbije poznatog korisnika i naznači da korisnik nije poznat. Lažna pogreška prihvaćanja koja se također naziva pogreška tipa 2, događa se kada sustav lažno identificira nepoznatog korisnika kao poznatog korisnika. Biometrijski sustavi obično se mogu prilagoditi za osjetljivost, ali osjetljivost utječe na točnost.[4]
- Nešto što korisnik može učiniti: potpis, gesta itd. Sustavi za provjeru autentičnosti temeljeni na gestama pokazuju potencijal za praktičnu primjenu. Tekstualne lozinke su dobre za korisnike koji koriste tipkovnice s tipkama, širenjem mobilnih uređaja zasloni osjetljivi na dodir postaju sve češći u primjeni. Na tim zaslonima, geste predstavljaju prirodniju i lakšu metodu autentifikacije nego tekstualna lozinka, jer je teže upisati znakovne nizove. Geste mogu biti slobodne forme, odnosno da su stvorene bez ograničenja ili mogu biti unaprijed definirane. Pri upotrebi u mobilnim uređajima vidljivo je više mogućnosti gesta; geste koje počinju i završavaju u jednom pokretu, koristi se samo jedan prst pri autentifikaciji,

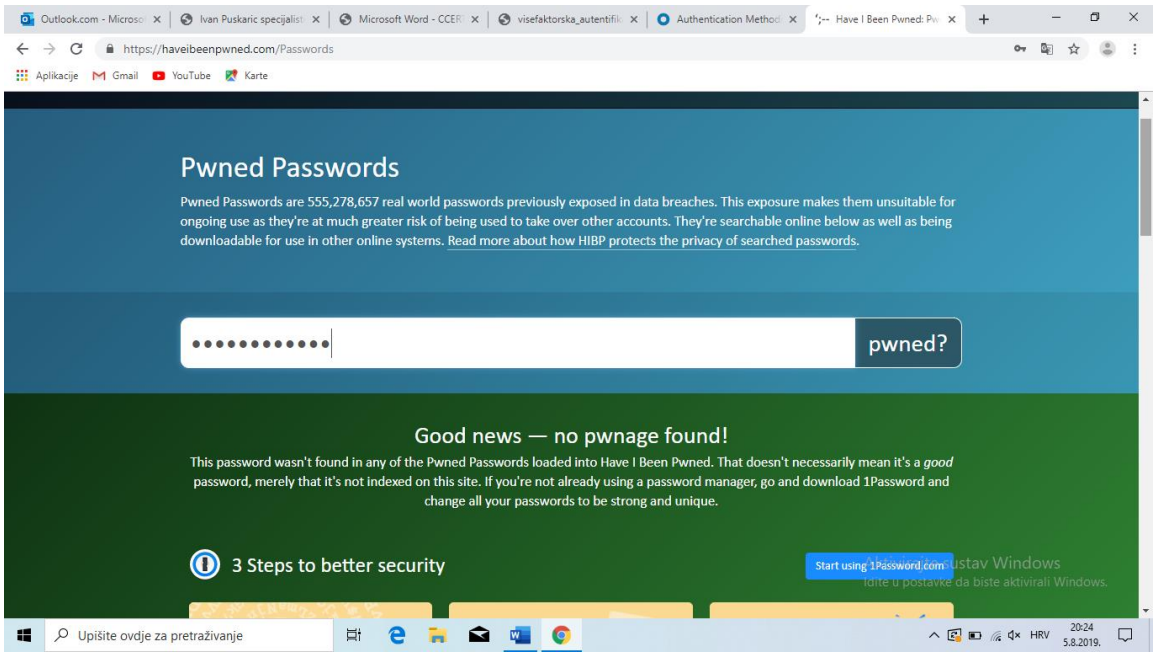
gesta s više dodira, također pored ovih gesta postoji i pokretna gesta na temelju senzora, stvorena rotacijom mobilnog uređaja. Geste koje se temelje na senzorima koriste senzore koji nisu fotoaparat ili zaslon osjetljiv na dodir, kao što je akcelerometar za pametni telefon.

Po potrebi se uključuje i peti faktor provjere autentifikacije:

- Korisnikov položaj: trenutna lokacija / položaj, informacije o trenutnom vremenu itd. [3] Autentifikacija na temelju lokacije rijetko se pojavljuje, ali ona se koristi s daljinskim pristupom kao dodatni faktor autentifikacije. Ako je korisnik ovlašten za rad od kuće koristeći se daljinskim pristupom za povezivanje s resursima. Poslužitelj za udaljeni pristup može se konfigurirati tako da se, čim korisnik pozove i potvrdi autentičnost, poslužitelj prekine i pozove korisničko računalo kod kuće.
  Sve dok se korisnik pokušava povezati s kućnim računalom, veza će raditi. Međutim, ako je napadač pokušao lažno predstavljati korisnika pomoću korisničkog imena i lozinke, napadač se nije mogao povezati. Umjesto toga, kada bi napadač potvrdio autentifikaciju korisnika, poslužitelj udaljenog pristupa bi pokušao nazvati korisnikovo računalo.

3. POSTOJEĆE AUTENTIFIKACIJSKE METODE

Pri korištenju samo lozinke za autentifikaciju, napadač može lako doći do lozinke prilikom korisnikove nepažnje, ako korisnik zapisuje lozinku na vidljiva mjesta ili ako korisnik misli da može imati povjerenja u osobu te mu kaže lozinku, ne znajući da je osoba potencijalni napadač. Korisnici često biraju prejednostavne lozinke, nerijetko istu lozinku koriste za pristup na više različitih sustava. Lozinku unosi korisnik u cijelosti te se prenosi od korisnika do sustava koji ga autentificira čime je izložena riziku da bude uočena i otkrivena i na toj relaciji. Mnogi sustavi pokušavaju zaštiti svoje korisnike davajući kriterije pri postavljanju lozinke kako bi ona postala što sigurnija, zahtijevajući minimalni broj znakova, kombinaciju velikih i malih slova te brojeva i simbola. Do sada je poznat velik broj napada pomoću korisničke lozinke, a na web stranici *Have I Been Pwned* može se provjeriti je li korisnička lozinka do sada ikome bila dostupna prilikom napada. Naravno, na web stranici nisu prikazani 100% sigurni podaci, budući da stranica nema pristup svim sustavima koje korisnik korisni, nego bilježi do sada zabilježene slučajeve napada koji su im poznati. Na slici 3.1. prikazana je provjera jedne lozinke koja se pokazala sigurnom.



Slika 3.1. Provjera lozinke

Ako se autentifikacija obavlja pomoću tokena, napadač može jednostavno ukrasti token na kome se nalaze kriptografski parametri za autentifikaciju te se lako prijaviti u željeni sustav. U proteklih nekoliko godina ovakve prijevare su sve češće te se sve više pažnje pridaje sprječavanju mogućih napada, odnosno prevenciji od napada jer je u većini slučajeva već kasno ako se napad uspješno

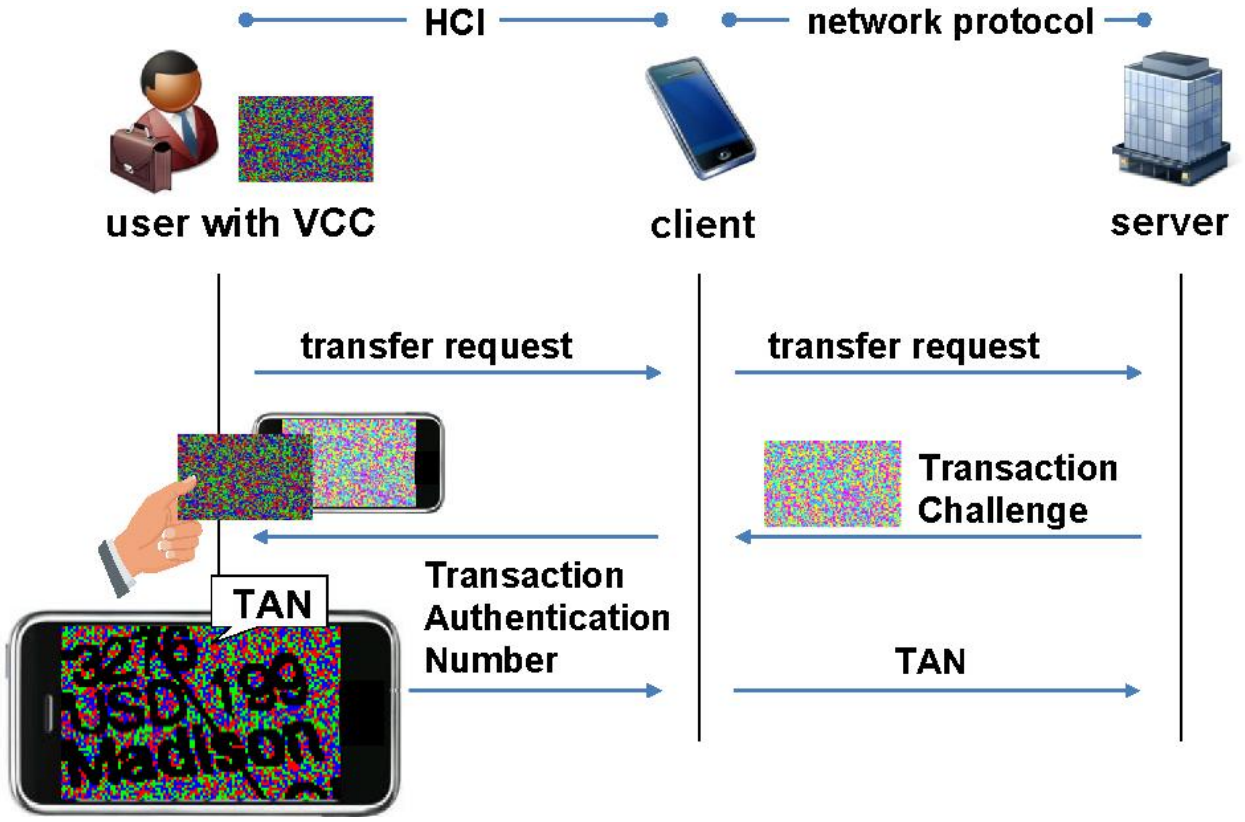
provede. Štete kod kriptografskih napada su ekstremno velike i u psihološkom pogledu, ali i u novčanom budući da su mnogi podaci jako povjerljivi i bitni. Postoji veliki broj metoda i protokola provjere autentičnosti koji se mogu koristiti, ovisno o aplikaciji i sigurnosnim zahtjevima. Neki od njih su :

• Kerberos
• SSL
• PAP i SPAP
• EAP
• RADIUS
• Digitalni certifikati i dr.

3.1.Transakcijska autentifikacija

Transakcijska autentifikacija traži pogreške kada se uspoređuju poznati podaci o korisniku s detaljima trenutne transakcije. Primjer bi bio ako pojedinac živi u Sjedinjenim Američkim Državama, a velike kupovine se pojavljuju dok je prijavljen s IP adrese u Europi. Postavlja se crvena zastava, a zbog opasnosti zahtijevaju se dodatni koraci za provjeru kako bi kupnja bila zakonita i da se obavi provjera da korisnik nije žrtva računalnog napada. Većina banki kao dodatnu sigurnost uvodi TAN-ove *(engl. Transaction authentication numbers).*

Financijske institucije obično daju popis zaporki koje se mogu koristiti za provjeru autentičnosti transakcije, pri čemu svaki TAN vrijedi samo za jednokratnu upotrebu. Financijska institucija koja daje popis TAN-ova održava bazu podataka u kojoj svaki TAN povezuje s određenim korisnikom. TAN se koristi u obradi mrežnih transakcija, on predstavlja dodatni sloj sigurnosti pored lozinke za sigurnu prijavu na račun ili provođenje transakcije. Primjer upotrebe TAN-a u transakcijama putem interneta prikazan je na slici 3.2.



Slika 3.2. Upotreba TAN-a u transakcijama [24]

TAN-ovi se najčešće koriste u mrežnim provjerama transakcija. Kada pojedinac ili poduzeće započne transakciju, njemu se može dostaviti TAN u e-pošti, SMS-u ili drugom metodom. Kada se transakcija provodi, korisnik će dobiti poruku s TAN kodom i od njega će se tražiti da unese taj kod u polje koje je za to predviđeno. Ako se kod točan, transakcija će biti obrađena.[25]

3.2. Biometrija

Biometrija je jedna od boljih autentifikacijskih metoda, a odnosi se na korištenje poznatih i dokumentiranih fizičkih osobina korisnika za provjeru identiteta. Ovo je idealno jer nijedna osoba ne dijeli iste fizičke osobine. Uobičajene biometrijske metode autentifikacije uključuju prepoznavanje otisaka prstiju, prepoznavanje glasa, skeniranje mrežnice i šarenice te skeniranje i prepoznavanje lica. S druge strane, ova metoda treba imati specijaliziranu opremu za skeniranje, što nije idealno za neke industrije te može biti veoma skupo za korištenje, primjer skenera prikazan je na slici 3.3.

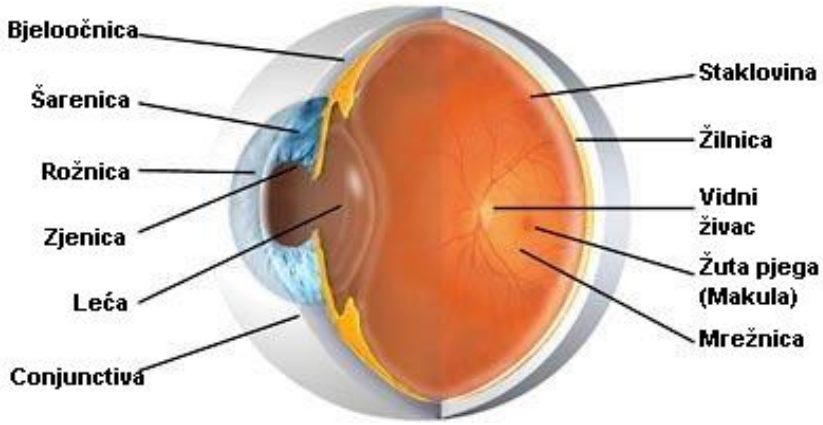
Slika 3.3. Skeniranje otiska prsta[15]

Postoje tri vrste skenera otiska prsta: optički, kapacitivni i ultrazvučni.

- Optički skener fotografira prst, identificira obrazac ispisa i zatim ga sastavlja u identifikacijski kod.
- Kapacitivni skener djeluje mjerenjem električnih signala koji se s prsta šalju na skener. Rubovi ispisa izravno dodiruju skener, šalju električnu struju, dok doline između redova ispisa stvaraju praznine u zraku. Kapacitivni skener u osnovi preslikava kontaktne točke i zračne praznine, što rezultira apsolutno jedinstvenim obrascem. Takvi skeneri se koriste u pametnim telefonima i prijenosnim računalima.
- Ultrazvučni skeneri pojavit će se u najnovijoj generaciji pametnih telefona. U osnovi, oni će emitirati ultrazvuk koji će se odraziti natrag u skener. Slično kapacitivnom, oni čine mapu prsta jedinstvenu za pojedinca.

Oko se smatra jednim od najpouzdanijih dijelova tijela za biometrijsku provjeru autentičnosti, jer mrežnica i šarenica ostaju gotovo potpuno nepromijenjeni tijekom života osobe. Pregled mrežnice osvijetlit će složene krvne žile u očima osobe infracrvenim svjetlom, čineći ih vidljivijim od

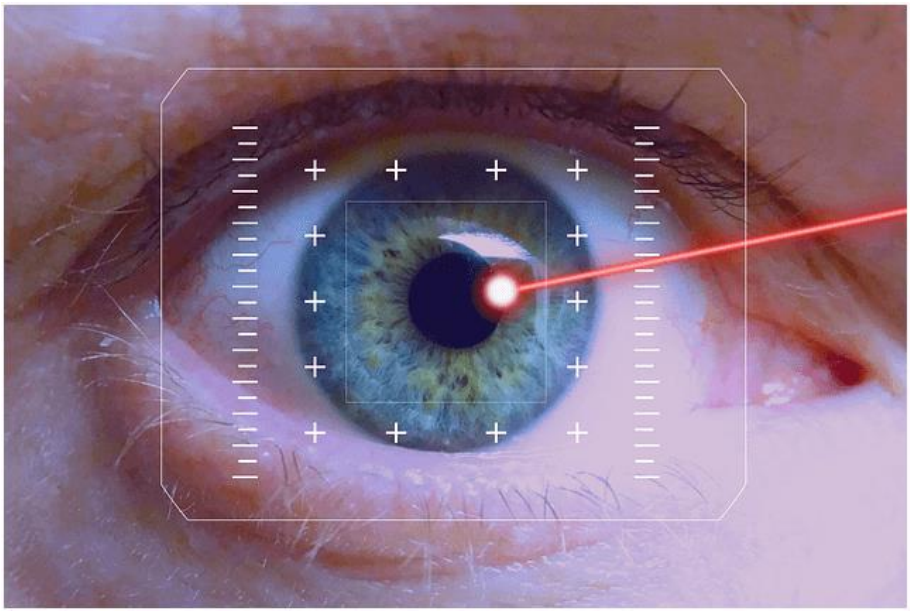
okolnog tkiva. Baš kao otisci prstiju, niti jedna osoba nikad neće imati isti oblik mrežnice. Na slici 3.4. prikazana je građa ljudskog oka.



Slika 3.4. Građa ljudskog oka [16]

Skeneri šarenice oslanjaju se na visokokvalitetne fotografije ili videozapise jedne ili obje šarenice osobe. Šarenice su jedinstvene za pojedinca. Međutim, pokazalo se da je skenere šarenice lako prevariti korištenjem visokokvalitetnih fotografija očiju ili lica subjekta gdje se lako mogu skenirati. Skeneri oka imaju mnogobrojne prednosti u odnosu na skenere prsta. Prst se lako može umazati ili ozlijediti čime se onemogućuje skeniranje. Dok otisak šarenice ostaje nepromijenjen i moguće ga je koristiti bilo kada. Slika 3.5. prikazuje skener šarenice oka.

Glavni nedostatak skenera šarenice je da kvalitetne fotografije lica ili očiju mogu prevariti skener i otključati uređaj.

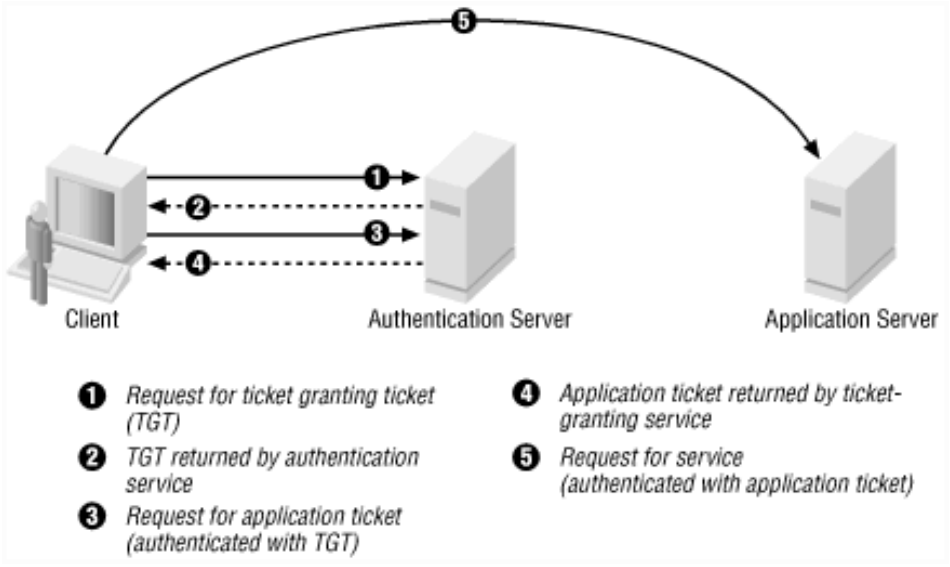


Slika 3.5. Skeniranje mrežnice i šarenice oka[15]

3.3. Kerberos

Kerberos je stvoren na MIT-u kao rješenje za mrežne sigurnosne probleme. Kerberos protokol koristi snažnu kriptografiju tako da klijent može dokazati svoj identitet na poslužitelju (i obrnuto) putem nesigurne mrežne veze. Kerberos koristi simetričnu ključnu kriptografiju i zahtijeva pouzdano ovlaštenje treće strane za provjeru identiteta korisnika.. Nakon što klijent i poslužitelj koriste Kerberos za dokazivanje svog identiteta, oni također mogu šifrirati sve svoje komunikacije kako bi se osigurala privatnost i integritet podataka tijekom njihovog poslovanja. Kerberos je besplatno dostupan na MIT-u. MIT pruža Kerberos u izvornom obliku, tako da svatko tko ga želi koristiti može pogledati kod. Naziv protokola Kerberos zasnovan je na figuri pasa s tri glave iz grčke mitologije poznatog kao Kerberos. Tri glave Kerberosa sadrže KDC *(engl. Key Distribution Center),* klijenta i poslužitelja sa željenom uslugom za pristup. KDC je instaliran kao dio kontrolera domene i obavlja dvije uslužne funkcije:

- AS *(engl. Authentication Service)* -usluge provjere autentičnosti
- TGS *(engl. Ticket-Granting Service)*-usluga izdavanja ulaznica



Slika 3.6. Tri razmjene zahtjeva Kerberos protokola[17]

Na slici 3.6. prikazane su razmjene zahtjeva kod Kerberos protokola.

AS razmjena prikazana je krugovima 1 i 2, razmjena TGS krugovima 3 i 4 i na kraju razmjena klijent /poslužitelj krugom 5.

1. AS razmjena:

Prilikom početne prijave na mrežu, korisnici moraju pregovarati o pristupu unošenjem imena i lozinke za prijavu kako bi ih AS dio KDC-a mogao potvrditi. Nakon uspješne provjere autentičnosti, korisniku se dodjeljuje ulaznica za dobivanje drugih ulaznica TGT *(engl. Ticket to*

Get Tickets) koja vrijedi za lokalnu domenu. TGT ima zadani vijek trajanja od 10 sati i može se obnavljati tijekom korisnikove sesije za prijavu bez potrebe da korisnik ponovno unese svoju lozinku. Ako KDC odobri zahtjev klijenta za TGT, odgovor (koji se naziva AS odgovor) sadrži dva odjeljka: TGT šifriran ključem koji samo KDC (TGS) može dešifrirati i sesijski ključ šifriran lozinkom korisnika za obradu budućih komunikacija s KDC-om. Budući da klijentski sustav ne može pročitati TGT sadržaj, on mora slijepo predstaviti kartu TGS-u za servisne karte. TGT uključuje vrijeme parametara, podatke o autorizaciji, ključ sesije koji se koristi za komunikaciju s klijentom i ime klijenta.

TGS razmjena:

TGS na KDC-u ovjerava TGT korisnika i stvara ključ karte i sesije i za klijenta i za udaljeni poslužitelj. Te informacije, poznate i kao servisna karta, lokalno se spremaju u memoriju klijenta. Korisnik prezentira TGT TGS dijelu KDC-a kada želi pristupiti usluzi poslužitelja. TGS na KDC-u ovjerava TGT korisnika i stvara ključ karte i sesije i za klijenta i za udaljeni poslužitelj. Te informacije, poznate i kao servisna karta, lokalno se spremaju u memoriju klijenta.

TGS prima klijentov TGT i čita ga pomoću vlastitog ključa. Ako TGS odobri zahtjev klijenta, generira se servisna karta i za klijenta i za ciljni poslužitelj. Klijent čita svoj dio pomoću ključa TGS sesije dohvaćenog ranije iz odgovora AS. Klijent predstavlja poslužiteljski dio TGS odgovora ciljnom poslužitelju u narednoj razmjeni klijent / poslužitelj.

Klijent/ poslužitelj razmjena:

Nakon što korisnik dobije uslugu klijent / poslužiteljske karte, može uspostaviti sesiju s uslugom poslužitelja. Poslužitelj može dešifrirati informacije koje dolaze iz TGS-a neizravno koristeći vlastiti dugoročni ključ s KDC-om. Servisna karta koristi se za autentifikaciju klijenta i uspostavljanje sesije usluge između poslužitelja i klijenta. Nakon prekoračenja životnog vijeka karte, servisnu je kartu potrebno obnoviti za upotrebu usluge.

3.3.2. Simetrična kriptografija

Simetrično šifriranje je vrsta šifriranja kod koje se samo jedan ključ (tajni ključ) koristi za šifriranje i dešifriranje elektroničkih podataka. Subjekti koji komuniciraju putem simetrične enkripcije moraju razmjenjivati ključ kako bi se mogao koristiti u postupku dešifriranja. Ova metoda šifriranja razlikuje se od asimetrične enkripcije gdje se par ključeva, jedan javni i jedan privatni, koriste za šifriranje i dešifriranje poruka. Pomoću simetričnih algoritama šifriranja podaci se pretvaraju u obrazac koji ne može razumjeti onaj tko nema tajni ključ za dešifriranje. Jednom kada primatelj, koji posjeduje ključ, primi poruku, algoritam radi tako da se poruka vrati

u izvorni i razumljivi oblik. Tajni ključ koji i pošiljatelj i primatelj mogu koristiti može biti određena lozinka ili slučajni niz znakova koji su generirani sigurnim generatorom slučajnih brojeva (RNG).

Postoje dvije vrste algoritama za simetrično šifriranje:

- Blok algoritmi: Postavljene duljine bitova šifriraju se u blokovima elektroničkih podataka pomoću posebnog tajnog ključa. Dok se podaci šifriraju, sustav drži podatke u svojoj memoriji dok čeka završetak bloka.
- Stream algoritmi: Podaci se šifriraju u toku umjesto da se zadržavaju u memoriji sustava.

Neki primjeri simetričnih algoritama za šifriranje su:

- AES (*engl. Advanced Encryption Standard*)
- DES (*engl. Data Encryption Standard*)
- IDEA (*engl. International Data Encryption Algorithm*)
- Blowfish (*engl. Drop-in replacement for DES or IDEA*)
- RC4 (*engl. Rivest Cipher 4*)
- RC5 (*engl. Rivest Cipher 5*)
- RC6 (*engl. Rivest Cipher 6*)

AES, DES, IDEA, Blowfish, RC5 i RC6 su blok algoritmi. Dok je RC4 je algoritam toka.

3.4. SSL

SSL*(engl. Secure Sockets Layer*) provjera identiteta temelji se na digitalnim certifikatima koji omogućuju web poslužiteljima i klijentima da provjere međusobni identitet prije nego što uspostave vezu. Čime ostvaruju međusobnu provjeru autentičnosti. Dakle, koriste se dvije vrste certifikata: certifikati klijenta i certifikati poslužitelja. SSL se koristi za osiguravanje sigurnog pristupa web stranicama, koristeći kombinaciju tehnologije javnih ključeva i tehnologije tajnih ključeva. Tajno šifriranje ključa, odnosno simetrično šifriranje je brže, ali asimetrično šifriranje javnih ključeva omogućuje bolju provjeru autentičnosti, tako da je SSL dizajniran da koristi prednosti oba.

Bez SSL-a, podaci poslani između klijenata i poslužitelja šalju se u običnom tekstu, što olakšava presretanje. Svi koji mogu oteti protok podataka imat će neograničen pristup običnom tekstu. Ako je SSL na mjestu, podaci se šifriraju - čak i ako ih presreću, neće ih biti moguće dešifrirati.

Za stvaranje SSL veze web-poslužitelju potreban je SSL certifikat. SSL certifikat može se dobiti od certifikacijskog tijela (ili CA), kao što je SSL.com. SSL certifikat obično sadrži ime domene, naziv tvrtke, adresu, grad i državu. Također će sadržavati datum isteka potvrde i detalje o CA koji

su odgovorni za izdavanje potvrde. Kada se preglednik poveže sa sigurnom web lokacijom, dohvatit će SSL certifikat te provjeriti je li istekao rok trajanja, je li ga izdalo certifikacijsko tijelo kojemu preglednik vjeruje, a koristi ga web mjesto za koje je izdano. Ako ne uspije ni u jednom od ovih provjera, preglednik će krajnjem korisniku prikazati upozorenje dajući mu do znanja da web mjesto nije zaštićeno SSL-om.[8]

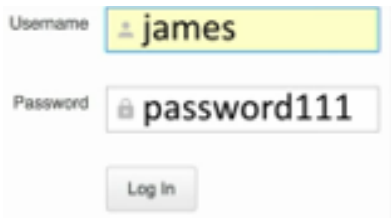
Slika 3.7. SSL provjera autentičnosti

1.Preglednik se povezuje na web poslužitelj (web stranicu) osiguran SSL-om (https). Preglednik traži da se poslužitelj identificira.
2. Server šalje kopiju svog SSL certifikata, uključujući javni ključ poslužitelja.
3. Preglednik provjerava korijen certifikata na popisu pouzdanih službenika za potvrdu te da je certifikat istekao, neiskorišten i da je njegovo uobičajeno ime važeće za web mjesto s kojim se povezuje. Ako preglednik vjeruje u certifikat, kreira ga, šifrira i vraća simetrični sesijski ključ pomoću javnog ključa poslužitelja.
4. Poslužitelj dešifrira simetrični ključ sesije svojim privatnim ključem i šalje potvrdu šifriranu ključem sesije da pokrene šifriranu sesiju.
5. Poslužitelj i preglednik kriptiraju sve prenesene podatke ključem sesije.

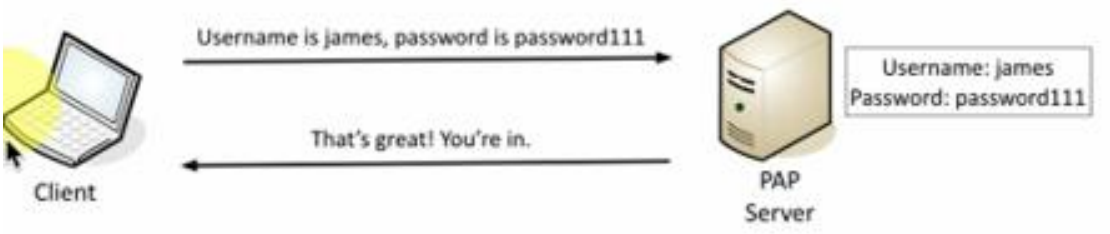
3.5. PAP

PAP (*engl. Password Authentication Protocol*) se koristi za provjeru autentičnosti korisnika putem daljinskog upravljačkog pristupa. Važna karakteristika PAP-a je da on šalje korisničke lozinke po mreži na poslužitelju za provjeru autentičnog teksta. To predstavlja značajan sigurnosni rizik, jer neovlašteni korisnik može snimiti pakete podataka pomoću analizatora *(engl. sniffer)* i dobiti lozinku.

Prednost PAP-a je što je kompatibilan s mnogim poslužitelja koji rade na različitim operativnim sustavima. PAP se treba upotrebljavati samo kad je to nužno za potrebe kompatibilnosti.



Slika 3.8. Forma za autentifikaciju korisnika



Slika 3.9. PAP autentifikacija[18]

Na slici 3.8. je prikazano slanje korisničkog imena i lozinke potrebnih za autentifikaciju korisnika. Kao što je vidljivo na slici 3.9., lozinka se šalje u izvornom obliku. PAP server sadrži bazu podataka koja također sadrži korisničko ime i lozinku gdje se povjerava odgovaraju li poslano korisničko ime i lozinka podacima iz baze. Nakon čega se odobrava ili odbija pristup korisniku.

3.6. SPAP

SPAP *(engl. Shiva Password Authentication Protocol)* je poboljšanje u odnosu na PAP u sigurnosnom pogledu, jer koristi šifriranje (koristi se Shiva poslužiteljima daljinskog pristupa). Klijent šalje korisničko ime zajedno sa šifriranom lozinkom, a udaljeni poslužitelj ga dešifrira. Ako se korisničko ime i zaporka podudaraju s podacima u bazi podataka poslužitelja, udaljeni poslužitelj šalje poruku potvrde (ACK) i omogućuje vezu. Ako nije, šalje se negativna potvrda (NAK) i veza je odbijena. Međutim, ovaj oblik autentifikacije ima i svoje nedostatke. Iako je zaštićen i šifriran, može doći do problema s hakiranjem takozvanim ponovnim napadima. Razlog za ovu osjetljivost je taj što se iste vjerodajnice šalju u svakom smjeru svaki put kada se korisnik pokuša prijaviti. Haker koji "sluša poslužitelj ili virtualnu mrežu" može hakirati taj signal i biti u mogućnosti koristiti taj signal za infiltraciju sustav. Ovaj oblik provjere autentičnosti sada je široko

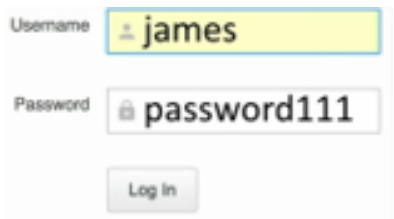
obeshrabren zbog ove ozbiljne sigurnosne prijetnje. Većina virtualnih mreža prekinula je upotrebu ovog oblika provjere autentičnosti. SPAP provjera autentičnosti je sigurnija od otvorenog teksta, ali manje sigurna od CHAP ili MS-CHAP protokola provjere autentičnosti.[9]

3.7. CHAP

CHAP *(engl. Challenge-Handshake Authentication Protocol*) je mehanizam provjere autentičnosti koji ne šalje lozinku poslužitelju. Umjesto toga, klijent stvara slučajni niz, koji se zove izazov, i izvodi hash MD5 radi kombiniranja izazova s lozinkom. Klijent tada šalje obje lozinke i izazov i hash na poslužitelju. Ako poslužitelj ima pristup Cleartext-lozinki, onda izvodi isti izračun MD5 i uspoređuje njegov hash s onim koji mu je poslao klijent. Prednost CHAP metode je u tome što se lozinka nikad ne šalje u paketu. Međutim, nedostataka je mnogo:

- ako poslužitelj nema pristup Cleartext-lozinki, provjera autentičnosti neće uspjeti;
- RADIUS paketi koji sadrže CHAP mogu se trivijalno reproducirati, što je sigurnosni problem;
- klijent nema potvrdu je li poslužitelj provjerio hash ili ga nikada nije provjerio jer nije vratio Access-Accept.

Zbog tih razloga CHAP ne treba koristiti. Još jedna prednost CHAP-a u odnosu na PAP je ta što se CHAP može postaviti tako da radi ponovljene provjere autentičnosti. Ovo je korisno za dial-up sesije PPP i druge sesije u kojima se port može ostaviti otvoren iako je udaljeni uređaj isključen. U ovom je slučaju moguće da netko drugi pokupi vezu usred sesije jednostavno uspostavljanjem fizičke povezanosti.



Slika 3.10. Forma za autentifikaciju korisnika

Slika 3.11. CHAP autentifikacija[18]

Na slici 3.11. prikazana je autentifikacija putem CHAP protokola:

1. Klijent šalje poruku poslužitelju, ali samo s korisničkim imenom
2. Poslužitelj sadrži podatke o korisničkom imenu i lozinki, te kreira posebnu poruku koja predstavlja izazov i šalje ju natrag prema klijentu.
3. Klijent uspoređuje dobiveni izazov s lozinkom i šalje posebni hash odgovor prema poslužitelju
4. Poslužitelj provodi isti izračun na svojoj strani i uspoređuje dobiveni hash od klijenta i svoj te ako su hashovi jednaki klijentu omogućava pristup, u suprotnom se klijent odbija.

3.8. MS-CHAP

MS-CHAP *(engl. Microsoft Challenge Handshake Authentication Protocol)* mehanizam sličan je CHAP metodi i dolazi u dva oblika: MS-CHAPv1 i MS-CHAPv2.

MS-CHAPv1 koristi algoritam MD4 umjesto MD5 koji mu omogućuje korištenje NT hash oblika lozinke, pored lozinke običnog teksta. MS-CHAPv2 dodaje dodatni korak „odgovor-izazov“ između klijenta i poslužitelja. Ovaj korak odgovor na izazov omogućuje klijentu i poslužitelju da provjere jedan drugomu lozinku. Dodatni korak znači da je MS-CHAP sigurniji i lakši za implementaciju od uobičajenog CHAP.[5]

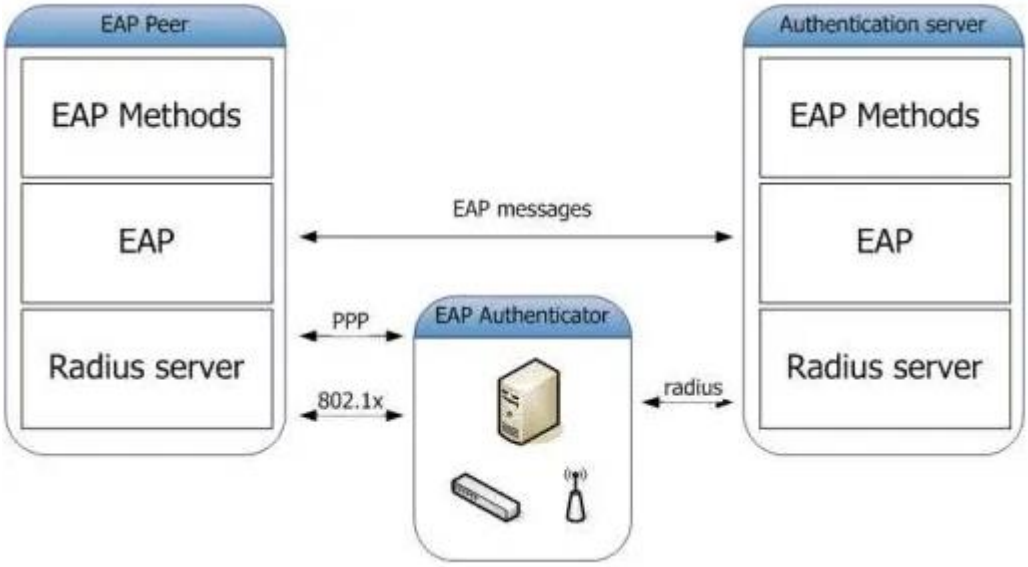
3.9. EAP

EAP *(engl. Extensible Authentication Protocol)* se koristi za autentifikaciju konekcije kod protokola točka-točka-PPP *(engl. Point-to-Point Protocol)* koja komunikacijskim računalima omogućuje pregovaranje o određenoj shemi provjere autentičnosti Ključna karakteristika EAP-a je njegova proširivost, naznačena njegovim nazivom. Moduli za dodavanje mogu se dodati i na strani klijenta i na strani poslužitelja za podršku novih EAP vrsta.

EAP se može koristiti s TLS-om, tzv. EAP-TLS, za pružanje međusobne provjere autentičnosti putem razmjene korisničkih i strojnih certifikata. EAP može podržati više mehanizama provjere

autentičnosti, poput token kartica, pametnih kartica, potvrda, jednokratnih lozinki i provjere enkripcije javnih ključeva.

U komunikacijama putem EAP-a korisnik zahtijeva povezivanje s bežičnom mrežom putem pristupne točke (stanica koja prenosi i prima podatke, ponekad poznate i kao primopredajnik). Pristupna točka zahtijeva identifikacijske (ID) podatke od korisnika i šalje ih na poslužitelju identiteta. Poslužitelj autentifikacije traži pristupnu točku za dokaz valjanosti ID-a. Nakon što pristupna točka pribavi tu provjeru od korisnika i pošalje je natrag na autentifikacijski poslužitelj, korisnik se povezuje na mrežu prema zahtjevu.[10]



Slika 3.12. EAP infrastruktura[20]

Osnovna EAP infrastruktura:

- EAP točka- računalo koje pokušava pristupiti mreži, poznato i kao pristupni klijent
- EAP autentifikator- pristupna točka ili poslužitelj mrežnog pristupa (NAS), koji zahtijeva EAP provjeru autentičnosti za pristup mreži
- Poslužitelj autentifikacije- poslužitelj koji pregovara o uporabi određene EAP metode. Obično je poslužitelj za provjeru identiteta poslužitelj RADIUS.

3.10. RADIUS

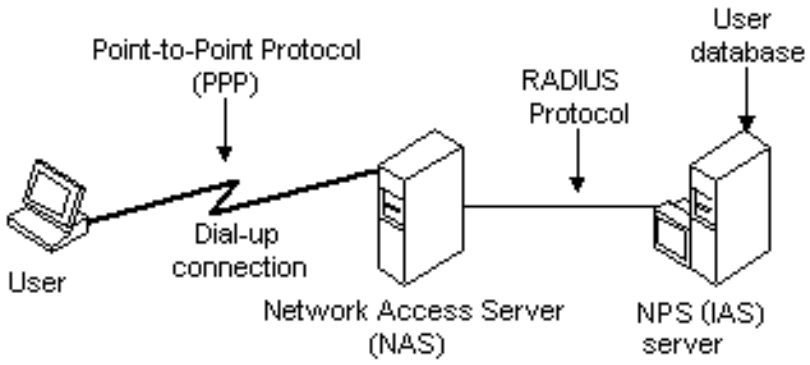
RADIUS *(engl. Remote Authentication Dial-In User Service)* korisnička usluga udaljene provjere autentičnosti mrežni je protokol koji mrežama pruža sigurnost od neovlaštenog pristupa. RADIUS osigurava mrežu omogućavanjem centralizirane provjere autentičnosti korisnika koji se biraju te autorizirajući njihov pristup korištenju mrežne usluge. Upravlja daljinskom provjerom

autentičnosti, autorizacijom i računovodstvom (AAA). RADIUS često koriste ISP*(engl. Internet Service Providers)* za autentifikaciju i autorizaciju dial-up ili VPN *(engl. Virtual Private Network)* korisnika. RADIUS poslužitelj prima korisničke vjerodajnice i podatke o povezivanju od dial-up klijenata i ovjerava ih u mreži.

Princip rada RADIUS protokola:

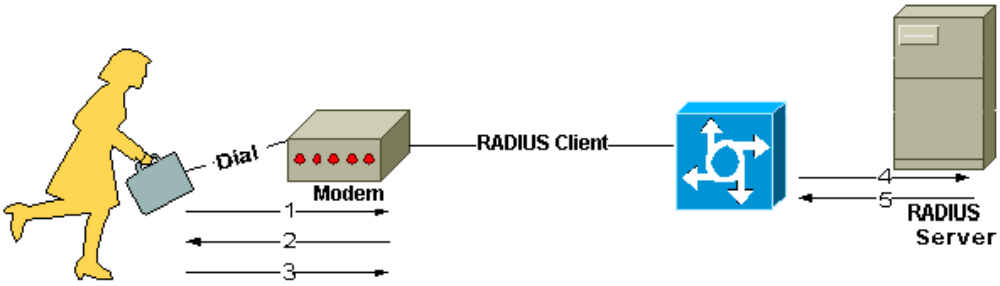
Korisnik ili uređaj šalje zahtjev poslužitelju mrežnog pristupa- NAS *(engl. Network Access Server)* radi dobivanja pristupa mrežnom resoru. Ovaj zahtjev uključuje pristupne vjerodajnice, kao što su korisničko ime i zaporka, koje se na protokol na razini veze šalju na NAS uređaj. Zahtjev može sadržavati i druge podatke o korisniku, kao što su mrežna adresa, telefonski broj ili fizička povezanost s NAS-om.

RADIUS poslužitelj provjerava jesu li informacije točne pomoću protokola za provjeru autentičnosti (npr. PAP, CHAP, EAP). Poslužitelj RADIUS vraća se s jednim od tri odgovora: pristup je odbijen, pristup izazovu, pristup je potvrđen. Svaki od ovih odgovora može se prenijeti korisniku na povratnoj web stranici. Nakon provjere autentičnosti korisnika RADIUS poslužitelj će provjeriti je li korisnik ovlašten za određenu mrežnu uslugu, slika 3.13 .



Slika3.13. Princip rada RADIUS protokola

EAP poruke mogu se proslijediti na RADIUS poslužitelj radi provjere autentičnosti. EAP je potrebno instalirati samo na RADIUS poslužitelju, dok nije potreban na klijentskom računalu. Windows 2000 uključuje uslugu RADIUS poslužitelja nazvanu IAS*(engl. Internet Authentication Services)*, koja implementira RADIUS standarde i omogućuje upotrebu PAP, CHAP i EAP.



Slika 3.14. Interakcija između korisnika i RADIUS klijenta i poslužitelja[21]

Na slici 3.14. prikazana je razmjena poruka između klijenta i poslužitelja.

1. Korisnik pokreće PPP provjeru autentičnosti na NAS-u.
2. NAS zahtijeva korisničko ime i lozinku, ako je protokol provjere autentičnosti lozinke PAP metoda ili izazov, ako je protokol provjere autentičnosti CHAP metoda.
3. Odgovor korisnika.
4. Klijent RADIUS šalje korisničko ime i šifriranu lozinku na RADIUS poslužitelj.
5. RADIUS poslužitelj reagira s prihvaćanjem, odbijanjem ili izazovom.

3.11. Digitalni certifikati

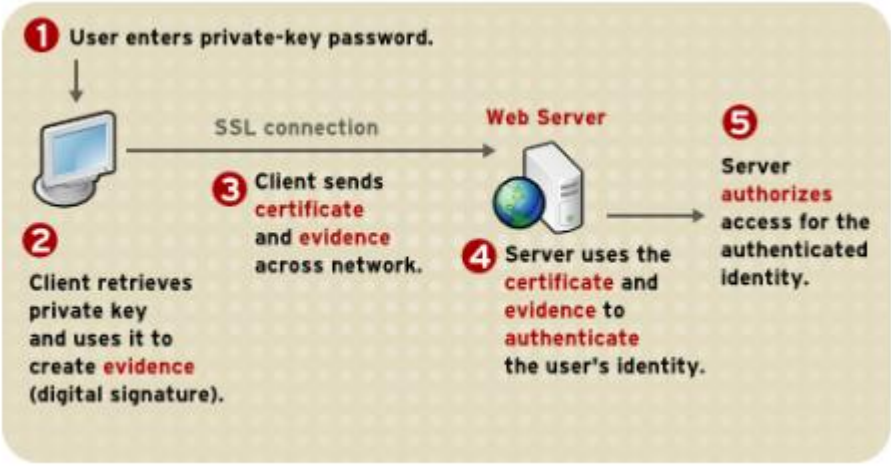
Autentifikacija na temelju certifikata je upotreba digitalne potvrde za identifikaciju korisnika, stroja ili uređaja prije nego što se odobri pristup resursu, mreži, aplikaciji itd. U slučaju provjere autentičnosti korisnika, često se primjenjuje u koordinaciji s tradicionalnim metodama kao što su kao korisničko ime i lozinku. Jedan od diferencijatora provjere autentičnosti na temelju certifikata jest taj što se za razliku od nekih rješenja koja djeluju samo za korisnike, kao što su biometrija i jednokratne lozinke (OTP), isto rješenje može koristiti za sve krajnje točke - korisnike, stroj, uređaje, pa čak i sve veći Internet Stvari (IoT).

Većina rješenja temeljenih na certifikatima danas imaju platformu upravljanja temeljenu na oblaku koja administratorima olakšava izdavanje certifikata novim zaposlenicima, obnavljanje certifikata i opoziv certifikata kad zaposlenik napusti organizaciju.

Za razliku od nekih metoda provjere autentičnosti poput biometrijskih ili OTP tokena, dodatni hardver nije potreban. Potvrde se pohranjuju lokalno na stroj ili uređaj. To ne samo da štedi troškove, već može i smanjiti posao oko distribucije, zamjene i povlačenja tokena.

Digitalni certifikati sastoje se od podataka koji se koriste za provjeru autentičnosti i sigurnosti komunikacija, posebno na nezaštićenim mrežama, npr. internetu. Potvrde pridružuju javni ključ korisniku ili drugom entitetu (računalu ili usluzi) koji ima odgovarajući privatni ključ. Potvrde izdaju certifikacijska tijela (CA), koji jamče identitet korisnika ili računala. CA digitalno potpisuje certifikate koje izdaju koristeći svoj privatni ključ. Potvrde vrijede samo određeno vremensko

razdoblje, te nakon isteka potvrde treba zatražiti novu. CA također može opozvati potvrde koje daju ako se uoče određene pogreške. Digitalni certifikati dio su infrastrukture javnih ključeva (PKI) [1].



Slika 3.15. Korištenje certifikata za provjeru autentičnosti klijenta na poslužitelju [22]

Na slici 3.15. prikazana je upotreba certifikata za provjeru autentifikacije korisnika po koracima:

1. Klijentski softver održava bazu podataka privatnih ključeva koji odgovaraju javnim ključevima objavljenim u svim certifikatima izdanim za tog klijenta. Klijent traži lozinku za ovu bazu podataka kada prvi put klijent treba pristupiti tijekom određene sesije, kao što je prvi put kada korisnik pokušava pristupiti poslužitelju koji podržava SSL i za koji je potrebna provjera autentičnosti klijenta. Nakon što jednom unese ovu lozinku, korisnik je ne mora ponovno unositi tijekom ostatka sesije, čak i kada pristupa drugim poslužiteljima koji podržavaju SSL.
2. Klijent otključava bazu podataka s privatnim ključem, dohvaća privatni ključ za korisnički certifikat i koristi taj privatni ključ za potpisivanje podataka nasumično generiranih iz ulaza i od klijenta i od poslužitelja. Ovi podaci i digitalni potpis dokaz su valjanosti privatnog ključa. Digitalni potpis može se kreirati samo tim privatnim ključem i može se potvrditi odgovarajućim javnim ključem prema potpisanim podacima, što je jedinstveno za SSL sesiju.
3. Klijent šalje i korisnikovu potvrdu i nasumično generirane podatke putem mreže.
4. Poslužitelj koristi certifikat i potpisane podatke za provjeru identiteta korisnika.
5. Poslužitelj može obavljati i druge zadatke provjere autentičnosti, poput provjere da li je certifikat koji je prikazao klijent spremljen u korisnikov unos u LDAP direktoriju. Poslužitelj zatim procjenjuje je li identificiranom korisniku dopušten pristup traženom

resoru. Ako je rezultat procjene pozitivan, poslužitelj omogućuje klijentu pristup traženom resursu.

Potvrde zamjenjuju dio provjere autentičnosti kod interakcije između klijenta i poslužitelja. Umjesto da od korisnika zahtijeva kontinuirano slanje zaporki preko mreže, jednokratna prijava zahtijeva da korisnik jednom unese lozinku, bez slanja putem mreže. Za ostatak sesije klijent predstavlja korisnikovu potvrdu za autentifikaciju korisnika na svakom novom poslužitelju na kojeg naiđe.

3.12. Višestruka autentifikacija

U praksi je pokazano da korištenje pojedinačnih metoda autentifikacije nije dovoljno dobra zaštita za određene sustave te se predlaže zajednička primjena više zasebnih mehanizama autentifikacije čime se osigurava veća zaštićenost sustava. Sve je veća primjena dvostruke, trostruke i višestruke autentifikacije što omogućava veću zaštitu sustava. Višestruka autentifikacija zahtijeva dva ili više neovisnih načina provjere identiteta. Na primjer nešto što korisnik posjeduje, poput telefona ili drugog fizičkog znaka, svojstvene čimbenike poput biometrijskih osobina ili nešto poznato poput lozinke. Bankomati su glavni primjeri višestruke autentifikacije jer je potrebna kartica (nešto što se posjeduje) i PIN (nešto poznato) da bi se transakcija mogla obaviti. U računalnoj sigurnosti višestruka autentifikacija slijedi isti princip. Nakon unosa korisničkog imena i lozinke, korisnici trebaju unijeti jednokratni kod s određenog fizičkog uređaja. Kod se može poslati na korisnički mobilni uređaj putem tekstualne poruke ili se može generirati pomoću mobilne aplikacije. Ako napadač pogodi lozinku, ne može nastaviti bez korisnikovog mobilnog uređaja; obrnuto, ako ukradu mobilni uređaj, i dalje ne mogu ući bez lozinke. Višestruka autentifikacija se provodi na sve većem broju web stranica o bankama, e-pošti i društvenim medijima. Kad god je ponuđena ta opcija za autentifikaciju, preporučuje se omogućiti ju za bolju sigurnost. Na slici 3.16. i slici 3.17. su prikazani mogući načini primjene višestruke metode autentifikacije.

Slika 3.16. .Kombiniranje lozinke i korisničkog imena s ostalim metodama autentifikacije[23]

Slika 3.17. Upotreba biometrije prsta na bankomatu [26]

Neki primjeri najčešće korištene dvofaktorske provjere autentičnosti su:

- Pomoću bankovne kartice (nešto što se ima) i PIN-a (nešto što se zna) za podizanje novca s bankovnog računa na bankomatu. Korištenje hardverskog tokena izdanog odjela korporativnog informatičkog odjela (nešto što se ima) koji generira određeni broj koji se treba unijeti s korisničkim imenom i lozinkom (nešto što se zna) za prijavu na svoju korporativnu mrežu.
- Pomoću aplikacije na pametnom telefonu ili tabletu koja ima ovlasti (nešto što se ima) s korisničkim imenom i zaporkom (nešto što se zna) za pristup privatnom bankarstvu.
- Određivanje računa e-pošte (nešto čemu se ima pristup) da bi se dobila potvrda kad se unese korisničko ime i lozinku (nešto što se zna) za pristup različitim sigurnim web stranicama.
- Primanje numeričkog koda u SMS poruci na korisnikovom pametnom telefonu (nešto što se ima) i korištenje istog u kombinaciji s korisničkim imenom i zaporkom (nešto što se zna) za prijavu na sigurnu web lokaciju.

Nužno je razumjeti da višefaktorsku autentifikaciju ne čine dvije iste metode, nego je bitno koristiti više različitih metoda iz različitih skupina. Korisnik mora uspješno obaviti identifikaciju na svim odabranim metodama kako bih pristupio željenom resursu.

4. IMPLEMENTACIJA I TESTIRANJE BESPLATNIH AUTENTIFIKACIJSKIH RJEŠENJA

U praktičnom dijelu rada prikazat će se dva besplatna rješenja za autentifikaciju korisnika, a to su Gluu poslužitelj i FreeRADIUS poslužitelj te nekoliko njihovih metoda. Predložena rješenja će se međusobno usporediti te predložiti moguću praktičnu primjenu svake od predloženih metoda.

4.1. Gluu poslužitelj

Gluu je besplatno rješenje za upravljanje identitetom i pristupom, IAM *(engl. Identity and Access Management).* Komercijalne web i mobilne aplikacije mogu koristiti Gluu poslužitelj za provjeru autentičnosti korisnika, podataka o identitetu korisnika i reguliranje pravila korištenja aplikacija.

Uobičajena uporaba Gluu poslužitelja uključuju:

- Pojedinačna SSO prijava *(engl. Single sign-on*)
- Mobilna provjera autentičnosti
- Upravljanje pristupom API-ju *(engl. Application programming interface)*
- Dvofaktorska provjera autentičnosti
- Identitet klijenata i upravljanje pristupom, CIAM (*engl. Customer identity and access management)*

Podacima identiteta i objekta kao što su korisnički profili, podaci o konfiguraciji, tokeni i vjerodajnice može se upravljati putem "oxTrust" administrativnog sučelja ili pomoću LDAP preglednika, kako je određeno u korisničkom vodiču za upravljanje. OxTrust je Gluu-ova aplikacija za administratore poslužitelja koja se koristi za upravljanje i konfiguriranje prijava, provjere autentičnosti, pristupa i skripti. Gluu Server također podržava SCIM protokol *(engl. System for Cross-domain Identity Management)* koji se može koristiti za upis podataka na Gluu Server iz vanjskih izvora podataka poput identitetskih sustava upravljanja identitetom i aplikacija u oblaku. SCIM je specifikacija dizajnirana da smanji složenost operacija upravljanja korisnicima pružanjem zajedničke korisničke sheme i obrazaca za razmjenu takve sheme pomoću HTTP-a *(engl. Hyper Text Transfer Protocol)* na platformi na neutralan način. Cilj SCIM-a je postizanje interoperabilnosti, sigurnosti i skalabilnosti u kontekstu upravljanja identitetom. Programeri mogu SCIM smatrati samo REST API-jem s krajnjim točkama koje otkrivaju CRUD funkcionalnost (kreiranje, čitanje, ažuriranje i brisanje).[12]

4.1.1. LDAP

LDAP *(engl. Lightweight Directory Access Protocol)* je softverski protokol koji omogućuje lociranje organizacija, pojedinaca i drugih resursa, poput datoteka i uređaja u mreži, bilo na javnom Internetu, bilo na korporativnom intranetu. Direktoriji pokazuju gdje se u mreži nešto nalazi. Na TCP / IP mrežama (uključujući Internet) sustav naziva domene, DNS *(engl. Domain Name System)* je sustav imenika koji se koristi za povezivanje imena domene s određenom mrežnom adresom (jedinstvena lokacija na mreži). Međutim, ime domene možda nije poznato. LDAP omogućuje pretragu pojedinaca bez saznanja gdje se oni nalaze.

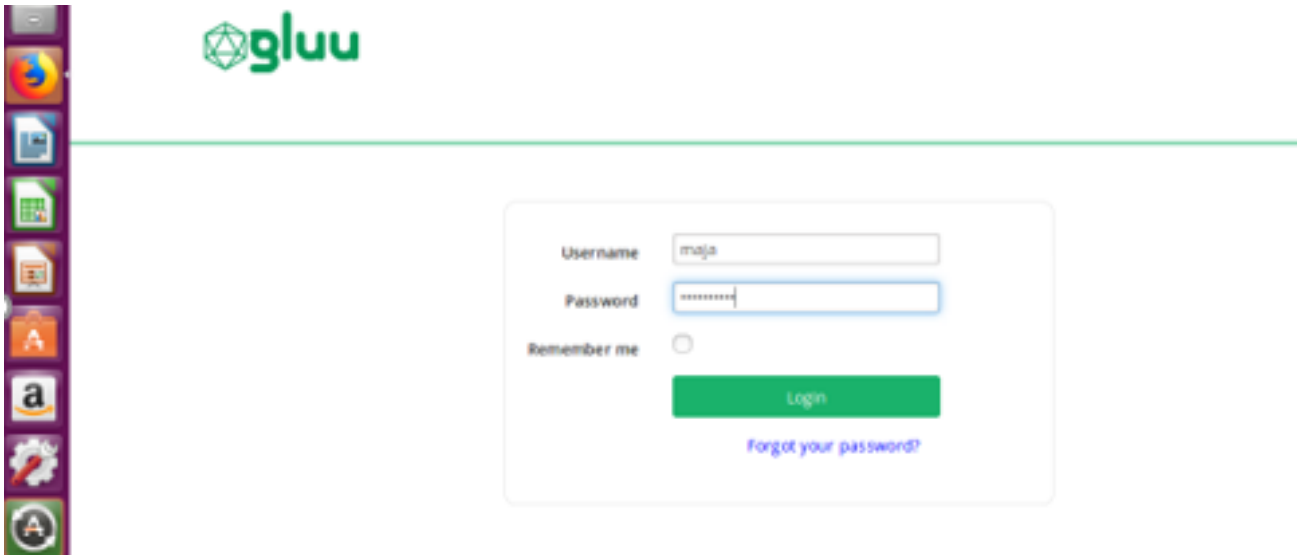
LDAP mapa je organizirana u jednostavnoj hijerarhiji "stabla" koja se sastoji od sljedećih razina:

- Korijenski direktorij (*engl.root*)
- Zemlje
- Organizacije
- Organizacijske jedinice (odjeljenja, odjeli i tako dalje)
- Pojedinci (što uključuje ljude, datoteke i zajedničke resurse poput pisača)

LDAP direktorij može se distribuirati na više poslužitelja. Svaki poslužitelj može imati repliciranu verziju direktorija koji se periodički sinkronizira. LDAP poslužitelj se naziva agent sustava direktorija, DSA *(engl. Directory System Agent).* LDAP poslužitelj koji prima zahtjev od korisnika ima odgovornost za zahtjev, prosljeđujući ga drugim DSA-ima po potrebi, ali osigurava jedan odgovor za korisnika.[13]

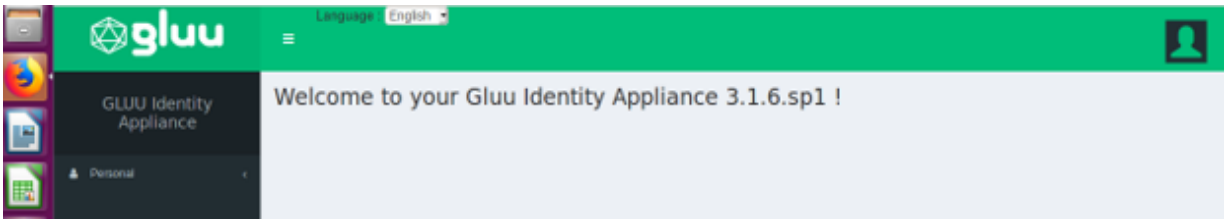
4.1.1.Osnovna autentifikacija

Metoda 'Basic' ili 'Internal' upotrebljava se za implementaciju autentifikacije korisničkog imena / zaporke. Osnovna autentifikacija prikazana je na slici 4.1.



Slika 4.1. Prijava korisnika pomoću osnovne autentifikacijske metode

Nakon svake uspješne prijave korisniku se prikazuje zaslon sa slike 4.2. gdje se obavještava da je uspješno prijavljen u sustav.



Slika 4.2. Zaslon nakon prijave

Osnovna provjera autentičnosti oslanja se na uspješnu LDAP BIND operaciju na LDAP direktoriju, bilo da je lokalni LDAP uključen u Gluu poslužitelju ili zamjenski LDAP poslužitelj poput Active Directory koji je konfiguriran za upotrebu s Gluu poslužiteljem.

Operacije vezanja (*engl. bind*) koriste se za provjeru autentičnosti klijenata (i korisnika i aplikacija) na poslužitelju, za uspostavljanje autorizacije koja će se koristiti za kasnije operacije koje se obrađuju na toj vezi, te za određivanje verzije protokola LDAP koju će klijent koristiti. Provjera identiteta sastoji se od najmanje dva dijela: identificiranja tko ili što potvrđuje autentičnost i pružanja neke vrste dokaza tog identiteta, obično nešto što samo korisnik treba znati ili imati, poput lozinke, certifikata, hardvera ili softverskog tokena ili biometrijskog podatka. Na mnogim poslužiteljima mogu biti dodatni koraci, poput pravila o zaporkama i drugih ograničenja koja moraju biti zadovoljena kako bi veza mogla uspjeti.

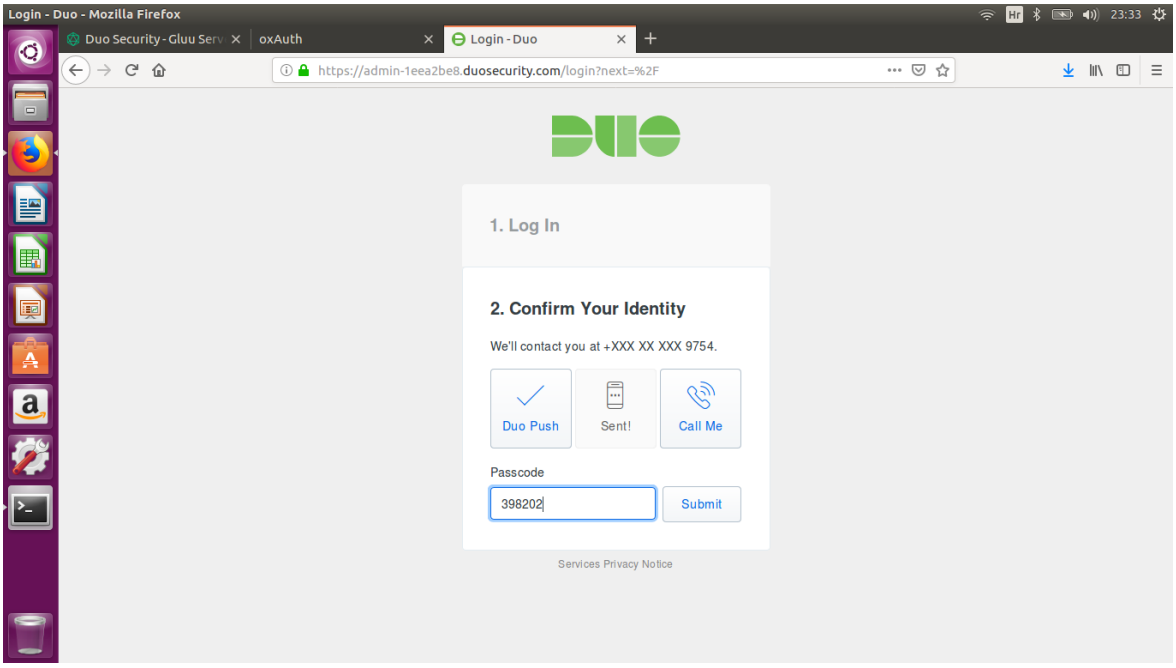
Skripta za ovu metodu je napisana u programskom jeziku Python. Uspješnost inicijalizacije može se provjeriti u terminalu pomoću sljedećih naredbi na slici 4.3. :

```
majabaja@localhost:~$ tail -f oxauth_script.log
2019-06-10 12:40:8,847 INFO [oxAuthScheduler_Worker-5]
[org.xdi.service.PythonService$PythonLoggerOutputStream] (PythonService.java:209) - Basic. Initialization
2019-06-10 12:40:8,853 INFO [oxAuthScheduler_Worker-5]
[org.xdi.service.PythonService$PythonLoggerOutputStream] (PythonService.java:209) - Basic. Initialized
successfully
```

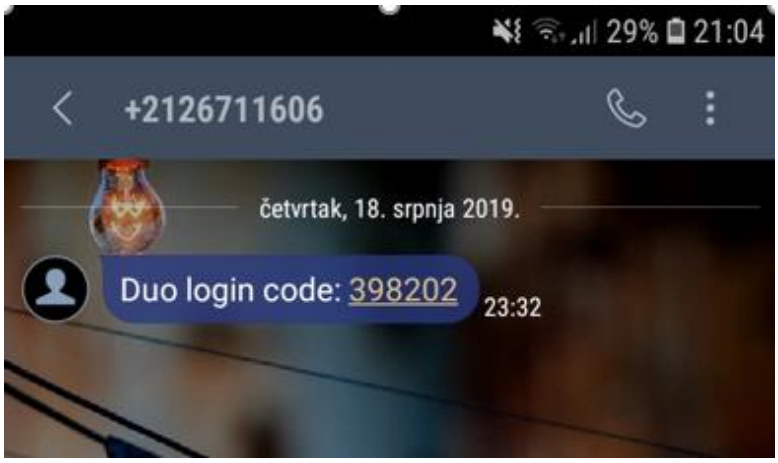
Slika 4.3. Inicijalizacija osnovne metode autentifikacije na Gluu poslužitelju

4.1.2. Dvostruka sigurnost

Pri upotrebi Duo metode autentifikacije, korisnici se prvo logiraju pomoću korisničkog imena i lozinke, kao što je prikazano na prvoj, osnovnoj metodi autentifikacije Gluu poslužitelja, a zatim se odrađuje Duo sigurnost kao drugi korak provjere. Potrebno je napraviti korisnički račun na Duo poslužitelju kako bi se isti mogao koristiti u kombinaciji s Gluu poslužiteljem. Na slici 4.4. je prikazana mogućnost odabira na koji način korisnik želi dobiti kod za pristup servisu. Korisnik u ovom slučaju odabire slanje koda u tekstualnoj poruci te pri upisu koda u polje pristupa željenom servisu.

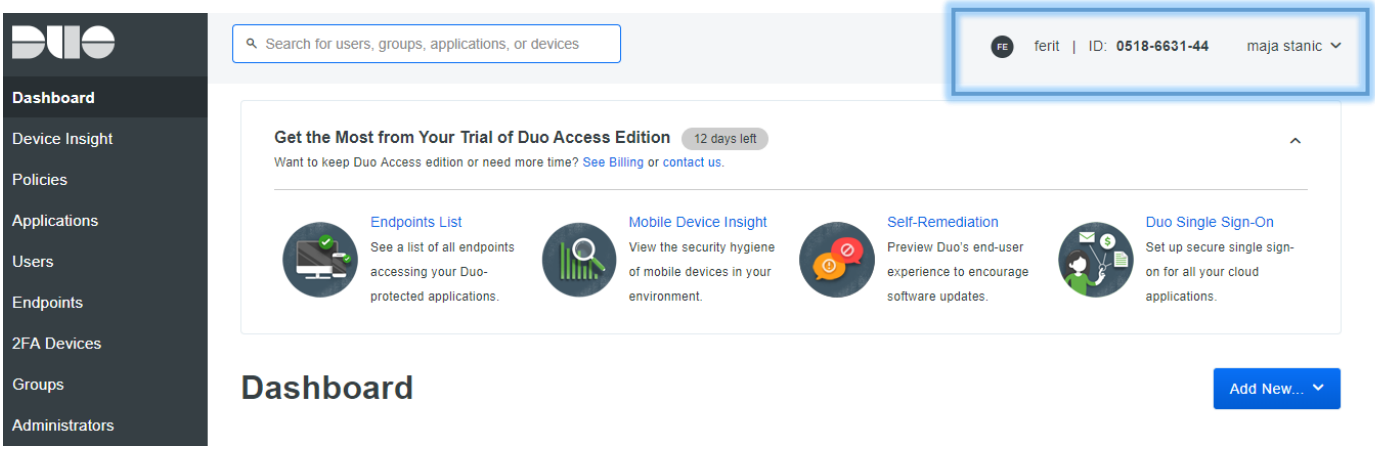


Slika 4.4. Odabir načina slanja koda



Slika 4.5. Tekstualna poruka s pristupnim kodom

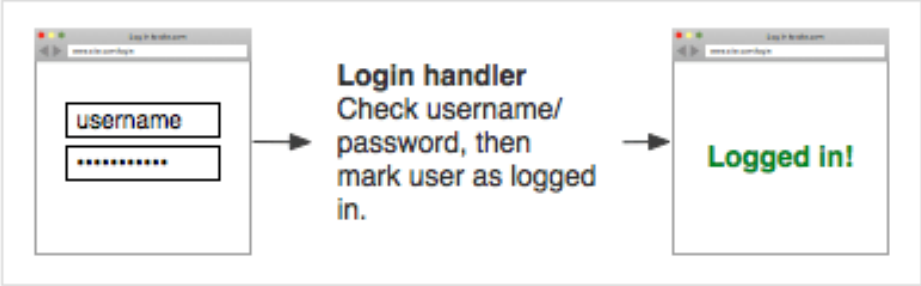
Nakon primitka koda kao na slici 4.5. i uspješne prijave korisnik se nalazi u Duo poslužitelju, slika 4.6. Duo skripta također je napisana u Python programskom jeziku. U usporedbi s prethodnom metodom daje mnogo veću sigurnost jer zahtjeva više sigurnosnih koraka od osnovne metode autentifikacije.



Slika 4.6. Duo poslužitelj

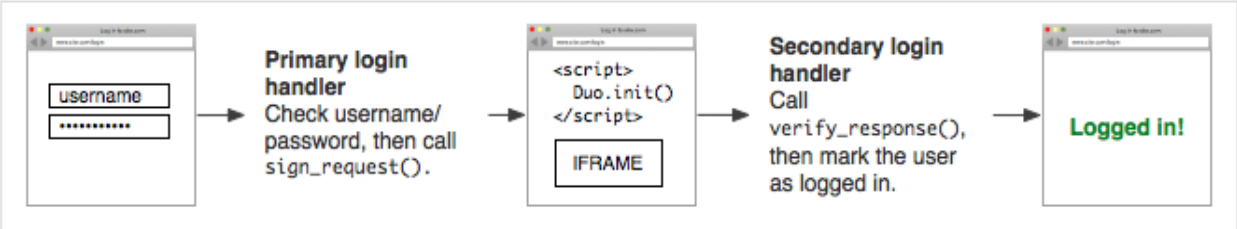
Pri uspješnoj prijavi u Duo poslužitelj vidljivi su podaci o korisniku: njegovo ime i prezime, identifikacijski broj korisnika te informacije o organizaciji kojoj korisnik pripada.

Tipična prijava korisnika izgledala bi kao na slici 4.7.



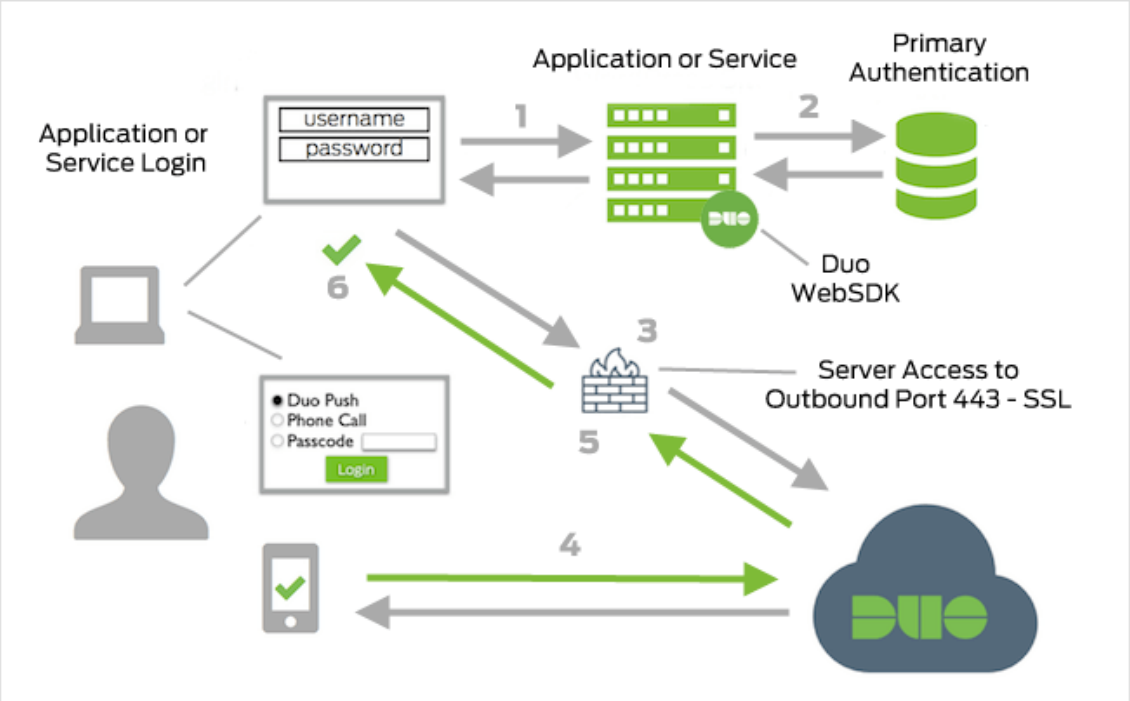
Slika 4.7. Prijava korisnika osnovnom metodom autentifikacije[14]

Nakon dodavanja Duo korisničkog računa u autentifikaciju, prijava korisnika izgleda kao na slici 4.8.



Slika 4.8. Prijava korisnika dodavanjem Duo računa[14]

Na mrežnom dijagramu na slici 4.9. prikazana je provjera prijave korisnika po koracima od 1-6.



Slika 4.9. Mrežni dijagram Duo metode autentifikacije[14]

1. Pokrenuta je internetska aplikacija ili usluga
2. Primarna provjera autentičnosti pomoću korisničkog imena i lozinke
3. Uspostavljena veza s web aplikacijom ili uslugom Duo Security preko TCP priključka 443
4. Sekundarna provjera autentičnosti putem usluge Duo Security
5. Web aplikacija ili usluga prima odgovor provjere autentičnosti
6. Web aplikacija ili sesija usluge uspješno su prošli sigurnosne provjere i prijavljeni su.

4.1.3. SuperGluu metoda

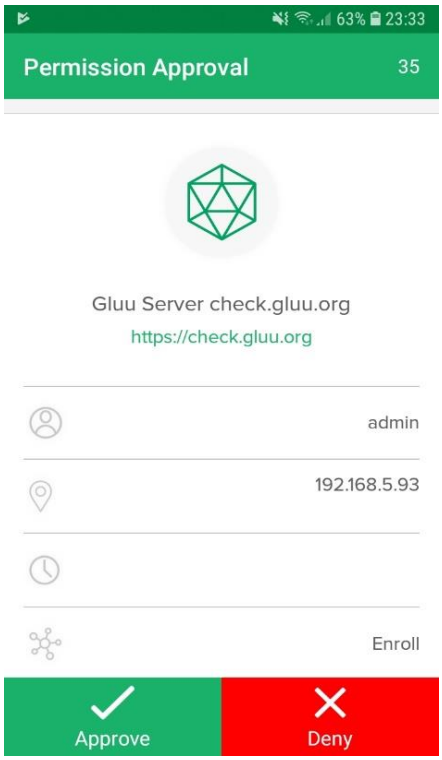
Super Gluu je push-notifikacijska mobilna aplikacija izgrađena za dvofaktorsku provjeru autentičnosti (2FA) za rad s Gluu poslužiteljem. Pri korištenju ove metode potrebno je instalirati Super Gluu aplikaciju za Android ili iOS uređaj.

Super Gluu podržava više radnih mogućnosti, a to su sljedeće:

- Jednostupanjska autentifikacija bez lozinke, gdje osoba skenira QR kod sa svojom aplikacijom Super Gluu, a Gluu Server traži koja je osoba povezana s tim uređajem.
- Autentifikacija u dva koraka, gdje osoba unosi svoje korisničko ime, a zatim na mobilni uređaj prima obavijest radi autorizacije .
- Autentifikacija u dva koraka, gdje osoba unosi svoje korisničko ime i lozinku, a zatim na mobilni uređaj prima obavijest radi autorizacije pristupa.

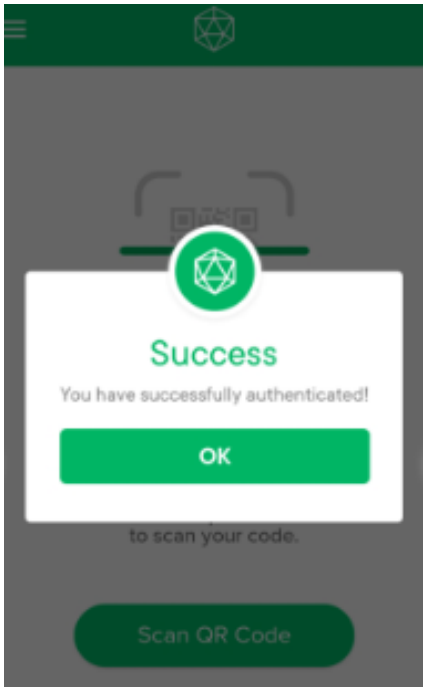
U sve tri mogućnosti od korisnika se traži da skeniraju QR kod na prvoj provjeri autentičnosti Super Gluu kako bi povezali svoj uređaj i račun. U drugoj i trećoj mogućnosti navedenima gore, korisnici počinju primati push obavijesti za sve provjere autentičnosti nakon početnog postupka registracije uređaja. U radu je odrađena prva mogućnost prijave, gdje se skenira QR kod te se Gluu poslužitelj povezuje s uređajem. Gluu poslužitelj radi više od provjere ID uređaja kako bi odobrio pristup. Super Gluu koristi FIDO U2F (*engl. FIDO Universal 2nd Factor*) krajnje točke Gluu poslužitelja za upis javnog ključa. Privatni ključ sprema se na uređaj. Za provjeru autentičnosti Gluu poslužitelj šalje odgovor uređaju da provjeri odgovarajući privatni ključ.

Nakon instalacije Super Gluu aplikacije, potrebno je odobriti pristup kameri kako bi se mogao skenirati QR kod, te izabrati ponuđenu metodu. Nakon odrađenog skeniranja QR koda, korisniku se na uređaju prikazuje zaslon sa slike 4.10.



Slika 4.10. Zaslon nakon skeniranja QR koda

Nakon što skenira kod i poslužitelj ispravno vrati zahtjev, aplikacija traži odobrenje ili odbijanje za nastavak prijavljivanja. Da bih se postupak autentifikacije nastavio potrebno je odobrenje, nakon čega se prikazuje poruka o uspješnoj autentifikaciji kao na slici 4.11.



Slika 4.11. Uspješna autentifikacija Super Gluu metodom

Aplikacija bilježi svaku prijavu u sustav, a prijave su spremljene u logovima što također predstavlja jedan od oblika sigurnosti jer korisnik može pratiti svoje prijave i vrijeme prijava kao i lokaciju prijave te uvidjeti ako što od vidljivih prijava ne odgovara njegovim prijavama.

4.2. FreeRADIUS poslužitelj

FreeRADIUS je sigurnosni program specijaliziran za bežične mreže (WiFi) i daljinsko upravljanje korisničkim AAA (autorizacija, provjera autentičnosti i računovodstvo). Naziv FreeRADIUS odnosi se i na slobodni open source RADIUS, također poznat kao RADIUS poslužitelj. FreeRADIUS se temelji na Unix kodu i može raditi na više operacijskih sustava, iako se najviše preporučuju Linux sustavi poput Debian, Red Hat, SUSE, TurboLinux, Ubuntu. Ostali sustavi su na primjer: AIX, Mac OSX i Solaris. Prednost ovih operativnih sustava su RAM i memorija, a i sam FreeRADIUS ne zauzima puno prostora. FreeRADIUS se oglašava kao najčešće korišteni RADIUS poslužitelj na svijetu,a popularnost se objašnjava pristupom koji je jednostavan za korištenje, izostanak troškova potrebnih za upotrebu, jednostavnost za korisnike, brza i jednostavna instalacija i sigurnost usporediva s poslužiteljima koji nisu besplatni kao ovo rješenje. Kad se odlučuje o ulaganju, kompatibilnost s postojećim hardverom je bitan faktor. FreeRADIUS nudi sve to. Taj besplatni softver koristi se bez dodatnih troškova. Kompatibilan je sa svim korištenim protokolima i ima mogućnosti proizvoditi vlastite "sigurnosne potvrde". Međutim, kao slobodan softver ima svoje osobine. Što se više koristi, to više treba naučiti i sve više vremena treba za proučavanje svih funkcija. Na temelju Unix-kodiranja, ne radi u istom sustavu kao Windows, što znači da ima svoj način ažuriranja i mijenjanja postavki. FreeRADIUS-u nedostaje GUI, opće korisničko sučelje, tako da je sve zasnovano na tekstu. To bi moglo predstavljati izazov korisnicima koje traže jednostavno i jeftino rješenje.[7]

Za početak korištenja potrebno je instalirati Freeradius poslužitelj. Instalacija se vrši na Linux operacijskom sustavu, u ovom slučaju na Ubuntu 18.04. Početak rada s FreeRADIUS poslužiteljem je pokretanje poslužitelja naredbom : $ radiusd -X, nakon nekog vremena na terminalu se ispisuje poruka: „*Ready to process requests*.“. FreeRADIUS može koristiti različite protokole: EAP, EAP-TLS, CHAP, PAP,TTLS, LEAP, PEAP.U radu će se implementirati PAP metoda autentifikacije. PAP metoda je prvi korak u FreeRADIUS autentifikaciji. Ovaj protokol uspoređuje lozinku koju je korisnik unio s lozinkom sadržanom u sustav provjere autentičnosti. Iako se mogu koristiti drugi protokoli za provjeru autentičnosti, PAP je najjednostavniji i najlakši za konfiguriranje. Testiranje provjere autentičnosti stoga treba uvijek započeti s PAP-om, jer ako jednom to uspije, lakše će se konfigurirati ostali protokoli za provjeru autentičnosti.

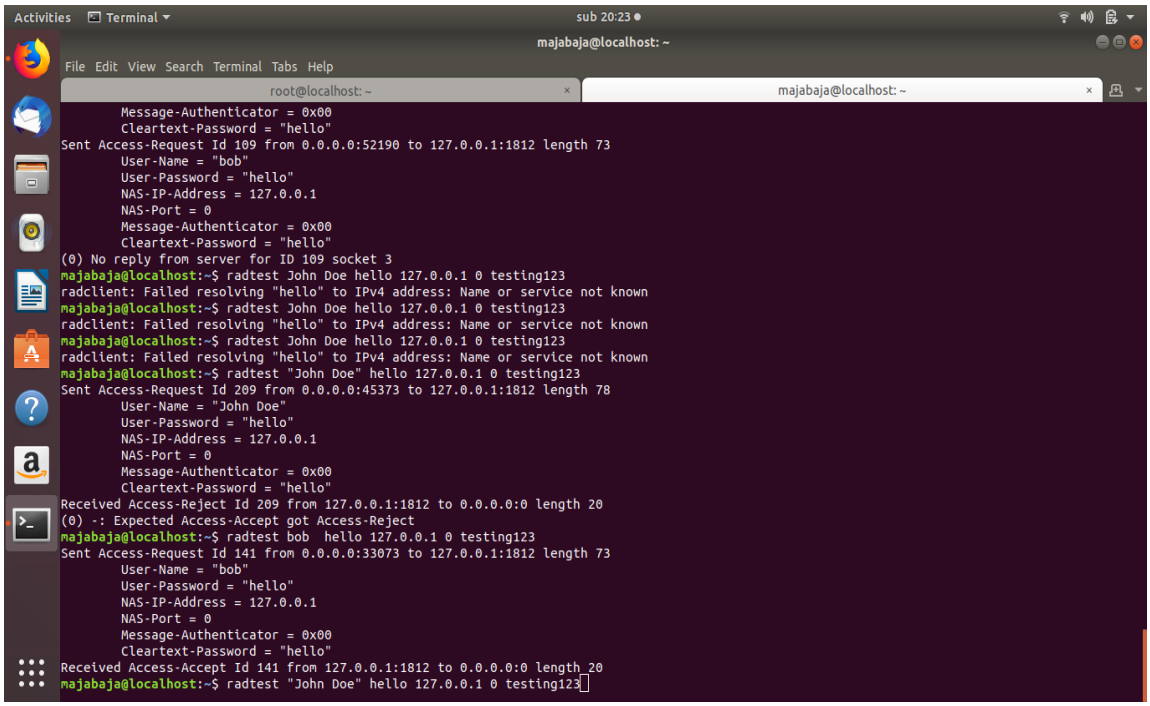
Od ostalih nabrojanih metoda najčešće se upotrebljavaju CHAP i MS-CHAP koje su već opisane u radu pod poglavljem „Postojeće autentifikacijske metode“. Zbog sličnog načina implementacije, praktično je odrađena samo PAP metoda, a CHAP i MS-CHAP su prikazane kako bi se pokazala razlika između metoda.

Klijent odabire metodu provjere autentičnosti koju želi koristiti, a poslužitelj prihvaća ili odbija zahtjev. Čak i ako je lozinka ispravna, poslužitelj može odlučiti odbiti zahtjev ako predstavljeni način provjere autentičnosti nije dopušten od strane poslužitelja. Umjesto da odbije sve vrste provjere autentičnosti koje poslužitelj ne dopušta, administrator nameće određenu vrstu provjere autentičnosti, što rezultira odbacivanjem svih ostalih vrsta. Glavni razlog zbog kojeg se nameće posebna metoda provjere autentičnosti je taj što će se to općenito "razbiti" svaki drugi način provjere autentičnosti; drugim riječima, prisiljavanje na uporabu jedne metode znači da je nemoguće da sustav krajnjeg korisnika koristi bilo koju drugu metodu. Najčešći problem koji se pojavljuje kod prisiljavanja metode provjere autentičnosti je odbacivanje autentičnosti krajnjeg korisničkog sustava koji koristi jednu metodu provjere autentičnosti, dok je administrator poslužitelja nametnuo drugu metodu. Tablica 4.1. pokazuje koje su metode provjere autentičnosti kompatibilne s postavkom nametanja autentifikacijske provjere.

Kompatibilnost metode provjere autentičnosti	
Metoda provjere autentičnosti	**Prihvaćanje nametnute metode provjere**
PAP	Da
CHAP	Da
MS-CHAP	Ne
EAP	Ne

Tablica 4.1. Metode kompatibilne s nametanjem autentifikacijske provjere

Za testiranje poslužitelja potrebno je pokrenuti radtest naredbu u debugging modu kao što je prikazano na slici 4.12.



Slika 4.12. Testiranje poslužitelja

Kada se korisnik pokuša autentificirati, uređaj šalje poruku RADIUS poslužitelju. Ako je RADIUS poslužitelj pravilno konfiguriran da uređaj ima kao klijenta, RADIUS šalje poruku prihvaćanja ili odbijanja na uređaj-NAS *(engl.Network Access Server).* [6]

4.2.1. PAP

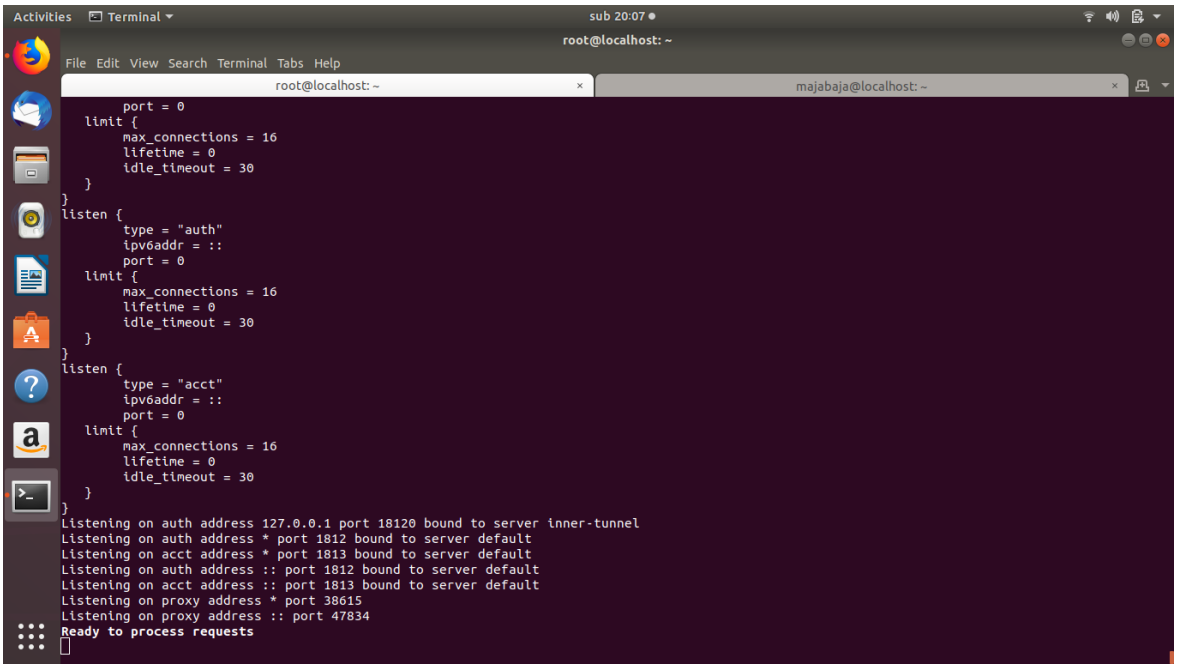
PAP autentifikacija se konfigurira tako što se upućuje poslužitelju da identificira određenog korisnika ("bob") i korisnikovu lozinku ("hello").U drugi prozor terminala upisuje se naredba:

$ radtest -x bob hello 127.0.0.1 0 testing123

Ova naredba poslužitelju šalje paket zahtjeva za provjeru autentičnosti, sa sljedećim parametrima:

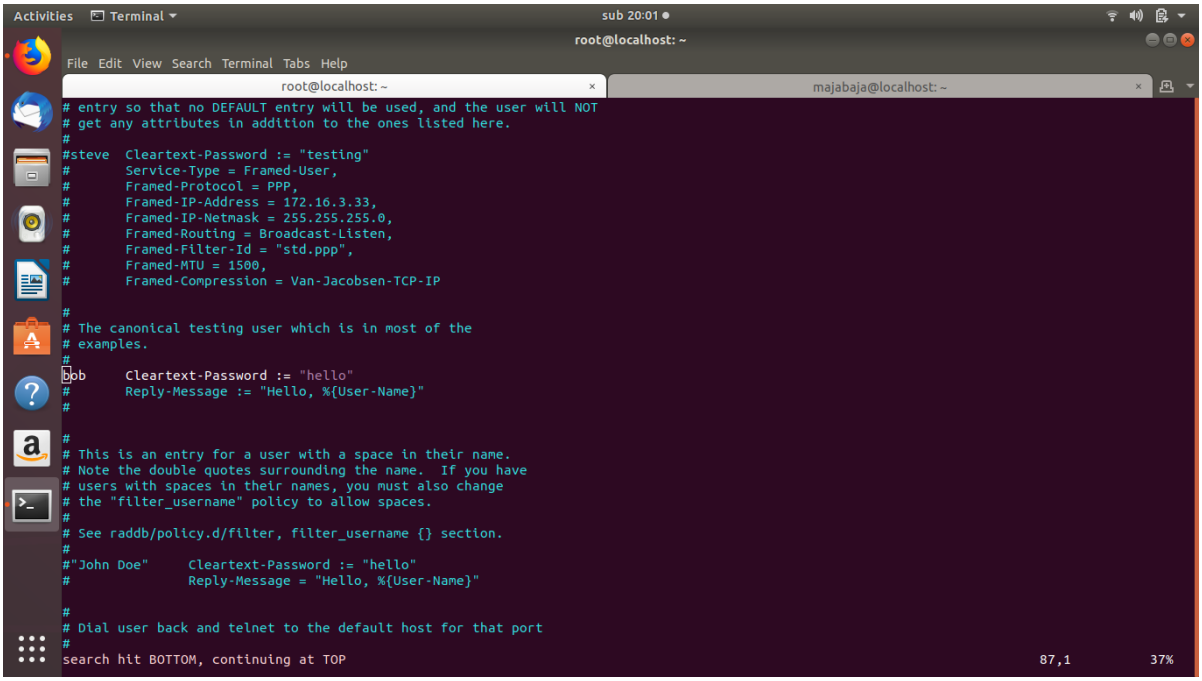
- Ime „bob“
- lozinka „hello“
- Za poslužitelja na adresi 127.0.0.1
- Prijava preko porta 0
- Koristi se zajednička tajna testing123

Kao što je vidljivo na slici 4.12. u terminal se ispisuje odgovor poslužitelja sa: Access-Accept ili Acces-Reject. Na slici 4.13. ispisana je konfiguracija dijela za slušanje kod poslužitelja kao i portovi koji se trenutno slušaju te popis IP adresa koje se koriste. [12]



Slika 4.13. Konfiguracija poslužitelja

Provjerava se autentifikacija korisnika koji se nalaze u mapi: vim /etc/freeradius/3.0/users. Gdje su vidljiva korisnička imena i lozinke za pristup kao na slici 4.14.



Slika 4.14. Mapa users

Smatra se da pohrana lozinki u običnom tekstualnom obliku predstavlja sigurnosnu opasnost. Zbog sigurnosti u praksi se primjenjuje hashiranje lozinki. Hashirane lozinke dobiju se izvođenjem

algoritma na uobičajeni tekstualni niz čime on dobije potpuno drugačiju vrijednost. FreeRADIUS podržava više vrsta lozinki, neke od njih su :

- Čisti tekst(*engl. Cleartext)*
- Kripto-lozinka.
- LM-lozinka:
- lozinka MD5
- lozinka NS-MTA-MD5
- NT-lozinka
- SHA-lozinka
- SMD5-lozinka
- SSHA-lozinka

Potrebno je koristiti lozinku čistog teksta kad god je to moguće. Sekundarni izbor bio bi lozinka NT. Treba izbjegavati sve ostale formate, jer su kompatibilni samo s PAP provjerom autentičnosti i nisu kompatibilni sa svim ostalim metodama provjere autentičnosti.

RADIUS poslužitelji dobro su poznati po svojim AAA mogućnostima - provjera autentičnosti, autorizacije i računovodstva. Glavna prednost centraliziranih AAA mogućnosti RADIUS poslužitelja je povećana sigurnost i veća učinkovitost. RADIUS poslužitelji pružaju mogućnost očuvanja privatnosti i sigurnosti kako sustava tako i svakog pojedinog korisnika.

RADIUS-ov protokol koji je baziran na klijent-server komunikaciji sadrži mnoge prednosti za korisnike:

- Laka izmjena podataka
- Odvojenost sigurnosnih i komunikacijskih procesa
- Prilagođenost većini sigurnosnih procesa
- Moguće je raditi s bilo kojim komunikacijskim uređajem koji podržava RADIUS protokol.

4.2.2. CHAP i MS-CHAP

Ako je PAP konfiguracija dobro odrađena, jednostavno je isprobati ostale metode autentifikacije. Jednostavnim naredbama u terminalu pokreću se željene metode, a izlazi svake od metoda prikazan je u tablicama 4.2. i 4.3.

Tablica 4.2. CHAP metoda autentifikacije [12]

Metoda	CHAP
Naredba	`$ radtest -x -t chap bob hello 127.0.0.1 0 testing123`

Izlaz	`Sending Access-Request of id 232 to 127.0.0.1 port 1812`
	`User-Name = "bob"`
	`CHAP-Password := 0xe834861ac62185fa5f1b610ef335df8b3b`
	`rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=232, length=20`

Tablica 4.3. MS-CHAP metoda autentifikacije[12]

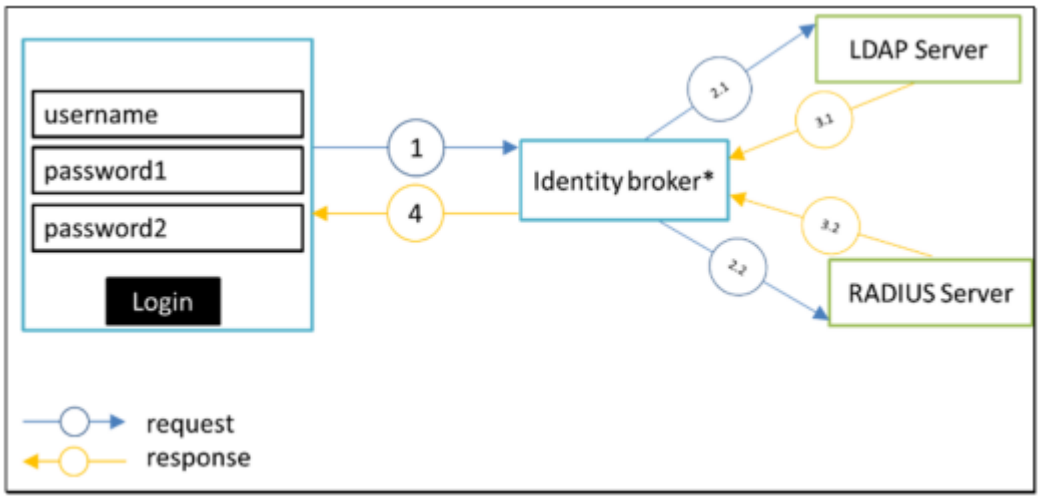
Metoda	MS-CHAP
Naredba	`$ radtest -x -t mschap bob hello 127.0.0.1 0 testing123`

Izlaz	`Sending Access-Request of id 79 to 127.0.0.1 port 1812`
	`User-Name = "bob"`
	`MS-CHAP-Challenge = 0x8804cc07e901067d`
	`MS-CHAP-Response = 0x000100000000000000000000000000000000000000000000004976cc59820ac2bfdab36c9d6de3e6292a025aa34a1a2a02`
	`rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=79, length=84`
	`MS-CHAP-MPPE-Keys = 0xfda95fbeca288d44ac0782e2de2337dee40e54ee732c1af50000000000000000`
	`MS-MPPE-Encryption-Policy = 0x00000001`
	`MS-MPPE-Encryption-Types = 0x00000006`

Vidljive su razlike u izlazima nakon obrade svake od metoda, primjećuje se da se nakon PAP autentifikacije kao izlaz prikazuje izvorna lozinka, u nepromijenjenom obliku. Kod CHAP metode poslana CHAP-lozinka izgleda kao slučajni niz znakova, a ne kao izvorna lozinka "hello". Kod MS-CHAP metode vidljivo je da izlaz sadrži MS-CHAP izazov i odgovor, a ne izvornu lozinku "hello" kao do sada. MS-CHAP Odgovor također uključuje i neke posebne Microsoftove atribute. [12]

FreeRADIUS podržava više vrsta provjere autentičnosti nego bilo koji drugi poslužitelj otvorenog koda. Na primjer, FreeRADIUS je jedini RADIUS poslužitelj otvorenog koda koji podržava EAP protokol. FreeRADIUS je i jedini RADIUS poslužitelj otvorenog koda koji podržava virtualne poslužitelje. Korištenje virtualnih poslužitelja znači da su složene implementacije

pojednostavljene i stalni troškovi podrške i održavanja za mrežne administratore uvelike se smanjuju; tako mogućnost FreeRADIUS-a da podržava virtualne poslužitelje daje mu veliku prednost u odnosu na druge poslužitelje. RADIUS je prihvaćen kod ISP- a za pružanje VPN usluga. Sukladno tome, RADIUS tehnologija omogućuje korisnicima sigurno korištenje ISP infrastrukture za komunikaciju. Distributivna priroda RADIUS-a učinkovito odvaja sigurnosne procese, koji se provode na poslužitelju identiteta od komunikacijskih procesa koji su implementirani s mrežne strane. Pristupni poslužitelj (NAS) pruža jedinstvenu centraliziranu dostupnost informacija za autorizaciju i provjeru autentičnosti. Ova centralizacija može značajno smanjiti teret kontrole pristupa velikom broju udaljenih korisnika. RADIUS sprema korisničke podatke na centralno mjesto i omogućuje laku administraciju. Podaci o korisnicima mogu biti spremljeni na RADIUS serveru ili nekoj od baza podataka,npr. LDAP. Pogodan je za korištenje u sustavima koji imaju mnogo korisnika, npr.za korištenje u hotelima, gdje RADIUS prima zahtjeve klijenta i regulira njihov pristup željenim resursima. Na slici 4.15. prikazana je upotreba RADIUS poslužitelja i prijava korisnika u sustav.



Slika 4.15. Autentifikacijski tok s RADIUS i LDAP [2]

U posljednje vrijeme implementacije RADIUS-a postaju sve popularnije jer pružaju mogućnost IT organizacijama da zaključaju svoje WiFi mreže i VPN-ove. FreeRADIUS omogućava IT administratorima mogućnost izbacivanja zajedničkih kombinacija SSID-a i zaporke samo za WiFi, a umjesto toga zahtijevaju od svakog korisnika da se prijavi s vlastitim jedinstvenim setom vjerodajnica.

SSID se najčešće susreće kada korisnici mobilni uređaj žele povezati s bežičnom mrežom. Na primjer, ako se prijenosno računalo odnese u kafić i želi se povezati s lokalnom Wi-Fi mrežom,

na zaslonu će se prikazati popis SSID-a, a to su imena svih mreža koja su u dosegu mobilnog uređaja. Izabrat će se naziv lokalne mreže na koju se želi povezati, a zatim se unesi lozinka (ako je potrebno) za povezivanje.

Još jedna sposobnost koja dolazi putem ovog uparivanja odnosi se na VLAN-ove.

VLAN-ovi (virtualni LAN-ovi) logično su grupiranje uređaja u istoj domeni za emitiranje. VLAN-ovi se obično konfiguriraju na prekidačima stavljanjem nekih sučelja u jednu odašiljačku domenu, a neka sučelja u drugu. VLAN-ovi se mogu širiti na više sklopki, pri čemu se svaki VLAN tretira kao vlastita podmreža ili odašiljačka domena. To znači da će se okviri emitirani na mrežu prebacivati samo između portova unutar iste VLAN mreže.

VLAN djeluje poput fizičkog LAN-a, ali omogućuje domaćinima da se grupiraju u istu emitiranu domenu, čak i ako nisu povezani na isti prekidač. Glavni razlozi korištenja VLAN-ova su:

- VLAN mreže povećavaju broj emitiranih domena uz istovremeno smanjenje njihove veličine.
- VLAN mreže smanjuju sigurnosne rizike smanjujući broj domaćina koji primaju kopije okvira koje preklopnici preplavljuju.
- Omogućuju čuvanje hostova koji čuvaju osjetljive podatke na zasebnom VLAN-u radi poboljšanja sigurnosti.
- Omogućuju stvaranje fleksibilnijeg mrežnog dizajna koji grupira korisnike po odjelima umjesto prema fizičkoj lokaciji.
- Mrežne promjene se postižu lakoćom samo konfiguriranjem porta u odgovarajući VLAN.

Kada su alati za IDP, FreeRADIUS i mrežnu infrastrukturu ispravno postavljeni, IT admini dobivaju mogućnost smještanja korisnika u zasebne virtualne lokalne mreže (VLAN-ove). Oba zadatka značajno povećavaju sigurnost za WiFi mreže.

5. USPOREDBA REZULTATA

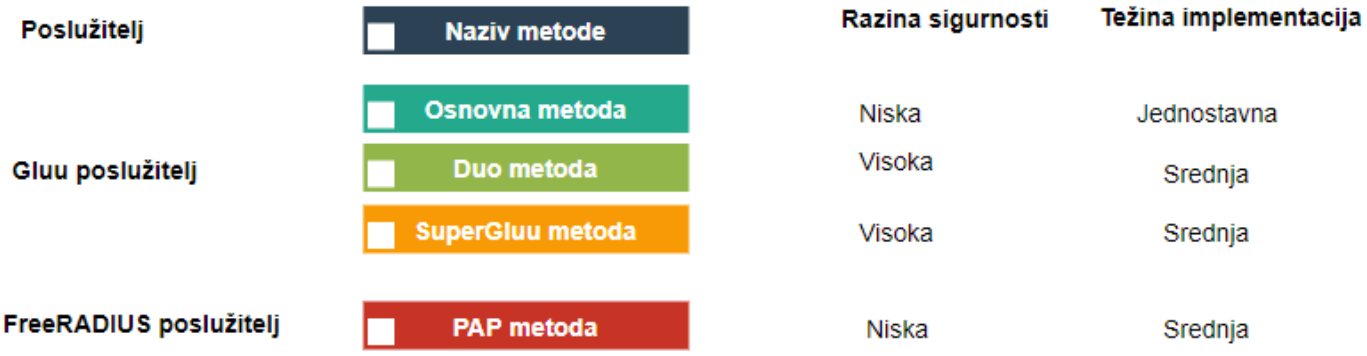
Pri implementaciji osnovne metode autentifikacije, kod Gluu poslužitelja, koja se sastoji od korisničkog imena i lozinke uočava se velika sigurnosna opasnost, budući da napadač može lako doći do tih podataka prilikom korisničke nepažnje. Sama implementacija osnovne metode je veoma jednostavna te je prigodna za prijavu na sustave koji ne zahtijevaju veliku sigurnost i koji ne sadrže skupe i povjerljive podatke, primjerice prijava na aplikacije s katalozima, tv emisijama i filmovima.

Druga metoda Gluu poslužitelja, Duo sigurnost, pokazuje značajan sigurnosni napredak u odnosu na prvu, osnovnu metodu, budući da se pored osnovne autentifikacije uvodi dodatni korak zaštite koji zahtjeva korisnički račun na Duo poslužitelju i posjedovanje mobilnog uređaja na koji stiže sigurnosni kod koji se upisuje za prijavu. Takva autentifikacija pogodnija je za prijavu na servise koji sadrže povjerljivije podatke.

Treća metoda Gluu poslužitelja, SuperGluu, pokazuje se kao najsigurnija metoda za autentificiranje korisnika budući da zahtjeva posjedovanje mobilnog uređaja preko kojeg se odobrava prijava u sustav, na mobilnoj aplikaciji moguće je vidjeti sve prijave određenog korisnika te korisnik može lako pratiti svoje prijave i vidjeti postoji li prijava koja nije njegova. Pored metode koja je obrađena u radu, daje još dvije dodatne mogućnosti prijave preko SuperGluu metode, čime se postiže još veća sigurnost.

FreeRADIUS poslužitelj u ovom slučaju pokazao se jednostavan za implementaciju, te pogodan za praktičnu primjenu jer pruža veoma dobru sigurnost, posebice za velike kompanije ili hotele koji imaju velike baze korisnika. Ukoliko korisnici više istražuju mogućnosti FreeRADIUS-a on postaje sve kompliciraniji za razumijevanje i implementaciju. Zbog kompliciranog rukovanja takvim sustavima, većina korisnika okreće se praktičnijim i jednostavnijim rješenjima, dajući prednost jednostavnosti nad sigurnosti što nije dobra praksa. Dakle, FreeRADIUS je jednostavan za korištenje ako se ne ulazi duboko u njegovu strukturu.

Na slici 5.1. tablično su prikazane implementirane metode i njihove sigurnosne razine, uzimajući u obzir i težinu implementacije svake od metoda.



Slika 5.1. Usporedba rezultata implementiranih metoda

6. ZAKLJUČAK

Zaštita podataka je veoma značajna mnogim organizacijama jer njihov opstanak ovisi o njima. Teži se postavljanju ograničenja za svakog pojedinog korisnika kako bi se smanjila mogućnost zlouporabe. Višefaktorska provjera identiteta prepoznata je kao najsigurnija metoda provjere autentičnosti za pristup podacima i aplikacijama te predstavlja najveći izazov potencijalnim napadačima. Prijava pomoću lozinke i korisničkog imena je dovoljna zaštita ako se ne radi o povjerljivim podacima, dok za sve ostalo predstavlja preslabu zaštitu. Međutim, istraživanja su pokazala da se 90% lozinki može probiti za manje od šest sati, a da dvije trećine ljudi koristi istu lozinku za prijavu na sve servise koje koriste. Što dovodi do velike zabrinutosti za sigurnost podataka. U radu je pokazano i uspoređeno nekoliko metoda koje su besplatne i lako primjenjive. Naravno, bez obzira na količinu zaštite koja je postavljena za pristup na određene aplikacije ili servise, ako korisnik koji nije dovoljno educiran o mogućim sigurnosnim opasnostima, izlaže svoje lozinke i tajne pristupa drugim korisnicima sva zaštita je uzaludna. Stoga je nužno provesti edukaciju zaposlenika koji rade s osjetljivim podacima i s razvojem trendova pravovremeno obavljati nove edukacije budući da razvojem novih tehnologija raste i mogućnost računalnih napada. Korisnicima koji tek ulaze u računalni svijet, učenicima, studentima i drugima, treba ukazati na važnost zaštite osobnih i drugih podataka kako bi već u početku rukovanja određenim tehnologijama postali svjesni mogućih opasnosti koje prijete. Autentifikacija samo osigurava da je pojedinac onaj za koga se predstavlja da jeste, ali ništa ne govori o pravima pristupa za svakog pojedinca. Te je svakog korisnika nužno podvrgnuti autorizacijskom postupku kako bi se utvrdilo treba li autoriziranom entitetu omogućiti pristup zaštićenom resursu ili sustavu. Korisnik se može prijaviti u sustav, ali mu neće biti omogućen pristup resursu ako tom korisniku nije odobreno pristupanje. Jaka autentifikacija predstavlja samo dio računalne sigurnosti.

7. LITERATURA

1. D. Shinder, Understanding and selecting authentication methods

Dostupno na: https://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/

2. E. Huseynov, J.M Seigneur, Enhancing RADIUS based multifactor-factor authentication systems with RESTful API for self-service enrolment

Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8686898

3. S. Z. S. Idrus, E. Cherrier, C. Rosenberger, J.J. Schwartzmann, A Review on Authentication Methods

Dostupno na : https://hal.archives-ouvertes.fr/hal-00912435/PDF/A_Review_on_Authentication_Methods.pdf

4. D. Gibbson, Understanding the Three Factors of Authentication

Dostupno na: http://www.pearsonitcertification.com/articles/article.aspx?p=1718488

5. The freeradius implementation guide

Dostupno na: https://networkradius.com/doc/FreeRADIUS-Implementation-Ch5.pdf

6. Freeradius documentation

Dostupno na: https://networkradius.com/freeradius-documentation/

7. J. Urpi, FreeRADIUS for small and medium-sized companies

Dostupno na : https://www.theseus.fi/bitstream/handle/10024/47101/Urpi_Joonas.pdf?sequence=1&isAllowed=y

8. H. Khan, What is SSL? 2014.

Dostupno na: https://www.ssl.com/faqs/faq-what-is-ssl/

9. Shiva Password Authentication Protocol (SPAP)

Dostupno na: http://www.certiology.com/tech-terms/network/shiva-password-authentication-protocol-spap.html

10. M. Rouse, Extensible Authentication Protocol (EAP)

Dostupno na: https://searchsecurity.techtarget.com/definition/Extensible-Authentication-Protocol-EAP

11. Gluu Server 3.1.6 Docs, SCIM 2.0 User Management

Dostupno na: https://gluu.org/docs/ce/user-management/scim2/

12. The freeradius implementation guide, poglavlje 5 - Basic Authentication Methods
Dostupno na: https://networkradius.com/doc/FreeRADIUS-Implementation-Ch5.pdf
13. LDAP (Lightweight Directory Access Protocol), M. Rouse
Dostupno na: https://searchmobilecomputing.techtarget.com/definition/LDAP
14. Documentation Duo Web
Dostupno na: https://duo.com/docs/duoweb
15. https://heimdalsecurity.com/blog/biometric-authentication/
16. https://sites.google.com/site/organvidaoko/home/grada-oka
17. A. Dascalescu, Biometric Authentication Overview, Advantages & Disadvantages
Dostupno na:
https://docs.typo3.org/typo3cms/extensions/ig_ldap_sso_auth/stable/SSO/Kerberos.html
18. PAP, CHAP, and MS-CHAP – CompTIA Security+ SY0-501 – 4.2
Dostupno na: https://www.professormesser.com/security-plus/sy0-501/pap-chap-and-ms-chap/
19. CHAP – Challenge Handshake Authentication Protocol,
Dostupno na http://joshpughpro.blogspot.com/2011/03/chap-challenge-handshake-authentication.html
20. EAP, Extensible Authentication Protocol
Dostupno na: https://net08.wordpress.com/security/used-protocols/
21. How Does RADIUS Work? 2006
Dostupno na: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html
22. Certificates and Authentication, Certificate-Based Authentication
Dostupno na: https://access.redhat.com/documentation/en-US/Red_Hat_Certificate_System/8.0/html/Deployment_Guide/Introduction_to_Public_Key_Cryptography-Certificates_and_Authentication.html
23. Information Technology Laboratory, Back to basics: Multi-factor authentication (MFA)
Dostupno na: https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication
24. Transaction authentication using complementary colors,
Dostupno na: https://www.semanticscholar.org/paper/Transaction-authentication-using-complementary-Maeng Mohaisen/121a61d325a4f364e642db60ea6fd25f95e8a542

25. J.Kagan, Transaction Authentication Number (TAN), 2018
Dostupno na: https://www.investopedia.com/terms/t/transaction-authentication-number-tan.asp
26. Mastercard unveils biometric card to replace ATM pin with fingerprint verification
Dostupno na:
https://www.livemint.com/Industry/eiwotgdAxZt98pGOgmJLCO/Mastercard-unveils-biometric-card-to-replace-ATM-pin-with-fi.html

SAŽETAK

U ovom radu opisani su mogući problemi u suvremenim računalnim mrežama vezani za područja sigurnost i privatnost. Opisano je nekoliko postojećih metoda koje se primjenjuju za rješavanje autentifikacijskih problema, zajedno s prednostima i nedostacima svake od njih. Implementirana su moguća besplatna rješenja te su prikazane njihove prednosti i mane. Odrađena je usporedba implementiranih rješenja i predstavljena praktična primjena svake od metoda. Također, bitan naglasak je stavljen na važnost adekvatne autentifikacije kao izrazito važnog faktora računalne sigurnosti.

Ključne riječi: autentifikacija, sigurnost, autorizacija, Gluu poslužitelj, FreeRADIUS poslužitelj

ADVANCED METHODS OF AUTHENTIFICATION IN COMPUTER NETWORKS

ABSTRACT

This paper describes possible problems in modern computer networks related to the areas of security and privacy. Several existing methods that are used to resolve authentication problems are described, along with the advantages and disadvantages of each. Possible free solutions are implemented and their advantages and disadvantages are presented. A comparison of the implemented solutions is made and a practical application of the methods is presented. Also, significant emphasis was placed on the importance of adequate authentication as an extremely important factor in computer security.

Keywords: authentication, security, authorization, Gluu server, freeRADIUS server

ŽIVOTOPIS

Maja Stanić, rođena 23.12.1995. godine u Slavonskom Brodu. Školovanje je započela u OŠ „Antun i Stjepan Radić" u Gunji. Zatim upisuje gimnaziju „Vaso Pelagić" u Brčkom, Bosna i Hercegovina. Po završetku srednje škole, 2014. godine upisuje "Fakultet elektrotehnike, računarstva i informacijskih tehnologija" u Osijeku, gdje se opredjeljuje za smjer Komunikacije i informatika. Titulu prvostupnice elektrotehnike stječe 2017. godine nakon čega upisuje diplomski studij elektrotehnike, smjer Komunikacije i informatika, podsmjer Mrežne tehnologije.