

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Marijan Kovač

DVOSTRUKA PRIJAVA

**SEMINARSKI RAD IZ KOLEGIJA ELEKTRONIČKO I MOBILNO
POSLOVANJE**

Varaždin, 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

Marijan Kovač

Studij: Informacijsko i programsko inženjerstvo

DVOSTRUKA PRIJAVA

SEMINARSKI RAD IZ KOLEGIJA ELEKTRONIČKO I MOBILNO POSLOVANJE

Mentor:

Izv. prof. dr. sc. Sandro Gerić

Varaždin, svibanj 2023.

Sadržaj

1. Uvod.....	1
2. Dvostruka prijava	2
2.1. Princip rada.....	3
2.2. Vrste.....	4
2.2.1. Mobilni uređaji	4
2.2.1.1. Sustav za autentifikaciju bez upotrebe interneta	5
2.2.1.2. Sustav za autentifikaciju upotrebom SMS poruka	6
2.2.2. Fizički tokeni	7
2.3. Prednosti	8
2.4. Nedostaci	8
2.4.1. Reverse engineering.....	9
2.4.2. SIM swapping	10
2.4.3. Krađa sesije.....	10
3. Implementacija	12
3.1. Dizajn sustava.....	12
3.2. Primjer korištenja aplikacije.....	13
3.2.1. Registracija.....	14
3.2.2. Prijava	15
4. Zaključak	17
Popis literature	18
Prilozi	19

1. Uvod

Digitalno doba u kojemu trenutno živimo obilježeno je brojnim online uslugama koje su sve prisutnije, pri čemu korisnici interneta koriste udaljene poslužitelje diljem svijeta kojima šalju i na koje pohranjuju brojne podatke. Ti podaci obično su vrlo osjetljivi, a često se radi i o transakcijskim podacima koji predstavljaju osobito velik sigurnosni rizik.

Kako bi se zaštitili od neovlaštenog pristupa, krađe identiteta i osobnih podataka svojih korisnika, mnoge organizacije i online platforme koriste sustave za dvostruku prijavu, poznatiju kao dvofaktorska autentifikacija (eng. *two-factor authentication* ili kraće, 2FA).

Dvostruka prijava pruža dodatni sloj sigurnosti jer od korisnika zahtjeva dvije različite potvrde identiteta prilikom prijave. Naime, tradicionalno se za prijavu koristi samo jedan faktor zaštite – korisničko ime i lozinka, koji jednostavno nisu dovoljni da se spriječi neovlašteni pristup i hakiranje računa.

U ovom će se radu najprije detaljnije opisati dvostruka prijava kao sigurnosna mjera, zatim će se navesti njene prednosti i nedostaci, a potom će se ponuditi primjer njene implementacije korištenjem Java programskog jezika i mobilne aplikacije Google Authenticator.

2. Dvostruka prijava

Dvostruka prijava (eng. *two-factor authentication* ili kraće, 2FA) je sigurnosna mjera koja se koristi za pružanje dodatnog sloja zaštite od online sigurnosnih prijetnji. U zadnjih nekoliko godina, došlo je do porasta u korištenju ove sigurnosne mjere u različitim organizacijama, kao što su banke, vladine aplikacije, zdravstvene ustanove, vojska, obrazovne ustanove, pa čak i društvene mreže. [1], [2]

Glavna je motivacija za korištenje dvostruke prijave kao zaštitne mjere porast broja kibernetičkih napada i povreda korisničkih podataka, nužnost usklađenosti sa zakonskim zahtjevima kao i pružanje poboljšane sigurnosti korisnicima. Unatoč tomu, većina današnjih sustava i dalje se oslanja na statične lozinke za provjeru identiteta korisnika. [1]

Problem korištenja samo tradicionalne provjere autentičnosti upotrebom korisničkog imena i lozinke je taj što to samo po sebi nije dovoljno sigurno jer omogućuje hakerima lako dobivanje pristupa korisničkim računima putem različitih vrsta napada kao što su krađa identiteta, društveni inženjering (eng. *social engineering*), snooping, sniffing, guessing, shoulder surfing i mnogi drugi. Dodatni problem, odnosno olakšica hakerima, je sklonost korisnika da koriste jednostavne lozinke koje je vrlo lako pogoditi, zapisuju lozinke i pohranjuju na lako dostupna mjesta, bilo u fizičkom obliku (npr. papir) ili u elektroničkom obliku (npr. čitljiva datoteka na računalu) te koriste istu lozinku za više različitih računa. [2]

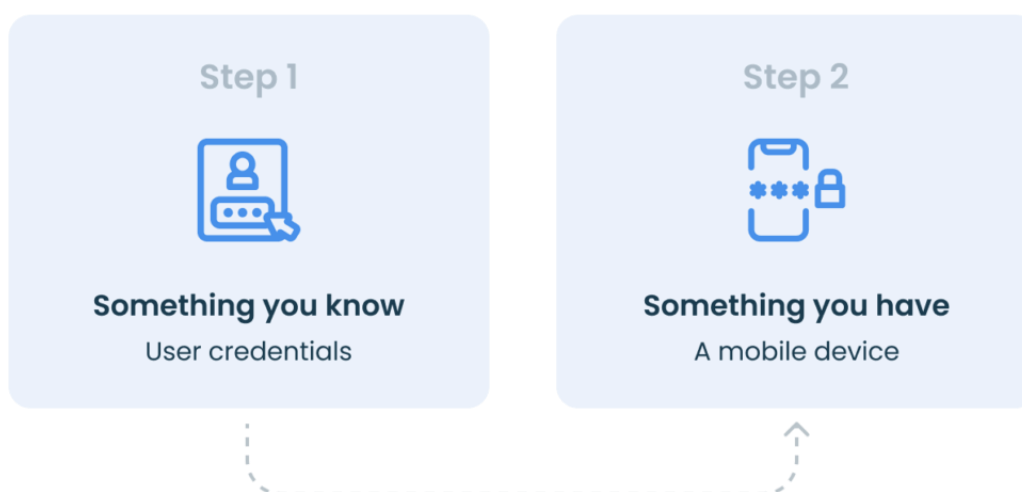
Iz navedenih je razloga dvostruka prijava ključan faktor zaštite jer pruža dodatni sloj sigurnosti osjetljivih podataka, kao što su financijski i osobni podaci. Naime, korištenjem dvostruke prijave, u slučaju da haker čak i ukrade podatke za prijavu, neće moći pristupiti podacima bez dodatnog oblika identifikacije, kao što je korisnikov otisak prsta ili sigurnosni token. [1]

Upotreba metode dvostruke prijave zapravo nije nikakva novost. Naime, bankomati (eng. *Automated Teller Machines – ATM*) koriste dvostruku prijavu već desetljećima, no u računalnome svijetu je to relativno mlad pojam. Naime, Google je svoj sustav dvostruke prijave lansirao prije desetak godina, no unatoč tomu usvajanje ove vrste zaštite do danas nije rasprostranjeno. [3]

U nastavku ovog poglavlja najprije će se objasniti koncept, odnosno princip rada dvostruke prijave, zatim će se navesti koje sve vrste, odnosno mogućnosti korištenja postoje, te će se naposljetku navesti nekoliko prednosti i nedostataka u korištenju ove metode zaštite.

2.1. Princip rada

Koncept dvostruke prijave temelji se na pružanju dva sloja autentifikacije korisnika, a najčešće je riječ o kombinaciji korisničkog imena i lozinke te jednokratne lozinke ili sigurnosnog tokena za pristup korisničkom računu ili obavljanje online transakcija. Koncept je poznat po sloganu, odnosno principu „nešto što znamo i nešto što imamo“ (eng. „*something you know and something you have*“). [1]



Slika 1: Ilustracija koncepta dvostruke prijave (Izvor: www.ekransystem.com)

Pojam „nešto što znamo“ (eng. *something you know*) odnosi se na znanje koje korisnik ima, točnije podatak koji on zna, a to najčešće uključuje lozinku, a može uključivati i sigurnosna pitanja (eng. *security questions*) koja se često koriste kod oporavka računa. S druge strane, pojam „nešto što imamo“ (eng. *something you have*) označava uređaj (npr. mobilni uređaj), objekt (npr. papir s popisom jednokratnih pristupnih lozinki), zatim softverski token (npr. aplikativno generirani token) ili hardverski token (npr. RSA SecurID). [3]

Valja napomenuti kako postoji i treća kategorija – „nešto što jesmo“ (eng. *something you are*), koja se odnosi na biometriju (npr. mrežnica oka ili otisak prsta) [3], no ta se kategorija najčešće ne koristi kod dvostruke prijave jer je skuplja za implementaciju. Iznimka za to su današnji mobilni uređaji koji uglavnom dolaze s ugrađenim senzorom za otisak prsta, a također imaju i softversko rješenje za prepoznavanje lica (eng. *face recognition*) putem prednje kamere (eng. *face cam*). Ipak, korištenje ove vrste zaštite usmjereno je na višestroku prijavu (eng. Multi-factor authentication – MFA) što nije tema ovoga seminarskog rada.

Kao što je već ranije spomenuto, koncept dvostruke prijave nije novitet. Naime, bankomati (eng. *Automated Teller Machines* – ATM) koriste dvostruku prijavu već desetljećima kako bi autentificirali korisnike. U tom je slučaju PIN (eng. *Personal Identification Number*) kategorija „nešto što znamo“ (eng. *something you know*), dok je sama bankovna kartica zapravo „nešto što imamo“ (eng. *something you have*). [3]

Danas u elektroničkom i mobilnom poslovanju postoji više načina implementiranja ovoga koncepta, a neke od vrsta implementacije ćemo prikazati u nastavku.

2.2. Vrste

Postoji više vrsta implementacije koncepta dvostruke prijave. S jedne strane imamo vrste koje su relativno jednostavne za implementaciju i korištenje, dok postoje i one koje su vrlo teške za korištenje ili pak ne zadovoljavaju sigurnosne probleme neke organizacije. [2]

Općenito se implementacije sustava dvostruke prijave mogu podijeliti na dvije kategorije – dvostruka prijava korištenjem mobilnih uređaja i dvostruka prijava korištenjem fizičkih tokena.

2.2.1. Mobilni uređaji

Mobilni se uređaji tradicionalno smatraju alatom za telefoniranje, no danas je, zahvaljujući napretku u hardveru i softveru, njihova upotreba uvelike proširena. S obzirom na to, danas mobiteli služe za obavljanje mnogih drugih aktivnosti uz telefoniranje, a osim toga, imaju i puno više mogućnosti povezivanja putem mobilne mreže. [2] Iz svih tih razloga, sve je veći broj ljudi koji koristi mobilne uređaje u svakodnevnom životu, te su upravo to glavni razlozi zbog kojih se isti mogu koristiti i kao drugi faktor za autentifikaciju.

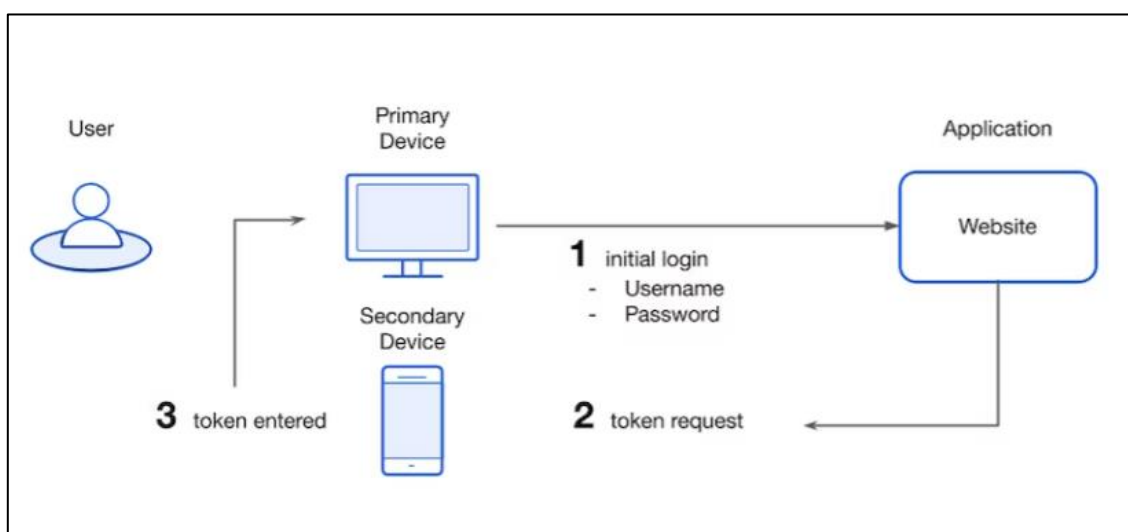
Ovaj sustav za dvostruku prijavu predstavlja zamjenu za korištenje fizičkih tokena, koji unatoč sigurnosti imaju brojne mane kao što su cijena njihove izrade i nepraktičnost korištenja. Općenito govoreći, sustav autentifikacije putem mobilnih uređaja najčešće se sastoji od dva dijela: [4]

1. aplikacija instalirana na mobilni uređaj
2. odgovarajući softver na poslužitelju

Također, postoji više načina na koji se može ostvariti potvrda u dva koraka, a najčešće je riječ o dva načina – sustav za autentifikaciju bez upotrebe interneta i sustav za autentifikaciju koristeći SMS poruke.

2.2.1.1. Sustav za autentifikaciju bez upotrebe interneta

Kod sustava za autentifikaciju bez upotrebe interneta općenito se upotrebljava jednokratna lozinka (eng. *One time password* – OTP). Jednokratna se lozinka generira bez upotrebe internetske veze, odnosno za generiranje iste nije potreban poslužitelj. Da bi to bilo moguće, koristi se upravo mobilni uređaj koji oponaša token, odnosno koristi odgovarajuću aplikaciju koja ima točno određene čimbenike jedinstvene za korisnika na temelju kojih se, korištenjem odgovarajućih algoritama, jednokratne lozinke generiraju. [2]



Slika 2: Dizajn sustava za autentifikaciju bez upotrebe interneta (Izvor: bitwarden.com)

S druge strane, poslužitelj također „zna“ za te čimbenike te na temelju istih može usporediti je li jednokratna lozinka generirana na strani klijenta (korisnikovog mobilnog uređaja) ista kao i ona koju je sam poslužitelj generirao, pri čemu se koristi isti algoritam kao i na strani klijenta, odnosno njegovoj aplikaciji. [4]

Danas postoji više aplikacija koje omogućavaju generiranje jednokratnih lozinki, a najpoznatije su Google Authenticator (koji će detaljnije biti prikazan u praktičnom dijelu rada), zatim Microsoft Authenticator, Authy i drugi.

2.2.1.2. Sustav za autentifikaciju upotrebom SMS poruka

Ova se metoda dvostruke prijave najčešće koristi za slučaj da nije moguće koristiti aplikacijski token, odnosno generiranje jednokratne lozinke. Metoda funkcionira tako da se direktno šalje zahtjev poslužitelju, koji i u tom slučaju „zna“ za karakteristične čimbenike vezane uz korisnika, te na temelju kojih generira jednokratnu lozinku (OTP). [2]

Nakon što poslužitelj dobije zahtjev za generiranje jednokratne lozinke, primjenjuje se algoritam za generiranje iste te se ona šalje korisniku putem SMS poruke. Pri tome korisnik ima određeno kratko vrijeme da upotrijebi jednokratnu lozinku prije no što ona istekne. [2]

Glavni nedostatak ove metode je taj što i poslužitelj, odnosno odgovorna organizacija, kao i klijent, odnosno vlasnik mobilnog uređaja (a samim time i broja mobitela), moraju platiti troškove telekomunikacijskih usluga. [2]

2.2.2. Fizički tokeni

Fizički token možemo opisati kao mali uređaj čija je namjena autorizacija korisnika. Karakterističan je po tome što je lako prenosiv, te obično sadrži kriptografske ključeve ili biometrijske podatke, a može imati i mali zaslon na kojem se prikazuju jednokratne lozinke (eng. *One time password* – OTP). [2]

Iako slove kao vrlo siguran način autorizacije korisnika, njihova je glavna mana ta što mogu biti vrlo skupi za organizacije koje ih koriste. Primjerice, da bi banka osigurala svim svojim klijentima fizičke tokene, morat će izdvojiti veliku količinu novca za njihovu kupnju, instalaciju i održavanje. Dodatno, morat će osigurati i stalnu podršku i edukaciju klijenata, pa i svojih zaposlenika za njihovu primjenu. Osim toga, u slučaju da klijent izgubi, ošteti ili mu netko ukrade token, njegova zamjena je puno skuplja nego, primjerice, promjena lozinke ili poništavanje kreditne kartice. [2]

Najpoznatiji primjeri fizičkih tokena su RSA SecurID, Keypad Token, Yubikey, Google Titan Security Key i drugi.



Slika 3: RSA SecurID (Izvor: www.cdw.com)



Slika 4: Yubikey (Izvor: www.yubico.com)

2.3. Prednosti

Općenito govoreći, dvostruka prijava ima brojne prednosti, a glavna od njih svakako je ta što omogućava višu razinu sigurnosti u odnosu na autentifikaciju putem tradicionalnih metoda kao što su upotreba korisničkog imena i lozinke. [1]

Dakle, u slučaju dvostruke prijave, ukoliko napadač uspije pridobiti korisničke podatke za prijavu, neće moći pristupiti računu bez drugog faktora autentifikacije, koji može biti na mobilnom telefonu korisnika ili na njegovom fizičkom tokenu.

Nadalje, većina platformi i usluga koje nude prijavu u dva koraka omogućavaju korisnicima njeno jednostavno postavljanje. To može uključivati potvrdu putem SMS-a, mobilne aplikacije ili upotrebu fizičkih tokena. Dakle, prednost je i u različitosti dostupnih metoda koje krajnji korisnik ima na izbor. [1]

2.4. Nedostaci

Što se tiče nedostataka, možda najveći nedostatak je taj što je korisniku za pristup računu potreban dodatan uređaj ili više njih, a koje mora uvijek imati uz sebe, što može biti vrlo nezgodno i nepraktično. Osobito velik problem javlja se kada korisnik izgubi takav uređaj, ošteti ga ili mu bude ukraden, a sve to može značiti otežan pristup računu ili čak trajni gubitak mogućnosti pristupanja istome. [1]

Nadalje, postoji veliki rizik od tehničkih poteškoća koji se mogu pojaviti prilikom korištenja dvostruke prijave. To najčešće uključuje probleme s mobilnom mrežom, a kada je riječ o sustavima za dvostruku autentifikaciju bez upotrebe interneta, onda se mogu javiti problemi s generiranjem jednokratnih lozinki, kao što je primjerice nesinkroniziranost (eng. *out of sync*) algoritma na strani klijenta i onog na strani poslužitelja. [1]

Što se tiče sigurnosnog aspekta dvostruke prijave, unatoč tomu što omogućavaju višu razinu sigurnosti, nikako nisu neprobojni te postoje brojni načini koje koriste napadači kako bi se ipak dokopali korisničkih računa. Temeljni sigurnosni nedostaci su:

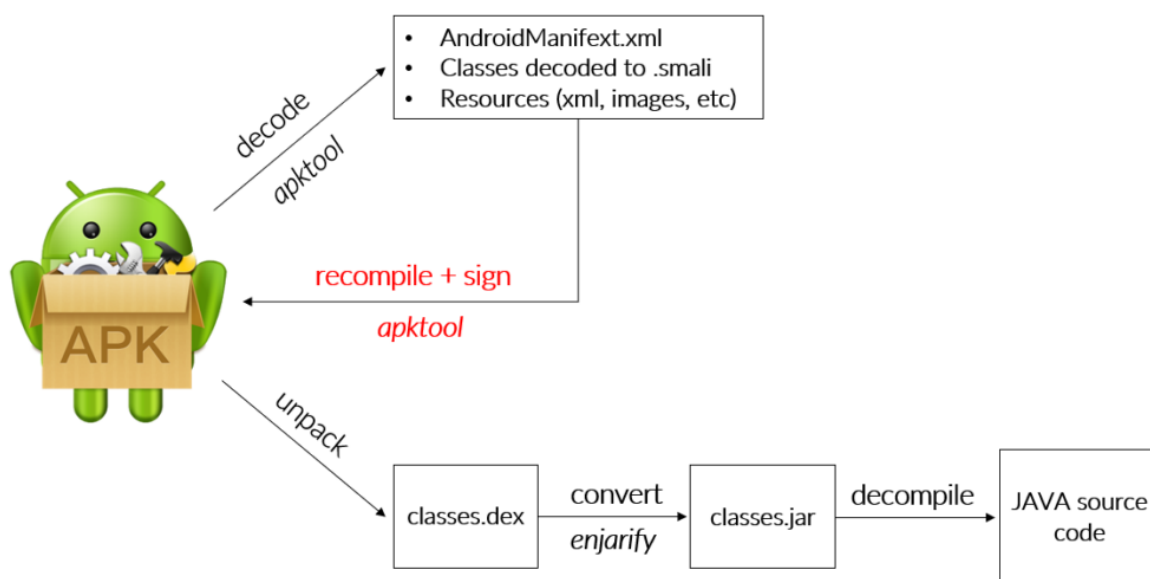
- Reverse engineering
- SIM swapping
- Krađa sesije

2.4.1.Reverse engineering

Reverse engineering je proces analiziranja sustava kako bi se prikupili podaci o njegovim komponentama i kako bi se kreirala njegova kopija da bi se isti mogao detaljnije analizirati, a to se osobito odnosi na njegove funkcionalnosti i skrivene komponente. [5]

Ovom tehnikom napadač može analizirati aplikacije instalirane na korisnikovom mobilnom uređaju te proučiti njihov izvorni kod, te na taj način otkriti temeljne karakteristike algoritma koji ta aplikacija koristi ili još gore – otkriti dijeljeni tajni ključ, odnosno tajno sjeme (eng. *seed*) na temelju kojega se generiraju jednokratne lozinke. Prema tome, tajni ključ, odnosno *seed*, ne bi smio biti zadan u čitljivom obliku, odnosno ne bi smio biti „hardkodiran“ (eng. *hardcoded*).

Tehnika *reverse engineering*-a vrlo je jednostavna za izvedbu, a sve što je potrebno je izvršna aplikacija te alat koji će obaviti proces „dekompajliranja“, odnosno „vraćanja“ koda iz binarnog oblika u oblik programskog koda. Za to postoje brojni alati kao što su apktool, Jadx-GUI, Frida, Objection, adb, a postoje i brojni drugi nekomercijalni i *open-source* alati. [5]



Slika 5: Postupak *reverse engineering*-a mobilne aplikacije (Izvor: www.securing.pl)

2.4.2.SIM swapping

SIM swapping, odnosno „zamjena“ SIM kartice, odnosi se na slabost u dvofaktorskoj autentifikaciji korištenjem SMS poruke ili poziva.

Ova se vrsta napada događa kada napadači kontaktiraju operatera korisnikovog mobilnog uređaja i prevarom ga navedu da aktivira SIM karticu koju imaju prevaranti. Kada se to dogodi, prevaranti imaju potpunu kontrolu nad telefonskim brojem korisnika. To znači da svatko tko nazove ili pošalje poruku na broj mobitela, umjesto uređaj korisnika, zapravo će se kontaktirati uređaj napadača. [6]

Prijevara zamjenom SIM kartice osobito je opasna za bankovne račune. Naime, ukoliko banka pošalje kod za dvostruku autentifikaciju putem SMS-a ili poziva, on neće stići na mobilni uređaj stvarnog korisnika, već na uređaj koji koristi napadač, te ako je isti ukrao i osobne podatke poput kartice, može lako pristupiti korisničkom računu na web stranici banke. [6]

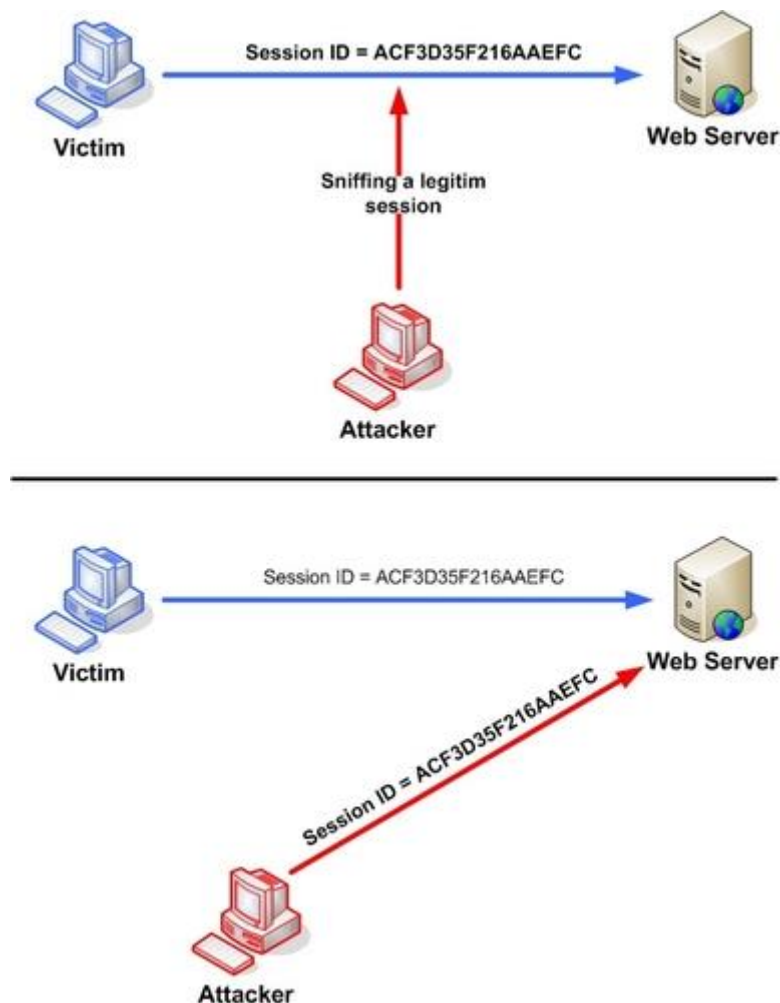
2.4.3.Krađa sesije

Ova se vrsta napada odnosi na iskorištavanje mehanizma kontrole web sesija, odnosno sjednica (eng. *session*). Za razliku od prethodno opisanih vrsta napada, kod krađe sesije nema direktnog utjecaja na sam sustav dvostruke prijave, već je on jednostavno – zaobiđen (eng. *bypassed*).

Web sesije se koriste kako bi poslužitelji mogli prepoznati vezu za svakog pojedinog korisnika, budući da HTTP komunikacija koristi mnogo različitih TCP veza. Najčešće je riječ o jedinstvenom tokenu u obliku niza nasumičnih znakova određene veličine, koji web poslužitelj šalje pregledniku na klijentovoj strani, i to nakon uspješne provjere autentičnosti (uključujući i dvostruku prijavu). [7]

Napadači najčešće pokušavaju ukrasti sesije za vrijeme kada korisnici, primjerice, provjeravaju stanje računa, plaćaju račune ili obavljaju kupovinu putem *online* trgovine. Da bi im to pošlo za rukom, koriste se različitim metodama, a najčešće se radi o: [8]

- napad grubom silom (eng. *brute-force attack*)
- cross-site scripting (XSS napad)
- zlonamjerni program (maliciozni JavaScript kod, Trojanski konj)
- session sniffing
- man-in-the-middle napad



Slika 6: Krađa session tokena sniffing metodom (Izvor: owasp.org)

Jedan od poznatijih i najrelevantnijih napada korištenjem krađe sesije je napad na tvrtku Linus Media Group te njihove YouTube kanale poznate pod nazivima Linus Tech Tips i Techquickie. U tom je napadu, prema vlasniku ove tvrtke, Linusu Sebastianu, netko od zaposlenika preuzeo PDF datoteku koja je bila dio „ponude sponzora“ od potencijalnog partnera. Kasnije se ispostavilo da je PDF datoteka zapravo u sebi sadržavala zlonamjerni program putem kojih je napadač pristupio svim podacima, a osobito onima u web-preglednicima, čime je ukrao i session tokene. Time je napadač preuzeo svu kontrolu nad korisničkim računima ove tvrtke, te je tu priliku iskoristio za prijenos uživo (eng. *livestream*) lažnih videa o kripto ulaganjima, mijenjanje naziva YouTube kanala, pa čak i brisanje videa. [9]

Prema tome, za krađu sesije najvećim su dijelom odgovorni servisi, poput Google-a i YouTube-a, jer su oni ti koji bi trebali osigurati zaštitu protiv ovog napada, a jedan od načina je zahtijevanje ponovne autentifikacije kada je korisnik prijavljen s druge geolokacije ili ako je session token isti na različitim računalima ili preglednicima.

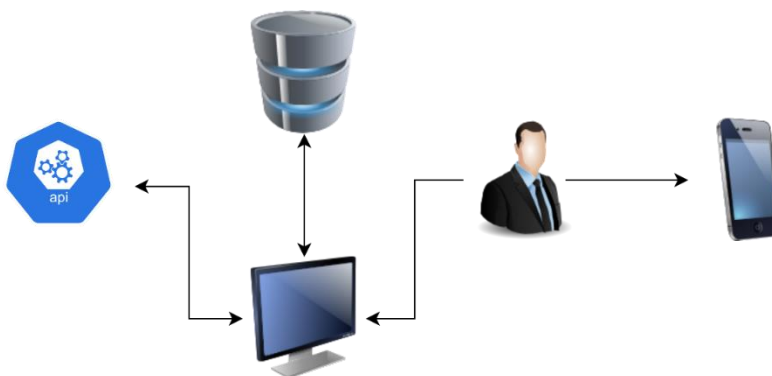
3. Implementacija

U ovom će se dijelu projekta pokazati princip rada dvostruke prijave na primjeru jednostavne Java web aplikacije koja za svoj rad zahtijeva mobilni uređaj i aplikaciju Google Authenticator. Izvorni kod aplikacije dostupan je u odjeljku Prilozi.

3.1. Dizajn sustava

Sustav funkcionira na vrlo jednostavan način. Web aplikacija za svoj rad koristi dva temeljna resursa – bazu podataka za pohranjivanje informacija o korisničkom računu i Google Authenticator API za kreiranje tajnog ključa te provjeru ispravnosti jednokratne lozinke.

Korisnik web aplikacije za registraciju i prijavu u sustav, osim korisničkog imena i lozinke treba i mobilni uređaj koji će imati instaliran Google Authenticator i koji će predstavljati token, odnosno drugi korak u postupku njegove prijave.



Slika 7: Dizajn sustava (Izvor: autorski rad)

Što se tiče baze podataka, ona će sadržavati samo jednu tablicu u koju će se pohranjivati korisničko ime, lozinka te tajni ključ za Google Authenticator aplikaciju – jedinstven za korisnika, koji služi kao sjeme (eng. *seed*) za generiranje jednokratnih lozinki.

emp_db korisnik	
id	int
korisnicko_ime	varchar(255)
lozinka	varchar(255)
secret_key	varchar(255)

Slika 8. Baza podataka (autorski rad)

3.2. Primjer korištenja aplikacije

Da bismo vidjeli kako aplikacija funkcionira u praksi, pokazat ćemo u nekoliko koraka kako se ona koristi. Web aplikacija se sastoji od tri stranice:

- početna stranica
- registracija
- prijava

Pokretanjem web aplikacije korisnik dolazi na početnu stranicu na kojoj može odabrati dvije opcije – registraciju ili prijavu (Slika 9).



Slika 9: Početna stranica web aplikacije (Izvor: autorski rad)

3.2.1.Registracija

Ukoliko korisnik odabere opciju *Registracija*, bit će preusmjeren na obrazac za kreiranje računa. Prilikom učitavanja stranice, automatski se generira tajni ključ (eng. *secret key*), koji se prikazuje na stranici kao i QR kod u odgovarajućem formatu za Google Authenticator.

Na tom obrascu korisnik unosi svoje željeno korisničko ime i lozinku, a potom postupava prema uputama vidljivim ispod tajnoga ključa i QR koda (Slika 10).

Nakon što su uneseni podaci o računu te nakon što je uspješno obavljen postupak dodavanja računa u aplikaciji Google Authenticator na mobilnom uređaju, korisnik može kliknuti na gumb *Registriraj se* kako bi se podaci o računu, uključujući i tajni ključ, spremili u bazu podataka.

Registracija — Mozilla Firefox

Applications x Registracija x localhost / localhost / emp_ x +

webpredmeti:8080/emp_projekt/mvc/registracija 120% ☆

Payara Console phpMyAdmin DZ2 DZ3


[Početna stranica](#)

Registracija

Ime autora: Marijan
Prezime autora: Kovac
Predmet: EMP
Godina izrade: 2023
Verzija: 1.00

Korisničko ime:

Lozinka:



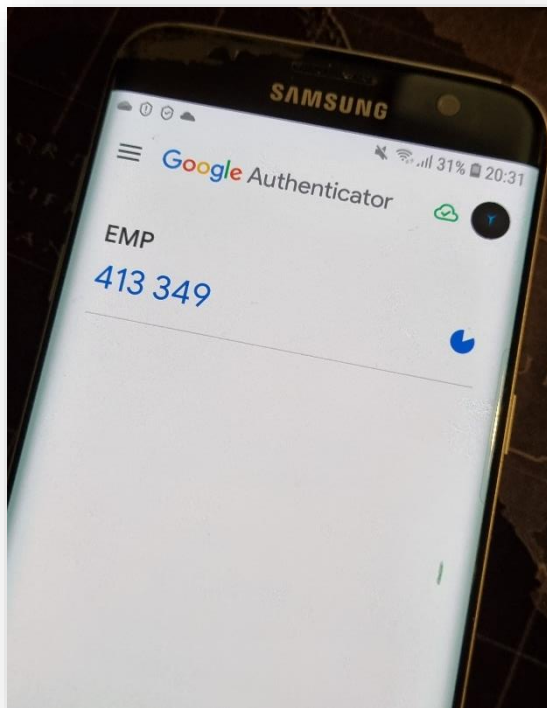
4YDJTVUGE74KZHR6C7KG3LAAV5PHNKBM

1. Instalirajte Google autentifikator na vaš mobilni uređaj
2. Skenirajte QR kod ili unesite ključ vidljiv na ekranu
3. Dodijelite naziv računa i spremite postavke
4. Prilikom svake prijave koristite vremenski kod iz autentifikatora

Slika 10: Stranica za registraciju (Izvor: autorski rad)

3.2.2. Prijava

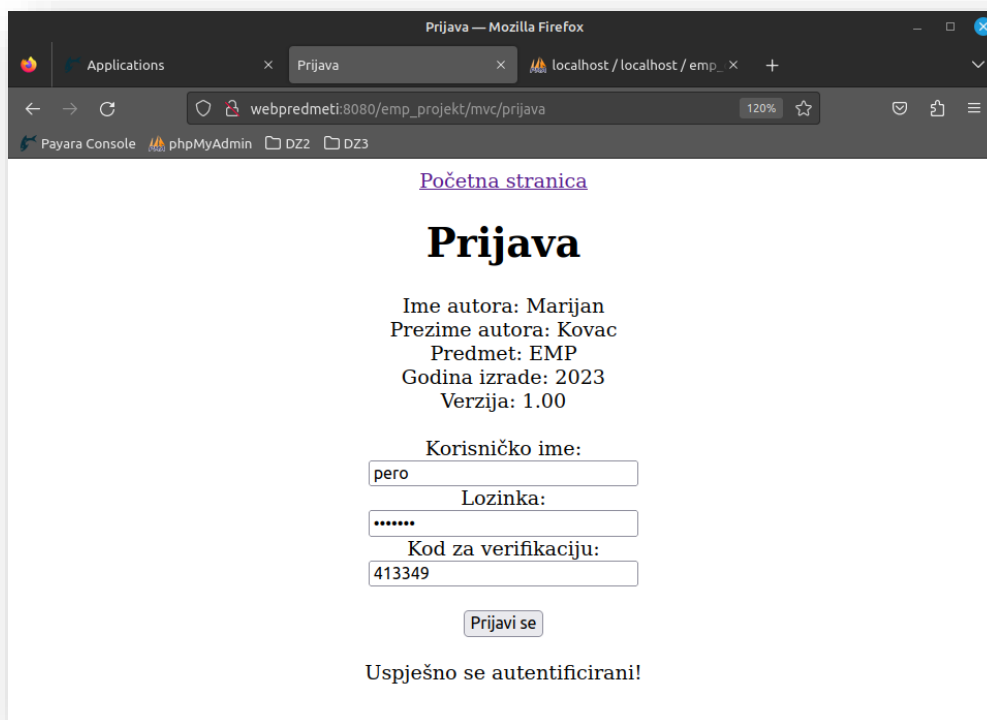
Nakon uspješne registracije i postupka dodjele računa u Google Authenticator, korisnik može odabrati opciju *Prijava*. Da bi se prijavio, korisniku neće biti dovoljni samo korisničko ime i lozinka, već će morati upotrijebiti i mobilni uređaj, odnosno Google Authenticator aplikaciju kako bi unio trenutno generirani jednokratni kod za prijavu (eng. Time-based one time password – TOTP). Na Slici 11 moguće je vidjeti primjer jednokratne lozinke koja je generirana u trenutku izrade ove demonstracije.



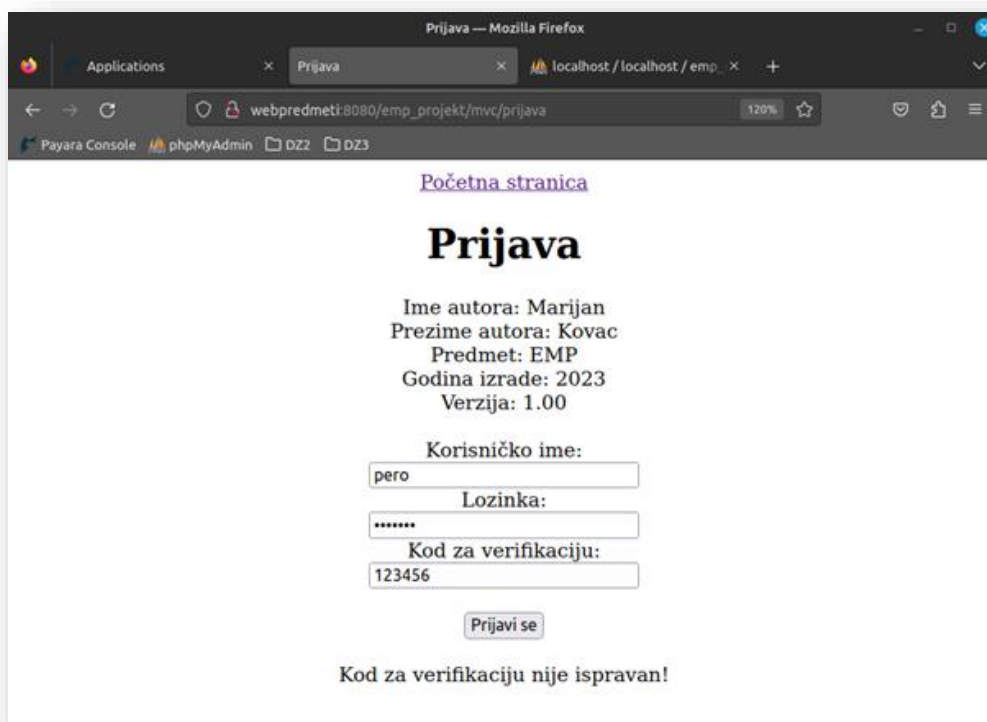
Slika 11: Mobilni uređaj i aplikacija Google Authenticator s jednokratnom lozinkom (Izvor: autorski rad)

Ukoliko su podaci za prijavu ispravni, odnosno ako uneseni korisničko ime i lozinka odgovaraju onima u bazi podataka, tada se još dodatno vrši i provjera ispravnosti jednokratne lozinke. Ukoliko trenutno generirana jednokratna lozinka u aplikaciji Google Authenticator odgovara onoj koju je generirao i algoritam koji koristi web aplikacija, tada će se korisniku nakon klika na gumb *Prijavi se* pokazati poruka „Uspješno ste autentificirani!“ (Slika 12).

U slučaju da se generirana lozinka iz aplikacije Google Authenticator i ona koju je generirao algoritam web aplikacije ne poklapaju, korisniku se nakon klika na gumb *Prijavi se* javlja poruka „Kod za verifikaciju nije ispravan!“ (Slika 13).



Slika 12: Stranica za prijavu – uspješna prijava (Izvor: autorski rad)



Slika 13: Stranica za prijavu – neuspješna prijava (Izvor: autorski rad)

4. Zaključak

Dvostruka je prijava sigurnosni mehanizam koji pruža dodatnu razinu zaštite prilikom pristupa korisničkim računima i podacima. Postupak dvostruke prijave obično zahtijeva da korisnik pruži dvije različite vrste identifikacijskih podataka kako bi potvrdio svoj identitet, a najčešće se radi o kombinaciji nečega što korisnik zna (npr. lozinku) i nečega što korisnik posjeduje (npr. mobilni uređaj).

Brojne su prednosti dvostruke prijave. Naime, ona značajno otežava neovlaštenim osobama pristup računima, čak i u slučaju da se iste dokopaju korisničkog imena i lozinke neke druge osobe. To je osobito važno kada je riječ o vrlo osjetljivim podacima poput financijskih podataka.

Postoje različiti oblici dvostruke prijave, a neke od njih su SMS poruke s jednokratnim kodovima, mobilne aplikacije za generiranje jednokratnih lozinki ili pak fizički ključevi, a mogu biti i biometrijski identifikatori kao što su otisak prsta ili prepoznavanje lica.

Unatoč brojnim prednostima, važno je znati da sustav dvostruke prijave nije u potpunosti neprobojan. Naime, napadači mogu koristiti sofisticirane tehnike kao što su phishing, krađa sesija, reverse engineering aplikacija za autentifikaciju, SIM swapping i brojne druge tehnike zaobilaženja ovog sigurnosnog mehanizma.

Bez obzira na moguće nedostatke, dvostruka je prijava snažan alat za poboljšanje sigurnosti korisničkih računa i podataka. Da bi se u potpunosti ostvarila sigurnost na internetu, važno je koristiti i druge sigurnosne mjere kao što je redovito ažuriranje softvera, korištenje snažnih lozinki te opća svijest o sigurnosti na internetu.

Popis literature

- [1] D. Bhanderi, M. Kavathiya, T. Bhut, H. Kaur, i M. Mehta, *Impact of Two-Factor Authentication on User Convenience and Security*. 2023. Pristupljeno: 20. svibanj 2023. [Na internetu]. Dostupno na: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10112421>
- [2] F. Aloul, S. Zahidi, i W. El-Hajj, „Two factor authentication using mobile phones“, u *2009 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, 2009, str. 641–644. doi: 10.1109/AICCSA.2009.5069395.
- [3] J. Colnago i ostali, „“It’s not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University“, *Association for Computing Machinery (ACM)*, tra. 2018, str. 1–11. doi: 10.1145/3173574.3174030.
- [4] S. Acharya, A. Polawar, i P. Y. Pawar, „Two Factor Authentication Using Smartphone Generated One Time Password“. [Na internetu]. Dostupno na: www.iosrjournals.org
- [5] C. Ozkan i K. Bicakci, „Security Analysis of Mobile Authenticator Applications“, u *2020 International Conference on Information Security and Cryptology, ISCTURKEY 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., pros. 2020, str. 18–30. doi: 10.1109/ISCTURKEY51113.2020.9308020.
- [6] D. Rafter, „SIM Swap Fraud“, 2022. <https://us.norton.com/blog/mobile/sim-swap-fraud> (pristupljeno 24. svibanj 2023.).
- [7] „Session hijacking attack“. https://owasp.org/www-community/attacks/Session_hijacking_attack (pristupljeno 24. svibanj 2023.).
- [8] Johnson Allie, „Session hijacking“, 2021. <https://us.norton.com/blog/id-theft/session-hijacking> (pristupljeno 24. svibanj 2023.).
- [9] Peters Jay, „How hackers took over Linus Tech Tips“, 24. ožujak 2023. <https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-channel-hack-session-token-elon-musk-crypto-scam> (pristupljeno 24. svibanj 2023.).

Prilozi

1. Github repozitorij: <https://github.com/mkovac700/emp>