

Kurs: Računarstvo i društvo  
**Bezbednost naših lozinki**

Autor: Aleksa Jovanović

Predmetni profesor: **dr. Sana Stojanović Đurđević**

Datum: 15. jun 2024.

# Sadržaj

<b>1</b>	<b>Uvod</b>	<b>2</b>
<b>2</b>	<b>Uticaj na druge sfere života</b>	<b>2</b>
2.1	Privatnost na internetu . . . . .	2
2.2	Spam . . . . .	2
2.3	Žene kao mete sajber napada . . . . .	3
<b>3</b>	<b>Česti napadi i greške korisnika</b>	<b>4</b>
3.1	Napad grubom silom . . . . .	4
3.2	Napad rečnikom . . . . .	4
3.3	Ponovno korišćenje šifara . . . . .	4
3.4	Ostale loše prakse . . . . .	4
<b>4</b>	<b>Mere prevencije</b>	<b>5</b>
4.1	Jačina lozinke . . . . .	5
4.2	Alati . . . . .	6
<b>5</b>	<b>Alternative i dodatna zaštita</b>	<b>7</b>
5.1	Jednokratne lozinke . . . . .	7
5.2	Biometrijska autentikacija . . . . .	9
5.3	Adaptivna autentikacija . . . . .	10
<b>6</b>	<b>Zaključak</b>	<b>12</b>

# 1 Uvod

Korišćenje šifara u današnjem digitalnom svetu je (trenutno) nezaobilazna realnost i prva linija odbrane od neželjenog pristupa našim profilima, podacima, finansijama i komunikacijama (društvenim mrežama poput Instagram-a, LinkedIn-a, X-a, platformama za komunikaciju poput Telegram-a i Signal-a, e-banking aplikacijama banki). Sigurnost celokupnog sistema je jaka samo koliko i najslabija karika, koja je pretežno korisnik. Loše prakse pri kreiranju i čuvanju lozinki, i korišćenju interneta olakšavaju zlonamernim akterima pristup privatnim podacima. Ovaj rad će se pretežno fokusirati na uvid u potencijalnu štetu koja može biti naneta, prvenstveno na individualnom nivou, kao i na predloge korekcija loših praksa.

Sekcija 2 je fokusirana na posledice slabih lozinki i potencijalnih postupaka napadača nakon što dobiju pristup nalogu. Metodi razotkrivanja šifara, loše korisničke prakse i mere prevencija su predstavljeni u sekcijama 3 i 4. Dodatni metodi zaštite naloga, njihove prednosti i mane su razrađeni u sekciji 5.

## 2 Uticaj na druge sfere života

Nesigurnost šifara, omogućavanjem lakšeg malicioznog pristupa nalogima, ima brojne štete po žrtvu koje mogu biti društvene prirode (povreda ugleda žrtve, korišćenje njihovog autoriteta na maliciozan način) ili revanšističke (bivši ili ljubomorni romantični partner koji maliciozno pristupa nalogima, napad usled neslaganja na poslu ili u društvenim krugovima).

### 2.1 Privatnost na internetu

Pristup nalogima omogućava zlonamernim akterima da nanese društvenu štetu žrtvi. Neki od mogućih načina su postavljanje neprimernog sadržaja, slanje privatnih poruka tokom kojih primalac ima pogrešnu pretpostavku o tome sa kime komunicira, čitanje i dokumentovanje privatnih poruka.

Slučaj u Njukaslu [11] je ekstremni primer u kojem je ljubomorni muž (student računarstva) neautorizovano pristupio ženinih mejlovima. Nakon otkrića afere kroz mejlove ju je ubio.

### 2.2 Spam

Kompromitovani nalozi su mnogo efikasniji u širenju spam poruka. Sama dinamika širenja tih spam poruka je drugačija od dinamike širenja „tradicionalnih” spam poruka. Ovo je posledica toga što primalac te poruke ima iluziju da je poruka poslata od osobe od poverenja, što povećava šansu da i oni sami dalje prošire taj spam. Potpuna automatizacija pomenutog procesa omogućava veoma agresivnu propagaciju [10]. Ovaj tip spama često širi i maliciozne linkove koji kompromituju naloge, što ih uvodi u svoju „mrežu botova”.

## 2.3 Žene kao mete sajber napada

Žene su češće mete nefinansijski motivisanih sajber napada poput desimenacije osvetničke pornografije, sajber uhođenja i krađe identiteta. Pored toga, procentualno više žena (u poređenju sa muškarcima) se oseća manje sigurno na internetu (35% i 27%, respektivno) i manje pod kontrolom javnih informacija o njima (53% i 47%, respektivno) [5] [6].

### 3 Česti napadi i greške korisnika

Načini otkrivanja šifara su mnogobrojni i mogu se podeliti na napade korišćenjem računara, greške korisnika i društveni inženjering (eng. *social engineering*). Napadi korišćenjem računara podrazumevaju otkrivanje lozinke ponovnim nagađanjem. Metodi za ovu svrhu podrazumevaju neki tip pretrage prostora mogućih lozinki. Loše prakse poput ponovnog korišćenja šifara ili njihovo nesigurno čuvanje čine sigurnosne propuste koji se mogu iskoristiti od strane malicioznih aktera. Slanje lažnih mejlova sa malicioznim linkovima je podrazumevano u *phishing* napade, što je jedan od najzastupljenijih oblika društvenog inženjeringa. Pristupom na te linkove napadač dobija neautoroizovani pristup mejlu i lozinki žrtve.

Za potrebe rada, biće reči samo o prva dva načina napada.

#### 3.1 Napad grubom silom

Jedan od osnovnih napada koji se oslanja na naivno nagađanje šifara kombinovanjem datih karaktera. Glavni adut je jednostavnost implementacije. Ako je dužina šifre nepoznata, započinje se minimalnom dužinom šifre koja se inkrementira nakon iscrpljenja svih kombinacija za tu dužinu, ukoliko nije došlo do pogotka [1].

#### 3.2 Napad rečnikom

Kolekcija reči se koristi za generisanje potencijalnih šifara. Rečnici mogu da budu opšte namene (npr. najčešće reči, imena i prezimena nekog jezika) ili specijalizovani (dodate su prethodno razotkrivene šifre iz skupa šifara koji je napadnut). U rečnike su često dodate sve kombinacije slova, brojeva i specijalnih karaktera do neke predodređene dužine [1].

#### 3.3 Ponovno korišćenje šifara

Česta praksa je ponovno korišćenje šifara zarad lakšeg pamćenja. Ova praksa je loša jer otkrivanje šifre jednog naloga je dovoljno za otkrivanje šifara svih ostalih naloga.

Slično tome, male varijacije šifre za različite naloge se smatraju nesigurnim. Hakeri se vode principom malih izmena šifre koja je kandidat, praćenjem nekih pravila npr. dodavanje broja na kraju, kapitalizacija slova, menjanje slova brojevima (i postaje 1, a postaje 4).

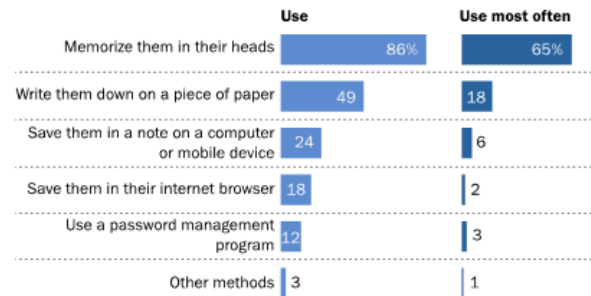
#### 3.4 Ostale loše prakse

Neredovno ažuriranje lozinki i njihovo nesigurno čuvanje su takođe faktori koji utiču na sveukupnu sigurnost lozinki. Nesigurno čuvanje podrazumeva njihovo zapisivanje na lako dostupnim papirima ili u neenkriptovane fajlove. Neažuriranje šifara čini naloge podložne napadima koji koriste prethodna curenja podataka.

Načini čuvanja šifara ne variraju značajno među demografijama, što nagoveštava da nivo tehnološkog obrazovanja nije značajan indikator o korišćenju sigurnijih metoda [3].

### Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for "use most often" category include those who use only one technique to manage their passwords.

Source: Survey conducted March 30-May 3 2016.

"Americans and Cybersecurity"

PEW RESEARCH CENTER

Slika 1: Načini pamćenja šifara građana SAD-a [3]

## 4 Mere prevencije

Povećanje nivoa sigurnosti se ostvaruje korišćenjem raznih mera prevencija. Ove mere su od krajnje važnosti - sanacija štete je previše komplikovana i zahteva veliku količinu vremena. Glavni načini povećanja nivoa su korišćenje jakih lozinki i menadžera lozinki.

### 4.1 Jačina lozinki

Smanjivanje uspešnosti napada grubom silom se dostiže korišćenjem većeg skupa karaktera i dužih reči. Primera radi, postoji 4096000000 mogućih šifara od 6 karaktera i skupom karaktera koji čine mala slova azbuke i cifre od 0 do 9. Korišćenjem extended ASCII karaktera i šifru dužine 15, dobijamo  $1.329228 \times 10^{36}$  mogućih šifara.

Osiguravanje od napada rečnikom se može izvesti na dva načina:

- Izbegavanje korišćenja reči u lozinki. Lozinka bi sadržala veliki broj nasumično generisanih karaktera.
- Veliki broj reči koji formira „frazu lozinke”.

Fraza lozinke je lozinka sačinjena od velikog broja realnih reči. Često se koriste kao jednostavan način generisanja dugačkih šifara koje su korisnicima jednostavne za pamćenje.

## 4.2 Alati

Da bi se pojednostavio proces generisanja jakih nasumičnih lozinki i njihovo sigurno skladištenje, koriste se menadžeri lozinki (eng. *password manager*) poput KeePassXC i Buttercup.

KeePassXC je alat otvorenog koda koji se koristi za enkriptovanje skladištenje i upravljanje korisničkim imenima, šiframa, linkovima i prioleženim fajlovima. Ne postoji ugrađena mogućnost sinhronizacije baze između većeg broja uređaja, ali je korisnicima dozvoljeno i učinjeno jednostavnim da sami urade rešenje po želji [4].

U odnosu na KeePassXC, Buttercup ima moderniji interfejs i ugrađenu podršku za sinhronizaciju baze [2].



(a) KeePassXC logo



(b) Buttercup logo

Slika 2

## 5 Alternative i dodatna zaštita

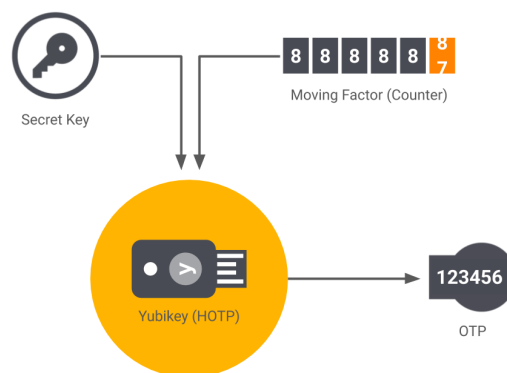
Korišćenje samo šifre često nije dovoljno, te se koriste dodatne mere: 2FA, Yubikey, sigurnosna pitanja, biometrijska autentikacija. Kombinacija ovih mera čini kompromitovanje naloga značajno težim, ali takođe stvara dodatno *trenje* između korisnika i pristupa njihovom nalogu. Pod ovim pojmom podrazumevamo niz koraka i barijera između korisnika i njihovog cilja (u našem slučaju, pristupanju nalogu ili podacima); veliki stepen vidljivih koraka često iritira korisnike, te se oni odlučuju za manje sigurne varijante (primer nevidljive sigurnosti je adaptivna autentikacija o kojoj će biti više reči na kraju poglavlja). Ovo, kao i *trenje* koje nastaje pri korišćenju menadžera lozinki, je razlog za česte loše prakse kod velikog broja korisnika. Trenutni cilj eksperata sajber sigurnosti nije samo podizanje stepena informatičke pismenosti šire javnosti, nego i konstrukcija sigurnih sistema sa minimalnim *trenjem*. Asimetrija informatičke pismenosti između ljudi kojima je

### 5.1 Jednokratne lozinke

Jedan od najčešćih oblika MFA (višeslojna autentikacija, eng. *Multi-Factor Authentication*) je OTP (jednokratne lozinke, eng. *one time passwords*). Korisnici mogu da pristupe jednokratnim lozinkama korišćenjem aplikacija (poput 2FAS ili Aegis Authenticator) ili da im budu dostavljene SMS porukama. Korišćenje aplikacija od poverenja za pristup jednokratnim lozinkama je sigurnije od korišćenja SMS poruka, zbog podložnosti SMS poruka napadima poput man-in-the-middle napadu. Lozinke su generisane korišćenjem konstantnog seed-a i pomerajućeg faktora. Varijante OTP-a se dele po načinu generisanja pomerajućeg faktora:

- HOTP (eng. *Hash-based Message Authentication Code One Time Password*)
- TOTP (eng. *Time-based One-time Password*)

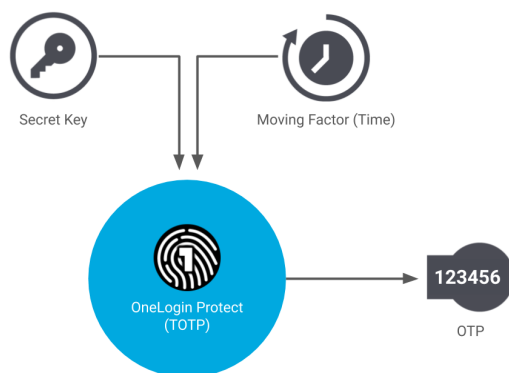
Osnovna ideja iza HOTP je baziranje pomerajućeg faktora na brojaču koji prati broj zahtevanih lozinki.



Slika 3: Shema rada HOTP sistema [8]



Za razliku od ovog pristupa, TOTP koristi vreme zahteva kao pomerajući faktor. Vremenski korak uglavnom iznosi između 30 i 60 sekundi i ukoliko lozinka nije iskorišćena tokom tog vremena ona prestaje da bude validna. U tom slučaju, potrebno je zahtevati novu lozinku [8].



Slika 4: Shema rada TOTP sistema [8]

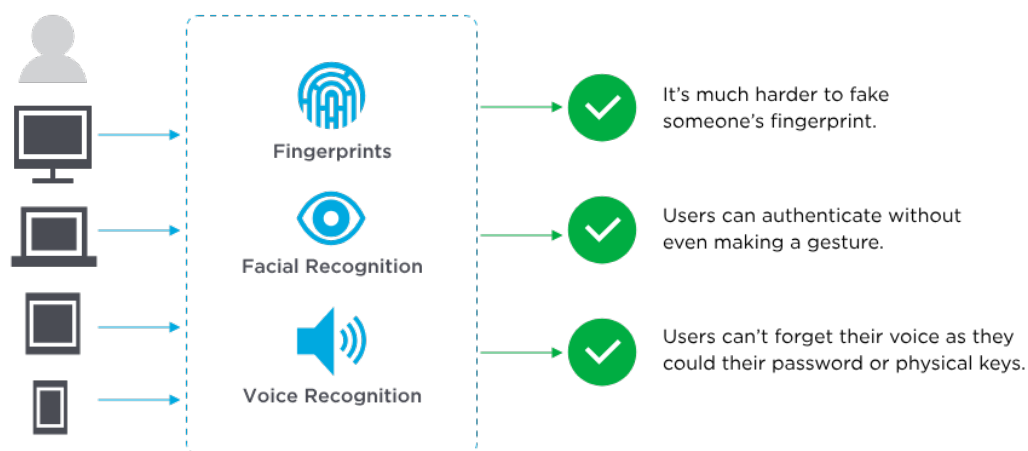
## 5.2 Biometrijska autentikacija

Biometrijska autentikacija podrazumeva metode verifikacije identiteta korišćenjem bioloških karakteristika ili ponašanja korisnika. Aduti ovog metoda su jednostavnost korišćenja, brzina i činjenice da ne zahtevaju dodatni trud od korisnika, budući da korisnik u svakom trenutku ima svoju „lozinku” sa sobom. Lozinka u ovom kontekstu može biti bilo koja od sledećih bioloških karakteristika:

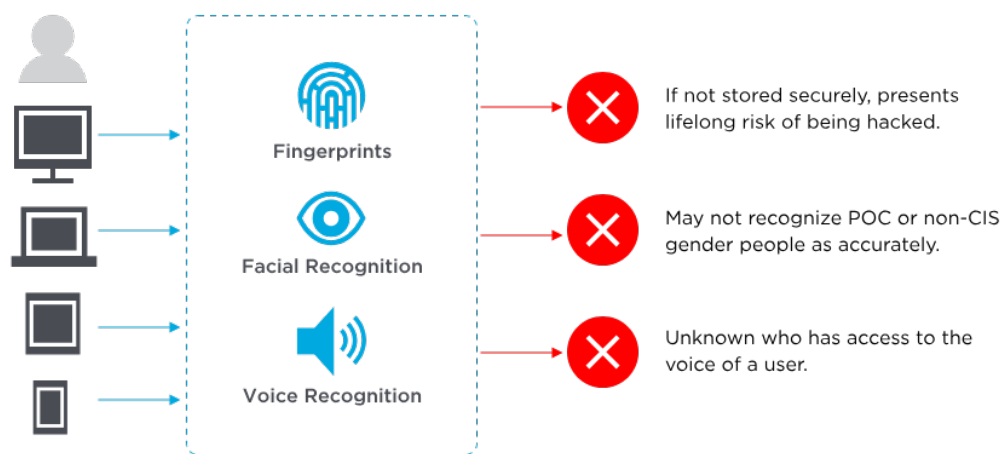
- Sken mrežnjače;
- Sken otiska prsta;
- Sken lica;
- Poklapanje DNK.

Korišćenje biometrijskih metoda autentikacije se ne sme smatrati stopostotno sigurnim, nego samo još jednim delom MFA lanca. Moguće je rekreirati neke od bioloških karakteristika, što potpuno negira prednosti koje ovaj vid zaštite donosi [7]. Pored toga, dodatne mane leže u:

- Nesigurnom čuvanju, što čini trajni rizik (veoma teško je promeniti biološke karakteristike);
- Algoritmi mašinskog učenja korišćeni za autentikaciju često nisu trenirani na dobro konstruisanim skupovima podataka - žene i etničke manjine često nisu adekvatno predstavljene;
- Porast u korišćenju korisnički generisanog audio i video sadržaja za posledicu ima lak pristup liku i glasu velikog broja ljudi. Pristup već postojećem sadržaju ove vrste je sam po sebi dovoljan za kompromitovanje integriteta sistema, a povrhu toga je moguće generisanje lažnih audio i video snimaka putem veštačke inteligencije zarad istog cilja.



Slika 5: Pozitivne strane biometrijske autentikacije [7]

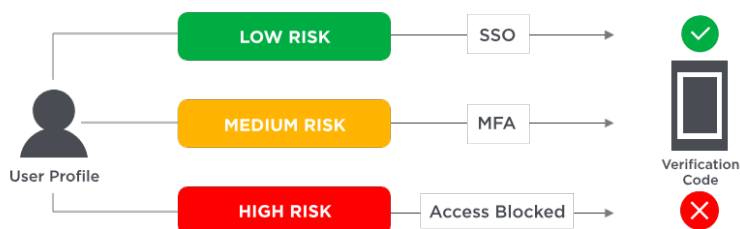


Slika 6: Negativne strane biometrijske autentikacije [7]

### 5.3 Adaptivna autentikacija

Jedan od sofisticiranijih načina koji se koristi zarad olakšavanja pristupa nalogima, dok još uvek očuvava zadovoljavajuć nivo sigurnosti jeste adaptivna autentikacija. Pri prijavljivanju, razni faktori su analizirani (geolokacija, vreme prijavljivanja, korišćeni uređaj...) i poređeni sa ponašanjima koja se smatraju očekivanim za datog korisnika. Ovom

analizom se kvantifikuje „rizik” neovlašćenog pristupanja nalogu, i shodno sa nivoom rizika traži se više slojeva autentifikacije. Primera radi, ako se korisnik prijavljuje iz njihovog doma, sa prethodno korišćenih uređaja tokom vremena kada uglavnom koriste dati nalog, kvantifikovani rizik će imati nisku vrednost i dopustiti prijavu korišćenjem samo korisničkog imena i šifre. Ako se isti taj korisnik prijavljuje korišćenjem novog uređaja sa nove lokacije, biće zatraženi dodatni koraci poput OTP. U slučajevima da je procenjeni rizik prevelik, moguće je potpuno blokiranje prijavljivanja [9].



Slika 7: Shema rada sistema adaptive autentifikacije [9]

## 6 Zaključak

Bez obzira na veliki značaj sigurnosti lozinki, i samim tim naloga, značajan broj ljudi ovu temu olako shvata i drži se ustaljenih loših praksi poput slabih lozinki, manjka MFA, ponovnog korišćenja istih lozinki i njihovog nesigurnog čuvanja. Nivo tehnološkog obrazovanja nije jak indikator boljih sigurnosnih praksi korisnika. Najveći napredak u sigurnosti koji korisnici mogu da naprave je korišćenje menadžera lozinki (npr. KeePassXC) i MFA metoda (poput OTP i biometrijske autentikacije). Fokus eksperata sajber sigurnosti treba biti okrenut ka kreiranju sistema koji su sigurni sa što manje vidljivih koraka, budući da upravo njihova brojnost demotiviše korisnike da biraju sigurnije metode.

## Literatura

- [1] L. Bošnjak. [https://www.researchgate.net/publication/326700354\\_brute-force\\_and\\_dictionary\\_attack\\_on\\_hashed\\_real-world\\_passwords](https://www.researchgate.net/publication/326700354_brute-force_and_dictionary_attack_on_hashed_real-world_passwords).
- [2] Buttercup. <https://buttercup.pw/>.
- [3] Pew Research center. <https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/>.
- [4] KeePassXC. <https://keepassxc.org/>.
- [5] David Klein. <https://www.occrp.org/en/daily/15343-report-minorities-and-women-are-more-likely-victims-of-cyber-crime>.
- [6] Ryan Morris-Reade. <https://itbrief.co.nz/story/women-and-bame-individuals-bear-the-brunt-of-cyber-attacks-malwarebytes-research>.
- [7] onelogin. <https://www.onelogin.com/learn/biometric-authentication>.
- [8] onelogin. <https://www.onelogin.com/learn/otp-totp-hotp>.
- [9] onelogin. <https://www.onelogin.com/learn/what-why-adaptive-authentication>.
- [10] Inderscience Publishers. <https://www.sciencedaily.com/releases/2014/11/141126111211.htm>.
- [11] DailyMail UK. <https://www.dailymail.co.uk/news/article-394976/life-sentence-jealous-husband-hacked-wifes-emails-killed-her.html>.