Kurs: Računarstvo i društvo

Bezbednost naših lozinki

Autor: Aleksa Jovanović

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

Datum: 18. maj 2024.

Sadržaj

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. 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 stoga glavno 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

2.1 Privatnost na internetu

Pristup nalozima omogućava zlonamernim akterima da nanesu društvenu štetu žrtvi. Neki od mogućih načina su postavljanje neprimernog sadržaja, obmanljivo slanje privatnih poruka, čitanje i dokumentovanje privatnih poruka.

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 (35% i 27%, respektivno) i manje privatno (53% i 47%, respektivno). [5] [6]

3 Česti napadi i greške korisnika

3.1 Napad grubom silom

Jedan od najosnovnijih 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, ako 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]

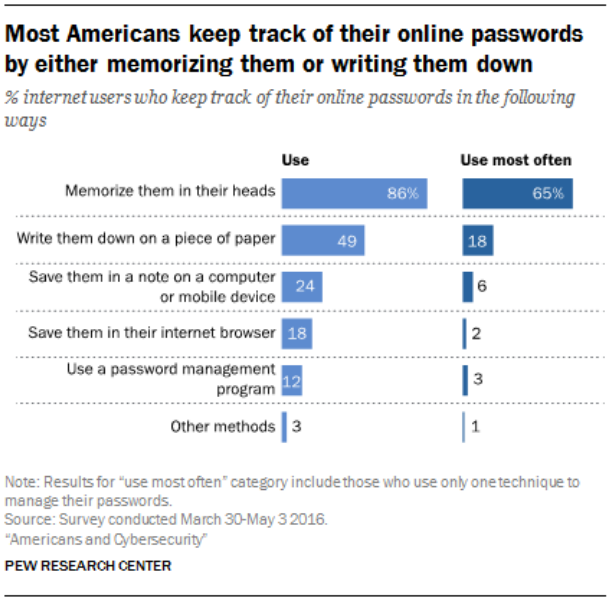
3.3 Ponovno korišćenje šifara

Česta (loša) praksa je ponovno korišćenje šifara zarad lakšeg pamćenja. Otkrivanje šifre jednog naloga je dovoljno za otkrivanje šifara svih ostalih naloga. Slično tome, male varijacije šifre za različite naloge se smatraju nesigurnim.

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 dostupinim papirima ili u neenkriptovane fajlove. Neuažuriranje 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]



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

4 Mere prevencije

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 1.329228e+36 mogućih šifara.

Osiguravanje od napada rečnikom se može izvesti na dva načina:

- Izbegavanje korišćenja reči u lozinci. Lozinka bi sadržala veliki broj nasumično generisanih karaktera.
- Veliki broj reči koji formira "frazu lozinke".

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 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

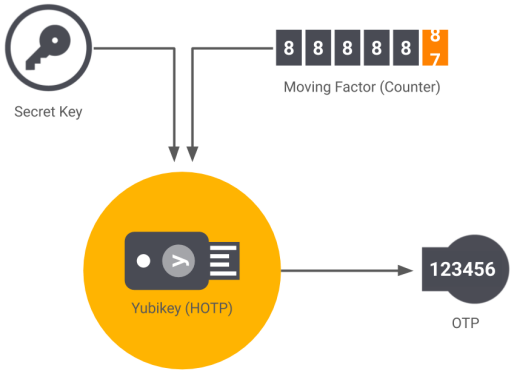
Korišćenje samo šifre često nije dovoljno, te se koriste dotatne mere: 2FA, Yubikey, sigurnosna pitanja, biometrijska autentikacija. Kombinacija ovih mera čini kompromitovanje naloga značajno težim, ali takođe stvara dodatno trenje između korisnika i pristupa njihovom nalogu. Ovo trenje, kao i trenje koje nastaje pri korišćenju menadžera lozinki, je razlog za česte loše prakse kod velikog broja korisnika. Trenutni cilj eksperata sajber sigurnosti nije samo edukacija što šire publike, nego i konstrukcija sigurnih sistema sa minimalnim trenjem.

5.1 Jednokratne lozinke

Jedan od najčešćih oblika MFA 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. Lozinke su generisanje korišćenjem konstantog seed-a i pomerajućeg faktora. [8] Varijante OTP-a se dele po načinu generisanja pomerajućeg faktora:

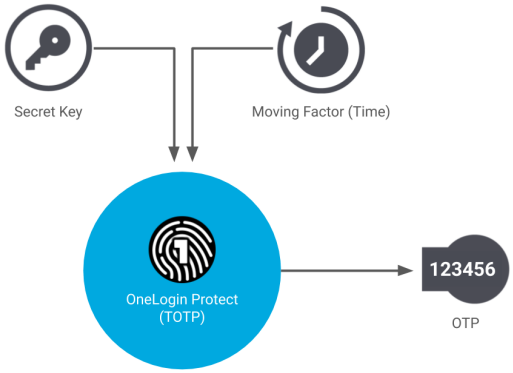
- HOTP (eng. *Hash-based Message Authentication Code One Time Password*)
- TOTP (eng. *Time-based One-time Password*)

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 ako lozinka nije iskorišćena tokom tog vremena ona prestaje da bude validna. U tom slučaju, potrebno je zahtevati novu lozinku.



Slika 4: Shema rada TOTP sistema. [8]

Korišćenje aplikacija od poverenja za pristup jednokratnim lozinkama je sigurnije od korišćenje SMS poruka, zbog podložnosti SMS poruka napadima poput man-in-the-middle napadu.

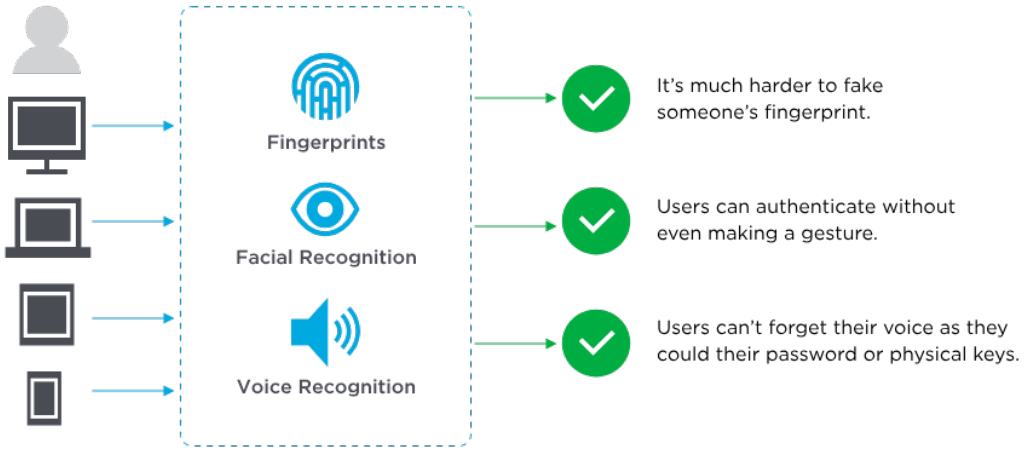
5.2 Biometrijska autentikacija

Način verifikacije identiteta korišćenjem bioloških karakteristika ili ponašanja korisnika. Biološke karakteristike korišćene za verifikaciju su:

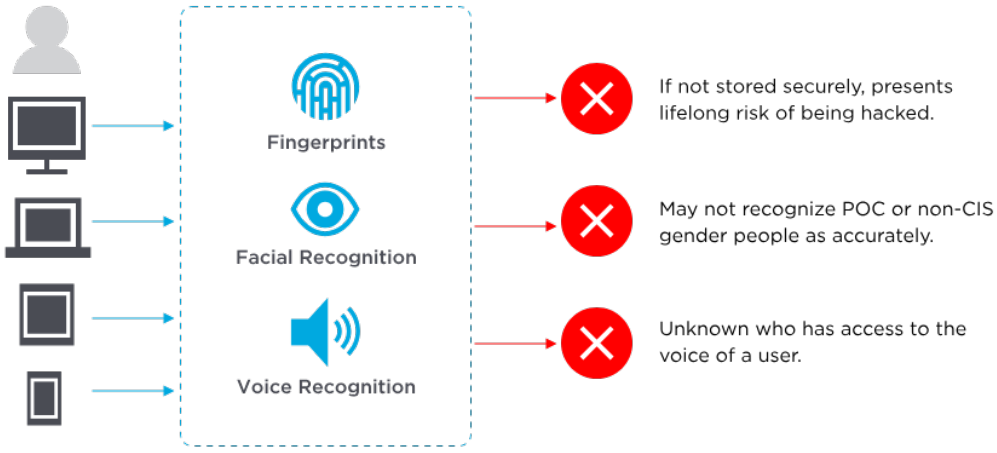
- Sken mrežnjače
- Sken otiska prsta
- Sken lica
- Poklapanje DNK

Ponašanje korisnika uključuje navike korišćenja miša, tastature ili tač-skrina, koje su analizirane i poređene sa standardnim navikama.

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]



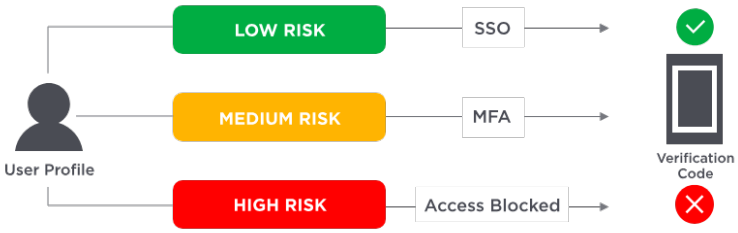
Slika 5: Pozitivne strane biometrijske autentikacije. [7]



Slika 6: Negativne strane biometrijske autentikacije. [7]

5.3 Adaptivna autentikacija

Jedan od sofisticiranijih načina koji se koristi zarad olakšavanja pristupa nalozima, dok još uvek očuvava zadovoljavajuć nivo sigurnosti. Pri prijavljivanju, razni faktori su analizirani (geolokacija, vreme prijavljivanja, korišćeni uređaj...) i poređeni sa uobičajenim ponašanjima asociranim sa korisnikom. Ovom analizom se kvantifikuje "rizik" neovlašćenog pristupanja nalogu, i shodno sa nivoom rizika traži se više slojeva autentikacije. 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 prijvaljivanja. [9]



Slika 7: Shema rada sistema adaptive autentikacije. [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 trenja sa korisničke strane, jer je to trenje glavni razlog manje sigurnosti.

Literatura

[1] L. Bošnjak. 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.