Kurs: Računarstvo i društvo

Bezbednost naših lozinki

Autor: Aleksa Jovanović

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

Datum: 17. maj 2024.

Sadržaj

1 Uvod **2**

2 Uticaj na druge sfere života **2**
2.1 Privatnost na internetu 2
2.2 Spam 2
2.3 Žene 2

3 Česti napadi i greške korisnika **3**
3.1 Napad grubom silom 3
3.2 Napad rečnikom 3
3.3 Ponovno korišćenje šifara 3
3.4 Ostale loše prakse 3

4 Mere prevencije **3**
4.1 Jačina lozinki 3
4.2 Alati 4

5 Alternative i dodatna zaštita **4**

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. 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. [4] Ovaj tip spama često širi i maliciozne linkove koji kompromituju naloge, što ih uvodi u svoju "mrežu botova".

2.3 Žene

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). [2] [3]

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.

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.

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 ciljevi eksperata sajber sigurnosti nije samo edukacija što šire publike, nego i konstrukcija sigurnih sistema sa minimalnim trenjem.

Literatura

[1] L. Bošnjak. https://www.researchgate.net/publication/326700354_brute-force_and_dictionary_attack_on_hashed_real-world_passwords.

[2] David Klein. https://www.occrp.org/en/daily/15343-report-minorities-and-women-are-more-likely-victims-of-cyber-crime.

[3] Ryan Morris-Reade. https://itbrief.co.nz/story/women-and-bame-individuals-bear-the-brunt-of-cyber-attacks-malwarebytes-research.

[4] Inderscience Publishers. https://www.sciencedaily.com/releases/2014/11/141126111211.htm.