

Sigurnost lozinki

Sažetak

Tijekom nekoliko posljednjih desetljeća sve veći broj ljudi stavljen je pred ranije nepoznate probleme generiranja i memoriranja više desetaka lozinki za pristup rastućem broju računalnih usluga, pri čemu se od njih traži neprestano povećavanje kompleksnosti lozinki ili njihovo često mijenjanje. Primjena novijih autentifikacijskih tehnologija poput mobilnih tokena ili nekih drugih načina dvostruke provjere, primjerice Google 2-Step Verification, još uvijek je ograničena na mali broj dostupnih usluga, dok je za preostalu većinu usluga korisničko ime i lozinka jedino što dijeli pojedinca od sigurnosti njegovih privatnih podataka ili dozvola za rad na nekom sustavu. Vidljivo je da i dalje postoji potreba za lozinkama, a ne postoji univerzalno rješenje za upravljanje njima. Cilj ovog rada je pregled nekoliko načina kreiranja i čuvanja lozinki, pregled sigurnosti tako kreiranih lozinki i općenito podizanje svijesti korisnika o važnosti lozinki i opasnostima od provala u računalne sustave.

1. Uvod

Lozinke kao nizovi znakova kojima se dokazuju identiteti pojedinaca i stječu određene privilegije ili prava pristupa određenim resursima poznate su još od antičkih vremena. Grčki povjesničar Polybius spominje praksu uporabe lozinki prilikom smjene straže u rimskoj vojsci[1]. Primjena lozinki kroz povijest uglavnom je bila povezana s vojnim svrhama i ograničena na užu krug ljudi. Pojavom računala lozinke su već od njegovih prvih inačica postale glavni način kojim pojedinac stječe dozvole za pristup i obavljanje određenih radnji na računalu.

2. Princip rada lozinkom zaštićenih sustava i usluga

Već su prvi računalni sustavi bili višekorisnički i imali ugrađenu autentifikaciju putem korisničkog imena i lozinke. Uobičajeni princip zaštite zasniva se na tri koraka. Prvi korak – identifikacija – korisnik se sustavu predstavlja svojim korisničkim imenom i lozinkom. Zatim slijedi drugi korak – autentifikacija – podaci koje je korisnik unio uspoređuju se s korisničkim imenom i lozinkom pohranjenima u sustavu, bilo u datoteci ili bazi podataka. U trećem koraku – autorizaciji – određuju se prava korisnika na sustavu.

2.1 Pohrana korisničkih imena i lozinki

Još 60-tih godina znanstvenici su shvatili da pohrana lozinki u tekstualnom obliku predstavlja sigurnosni problem uslijed opasnosti da se, zbog greške na sustavu, potencijalnog napadača ili nesavjesnog administratora sustava, kompromitiraju zaštićeni podaci [2]. Nakon

eksperimentiranja s različitim vrstama šifriranja lozinki trenutno je u uporabi tehnika kriptografskih hash funkcija. Primjenom hash funkcije dobije se niz znakova fiksne dužine (hash vrijednost) koji se pohranjuju u datoteci ili bazi podataka. Osnovne značajke idealne hash funkcije za pohranu lozinki bile bi: jednostavni izračun hash vrijednosti, nemogućnost izračuna lozinke iz poznate hash vrijednosti u realnom vremenu, te nepostojanje dvije različite lozinke koje imaju istu hash vrijednost. Iz sljedećeg primjera je vidljivo da i najmanja promjena lozinke uzrokuje veliku promjenu hash vrijednosti [3].

```
SHA256("The quick brown fox jumps over the lazy dog")
0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592
SHA256("The quick brown fox jumps over the lazy dog.")
0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c
```

Svaki put kada korisnik unese lozinku za prijavu na sustav ona prolazi isti postupak kao i kod prvog generiranja hash vrijednosti. Ukoliko je tako dobivena vrijednost ista kao ona pohranjena na sustavu korisnik je autentificiran.

U svrhu izbjegavanja primjene raznih metoda *Lookup* i *Rainbow* tablica korištenih pri napadima na hash vrijednosti sve novije hash funkcije koriste i dodatni jedinstveni *salt*. Salt je niz karaktera koji sustav automatski dodaje korisnikovoj lozinki, a pohranjuje se nešifriran. Služi da bi se onemogućila izrada popisa gotovih hash vrijednosti koje bi onda vrijedile na svakom sustavu i znatno ubrzale probijanje lozinki.

Za razliku od lozinki, korisničko ime se na sustavima uobičajeno pohranjuje u tekstualnom formatu i uglavnom predstavlja javno dostupnu informaciju.

2.2 Pronalaženje lozinki iz poznate hash vrijednosti

Kada bi se potencijalni napadač domogao hash vrijednosti lozinke generirane pomoću algoritma koji nema poznatih slabosti, jedino što bi mu preostalo za otkrivanje lozinke je *brute force* napad - generiranje jednog po jednog niza znakova i ispitivanje da li hash vrijednost pojedinog niza odgovara izvornoj. Ovisno o dužini lozinke, a uz pogađanje svih mogućih kombinacija sastavljenih od velikih i malih slova, brojeva i posebnih znakova, takva aktivnost bi mogla potrajati duži niz godina. Primjerice, uz pretpostavku korištenja svih navedenih 95 ASCII znakova, lozinka dužine 8 znakova imala bi 6.63×10^{15} kombinacija. Prosječno kućno računalo danas je u stanju ispitati 2×10^7 kombinacija u sekundi, što znači da bi za pogađanje lozinke trebalo otprilike 11 godina [5]. Pojavom grafičkih procesora (GPU) hardverski optimiziranih za paralelno računanje pojavljuju se klasteri namijenjeni probijanju

lozinki koji mogu ispitati po 35×10^{10} kombinacija lozinki u sekundi [6]. Takvom računalu je za probijanje lozinke od 8 znakova potrebno maksimalno 6 sati. Pri tome treba imati na umu da je prosječno vrijeme probijanja lozinke upola manje od maksimalnog.

2.3 Nesavršenost kriptografskih funkcija

Razvoj kriptografskih algoritama i neprestani rast procesorske snage računala s vremenom dovode do otkrivanja slabosti pojedinih metoda šifriranja. Prve kriptografske hash funkcije razvijene su krajem osamdesetih godina prošlog stoljeća [4]. Trebalo je nešto manje od deset godina da se dokaže nesavršenost (ranjivost) MD2 algoritma osmišljenog 1989. godine. Prve slabosti MD5 algoritma iz 1991. godine otkrivene su već 1996. godine, ali se unatoč nizu otkrivenih ranjivosti zadržao u službenoj uporabi sve do prije nekoliko godina.

Hash funkcija se smatra probijenom kada se u praksi može realizirati algoritam kojim se u ograničenom realnom vremenu mogu konstruirati kolizije – dvije različite poruke koje imaju istu hash vrijednost. Nakon toga lozinke zaštićene probijenim algoritmom više nije potrebno unedogled pogađati nego se, bez obzira na njenu dužinu, može izračunati zamjenska lozinka čija hash vrijednost odgovara izvornoj. Godine 2008., uz pomoć više od 200 Sony Playstation računala, grupa znanstvenika je uspješno probila MD5 algoritam te generirala lažni CA certifikat za SSL protokol koji im je omogućavao da se proizvoljno predstave kao bilo koje internetsko sjedište [7].

Trenutno aktualna inačica hash algoritma koji se preporuča kao siguran za uporabu je SHA-2 (inačica SHA-256 i veća) [8]. Primjena SHA-256 hash funkcije rezultira izlaznim nizom od 256 bitova odnosno 2^{256} mogućih kombinacija hash vrijednosti. Usporedbe radi, pretpostavka je da na zemlji postoji 2^{62} zrnaca pijeska [9] ili da u vidljivom svemiru postoji otprilike 2^{77} zvijezda.

3. Provale u računalne sustave

Kako bi se objasnila važnost pravilnog izbora i čuvanja lozinki potrebno je izložiti zašto lozinka pojedinca može postati objekt napada. U ovom poglavlju navedeni su neki od razloga zašto dolazi do pokušaja probijanja lozinki, te nekoliko vrsta napada kojima se napadači mogu služiti u ostvarenju svog cilja.

3.1 Razlozi provala

Populacija pojedinaca koji se bave pokušajima provala lozinki može se podijeliti na tri

kategorije:

- ◆ White hat – etički hakeri, pojedinci koji istražuju sigurnosne propuste u računalnim sustavima, uobičajeno ugovorno vezani s klijentom u čije sustave pokušavaju provaliti;
- ◆ Grey hat – pojedinci koji provaljuju u sustave tražeći sigurnosne propuste, koristeći se ponekad nezakonitim sredstvima, a da pri tome najčešće nemaju zlu namjeru;
- ◆ Black hat – maliciozni pojedinci koji provaljuju zbog direktne materijalne ili neke druge koristi.

Razlozi njihovog djelovanja uvjetovani su uobičajenim ljudskim nagonima koje nije moguće kategorizirati u nekoliko paragrafa, ali neke od češćih odgovora na pitanje "Zašto?" mogu se razvrstati u sljedeće skupine:

- ◆ Zato što mogu. Osobni izazov i pronalaženje zadovoljstva u svladavanju kompliciranih prepreka neki su od češćih razloga zbog kojih pojedinci započinju s takvim aktivnostima.
- ◆ Nesmotrene i zlonamjerne podvale ili osvete. U ovu kategoriju mogu se smjestiti pojedinci koji uživaju u javnom sramoćenju drugih osoba ili izazivanju panike. Širenjem uporabe društvenih mreža sve više osjetljivih i za osobu potencijalno neugodnih digitalnih sadržaja postaje dostupno putem interneta.
- ◆ Haktivizam. Način izražavanja političkog mišljenja napadima na računalne sustave. Najčešće posljedice ovakvih napada su mijenjanje izgleda napadnute web stranice ili objava privatnih i tajnih komunikacija državnih agencija ili poznatih osoba iz raznih međunarodnih tvrtki.
- ◆ Materijalna dobit.
 - Krađa intelektualnog vlasništva
 - Provale bankovnih računa korisnika, krađa informacija o kreditnoj kartici, krađa identiteta, ucjena, ...
 - Iskorištavanje korisnikovog računa za širenje neželjene elektroničke pošte (spam), preusmjerenje prometa radi zarade od reklama (adware), pretvaranje korisnikovog računala u dio botneta, ...

3.2 Vrste i ciljevi napada

Ponašanje napadača i vrsta napada koja se koristi pri pokušaju provale u praksi ovisi o tome da li je cilj napada konkretan pojedinac, grupa pojedinaca ili je napadaču u interesu provaliti na što više korisničkih računa. Različite tehnologije računalnih sustava skrivaju

brojne nesavršenosti i napadaču je dostupan širok spektar načina na koji može ostvariti svoj cilj. Napadi poput krađa sesije ili iskorištavanja neke ranjivosti usluge koja napadaču daje direktnu kontrolu nad korisničkim računom ne ovise o izboru i dužini lozinke, a korisnik ne može utjecati na njih. Za ovaj rad zanimljivi su oni napadi koji iskorištavaju loše lozinke te nemarno ponašanje korisnika pri izboru, čuvanju i korištenju lozinki.

Većina današnjih društvenih mreža i ostalih web servisa koristi zaštite koje onemogućavaju višestruke pokušaj pogađanja lozinke. Neki servisi već nakon dva-tri neuspjela pokušaja prijave na sustav zaključavaju korisnički račun ili pri neuspjelom spajanju obavještavaju korisnika elektroničkom poštom.

Moguće akcije napadač će, u slučaju napada na korisnički račun određenog pojedinca na društvenoj mreži, prilagoditi vrsti zaštite koju ta mreža koristi. Raznim metodama socijalnog inženjeringa napadač može pokušati navesti žrtvu da mu oda lozinku. Jedna od najpoznatijih metoda je ciljani *phishing*. Napadač kreira do detalja istovjetnu kopiju izvornog web sjedišta i šalje elektroničku poštu lažno se predstavljajući, primjerice kao žrtvin poznanik. U pošti je hiperveza na lažno web sjedište namijenjeno krađi lozinke. Pri tome napadač primjenjuje razne metode lažiranja i skrivanja stvarne URL adrese. Ukoliko neoprezna žrtva ne primijeti da je riječ o prijevari, pokušajem prijave na lažno web sjedište svoje će korisničke podatke predati napadaču. Zato uvijek treba obratiti pažnju na URL koji se poziva pri učitavanju hiperveze iz elektroničke pošte.

Najčešća u nizu pogrešaka koje korisnici uobičajeno čine je korištenje iste lozinke za više web sjedišta. Tako napadač može istražiti koje druge internetske usluge žrtva koristi i svoj napad usmjeriti prema nekima od tih usluga za koje zaključi da imaju daleko nižu razinu sigurnosti od ciljanog web sjedišta. Primjerice neki od servisa na kojima se žrtva prijavljuje ne koriste SSL pa je moguće presresti mrežni promet i otkriti lozinku. Takva web sjedišta treba izbjegavati ili imati zasebnu lozinku za njih. Ukoliko neka od usluga nema implementirane metode zaključavanja korisničkog računa napadač može pokušati online brute force napad. Pri tome će u postupku izviđanja napadač pokušati doći do raznih javno dostupnih informacija o žrtvi, primjerice imenima oca, majke, djece, psa, itd. Nedavno je Google sastavio listu deset najgorih ideja za lozinke [10]: 1. Imena kućnih ljubimaca; 2. Važni datumi (rođenje, vjenčanje); 3. Datum rođenja člana obitelji; 4. Ime djeteta; 5. Ime člana obitelji; 6. Mjesto rođenja; 7. Najdraži praznik; 8. Nešto vezano za najdraži tim; 9. Ime momka/djevojke; 10. Riječ "password".

Jedna od opasnijih vrsta napada je podmetanje keylogger programa na žrtvino računalo. Takav program evidentira sve što se unese na tipkovnici. Moguća zaštita je korištenje nekog

od programa za upravljanje lozinkama (*password manager*) koji imaju implementiranu zaštitu pri unosu podataka u web sučelje. Također je važno izbjegavati unos lozinki pri korištenju nepoznatih računala, internetskih kioska i sl.

Ukoliko napadač ne cilja pojedinca već sve korisnike usluge može primijeniti slične metode napada. Primjerice, phishing bi u tom slučaju mogao izgledati malo drugačije - napadač se predstavlja kao autoritativna osoba (IT administrator) i šalje elektroničku poštu s naputkom da mu se pošalje lozinka kako bi spasio korisnikove podatke. Čak i u slučaju kad bi se radilo o legitimnom administratoru, korisnik nikad ne smije davati lozinku jer je ona administratoru nepotrebna da bi obavio neki zahvat na sustavu.

Važnost dobre lozinke može se vidjeti na primjeru napada koji se može izvesti i na web sjedištima koji imaju politiku zaključavanja računa. Ukoliko napadač dođe do popisa korisničkih imena može pokušati napad korištenjem jedne lozinke za sve račune. Liste najčešće korištenih lozinki su javno dostupne te je dovoljno da napadač izabere jednu ili dvije i na uzorku od nekoliko tisuća računa vjerojatno će pogoditi nekoliko njih.

3.3 Siguran prijenos lozinki

Kako je već spomenuto u ranijem tekstu, korisnik uvijek mora biti na oprezu kojim komunikacijskim protokolom pristupa pojedinoj usluzi. Kod pristupa web uslugama potrebno je obratiti pozornost da li je između poslužitelja usluge i web preglednika uspostavljena sigurna komunikacija putem SSL/TLS protokola. Korisnik o uspostavi sigurne veze uobičajeno biva obaviješten sličicom lokota ili promjenom boje prostora za unos web adrese, a početak URL-a se mijenja iz http u https. Ovaj protokol ima višestruku funkciju, pa se tako, osim same uspostave sigurne šifrirane veze, korisniku kroz digitalni lanac povjerenja pruža garancija da je zaista pristupio pravom poslužitelju. Ukoliko poslužitelj koristi neispravan certifikat, web preglednik će o tome obavijestiti korisnika. Takvom poslužitelju se pristupa samo ako je korisnik potpuno siguran da zna o čemu se radi.

3.4 Razbijanje lozinki

Ukoliko web sjedište ima primijenjene metode zaključavanja računa to ne isključuje potrebu za dobrom lozinkom. Često se događa da napadači iskoriste sigurnosni propust na sustavu i dođu do popisa šifriranih korisničkih lozinki. U tom trenutku postaje važno samo dvije stvari: snaga lozinke i metoda kojom su šifrirane. Ukoliko pretpostavimo da su šifrirane kvalitetnim algoritmom napadaču, uz *brute force* metodu, ostaje primjena više kriptografskih tehnika koje dodatno olakšavaju probijanje lozinki. Neke od njih su:

- ◆ Napad rječnikom: rječnici koji se koriste imaju popis i do milijardu riječi, skraćenica,

riječi sa zamijenjenim znakovima, najčešće korištenih lozinki, ...

- ◆ Razna pravila koja omogućavaju spajanje riječi iz liste, uobičajenu zamjenu znakova (poput "e" s "3" ili "i" s "1"), dodavanje brojeva na kraju riječi, ...
- ◆ Uporaba vjerojatnosti pojavljivanja znaka korištenjem Markovljevog lanca
- ◆ Tehnika maskiranja omogućava napadaču da brže isproba kombinacije uz pretpostavku da se u lozinki nalaze određeni znakovi ili da pozna dio lozinke.

Primjerice, pri pogađanju lozinki napadač može krenuti od činjenice da otprilike trećina korisnika ima lozinku dužine točno osam znakova. Vjerojatan razlog tome je što se navedena dužina dugi niz godina spominje kao preporučena ili kao minimalna dužina koju web sjedišta uopće prihvaćaju pri postavljanju.

4. Izbor lozinki

Pri izboru lozinki postoji pravilo koje kaže da je jednostavnu lozinku lako zapamtiti, ali i lako probiti. Naravno, vrijedi i obrat – kompleksnu lozinku je teško probiti, ali ju je teško i memorirati.

4.1 Definicija dobre lozinke

Dobra lozinka je ona koju je teško probiti *brute force* napadom ili nekom drugom metodom pogađanja. Ona se sastoji od slučajno izabranih znakova iz svih skupova – velika i mala slova, brojevi, specijalni znakovi – ukupno 95 ASCII znakova. Dijakritičke znakove je, nažalost, zgodno izbjegavati iz nekoliko razloga, a pogotovo ukoliko se korisnik na uslugu spaja s različitih uređaja koji možda nemaju hrvatsku tipkovnicu.

Snaga lozinke mjeri se entropijom – ekvivalent slučajno izabranom nizu bitova – čija vrijednost u potenciji broja dva predstavlja broj pokušaja potrebnih za uspješno pogađanje lozinke. Potpuno slučajni niz od osam znakova iz skupa 26 malih slova ima entropiju od otprilike 38 bitova i njegovo pogađanje iziskuje 2^{38} pokušaja. Međutim, ukoliko je ukupan broj stvarnih riječi od osam znakova u engleskom jeziku 32000 (otprilike 2^{15}), tada se može smatrati da je entropija jedne stvarne engleske riječi od osam znakova samo 15 bitova.

Primjer veze entropije i snage lozinke uporabom KeePass programa v. 2.19 [11]:

Bitovi	Primjer 1 (bitovi)	Primjer 2 (bitovi)	Snaga
0-64	abcdefghijkl (19)	A1b2C3d4E5 (44)	Vrlo slaba
64-80	IDontKnow2244 (69)	Moja!Lozinka2 (79)	Slaba
80-112	UmjerenalOzinka? (90)	o6DHjGUZUCjc'n#x*8 (105)	Umjerena
112-128	o@w"6VP/CyrmRKohA9W9 (114)	nWf/r1Llt6TWGPJXfl&kH (127)	Jaka

Bitovi	Primjer 1 (bitovi)	Primjer 2 (bitovi)	Snaga
≥ 128	[vA)>3<%&>v\ZKA9AE"}zY (129)	=m'9c-3PVz;<\$.sxak*^Km> (142)	Vrlo jaka

Primjeri poput *Moja!Lozinka2* i *UmjerenalOzinka?* bez obzira na svoju dužinu u stvari pripadaju slabijoj grupi lozinki jer se primjenom hrvatskog rječnika njihova entropija dodatno smanjuje.

4.2 Kreiranje dobre lozinke

Poznato je da ljudi lakše pamte nizove znakova ako ih mogu povezati nekim obrascima, ali upravo korištenje obrazaca pri kreiranju lozinki je ono što ih čini slabijima. Osim navedenoga, jedna od glavnih prepreka za kreiranje dobre lozinke je njena dužina. Korisnici često doživljavaju napornim unos lozinke dužine dvadeset znakova pogotovo jer ih ne vide pri unosu.

Neke od metoda kreiranja lozinke koje preporučuju stručnjaci su:

- ◆ Schneier metoda [12] – Zapamtite neku rečenicu i pretvorite je u lozinku. Primjer: "This little piggy went to market" postaje "tlpWENT2m"
- ◆ GRC Haystack metoda [13] – Dužina lozinke je bitna. Primjer: Dug0>>>>>>-----
- ◆ XKCD metoda [14] – Izaberite nekoliko nasumičnih riječi. Primjer: mikser kabanica traktor poruka vrabac
- ◆ Dobro bi bilo koristiti neku kombinaciju navedenih primjera

5. Zaključak

Iako zbog razvoja kriptografskih metoda i brzih računala postoji opasnost da zaštita podataka lozinkama postane zastarjela, ona još uvijek predstavlja dovoljnu obranu od napada na privatne podatke. Dok se ne uvedu i ne usavrše nove metode zaštite koje uključuju dodatni korak pri autentifikaciji, korisnici bi trebali ozbiljnije shvatiti opasnosti od probijanja lozinki i time unaprijediti sigurnost računalnih sustava. Danas, više nego ikad, treba navesti da je lozinka dužine osam znakova slaba lozinka te da se u ljudskim umovima uvriježi veći broj, primjerice minimalno dvanaest ili četrnaest znakova. Razni *password manager* programi, bilo komercijalni ili otvorenog koda, mogu znatno doprinijeti sigurnosti lozinki uz bitnu napomenu da, u slučaju njihove uporabe, korisnik svoju sigurnost povjerava autoru programa.

6. Literatura

1. *The History of Polybius The Megalopolitan, Vol 2,3*, Printed for Samuel Briscoe,

1698.

2. Morris R., Thompson K. *Password Security: A Case History*, Bell Laboratories, 1978
3. *SHA-2 [online]*, Wikipedija, [citirano 29.05.2014.],
<<http://en.wikipedia.org/wiki/SHA-2>>
4. *Frequently Asked Questions about Today's Cryptography*, RSA Laboratories, verzija 4.1- svibanj 2000
5. *John the Ripper benchmarks [online]*, Openwall, [citirano 29.5.2014.],
<<http://openwall.info/wiki/john/benchmarks>>
6. *25-GPU cluster cracks every standard Windows password in <6 hours [online]*, Arstechnica, [citirano 29.05.2014.], <<http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/>>
7. *MD5 considered harmful today [online]*, grupa autora, [citirano 29.05.2014.],
<<http://www.win.tue.nl/hashclash/rogue-ca/>>
8. *NIST's Policy on Hash Functions [online]*, NIST, [citirano 29.05.2014.],
<<http://csrc.nist.gov/groups/ST/hash/policy.html>>
9. Grains of sand on the World's beaches [online], University of Hawaii, [citirano 29.08.2014.], <<http://www.hawaii.edu/suremath/jsand.html>>
10. *Google Reveals the 10 Worst Password Ideas [online]*, Time, [citirano 29.05.2014.],
<<http://techland.time.com/2013/08/08/google-reveals-the-10-worst-password-ideas/>>
11. KeePass Password Safe [online], KeePass, [citirano 29.05.2014.],
<<http://keepass.info/>>
12. Choosing Secure Passwords [online], B. Schneier, [citirano 29.05.2014.],
<https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html>
13. How big is your haystack? [online], GRC, [citirano 29.05.2014.],
<<https://www.grc.com/haystack.htm>>
14. Password strength [online], XKCD, [citirano 29.05.2014.],
<<http://www.xkcd.com/936/>>