CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje lozinkama

NCERT-PUBDOC-2009-11-283

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Lozinka predstavlja tajni niz znakova koji korisnicima omogućuje pristup datotekama, programima ili računalima. Ujedno, onemogućuje pristup neovlaštenim osobama.

U idealnom slučaju lozinka treba biti nešto što nitko neće moći otkriti. Praksa je ipak pokazala kako ljudi vrlo često izabiru jednostavne lozinke (kao npr. njihove inicijale) kako bi ih što lakše zapamtili. To je jedan od osnovnih razloga zašto napadači jednostavnim metodama izvode napade na pojedinačne korisnike, ali i na veće tvrtke ili organizacije.

Odabir tzv. jake lozinke je kritična komponenta za osobnu sigurnost jer zahtijeva od napadača dodatne napore za njeno otkrivanje. Slaba lozinka, osim što stvara lažan osjećaj sigurnosti, olakšava posao potencijalnim zlonamjernim korisnicima. Njenim otkrivanjem napadač može otkriti različite osobne podatke i dobiti pristup resursima na računalu. Situacija je posebice opasna ukoliko napadač na taj način može saznati tajne podatke organizacija i tvrtki u kojima su korisnici zaposleni.

U ovom su dokumentu opisana osnovna obilježja lozinki, metode kako ih ojačati i alati za upravljanje njima. Osim toga, u svrhu zaštite i sigurnosti podataka, dan je i pregled najčešćih vrsta napada na lozinke kako bi se korisnike upozorilo na potencijalne opasnosti, ali i načine njihova rješavanja.

2. Što je lozinka?

Lozinka ili zaporka je oblik tajnog podatka kojeg je potrebno znati kako bi se moglo pristupiti određenim resursima. Drugim riječima, lozinka se koristi za autentikaciju i dokazivanje identiteta korisnika koji žele pristupiti određenim informacijama na nekom sustavu.

Njihova upotreba bila je uobičajena još u davnoj prošlosti kada su pojedini stanovnici Mezopotamije koristili posebne znakove za zaštitu teksta. U tu su svrhu koristili pismo koje se zasnivalo na principu zamjene slova abecede (npr. slovo A je zapisivano kao Z).

I od samih početaka računarstva, vodilo se računa o identifikaciji korisnika. 1961. godine na MIT-u (eng. *Massachusetts Institute of Technology*) je razvijen CTSS sustav koji je od korisnika zahtijevao upis pristupne lozinke. CTSS (eng. *Compatible Time-Sharing System*) se koristio za nadzor nad I/O konzolom, rasporedom redoslijeda poslova (sistemskih i korisničkih), privremenom memorijom, diskom te je imao izravnu mogućnost upravljanja pozivima prekida (eng. *interrupt*).

U današnje je vrijeme također uobičajena upotreba korisničkog imena i lozinke prilikom prijave na računalo, za pristup sandučiću elektroničke pošte, mobilnim uređajima i dr. Pritom je za zaporke uobičajeno koristiti kombinaciju različitih znakova (slova, simbola, brojeva).

Slika 1. Prijava na sustav koji zahtijeva autentikaciju

Usporedba s ostalim tehnikama za autentikaciju

Identifikacija korisnika je bitan preduvjet za osiguranje privatnosti, integriteta i zaštite podataka općenito. Korištenje pristupnih lozinki predstavlja jednostavnu, ali i najjeftiniju metodu kojom se osigurava proces određivanja identiteta nekog subjekta. Ali ova metoda ima i nekoliko nedostataka kao što su npr. krađa lozinke ili zaboravljeni korisnički podaci. U konačnici takva situacija najčešće rezultira otvaranjem novog korisničkog računa ili određivanjem novih lozinki. U praksi postoji niz drugih (ili sličnih) tehnika za autentikaciju korisnika:

- **Korištenje jednokratnih lozinki** (eng. *single-use password*)
  Ovom metodom se smanjuju mogućnosti neovlaštenog pristupa povjerljivim podacima (korisnička imena, lozinke, brojevi kreditnih kartica, itd.), informacijama i/ili datotekama jer istu lozinku nije moguće upotrijebiti više nego jednom, a za svaku sljedeću prijavu je potrebno oblikovati novu lozinku. Primjer korištenja su jednokratne lozinke primljene SMS porukom koje se koriste za pristup pojedinim web uslugama. Pružaju zaštitu od napada ponavljanjem (eng. *replay attack*) i prisluškivanjem jer jednom korištena zaporka više nije upotrebljiva.

- **Sigurnosni token**
  Ova metoda za identifikaciju korisnika uglavnom se koristi u Internet bankarstvu. Vrlo je slična jednokratnim lozinkama, s tim što korisnici dobivaju posebne uređaje koje koriste kako bi dokazali svoj identitet. Uređaj, nakon što je aktiviran, od korisnika zahtijeva upis PIN-a (eng. *Personal Identification Number*), nakon čega vraća određenu numeričku vrijednost. Nju korisnik upisuje (preko web stranice) u polje za prijavu te tako dobiva (ukoliko je ispravna) pristup željenoj usluzi. Opasnost od zlonamjerne upotrebe postoji u slučaju da napadač sazna korisnički PIN.

Slika 2. Prijava na sustav za Internet bankarstvo

- **Biometrijske metode**
  Biometrija je tehnika za provjeru identiteta koja koristi jedinstvene fiziološke osobine svakog čovjeka (otisak prsta, skeniranje rožnice oka, DNK, itd). Biometrijski podaci se prikupljaju pomoću senzora i šalju na analizu, a pomoću njih se stvara biometrijski uzorak koji se uspoređuje s ranije dobivenim uzorkom. Radi se o metodi koja je sigurnija od zaporki jer se temelji na specifičnostima svakog pojedinca. Njezini su nedostaci cijena (koja ovisi o tipu biometrijske provjere) i činjenica da se korisnički podaci ne mogu promijeniti ukoliko dođe do njihove kompromitacije.

- **Sustav jedinstvene autentikacije** (eng. *Single Sign-On, SSO*)
  Riječ je o mehanizmu koji korisnicima omogućuje predočenje akreditacijskih podataka samo jednom, nakon čega dobivaju pristup različitim resursima (za vrijeme trajanja jedne korisničke sjednice). Osnovni problem ove metode je nepostojanje jedinstvenog standarda za primjenu navedenog pristupa. Opasnost za korisnike je upotreba jedinstvenih korisničkih podataka za pristup raznim sustavima čime se izravno ugrožava korisnik, ali i sustavi na koje se spaja. Tako primjerice, ako napadač otkrije podatke za pristup e-mail poslužitelju tvrtke, može iskoristiti propust za izmjenu/brisanje postojećih računa, ali i za spajanje na ostale poslužitelje ili aplikacije. Odnosno, ako se „provali“ u jedan sustav, svi ostali mogu postati djelomično ili u cijelosti kompromitirani, ovisno o stupnju ovlasti korisnika čiji su podaci otkriveni.

- **Korištenje ne-tekstualnih zaporki**
  Umjesto upisa kombinacije znakova korisnik može upotrebljavati grafičke lozinke ili određene poteze mišem.

Slika 3. Grafička zaporka

Kod grafičkih zaporki korisnik može izabrati niz slika koje se slažu određenim redoslijedom. Opasnost kod ovakve metode je što korisnici najčešće odabiru nizove prema jednostavnom obrascu (kao što je npr. prve tri slike u nizu) što napadač može vrlo lako otkriti.

- **Primjena digitalnih certifikata**
  Digitalni certifikat je skup podataka u elektroničkom obliku koji predstavlja elektronički identitet u raznim interakcijama te omogućuje sigurnu i povjerljivu komunikaciju Internetom. Problem koji se javlja u ovoj situaciji može biti neodgovarajuća provjera pojedinih parametara certifikata, što napadaču omogućuje lažiranje poslužitelja (eng. *spoofing*) i podmetanje nevaljanih certifikata.

Najčešći pristupi koji se koriste za identifikaciju korisnika su lozinke, tokeni i biometrija. Tablica 1. prikazuje njihove najbitnije sličnosti i razlike:

Karakteristike	Lozinke	Tokeni	Biometrijski podaci
Pouzdanost identifikacije	Dobra	Vrlo dobra	Izvrsna
Zahtijeva dodatne uređaje	Ne	Ponekad	Da
Zahtijeva dodatne programe	Ne	Ponekad	Da
Prosječna cijena implementiranja	0$	50$	100$

Tablica 1. Usporedba pojedinih tehnika za identifikaciju korisnika

3. Metode za zaštitu lozinki na razini sustava

Sustavi koji provode autentikaciju korisnika mogu koristiti dodatne funkcionalnosti u svrhu zaštite. U nastavku slijedi njihov opis.

3.1. Sigurna komunikacija korištenjem SSL/TLS protokola

Zaporke je moguće otkriti na razne načine, a najčešći od njih je prisluškivanjem prometa na mreži koja nije zaštićena. Ponekad se putem elektoničke pošte korisnike obavještava o njihovim računu tj. šalju im se podaci koji navode kako glasi njihovo korisničko ime i pristupna lozinka. Ako se pritom poruka šalje kao čisti tekst (ne koristi se enkripcija podataka), potencijalni napadač je u mogućnosti izvesti napad prisluškivanjem (eng. *eavesdropping*) te tako otkriti spomenute podatke. Zlonamjernim korisnicima je tako omogućen neovlašten pristup računalnom sustavu. Kako bi omogućili sigurnu komunikaciju preko Interneta moguće je koristiti SSL/TLS protokol.

SSL (eng. Secure Sockets Layer) i TLS (eng. Transport Layer Security) su protokoli za uspostavu sigurnog komunikacijskog kanala između klijenta i poslužitelja. Uobičajena je primjena ovih protokola u komunikaciji između preglednika i poslužitelja kada je potrebno osigurati povjerljivost podataka. Time se sprječava prisluškivanje, uplitanje druge strane, ali i krivotvorenje poruka. Wikipedia je primjer stranice koja koristi ove protokole (slika 4).

Slika 4. Prijava korisnika na stranicu Wikipedie

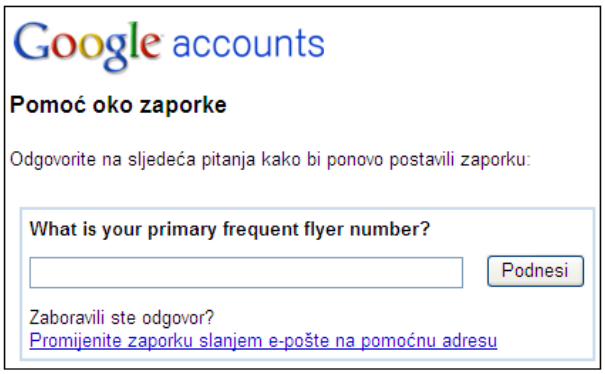
Za više detalja o ovoj temi preporuča se pogledati dokumente „TLS protokol i“ „Secure Socket Layer“ na stranicama CERTa:

http://www.cert.hr/documents.php?lang=hr

3.2. Samostalna promjena zaporki

Sustavi za upravljanje identitetom korisnika imaju ugrađenu funkcionalnost koja korisnicima omogućuje da samostalno promijene izgubljene i/ili ukradene zaporke. Na taj se način smanjuje broj upita koje korisnici šalju sistem administratorima, ali i lozinke ostaju poznate samo korisnicima.

Korisnik se prijavljuje na poslužitelj na način da odgovori na određena pitanja koja se zatim uspoređuju s odgovorima koje je korisnik unio kada je prvi put otvarao račun. Ta pitanja mogu biti „Gdje ste rođeni?“, „Koji Vam je omiljeni film?“, i sl. Ukoliko su odgovori točni, podaci se korisniku šalju na alternativnu navedenu e-mail adresu. Nedostatak ove funkcionalnosti je to što se mnogi od ovih odgovora mogu pogoditi (posebice ukoliko napadač poznaje žrtvu čije podatke želi otkriti).



Slika 5. Promjena zaporke na Google servisima

3.3. Zastarijevanje lozinki

Sljedeći način zaštite lozinki je tzv. „zastarijevanje zaporki“ (eng. *password aging*). Radi se o funkcionalnosti dostupnoj na većini operacijskih sustava (Linux, Solaris, Windows, i dr.), ali i specijaliziranih poslovnih programa. Ovim se mehanizmom postiže određivanje vremenskog roka nakon kojeg se zaporka mora promijeniti (mjesečno, jednom u pola godine, jednom u tri mjeseca).

Međutim, korisnici vrlo često imaju otpor prema ovim „previše čestim“ izmjenama tako da koriste uzorke postojećih lozinki. Primjer takve varijacije može biti npr. „korisnik“ i „korisnik123“. Ali korištenje ovakvih zanemarivih promjena može predstavljati sigurnosni rizik. Posebno je opasno ovakve modifikacije koristiti za administratorske lozinke jer jednom kada napadač dođe u posjed informacija koje mu omogućavaju pristup, može mijenjati konfiguracijske postavke, dodavati nove račune ili čak onemogućiti rad sustava.

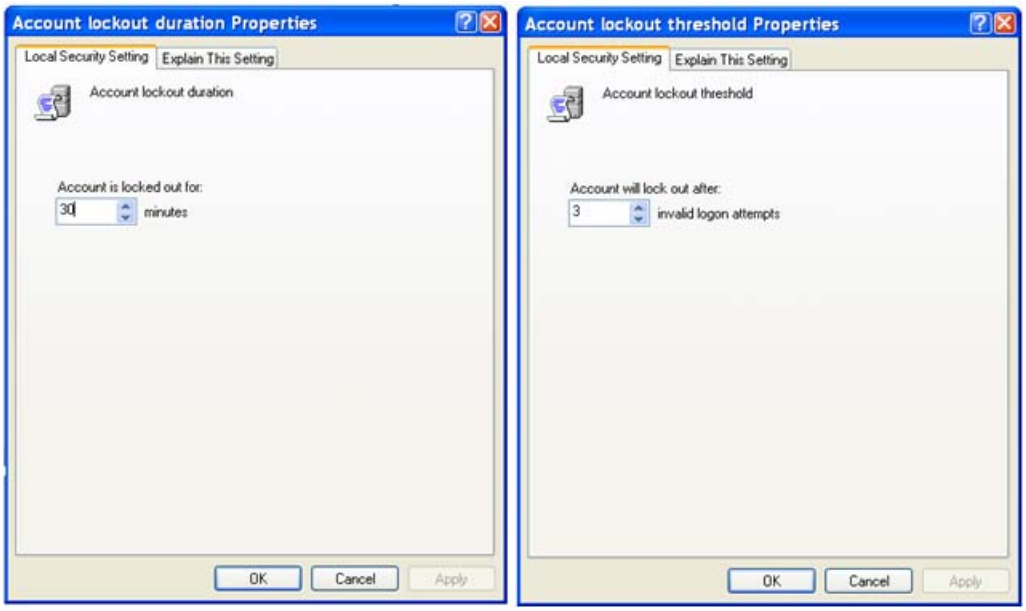
```
login as: <user>

<user> 's password:
You are required to change your password immediately (password aged)
Your password has expired, the session cannot proceed.
Last login: Tue Aug 19 10:46:39 2008 from 192.168.5.186
You must change your password now and login again!
Changing password for user xxxVRanger.
Changing password for xxxVRanger
(current) UNIX password:
```

Slika 6. Zastarijevanje pristupne lozinke

3.4. Zaključavanje korisničkog računa

Korisnici i sistem administratori mogu postaviti ograničenje na broj neuspješnih unosa lozinke prije zaključavanja računa (eng. *lockout*). Tako se na operacijskim sustavima Windows može postaviti najveći broj pokušaja (0-999). Nakon što korisnik prekorači ovu brojku, sustav ostaje „zaključan“ definirani period vremena (0-99,999 minuta). U tom vremenu korisnik ne može pristupiti svom korisničkom računu niti u slučaju da upiše ispravne podatke.



Slika 7. Zaključavanje računa na Windows platformi

3.5. Dvo-faktorska autentikacija

Tradicionalno se autentikacija temeljila samo na upotrebi korisničkog imena i zaporke. Ovakav se pristup u pojedinim slučajevima (npr. u bankarstvu za novčane transakcije) smatra nesigurnim. Pojam dvo-faktorska autentikacija (T-FA ili 2FA) je termin koji se koristi za opisivanje mehanizma za identifikaciju korištenjem 2 parametra. Dva osnovna faktora koja se pritom uzimaju u obzir su:

- **nešto što je poznato korisniku** – to može biti npr. PIN broj i
- **nešto što korisnik posjeduje** – najčešće se odnosi na elektronički uređaj koji na zaslonu prikazuje znamenke nakon što korisnik upiše podatak koji zna (PIN).

Te se znamenke mijenjaju svakih 60-90 sekundi. Sustav kojem korisnik želi pristupiti zna koji brojevi trebaju biti prikazani i uspoređuje ih s onim što je korisnik upisao. Na temelju toga se provodi autentikacija. Primjer takvih uređaja su token i/ili pametna kartica (slika 8). Osim navedenih uređaja moguće je na mobitel dobiti SMS poruku koja se koristi u postupku prijave.

Slika 8. Token i pametna kartica

Budući da u ovom slučaju napadaču nije dovoljna samo korisnička lozinka, značajno se povećava sigurnost. Dvo-faktorska autentikacija bi mogla drastično smanjiti broj incidenata vezanih uz *online* krađu korisničkih pristupnih podataka i *online* prijevare.

Novije sigurnosne procedure zahtijevaju autentikaciju koja se temelji na tri faktora pri čemu se pored spomenutih koristi i biometrijski podaci.

3.6. Zaštita korištenjem funkcija za računanje sažetaka

Pojedini sustavi pohranjuju zaporke u obliku čistog teksta. U cilju zaštite od napadača moguće je koristiti napredne tehnike kao što je određivanje sažetka poruke (eng. *hash*) primjenom određenih kriptografskih algoritama. U tu se svrhu koriste različiti programi dostupni preko Interneta. Jedan od njih je *Hash Generator*, dostupan na stranici:

http://www.sinfocol.org/herramientas/hashes.php

Nova zaporka nastaje upisom predviđenog korisničkog zapisa kojemu se dodaje tzv. *salt* vrijednost. Ova je vrijednost opcionalna, ali treba uzeti u obzir da se njenim korištenjem napadaču otežava posao računanja sažetka čak i za uobičajene lozinke (kao što je npr. *admin*).

Potom se, korištenjem neke od *hash* funkcija, oblikuje nova vrijednost na osnovu ulaznih podataka na način da je teško (ili neizvedivo) otkriti izvornu poruku. Kriptografske funkcije za izračunavanje sažetaka koje se najčešće koriste u ovu svrhu su MD5 i SHA1.

MD5 (eng. *Message-Digest algorithm 5*) je ime za kriptografsku funkciju koja uzima ulaznu poruku proizvoljne duljine i izračunava 128-bitni sažetak Ratificirana je internetskim standardom RFC 1321. SHA (eng. *Secure Hash Algorithm*) je algoritam koji služi za provjeru autentičnosti datoteka ili poruke prilikom prijenosa između pošiljaoca i primatelja, a predstavlja nasljednika MD5 algoritma. SHA1 koristi 160 bitnu duljinu sažetka poruke. Sigurnosni stručnjaci preporučaju korištenje SHA algoritma koji je otporan na koliziju (za razliku od MD5). Otpornost na koliziju (eng. *collision resistance)* je svojstvo funkcije za izračunavanje sažetka koje osigurava da se ne može pronaći neka druga ulazna poruka koja bi imala isti sažetak.

3.7. Lista pravila za tvrtke/organizacije u svrhu zaštite zaporki

Uobičajene tehnike za sustave koji zahtijevaju identifikaciju korisnika, a koje se koriste u pojedinim tvrtkama, trebale bi primjenjivati sljedeća pravila:

1. Korištenje lozinki odgovarajuće duljine (ranije inačice Unix i Windows sustava su imale ograničenje od 8 znakova)
2. Poluautomatska odjava sa sustava (eng. *semi log-off policy*) – nakon određenog perioda neaktivnosti (npr. 15 minuta) korisnik se mora ponovno prijaviti. Pritom svi korisnički procesi ostaju aktivni, a korisniku se time samo osigurava ponovni ulaz u sustav (tj. provjerava se njegov identitet)
3. Nametanje sigurnosne politike tvrtke koja uključuje:
    i. Periodičnu promjenu lozinki
    ii. Dodjeljivanje nasumično odabranih zaporki
    iii. Omogućivanje autentikacije nekim drugim načinima koji ne zahtijevaju upis podataka putem tipkovnice (npr. glasovno raspoznavanje, biometrija i sl.)
    iv. Korištenje različitih znakova za lozinku (slova, brojke, simboli, velika i mala slova)
4. Preusmjeravanje nezaštićenog prometa (HTTP, telnet, rlogin, rsh i FTP) preko zaštićenog SSH kanala. SSH (eng. Secure Shell) protokol uvodi zaštitu tajnosti podataka korištenjem kombinacije simetrične (npr AES, DES, 3DES algoritmi) i asimetrične (DSA i RSA) enkripcije podataka.
5. Ograničavanje broja mogućih pokušaja za upis lozinke u nekom vremenskom periodu. Time se pokušava spriječiti napad pogađanjem lozinki (eng. *brute force attack*). Jednom kada se dosegne granica (npr. nakon tri pokušaja), nije se moguće prijaviti na sustav čak niti ako se unese ispravna lozinka. Tek kada istekne vremenski rok (koji može iznositi npr. pola sata), korisnik se može ponovno pokušati prijaviti. Međutim, u ovom slučaju napadač može pokušati izvesti DoS (eng. *Denial of Service*) napad slanjem pretjerano velikog broja zahtjeva za prijavom. Neki od načina za zaštitu od DoS napada su korištenje vatrozida (eng. *firewall*), usmjerivača koji koriste ACL liste za provjeru pristupa ili sustavi za detekciju/sprječavanje neovlaštenog pristupa
6. U organizacijama/tvrtkama se ne preporuča različitim korisnicima dodjeljivati identično korisničko ime i lozinku za pristup pojedinim aplikacijama jer se na taj način ne može točno odrediti tko je kada unio promjene u sustav.

4. Jačina lozinki

Jačina lozinke je mjera učinkovitosti u očuvanju zaporke izložene napadima pogađanjem (eng. *guess attack*) i ponavljanjem (eng. *brute force attack*). Moguće je, također, reći da se jačina lozinke odnosi na vjerojatnost da nije moguće pogoditi niti otkriti neku lozinku. One zaporke koje je jednostavno saznati nazivaju se slabe ili ranjive, dok se one druge (koje se saznaju vrlo teško ili ih nije moguće pogoditi) nazivaju jakim zaporkama.

Na temelju raznih istraživanja otkriveno je da većina ljudi koristi upravo slabe lozinke. Na sveučilištu Columbija u New Yorku 22% korisnika upotrebljava vrlo jednostavne lozinke koje napadači otkriju vrlo brzo. Prema istraživanju koje je 2006. proveo Bruce Schneier utvrđeno je da se 55% zaporki koje se koriste na popularnoj web stranici MySpace mogu otkriti za 8 sati korištenjem komercijalno dostupnog alata „*Password Recovery Toolkit*".

Na tržištu postoji i niz programa koji omogućuju otkrivanje zaporki. Neki od najpoznatijih su L0phtCrack, John the Ripper ,Cain i Hydra.

4.1. Ljudski faktor

Poznato je da su lozinke uobičajeni način pristupa različitim sustavima. Stoga ih treba pažljivo odabrati.
Ukoliko su sigurnosna pravila za definiranje zaporki previše stroga, mnogi korisnici će upotrebljavati takav oblik podataka koji nema smisla čak niti njima samima. Rezultat je da će zaboraviti svoje korisničke podatke, što se dalje može odraziti na višestruko registriranje na pojedine stranice. Vrlo često, ljudi imaju otvoreno po nekoliko računa za pojedinu web stranicu. Osim toga, korištenje velikog broja računa rezultira time da se takvi podaci zapisuju na različite papiriće, stavljaju u novčanik ili zapisuju na računalo čime se povećava sigurnosni rizik.
Sljedeća učestala pogreška je korištenje sličnih ili istih pristupnih lozinki za različite sustave. Napadač koji otkrije takvu zaporku može ozbiljno ugroziti pojedinca. U nekim slučajevima posljedice su minorne, ali mogu poprimiti i veće razmjere. Napadači mogu ukrasti osnovne matične podatke, razne lozinke, brojeve kreditnih kartica, a onda ih upotrijebiti za prebacivanje novca s korisničkih računa ili čak za krađu identiteta. Istraživanjem koje je 2006. proveo Javelin Strategy & Research otkriveno je da je čak 13% korisnika Interneta u SAD-u bilo žrtvom krađe identiteta.

4.2. Slabe lozinke

Lozinke je ponekad moguće odrediti ukoliko napadač poznaje korisnika i zna njegove osobne podatke (ime, datum i mjesto rođenja, omiljeni film). Ali to nije nužan uvjet za otkrivanje zaporki. Ljudi vrlo često koriste neke od ovih slabih lozinki:

- *pasword, admin* i izvedenice ovih riječi (password123, administrator),
- *asdf, qwerty, yxc* - radi se o nizu slova na tipkovnici u istom redu,
- zaporka glasi isto kao i korisničko ime,
- korištenje riječi koje postoje u rječniku,
- uporaba osobnih podataka kao što su imena, rođendani i sl.,
- imena poznatih osoba, gradova ili pojmova. Primjeri su : *Madonna, transformers, Pariz*, i dr.,
- riječi kod kojih su pojedina slova zamijenjena predvidljivim riječima: *l0ve, dr@gon, s3cr3t* i
- ponavljanje prethodnih lozinki – u ovim se slučajevima preporuča promijeniti pojam barem pet puta prije nego se dodijeli stara zaporka

4.3. Jake lozinke

Jaka je lozinka ona koju napadač ne može otkriti ili može uz izuzetni napor. Prema Jamesu Quinu, višem analitičaru u Info-Tech istraživačkoj skupini, ključ uspjeha u oblikovanju jakih lozinki ovisi o njihovoj dužini i složenosti. Pritom se dužina odnosi na broj znakova koji se koriste, a složenost na tehnike koje se koriste prilikom stvaranja zaporki.

Iako postoje razna pravila za oblikovanje lozinki, stručnjaci iz polja računalne sigurnosti se slažu oko onih osnovnih: trebaju se sastojati od barem 8 znakova (simbola, slova i znamenki), ne sadržavati nikakve osobne informacije, niti se koristiti u rječnicima.

U nastavku teksta slijedi pojašnjenje ovih, ali i ostalih spomenutih pravila:

- Prilikom oblikovanja lozinki savjetuje se korištenje kombinacije slova (malih i velikih), brojeva i simbola.
- Također, dobro je koristiti supstituciju za pojedina slova i brojeve (3→E, o→0, I→1). Ova tehnika nije primarna metoda za zaštitu, ali svakako uvodi dodatni stupanj sigurnosti.
- Ukoliko se koristi nekoliko znakova za lozinku, savjetuje se osmišljavanje fraze koja simbolizira određenu izjavu. Primjer toga je rečenica „John Jacob Jingleheimer Schmidt, his name is my name too“, dok fraza glasi „jJjshnImn2“. Iz ovog je primjera očito kako je moguće koristiti početna slova riječi, ubaciti velika slova te uvesti supstituciju brojevima za neka slova.
- Ukoliko korisnik nasluti da mu/joj je korisnički račun kompromitiran, potrebno je odmah izmijeniti postojeću zaporku. Kako bi se pokušaji kompromitacije smanjili na minimum, korisnicima se savjetuje da ne slijede poveznice (eng. link) na web stranice poslane u poruci s nepoznate adrese ili IM (eng. *instant messaging*) klijenta.
- Ne koristiti istu zaporku za pristup različitim sustavima, posebice ako se ti sustavi ne koriste u istu svrhu. Lozinke koje korisnici upotrebljavaju na Internet forumima, za igrice itd. se ne smiju upotrebljavati na važnijim sustavima kao što su elektronička pošta ili za prijavu na računalo.
- Također, ne preporuča se razmjenjivati identifikacijske podatke preko poruka elektroničke pošte, foruma, mobitela ili aplikacija jer nije osigurana privatnost komunikacije. Pritom se savjetuje ne otkrivati vlastitu zaporku nikome.
- Ne zapisivati identifikacijske podatke kako ne bi došle u posjed potencijalnih napadača. Ukoliko je podatke ipak potrebno negdje zabilježiti, savjetuje se pohrana na mjestima koja su dostupna samo pojedinom korisniku. Na UNIX sustavima su se zaporke automatski pohranjivale u datoteku */etc/passwd*. Danas se spremaju u datoteku */etc/shadow* kojoj mogu pristupiti samo korisnici i programi s administratorskim ovlastima.
- Učestala promjena korisničke lozinke – preporuka je da se takva promjena napravi barem jednom u šest mjeseci.
- Stvaranje i provjera jačine lozinke korištenjem alata koji se primjenjuju u tu svrhu (npr. *password generator, password checker*).
- Pridržavati se pravila spomenutih kod slabih zaporki.

4.3.1. Primjer stvaranja jakih lozinki

Jedan od načina za stvaranje jakih lozinki je sljedeći:

1. Smisliti rečenicu koju je lako zapamtiti
   Moj pas je star tri godine
2. Izbaciti razmake
   Mojpasjestartrigodine
3. Zamijeniti neka od slova velikim slovom. Da bi se zapamtilo koja su to slova, savjetuje se da ta slova predstavljaju neku riječ. Ovdje je to riječ MOJE
   MOjpasJEstartrigodine
4. Zamijeniti slova simbolima
   MojpasJEstartr1g0d1ne
5. Izbaciti prva i posljednja dva znaka/slova
   jpasJEstartr1g0d1

Ovu novooblikovanu zaporku moguće je provjeriti s programima za provjeru jačine lozinki. Na danom primjeru koristi se ranije navedeni alat *password checker* (slika 9):

Slika 9. Provjera jačine zaporke korištenjem programa *Password checker*

Još neki od primjera jakih lozinki su *4pRte!ai@3, Tp4tci2s4U2g!, BBslwys90!, tDI"60Hs7* i *l52@36291QBs.* Međutim, treba uzeti u obzir da su javno objavljeni te ih stoga ne treba upotrebljavati kao stvarne zaporke.

5. Alati za upravljanje lozinkama

Programi za upravljanje lozinkama (eng. *password manager*) omogućuju korisnicima u organiziranju vlastitih lozinki i PIN kodova. Riječ je o programima koji koriste lokalnu bazu podataka s listom kriptiranih lozinki za pristup različitim sustavima, servisima i aplikacijama. Osim toga, ovi programi mogu sadržavati dodatne funkcionalnosti kao što su oblikovanje nasumičnih zaporki ili ispitivanje postojećih.

Postoje tri vrste ovakvih programa:

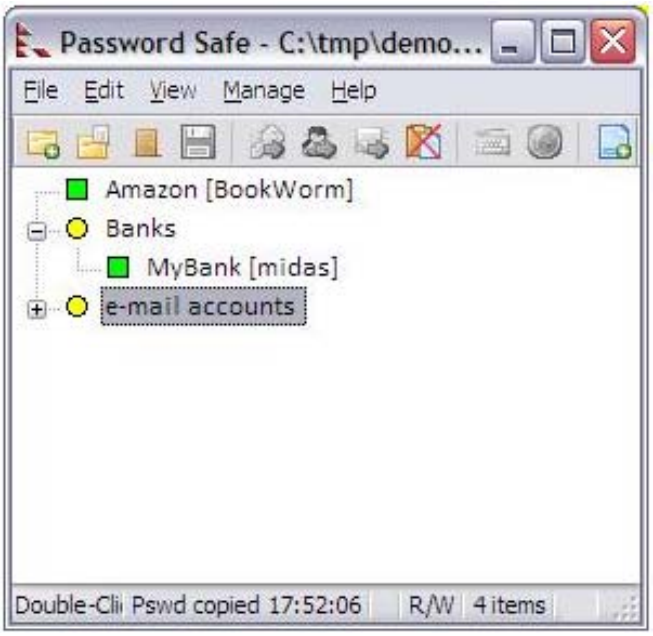
1. **Za radnu površinu** (eng. *desktop*) – svi se podaci pohranjuju na čvrstom disku računala (eng. *hard disk drive, HDD*)
2. **Portabilni** – za pohranu podataka na mobilnim uređajima kao što su PDA ili pametni telefoni
3. ***Online* alati** – riječ je o web stranici koja omogućuje pohranu lozinki na poslužitelj i to u kriptiranom obliku korištenjem *Blowfish* algoritma. Riječ je o simetričnom kriptografskom algoritmu koji je razvio Bruce Schneier. U svom radu koristi blok s promjenjivom duljinom ključa od 32 do 448 bita (u skokovima od 8 bita).

Navedeni se alati upotrebljavaju ovisno o željama i potrebama korisnika. Tako npr. korisnik koji svim servisima i aplikacijama pristupa od kuće može koristiti programe koji su pohranjeni na *HDD-u.* Online alatima je moguće pristupiti s bilo kojeg računala koje ima pristup Internetu (npr. na poslu i od kuće), a portabilni su idealni za one korisnike koji su često u pokretu.

Spomenuti programi koriste samo jednu glavnu lozinku (eng. *master password*) koja se koristi kao ključ za dekriptiranje zaštićenog sadržaja. Međutim, i glavna lozinka može biti otkrivena praćenjem unosa znakova preko tipkovnice (eng. *keylogging*). Ukoliko ju otkrije, napadač može pristupiti svim sustavima koji su definirani u ovakvim programima (jer ima uvid u podatke o kojim stranicama se radi te kako glasi korisničko ime i zaporka za njih).

Password Safe

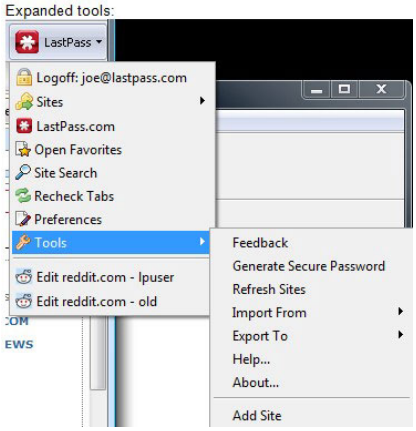
Password Safe je alat koji omogućuje pohranu podataka o višestrukim korisničkim računima. Podaci su kriptirani pomoću Blowfish algoritma, a program je dostupan za sve Windows platforme.



Slika 10. Password Safe program

KeePass

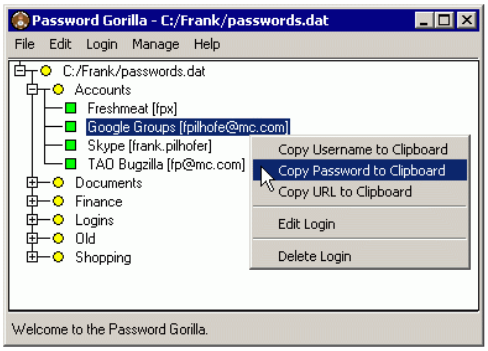
Radi se o programu otvorenog koda namijenjenog korištenju na gotovo svim danas popularnim operacijskim sustavima (Windows, Linux, Mac OS). Moguće ga je koristiti i na mobilnim uređajima tj. PocketPC, Symbian, BlackBerry i PalmOS platformama.



Slika 11. KeePass

Password Gorilla

Ovaj je program namijenjen za primjenu na Mac OS platformama te raznim distribucijama Linux sustava. Kompatibilan je s alatom Password Safe za operacijske sustave Windows.



Slika 12. Password Gorilla

RoboForm

Namijenjen je web preglednicima Internet Explorer 6,7 i 8, te Mozilla Firefox 2,3 i 3.5 inačicama

Slika 13. RoboForm

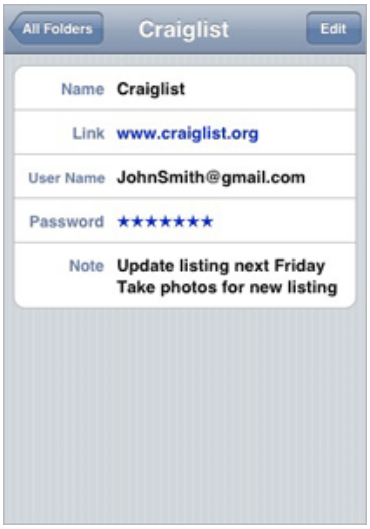
Sxipper

Riječ je o *online* alatu (dodatku za preglednik Firefox) za upravljanje lozinkama s brojnim funkcijama koje korisnicima omogućuju vizualno odvajanje određenih lozinki (poslovnih, privatnih, bankovnih, itd).

Slika 14. Sxipper program

Memengo Wallet Pro

Ovaj je program dostupan za korištenje na iPhone-u. Pruža podršku za sinkronizaciju nekoliko spomenutih uređaja preko web stranice memengo.com. Zaštita podataka se obavlja korištenjem 256-bitnog simetričnog AES (eng. Advanced Encryption Standard) enkripcijskog algoritma.



Slika 15. Memengo Wallet Pro

6. Vrste napada

Jednom kada napadač otkrije kako provaliti u neki sustav, otvaraju mu se brojne mogućnosti. Osim pregleda podataka na lokalnom računalu, može dalje pokušati pristupiti ostalim korisničkim/sistemskim podacima na poslužiteljima na mreži kojima spomenuti korisnik ima pristup.

Tipovi napada koje napadači mogu primijeniti kako bi otkrili osjetljive korisničke podatke kao što je pristupna lozinka su:

- **Napad pogađanjem lozinki** (eng. *password guessing*)
  Odnosi se na napade u kojima napadač koristi različite lozinke (pojmove) kako bi se prijavio na sustav kao određeni korisnik. Početni cilj napada je otkrivanje zaporke, dok se kasnije ova situacija može proširiti u napad s ciljem izmjene podataka (npr. promjena podataka za korisnički račun kako bi se onemogućio pristup). Postoje dva oblika ovog napada:
  a) Napad uzastopnim pokušavanjem (eng. *brutte force attack*)
  U ovom slučaju napadač isprobava različite zaporke dok ne pronađe ispravnu. Obično se izvodi u dužem vremenskom periodu, dok se ne isprobaju sve moguće kombinacije. Kako bi se otežao napad savjetuje se korištenje najmanje 6 znakova za lozinku koji su strukturno različiti (npr. velika i mala slova). Tablica 2 prikazuje koliko je vremena potrebno za otkrivanje lozinki ovisno o njihovoj duljini i znakovima koji se koriste.

Broj znakova	Mala slova	Mala slova i znamenke	Mala i velika slova	ASCII znakovi
<=4	1 min	1 min	1 min	2 min
5	1 min	2 min	12 min	4 h
6	10 min	72 min	23 dana	18 dana

Tablica 2. Otkrivanja zaporki ovisno o tipu i broju znakova

  b) Napad pomoću rječnika (eng. *dictionary attack*)
  Napadač koristi listu često upotrebljavanih izraza (tj. rječnik) te ih redom upotrebljava dok ne nađe pravu. Osim liste iz rječnika, napadač može koristiti i pojmove kao što su osobni podaci. Kao sigurnosna mjera savjetuje se konfiguriranje autentikacijskog sustava na način da odbija nepotpune prijave, odnosno da prihvaća samo cjelokupne korisničke podatke (ime i lozinku). Drugi način obrane jest zabraniti riječi i fraze iz rječnika.
- **Praćenjem unosa znakova preko tipkovnice** pomoću tzv. *keylogger* programa koji prate i bilježe svaku tipku koju korisnik pritisne. Ovi se alati dijele u dvije kategorije: programske i sklopovske. Sklopovski uređaji se postavljaju u tipkovnicu ili računalo, dok se programski sastoje od alata koji prate akcije korisnika na razini operacijskog sustava. Kao rješenje preporuča se uporaba antivirusnih alata, korištenje jednokratne zaporke ili dvo-faktorska autentikacija.
- **Napad zasnovan na socijalnom inženjeringu -** Socijalni inženjering je vrsta napada na računalne sustave s ciljem nagovaranja ljudi da ispune zahtjeve napadača. Radi se o načinu stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Najčešće metode prijevare su lažno predstavljanje (kao sistem administrator) ili molba za pomoć nekome/nečemu. Jedini mogući način zaštite od socijalnog inženjeringa je educiranje korisnika kako prepoznati ovu vrstu napada te kako se obraniti.
- **Phishing napad** je vrsta napada u kojem napadač putem elektroničke pošte ili lažnih Internet stranica pokušava doći do povjerljivih informacija u cilju stjecanja financijske koristi. Najčešće je riječ o zaporkama, PIN brojevima, brojevima kreditnih kartica te drugim sličnim povjerljivim informacijama. Ukoliko napadač uspješno izvede napad i prikupi željene informacije, pruža mu se mogućnost pristupa informacijskim sustavima financijskih ustanova ili nekim drugim sustavima preko kojih može steći određenu financijsku korist.

7. Zaključak

U današnje vrijeme pristupne lozinke su postale vrlo značajne i predstavljaju bitan aspekt u računalnoj sigurnosti. Odnosno, zaštita zaporki predstavlja osnovni preduvjet za zaštitu informacijskih sustava. Korisnici, kao i sistem administratori, imaju moralnu obvezu podržavati korištenje jakih lozinki kako bi doprinijeli očuvanju sigurnosti.

Iako mnogi sustavi u svrhu autentikacije koriste pristupne lozinke, za očekivati je kako će se takav trend smanjivati u budućnosti. Odnosno, zaporke će se koristiti i dalje, ali u kombinaciji s drugim sigurnosnim metodama i tehnikama kao što je dvo/tro faktorska autentikacija ili primjenom SSO mehanizama.

Korisnici gotovo svaki dan imaju potrebu pristupati različitim servisima i programima: email poslužitelju, komercijalnim web stranicama, bankarskim servisima, itd. Slaba lozinka može kompromitirati korisnika, ali i cijelu korporativnu mrežu. Stoga se savjetuje da zaporke ne budu previše kratke (potrebno je koristiti najmanje 8 znakova uključujući slova, brojke i simbole), da to ne budu riječi koje postoje u rječnicima te da se redovito mijenjaju. Također, ako korisnik ima pristup na više sustava, preporuča se korištenje različitih korisničkih računa u svrhu očuvanja sigurnosti i integriteta podataka.

8. Reference

[1] Choosing Passwords: Security and Human Factors, http://research.csc.ncsu.edu/efg/ethics/papers/passwords.pdf, srpanj 2008.

[2] Passwords, http://en.wikipedia.org/Passwords, listopad 2009.

[3] Password Cracking, http://en.wikipedia.org/wiki/Password_cracking, listopad 2009.

[4] PasswordSafe, http://passwordsafe.sourceforge.net/, 2008.

[5] Kurt Marko: What Makes a Strong Password, http://processor.com/editorial/article.asp?article=articles/P3119/37p19/37p19/37p19.asp, srpanj 2009.

[6] 12 Tools for Managing Your Passwords, http://www.webmastersgossip.com/blogs/jani/82-12-tools-managing-your-passwords.html, rujan 2009.

[7] Password Strength, http://en.wikipedia.org/wiki/Password_strength, listopad, 2009.

[8] Praćenje unosa znakova preko tipkovnice, www.cert.hr/filehandler.php?did=312, studeni 2007.

[9] Lider, http://www.liderpress.hr/Default.aspx?sid=1118, siječanj 2006.