Centar Informacijske Sigurnosti

# Rukovanje lozinkama


travanj
2012.



CIS-DOC-2012-04-046

# Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

# O CIS-u

**CIS izrađuje** pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

**Smisao CISa** je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

# Prava korištenja

# Sadržaj

# 1. Uvod

Lozinke predstavljaju osnovni način autentifikacije korisnika u većini informacijskih sustava. Većina sustava, neovisno o primjeni, često ima potrebu razlikovati određene korisnike. Ovo se postiže davanjem posebnog identiteta za svakog korisnika sustava. No, sustav mora moći odrediti je li korisnik koji koristi sustav zaista onaj korisnik kojemu pripada dodijeljeni identitet.

Iako je područje kriptografije dalo velik niz doprinosa u pogledu algoritama i protokola za autentifikaciju, lozinke su i dalje nezaobilazne. Naime, one čine najpraktičniji i najjeftiniji način provjere identiteta. Kod provjere identiteta lozinkom, korisnik mora zapamtiti određenu tajnu te ju prilikom prijave reproducirati. Korisniku se ne mora izdavati nikakav dodatni uređaj kako bi dokazao svoj identitet. Međutim, ova jednostavnost često ima utjecaj na sigurnost identiteta, što zloćudni korisnici često iskorištavaju. Postoje različite metode autentifikacije ovisno o razini pouzdanosti i zaštite koju sustav mora osigurati. U poglavlju 2. analiziraju se načini autentifikacije te uloga lozinki u tom postupku.

Zbog tako velike uloge u autentifikaciji korisnika, lozinkama je potrebno na ispravan način upravljati. Lozinke imaju vlastiti životni ciklus koji treba poštivati kako bi se osigurao identitet korisnika. Samim time, korisnici i sustavi imaju dužnost rukovati lozinkama na siguran način. Rukovanje lozinkama obuhvaća niz radnji, a one su detaljnije opisane u poglavlju 3. Obzirom da je rukovanje lozinkama složen zadatak, postoje mnogi načini na koje zloćudni korisnici mogu pokušati otuđiti identitet drugog korisnika krađom lozinke. Ovisno o vektoru napada, metode otuđivanja identiteta mogu biti raznolike. Metode napada na lozinke opisane su u poglavlju 4.

Kako je rukovanje lozinkama složen postupak, često se događaju različite ljudske greške. Kako bi se broj tih grešaka smanjio, razvijeni su različiti alati koji olakšavaju rukovanje lozinkama. Neki alati su namijenjeni krajnjim korisnicima, dok su drugi namijenjeni sustavima za upravljanje lozinkama. No, neki alati su stvoreni isključivo za otuđivanje lozinki. Zloćudni korisnici često koriste takve alate kako bi otkrili lozinke drugih korisnika i otuđili im identitete. U poglavlju **Error! Reference source not found.**. se detaljnije opisuju neki od navedenih alata.

# 2. Autentifikacija korisnika

Informacijski sustavi imaju sve veću ulogu u današnjem društvu. Tokom dana, prosječan korisnik koristi razne usluge Interneta kako bi obavljao određene zadatke. Korisnici obično obavljaju bankovne transakcije putem Internet bankarstva, upravljaju elektroničkom poštom, posjećuju razne društvene mreže te druge usluge. Svaki od tih sustava mora zadovoljavati određeni skup sigurnosnih zahtijeva kako bi korisnicima pružao najmanju razinu sigurnosti. Najosnovniji sigurnosni zahtijev predstavlja upravljanje pristupom. Korisnicima se obično dodjeljuju određene funkcionalnosti i mogućnosti ovisno o njihovoj ulozi, identitetu i drugim značajkama. No, prethodno je potrebno autentificirati korisnika kako bi se otkrilo koja prava posjeduje. Autentifikacija korisnika je neophodan dio u osiguravanju osnovnih sigurnosnih zahtijeva. Korisnik stvara svoj digitalni identitet putem registracije na željenu uslugu, a kasnije potvrđuje svoj identitet postupkom autentifikacije.

Sama autentifikacija je široko područje koje obuhvaća niz metoda. Općenito, autentifikacija se postiže tako da korisnik predoči neku vrstu faktora kojim dokazuje svoj identitet. Autentifikacijski faktori mogu uključivati jednu ili više stvari. Faktori autentifikacije opisuju se u nastavku dokumenta, a više informacije može se pronaći u dodatnoj literaturi pod [10] i [11].

- **Nešto što korisnik zna** – obično se radi o tajnom podatku koji je poznat samo korisniku. Na primjer, lozinka je najčešće ostvarenje ovog faktora autentifikacije. Kako je naglasak ovog dokumenta na lozinkama, njihova uporaba se detaljno razmatra u narednim poglavljima.
- **Nešto što korisnik ima** – podrazumijeva uporabu dodatnih uređaja kojima korisnik potvrđuje svoj identitet. Takvi uređaji se obično nazivaju tokenima te se često koriste u bankarstvu. Glavna značajka je da se korisnik autenticira putem tog uređaja, odnosno, informacijama koje uređaj proizvodi. Tokeni u bankarstvu obično proizvode jednokratne lozinke kojima se korisnik autentificira. Kreditne kartice koriste kombinaciju ovog i prethodno faktora za autentifikaciju korisnika. Kreditne kartice predstavljaju fizički faktor autentifikacije, dok se PIN (engl. *Personal Identification Number*) lozinka koristi kao faktor znanja.
- **Nešto što korisnik jest** – autentifikacija se oslanja na fizička svojstva korisnika. Na primjer, otisci prstiju, raspoznavanje glasa, uzorak vena u očima, geometrija ruke te drugo. Ovakav način autentifikacije se naziva biometrija te predstavlja posebnu znanstvenu disciplinu.

## *2.1. Uloga lozinki u autentifikaciji korisnika*

Autentifikacija korisnika lozinkom je danas najraširenija oblik autentifikacije. Oslanja se na prvi od ranije spomenutih faktora dokazivanja identiteta, korisničkom znanju. Točnije, oslanja se na autentifikaciju korisnika dijeljenim znanjem. Korisnik dokazuje svoj identitet tako da šalje vlastitu lozinku, a sustav mora prepoznati je li priložena lozinka ispravna. Odnosno, sustav i korisnik moraju podijeliti znanje o tajnoj lozinki kako bi se korisnik uspješno autentificirao. U tu svrhu se obično koristi registracija korisnika. Naime, prilikom postupka otvaranja novog korisničkog računa na sustavu, korisnik odabire lozinku. Neki sustavi ne dopuštaju korisnicima odabir vlastitih lozinki već ih samostalno generiraju i šalju u porukama elektroničke pošte. Ova metoda registracije se pokazala iznimno lošom u praksi jer korisnici često ne brišu stare poruke, a napadači ih često i presreću. Dodatno, kako te poruke često nisu šifrirane, napadač može lako očitati lozinku.

Autentifikacija korisnika lozinkom smatra se najneprikladnijom metodom provjere identiteta. Ipak, zbog velike praktičnosti se i dalje jako često koristi. Općenito, autentifikacija korisnika uporabom metode dijeljenog znanja ima velike nedostatke. Na primjer, zloćudni korisnik mora otuđiti samo jednu informaciju kako bi ukrao identitet legitimnog korisnika. Dodatno, postoje veliki problemi u odabiru kvalitetnih lozinki. Korisnici često iz praktičnih razloga odabiru lozinke koje zloćudni korisnici mogu lako pogoditi. Poglavlje 3.1. detaljno opisuje ovaj problem. Drugi veliki nedostatak autentifikacijom lozinki je njihova pohrana na sustavu. Naime, kako bi sustav potvrdio identitet korisnika mora pohraniti lozinku radi kasnije usporedbe. Ukoliko sustav pohranjuje lozinke na nesiguran način, vješt napadač moći će otuđiti lozinke korisnika napadom na sustav. Time se dokazuje kako sigurnost ove metode autentifikacije ne ovisi samo o korisnicima već i o sustavu

koji obavlja njihovu autentifikaciju. Poglavlje 3.2. opisuje metode pohrane lozinki. No, ove metode se često ne primjenjuju u informacijskim sustavima. Mnogi sustavi opravdavaju svoje loše politike pohrane lozinki. Kao primjer, moguće je razmatrati sustav koji nudi uslugu pregledavanja video sadržaja. Neka sustav omogućuje pregledavanje video sadržaja svim korisnicima, dok samo registrirani korisnici imaju pravo ocijeniti sadržaj. Svaki korisnik može samo jednom ocijeniti pojedini video sadržaj. Vlasnici sustava mogli bi opravdati lošu politiku pohrane lozinki činjenicom da čak ako se lozinka otuđi, korisnik neće pretrpjeti štetu. Lažnim predstavljanjem zloćudni korisnik može samo ocjenjivati sadržaj u ime legitimnog korisnika. Kako sustav ne traži novčanu naknadu, nema materijalne štete po korisniku[1]. Iako korisnik teoretski nije pretrpio štetu, uporabom ovakvog sustava korisnik je unio sigurnosni rizik za vlastiti identitet. Ukoliko korisnik koristi istu ili sličnu lozinku za pristup nekom drugom sustavu, otkrivanjem lozinke na opisanom sustavu može napadaču pomoći u daljnjem otuđivanju korisnikova identiteta. Na primjer, ukoliko korisnik koristi istu lozinku za pristup elektroničkoj pošti, napadač će moći nesmetano čitati i pisati poruke u ime korisnika. Zbog ovakvih i sličnih ranjivosti, postoje brojni napadi na lozinke, a poglavlje 4. detaljnije opisuje neke od njih.

Prema povijesnim podatcima, jedno od prvih sustava široke primjene koji su za autentifikaciju korisnika koristili lozinke bile su benzinske postaje. Točnije, sustavi za automatizirano doziranje i upravljanje benzinom koristili su brojčane lozinke za autentifikaciju kako bi ograničili pristup sustavu. Takve brojčane lozinke su se ubrzo počele koristiti u drugim industrijama, a postale su poznate pod nazivom PIN (engl. *Personal Identification Number*) lozinke. U bankarskim sustavima počeli su se koristiti 1967. godine kada je napravljen sustav Barclays-De La Rue[2]. Za autentifikaciju su se inicijalno trebale koristiti PIN lozinke od 6 znamenaka. No, kasnije se ipak odabrao sustav koji je koristio četiri znamenke[3].

[1] Moglo bi se argumentirati kako čak i u ovom slučaju postoji šteta za sam sustav. Naime, lažiranjem ocjena u sustav se uvode neispravne informacije. Ukoliko se informacije o ocjeni sadržaja koriste prilikom rada sustava, kvaliteta usluge može patiti zbog lažnih ocjena.

[2] Barclays-De La Rue predstavlja jedan od prvih sustav za automatiziranu isplatu novca. Preteča je današnjih modernih bankomata, a glavni razvojni inženjer bio je John Shepherd-Barron.

[3] Prema glavnom razvojnom inženjeru John Shepherd-Barron, njegova supruga nije mogla zapamtiti šest nasumičnih znamenki te se zato skratio PIN na četiri znamenke. Ovo ukazuje na probleme prilikom korištenja lozinki za autentifikaciju. Više detalja dano je u poglavlju 3. i 4.

# 3. Rukovanje lozinkama

Kako je opisano u prethodnom poglavlju, metoda autentifikacije korisnika lozinkom ima nekoliko nedostataka. Korisnici i sustavi moraju na siguran način rukovati lozinkama kako bi ih zaštitili od zloćudnih korisnika. Drugim riječima, mora se osigurati tajnost lozinki kroz čitav sustav.

Tajnost se u moderno doba ne smatra zadovoljavajućom metodom zaštite informacija. Ovaj trend se nabolje očituje u kriptografiji. Prije nastanka današnjih otvorenih kriptografskih algoritama, organizacije su razvijale vlastite ili koristile vlasničke algoritme. Ti algoritmi su često bili matematički vrlo jednostavni i nisu pružali veliku razinu zaštite u usporedbi s današnjim algoritmima. Osnova vlasničkih algoritama bila je tajnost. Naime, smatralo se da ukoliko napadač ne zna kako algoritam radi, neće ga moći probiti. Bruce Schneier[4] [4] ovakvo razmišljanje uspoređuje s tajnim društvima ili sektama. Na primjer, uzmimo da postoji tajno društvo koje svoje članove identificira pomoću tajne riječi ili algoritma. Radi jednostavnosti, pretpostavimo kako su tajna riječ i algoritam dovoljno jednostavni da se mogu zapamtiti i reproducirati u bilo koje doba[5]. Kada vođa društva odluči sazvati sastanak šalje šifriranu poruku svim svojim članovima. Članovi mogu pročitati poruku zato što znaju tajni algoritam za šifriranje. Prilikom dolaska na sastanak članovi izriču tajnu riječ kako bi dokazali da su zaista članovi. Ukoliko neki član odluči napustiti tajno društvo ili se pridružiti konkurentnom društvu, nastaje sigurnosni rizik. Kako član poznaje tajni algoritam i riječ može dolaziti na sastanke i prisluškivati komunikaciju s ostalim članovima. Dodatno, poznavanje, tih tajni može presresti poruke koje vođa društva šalje ostalima i zamijeniti ih s lažnim porukama. Stoga, tajno društvo mora promijeniti svoju tajnu riječ i algoritam te ponoviti to svaki put kada neki član napusti društvo. Ovakav pristup ne osigurava odgovarajuću razinu zaštite. Postalo je jasno da se tajnošću neće postići zadovoljavajuća zaštita informacija. Moderna kriptologija napredovala je do tolike mjere da tajnost algoritama nije imala smisla. Tijekom osamdesetih i devedesetih godina prošloga stoljeća kriptografija se počela razvijati u novom smjeru. Naime, kriptografski algoritmi postali su javni. Svatko je mogao vidjeti kako funkcioniraju te ih samostalno ocijeniti, komentirati ili nadopuniti. Ovim pokretom, vlasnički kriptografski algoritmi su nestali s tržišta. Danas gotovo niti jedna organizacija ne koristi vlasničke algoritme, već se oslanja na otvorene i javno provjerene kriptografske algoritme. Time je tajnost u potpunosti napustila područje kriptografskih algoritama.

Iz opisanog razloga se autentifikacija lozinki smatra iznimno nepovoljnom metodom autentifikacije. Autentičnost korisnika se zasniva na samo jednom podatku, a integritet tog podatka ovisi o njegovoj tajnosti. Kako je uočeno u kriptografiji, tajnost nije odgovarajuća metoda zaštite. Dodatno, kod autentifikacije korisnika postoji nekoliko mogućih ranjivosti koje se mogu iskoristiti za otuđivanje identiteta. U općem slučaju, krajnje točke su korisnik i sustav. Utjecaj korisnika na lozinke analizira se u poglavlju 3.1., a utjecaj sustava se opisuje u poglavlju 3.2.

## *3.1. Odabir lozinke*

Odabir lozinke smatra se najvažnijim korakom u osiguravanju vlastitog identiteta na Internetu. Upravo iz ovog razloga smatra se kako su korisnici sustava prvi neprijatelji. Bruce Schneier smatra kako prosječan korisnik ne može ili neće niti pokušati zapamtiti dovoljno složene lozinke kako bi osigurao vlastiti identitet. Neovisno o niskoj razini sigurnosti koje lozinke pružaju, korisnici su oni koji mogu tu razinu dodatno spustiti. Razna istraživanja su pokazala kako korisnici uspješno zaobilaze sigurnosne politike namijenjene poboljšanju lozinki. Na primjer, mnoge organizacije provode sigurnosnu politiku kojom se svakog korisnika prisiljava da promijeni lozinku svaki mjesec[6]. U takvim okolnostima korisnici često zapisuju lozinke na papirima kako ih ne bi zaboravili. Također, često imaju samo dvije različite lozinke koje onda koriste naizmjenično svaki put kada ih se traži da promijene lozinku.

[4] Bruce Schneier je međunarodno poznati kriptolog i stručnjak za informatičku sigurnost. Autor je jedne od najpoznatijih knjiga na području kriptografije, *Applied Cryptography*. Dodatno, autor je brojnih znanstvenih doprinosa na području moderne kriptografije.

[5] Ovo svojstvo ne utječe na snagu mehanizma autentifikacije. Da su tajna riječ ili algoritam složeniji i dalje bi bili ranjivi na iste napade kao što se opisuje u nastavku.

[6] Ovisno o primjeni i informacijskom sustavu, vremenski razmak može varirati.

Neki informacijski sustavi koriste lozinke koje se sastoje isključivo od brojeva. Na primjer, PIN lozinke kod kreditnih i SIM (engl. *Subscriber Identity Module*) kartica. Zbog skupa tehničkih i ekonomskih razloga, PIN lozinke se najčešće sastoje od samo četiri znamenke. Kod odabira vlastite PIN lozinke preporuča se izbjegavanje vlastitog datuma rođenja ili datum rođenja članova obitelji. Kako je pokazano u poglavlju 10., takve lozinke se lako pogađaju. Informacije o datumu rođenja su obično lako dostupne te ih napadač može iskoristiti kako bi pogodio PIN lozinku drugog korisnika. Više o nedostatcima PIN lozinki može se pronaći u dodatnoj literaturi pod [6].

Istraživanja pokazuju kako sigurnost kod korisnika nije prioritet te da se autentifikacija lozinkom smatra smetnjom. Iako se s vremenom sve više i više podiže svijest prosječnog korisnika o sigurnosnim prijetnjama na Internetu, neki korisnici se i dalje odupiru promjenama. Više informacija o ovom problemu može se pronaći u dodatnoj literaturi pod [2]. Velik broj istraživanja potvrđuje kako korisnici preferiraju lozinke iz skupa popularnih i lako predvidivih znakovnih nizova. Ova pristranost lošim lozinkama je analizirana u radovima poput [8] i [9].

- **Duljina** – najvažnije svojstvo kvalitetnih lozinki je njihova duljina. Što je lozinka dulja, to ju je teže pogoditi. Ukoliko je lozinka kratka, moći će se lakoćom pogoditi metodama opisanim u poglavlju 4.3. Na primjer, lozinke koje imaju manje od 5 znakova smatraju se iznimno lošim. Preporuča se korištenje osam ili više znakova prilikom odabira vlastitih lozinki.
- **Složenost** – osim duljine lozinke, na vrijeme koje je potrebno za pogađanje lozinki najviše utječe korištena abeceda. Abeceda predstavlja korišteni skup znakova iz kojeg se stvara lozinka. Što je ovaj skup veći, raste mogući broj kombinacija. Preporuča se korištenje velikih i malih slova, znamenki te posebnih znakova kao što su interpunkcije, zagrade i drugi znakovi.
- **Raznolikost** – preporuča se korištenje zasebnih lozinki za svaki korisnički račun. Uporaba istih lozinki bitno utječe na sigurnost korisničkog identiteta. Ukoliko zlćudni korisnik uspje otuđiti lozinku koja se ponavlja, olakšava se ovladavanje drugih računa.
- **Česta promjena** – ukoliko se radi o iznimno povjerljivim korisničkim računima, preporuča se mijenjanje vlastite lozinke nekoliko puta godišnje. Promjena lozinki je dobar način otežavanja uobičajenih napada na lozinke. No, korisnici se često odupiru ovakvim sigurnosnim politikama te ovaj pristup obično postiže suprotan učinak. Korisnici namjerno biraju lozinke koje su prethodno koristili ili biraju lozinke koje se lako pamte i pogađaju. Ukoliko se koristi ova metoda, preporuča se uporaba kvalitetnih lozinki koje zadovoljavaju prethodno odabrane kriterije.

## 3.2. Pohrana lozinki

Autentifikacija korisnika lozinkom podrazumijeva njezinu pohranu na sustavu koji obavlja autentifikaciju. Odnosno, sustav mora imati neki oblik lozinke kojime će potvrditi da se radi o legitimnom korisniku. U općem slučaj postoje dvije metode pohrane lozinki. Moguće je lozinke pohraniti u izvornom obliku ili ih šifrirati jednosmjernim algoritmom stvaranjem sažetka (engl. *Hash function*). Ukoliko se lozinka pohranjuje u izvornom obliku, sustav prilikom autentifikacije treba samo usporediti jesu li unesena i pohranjena vrijednost identične. Dodatna prednost ovog oblika pohrane je da se u slučaju kada korisnik zaboravi lozinku ona lako može poslati korisniku putem elektroničke pošte. No, ovo samo po sebi predstavlja potencijalnu ranjivost. Ukoliko zlćudni korisnik uspije dobiti pristup korisnikovoj elektroničkoj pošti, moći će očitati poruku s lozinkom. Iako jednostavna za implementaciju, ova metoda pohrane lozinki je iznimno loša. Naime, ukoliko zlćudni korisnik ostvari pristup bazi podataka, može izravno pročitati lozinke svih korisnika te im ukrasti identitet. Ovaj pristup je izrazito osjetljiv na napade iznutra. Na primjer, ukoliko zlćudni administrator odluči otuđiti identitete svojih korisnika treba ih samo pročitati iz baze. Korisnici često koriste iste lozinke za više sustava. Popis stvarno korištenih lozinki može napadačima koristiti za izvođenje napada na druge sustave. Neovisno o primjeni sustava, lozinke korisnika se nikada ne bi trebale čuvati u izvornom obliku.

Drugi oblik pohrane lozinki podrazumijeva njihovo šifriranje. Postoje različite metode sigurne pohrane lozinki njihovim šifriranjem. No, sve one uključuju uporabu jednosmjernih funkcija za

šifriranje. Samo ime označava kako se radi o jednosmjernoj operaciji. Naime, nakon šifriranja dobiva se sažetak lozinke koji jedinstveno identificira samo tu lozinku. Dodatno, iz sažetka nije moguće rekonstruirati izvornu lozinku. Najpopularnije lozinke za izradu sažetaka su MD5 (engl. *Message-Digest 5*) i SHA (engl. *Secure Hash Algorithm*) algoritmi. MD5 se danas smatra nesigurnim algoritmom, a za izradu sažetaka predlaže se korištenje SHA algoritma koji je trenutno siguran. Prije nekoliko godina uočene su kolizije kod MD5 algoritma. Dodatno, zbog sve jačih računalnih resursa uporaba 128 bita za reprezentaciju sažetka nije dovoljna. Takva veličina sažetka postaje sve jednostavnija za pogađanje obzirom na porast u performansama računala. Više o nedostatcima MD5 algoritma može se pronaći u dodatnoj literaturi pod [21]. Opširnije objašnjenje jednosmjernih funkcija za stvaranje sažetaka može se pronaći u dodatnoj literaturi pod [4].

Kako bi se lozinke zaštitile prilikom pohrane, umjesto njezinog stvarnog oblika pohranjuje se sažetak lozinke. Prilikom prijave stvara se sažetak lozinke koju je korisnik unio te se uspoređuje sa sažetkom koji je pohranjen u bazi. Budući da su funkcije za stvaranje sažetaka jednosmjerne, zloćudni korisnici neće moći na jednostavan način otkriti lozinku korisnika. Nedostatak ovog pristupa je što lozinku nije moguće rekonstruirati u slučaju zaboravljanja. Sustav mora korisnicima omogućiti stvaranje nove lozinke čak i onda kada oni zaborave staru lozinku. Ovo se obično postiže porukama elektroničke pošte ili putem telefona. No, niti ovaj pristup nije neprobojan. Iako se lozinke ne mogu jednostavno iščitati iz baze, postoje napredne metode pogađanja. Uporabom rječnika s unaprijed izračunatim sažetcima (engl. *Rainbow table*), moguće je ubrzati postupak pogađanja. Za svaku riječ iz rječnika (objašnjeno u poglavlju 4.3.2.) proizvodi se sažetak. Kada napadač želi otkriti stvarnu vrijednost sažetka, može ju usporediti sa sažetcima riječi iz rječnika. Jednostavnom usporedbom napadač može otkriti o kojoj lozinki se radi ukoliko se ona nalazi u rječniku.

Kako bi se ovaj postupak otežao, uvodi se novi mehanizam pohrane lozinki. Prije stvaranja sažetka, korisnikova lozinka se spaja s nasumičnom vrijednošću. Ova vrijednost se naziva *salt*. Obično se dodaje na početak lozinke te se iz dobivenog niza stvara sažetak. Nasumična vrijednost se također pohranjuje u bazi. Ukoliko zloćudni korisnik dobije pristup bazi podataka i *salt* vrijednosti, ne može na jednostavan način otkriti lozinku. *Salt* vrijednost, sama po sebi nije tajna. Jedina korist te nasumične vrijednosti je što napadač mora iznova izračunati sažetke za sve riječi u svom rječniku koristeći *salt*. Obzirom da su rječnici izrazito veliki te postupak izračunavanja sažetka računalno zahtijevan, računanje novih sažetaka za sve riječi može trajati i do nekoliko dana ili čak tjedana.

# 4. Napadi na lozinke

Uporaba lozinki smatra se najraširenijom metodom za autentifikaciju korisnika. Obzirom na ovakvu raširenost, postoji rastuća zabrinutost. Naime, lozinku je moguće otuđiti na niz različitih načina i time ukrasti tuđi identitet.

Prosječan korisnik služi se velikim brojem različitih usluga na Internetu. Na primjer, korisnik često koristi Internet bankarstvo, obavlja kupovinu putem weba, izdaje i pregledava oglase, provjerava vlastitu elektroničku poštu i drugo. Sve ove usluge zahtijevaju registraciju korisnika kako bi se ostvario pristup određenom sadržaju ili funkcionalnostima. Na primjer, web aplikacija za oglašavanje može svim korisnicima omogućiti pregledavanje oglasa. No, samo registrirani korisnici mogu postavljati oglase. Prilikom registracije korisnik obično mora odabrati lozinku za svoj korisnički račun. Obzirom na velik broj usluga na webu, korisnici su prisiljeni otvarati velik broj novih računa. Radi jednostavnijeg pamćenja korisničkih podataka, često se koriste iste lozinke za različite račune. Znanstveno istraživanje dostupno pod [1] analizira rukovanje lozinkama 49 studenata. Istraživanjem se htjelo vidjeti koliko različitih lozinki će studenti koristiti prilikom korištenja različitih usluga na webu. Pokazalo se kako se lozinke s vremenom sve više i više dupliciraju razmjerno s količinom korisničkih računa koje korisnik posjeduje. Druga slična istraživanja dolaze do istog zaključka. Istraživanje dostupno pod [7] analizira ista svojstva korisnika, ali na uzorku od pola milijuna ljudi.

Uporabom iste lozinke korisnici povećavaju vlastitu ranjivost svih svojih korisničkih računa. Ukoliko zlćudni korisnik uspije otkriti lozinku samo jednog računa, ima lozinku za sve ostale korisnikove račune. U nastavku ovog poglavlja se opisuju različite metode otuđivanja lozinke.

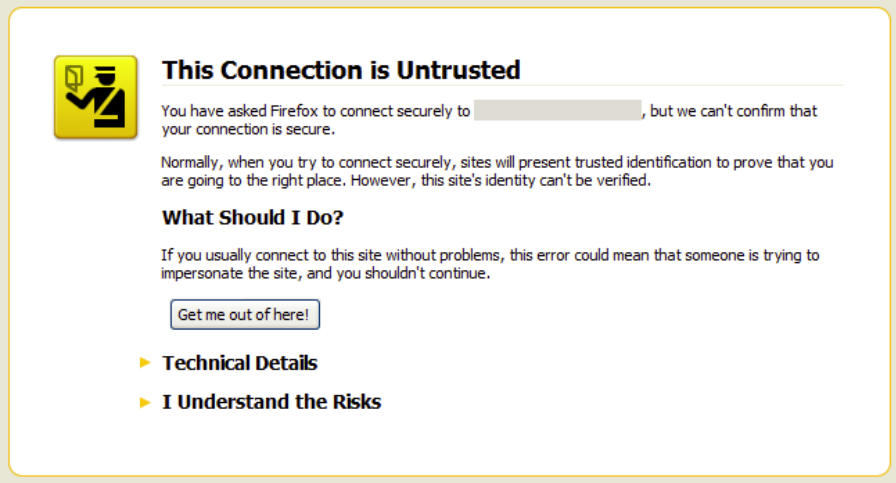
## *4.1. Napadi prisluškivanjem*

Napadi prisluškivanjem, poznati i kao MITM napadi (engl. *Man-in-the-middle attack*), predstavljaju jedan od osnovnih problema TCP/IP (engl. *Transmission Control Protoco/Internet Protocol*) protokola. Uporabom SSL/TLS (engl. *Secure Sockets Layer/Transport Layer Security*) protokola, ovaj problem se trebao riješiti. No, zbog raznih nedostataka napadi prisluškivanjem mogu se izvesti čak i onda kada se koristi SSL/TLS za zaštitu komunikacije. SSL sjednica omogućuje autentifikaciju poslužitelja korisniku koristeći PKI (engl. *Public-key infrastructure*) X509 certifikat. No, ovim modelom se ne omogućuje autentifikacija korisnika poslužitelju. Ovaj nedostatak omogućuje izvođenje napada prisluškivanjem, pod uvjetom da korisnik ne obraća pažnju na certifikat koji potvrđuje. Naime, prilikom uspostave SSL sjednice, preglednik korisnika će obično upozoriti korisnika da provjeri certifikat poslužitelja. Preglednik neće prikazati upozorenje korisniku samo onda ukoliko je certifikat potpisan od povjerljivog izdavača ili ako ga je korisnik već prethodno odobrio. Dodatno, preglednik će upozoriti korisnika ukoliko se ime na certifikatu razlikuje od DNS (engl. *Domain Name System*) zapisa poslužitelja. Slika 1. prikazuje upozorenje o nepoznatom poslužiteljskom certifikatu u web pregledniku Firefox.

Neovisno o tome radi li se o komunikaciji šifriranoj pomoću SSL/TLS protokola ili ne, napad prisluškivanjem se konceptualno izvodi na isti način. Napadač se mora korisnikovom računalu predstaviti kao posrednik između odredišnog poslužitelja. Ovo je moguće napraviti na niz načina. Na primjer, metodom trovanja ARP zahtijevima (engl. *ARP Poisoning*). ARP (engl. Address *Resolution Protocol*) protokol se koristi za razlučivanje adresa u lokalnoj mreži. Točnije, omogućuje se prevođenje MAC (engl. *Media Access Control*) adresa u IP (engl. *Internet Protocol*) adrese. Trovanjem ARP zapisa, napadač vlastitu MAC adresu povezuje s IP adresom drugog računala. Obično se odabire mrežni usmjernik jer preko njega ide sva komunikacija izvan lokalne mreže. Konkretan primjer izvođenja napada trovanjem ARP zahtijevima može se pronaći u dodatnoj literaturi pod [18].

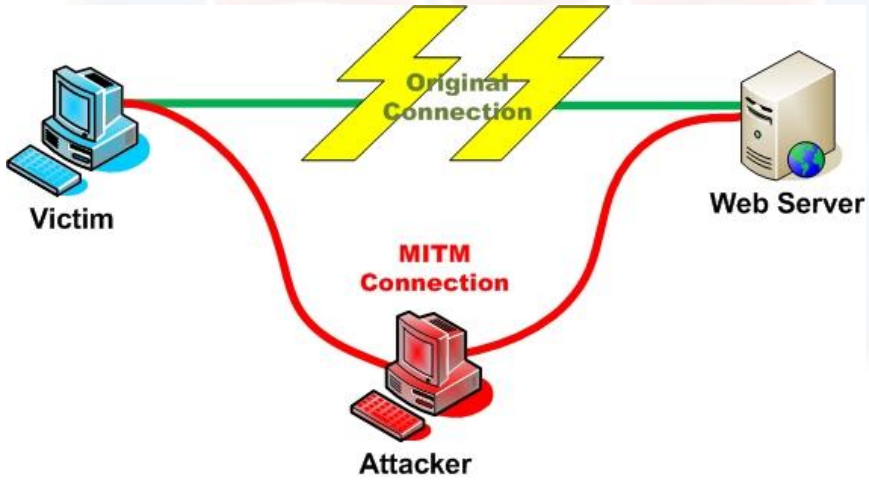
Ukoliko napadač uspješno postavi vlastito računalo kao posrednika, napad se nastavlja. Kada korisnik pošalje zahtijev prema poslužitelju, zahtijev se prvo prosljeđuje napadaču koji ga šalje do poslužitelja. Nakon obrade, poslužitelj šalje odgovor napadaču, koji odgovor prosljeđuje korisniku. Neovisno o tome je li promet šifriran ili ne, napadač može pregledavati i mijenjati podatke koje korisnik i poslužitelj mijenjaju. Samim time, napadač može vidjeti i lozinke kojima se korisnik autentificira poslužitelju. Slika 2. prikazuje skicu napada prisluškivanjem. Primjer

izvođenja napada prisluškivanjem može se pronaći u dodatnoj literaturi pod [17]. Više općenitih informacija o napadima prisluškivanjem može se pronaći u dodatnoj literaturi pod [15] i [16].




*Slika 1. Upozorenje o certifikatu u pregledniku Firefox*

*Izvor: www.blog.ivanristic.com*




*Slika 2. Skica napada prisluškivanjem*

*Izvor: www.owasp.org*

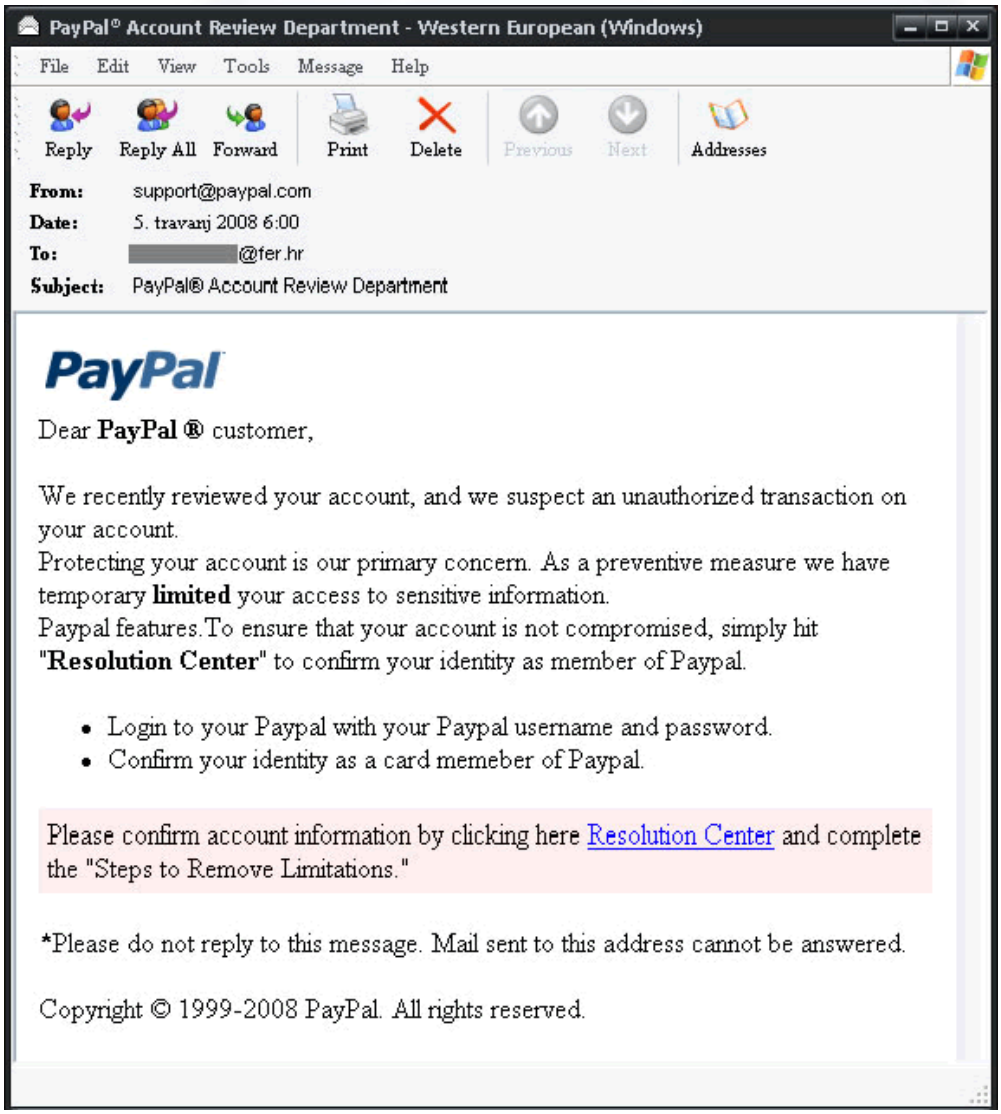
## 4.2. Napadi društvenim inženjeringom

Društveni inženjering je tehnika napada na informacijske sustave koja iskorištava ljudske ranjivosti. Cilj je dobiti povjerenje žrtve kako bi se otuđila određena informacija ili resurs. Iako društveni inženjering obuhvaća velik niz metoda kojima se iskorištavaju ljudske slabosti, u nastavku će se analizirati samo *phishing* napadi.

Kao najčešća metoda napada, *phishing* predstavlja najveću opasnost za korisnikov identitet. *Phishing* podrazumijeva skup aktivnosti kojima napadač pokušava legitimne korisnike navesti na

otkrivanje osobnih podataka. Na primjer, osobni podaci mogu biti lozinke korisničkog računa, broj ili PIN kreditne kartice te druge povjerljive informacije. Aktivnosti mogu obuhvaćati lažiranje poruka elektroničke pošte i web stranica. U općem slučaju, napadač će korisniku poslati lažnu obavijest koja naizgled dolazi od stvarnog pružatelja usluge. U sadržaju poruke će se nalaziti poveznica na lažiranu web stranicu. Slika 3. prikazuje primjer lažirane poruke elektroničke pošte. Problem kod ovakvog napada je što napadač može napraviti web stranicu koja je identična stvarnoj stranici usluge. Naime, HTML (engl. *HyperText Markup Language*) zapis svih web stranica je javno vidljiv te se lako kopira. No, jedan atribut web stranice nije moguće lažirati. Napadač ne može napraviti kopiju domene web stranice, već samo približnu kopiju. Na primjer, ukoliko legitimna adresa usluge glasi www.cis.hr, napadač bi mogao odabrati približnu adresu kao što je www.cis1.hr.

Lažirana stranica će korisnika navodit na prijavu s legitimnim računom. Kada korisnik unese svoje podatke, napadač će ih vidjeti i time ukrasti korisnikovu lozinku. Nakon toga, napad završava i napadač uspijeva otuđiti korisnikov identitet. Ovisno o složenosti lažirane stranice, korisnik se preusmjerava na legitimnu web stranicu. Kako bi smanjili sumnju i spriječili otkrivanje lažirane stranice što je dulje moguće, napadač može implementirati dodatne funkcionalnosti na lažiranoj stranici. Na primjer, prilikom preusmjeravanja korisnika na ispravnu stranicu šalju se uneseni korisnički podatci kako bi se spriječilo ponovno učitavanje forme za prijavu. Na ovaj način korisnik nije svjestan da je prethodna stranica bila lažirana. Više informacija o ovim oblicima napada moguće je pronaći u dodatnoj literaturi pod [19] i [20].




***Slika 3. Primjer phishing poruke***

*Izvor: os2.zemris.fer.hr*

## 4.3. Napadi pogađanjem

Najčešća metoda napada na lozinke predstavlja pogađanje. Kako je opisano u poglavlju 3.1., korisnici često zanemaruju važnost odabira kvalitetne lozinke. Oni često odabiru lozinke kako bi ih što lakše zapamtili ili lozinke koje već koriste. Tako odabrane lozinke se lako pogađaju, a u nastavku ovog poglavlja se opisuju metode kojima se postiže otkrivanje lozinki. Ove metode se obično koristi kada nije moguće iskoristiti druge slabosti ili ranjivosti u sustavu koji je zadužen za zaštitu ili pohranu lozinki. Najvažnija mjera učinkovitosti je vrijeme. Neke od navedenih metoda jamče pronalazak lozinke. No, pronalazak je ovisan o vremenu koje je potrebno utrošiti za otkrivanje. Neke metode ne jamče pronalaženje lozinke, ali i kod takvih metoda je najvažnije vrijeme izvođenja napada. Pogađanje lozinke je igra vremenom. Ovisno o koristi koju napadač dobiva otkrivanjem lozinke, razlikuje se definicija prihvatljivog vremena. Ukoliko se lozinkom ostvaruje pristup važnim ili dragocjenim resursima, prihvatljivo je uložiti mjesece, pa čak i godine za njihovo probijanje.

### 4.3.1. Napad grubom silom

Napad grubom silom (engl. *Brute-force attack*) predstavlja metodu pogađanja lozinke kojime se isprobavaju sve moguće kombinacije lozinke dok se ona ne pronađe. Ova metoda pogađanja ima različite prednosti, ali i nedostatke. Iscrpljivanjem svih mogućih kombinacija jamči se da će napadač otkriti lozinku. No, ovisno o složenosti lozinke, vrijeme koje je potrebno za isprobavanje svih mogućih kombinacija možda nije prihvatljivo. Duljina lozinki je najvažniji faktor koji utječe na brzinu pogađanja. Vrijeme pogađanja raste eksponencijalno s povećanjem duljine lozinke. Napad grubom silom se koristi onda kada ne postoji niti jedan drugi način otkrivanja lozinke. Snaga algoritama za šifriranje podataka se često izražava vremenom koje je potrebno da se otkriju podaci ovakvim napadom.

Resursi koji su potrebni za izvođenje napada grubom silom rastu eksponencijalno s povećanjem veličine lozinke. Dakle, povećavanjem veličine lozinke dva puta potrebno je ostvariti četiri puta više operacija prilikom napada grubom silom. Današnji algoritmi za šifriranje podataka prelaze na sve veće duljine tajnih ključeva. Zastarjeli algoritmi za šifriranje kao što su DES (engl. *Data Encryption Standard*) koriste ključeve duljine 56 bita. Drugim riječima, postoje $2^{56}$ mogućih kombinacija koje je potrebno isprobati prilikom pogađanja. Iako je ova duljina i dalje prevelika za prosječno računalo, uporabom raspodijeljenih sustava pogađanje ovakvog broja kombinacija postaje moguće. Pogađanje lozinki je idealan zadatak za paralelna ili raspodijljena okruženja. Naime, prilikom raspoređivanja zadataka svaki proces dobiva određeni raspon znakova koje treba provjeriti. Prilikom izvođenja, procesi ne moraju međusobno komunicirati niti se usklađivati. Nakon što završe s obradom, procesi javljaju rezultat izvođenja glavnom procesu koji je zadužen za upravljanje.

Osim raspodijeljenih sustava, razvijaju se sklopovlja koja su pogodna za izvođenje napada grubom silom. Jedno od tih sklopovlja predstavljaju grafički procesori koji svojom snagom postavljaju sve veće i veće kriterije za duljine lozinki. Zahvaljujući širokoj dostupnosti i prihvatljivoj cijeni, smatraju se najpogodnijim sklopovljem za izvođenje napada grubom silom. Moderni grafički procesori sastoje se od velikog broja procesorskih jezgri koji ih čine pogodnijim za izvođenje paralelnih zadataka. Neki grafički procesori imaju i do 100 procesorskih jedinica, što ih čini znatno pogodnijih za izvođenje paralelnih operacija nego obični procesori. Tablica 1. prikazuje vremena koja su potrebna za pogađanje lozinki

metodom grube sile. Vrijednosti su obračunate za sustav koji može provjeriti 15 milijuna lozinki u sekundi[7].

Drugo sklopovlje predstavlja tehnologija FPGA (engl. *Field-Programmable Gate Array*). Pogodni su za izvođenje napada grubom silom zahvaljujući mogućnosti paraleliziranja zadataka. No, ističu se i energetskom učinkovitošću prilikom obavljanja složenih zadataka. Broj procesorskih jedinica u FPGA sklopovima mjeri se i u tisućama. Na primjer, COCACOBANA FPGA grozd koristi napajanje od 600W, a za određene algoritme postiže brzinu od 2.500 umreženih računala.

U slučaju kada se napad grubom silom može obavljati lokalno, bez pristupa Internetu, napadač može izvesti neograničeno puno pokušaja pogađanja. No, kada se postupak pogađanja šifri obavlja preko Interneta, postoje određene metode kojima se onemogućuje napad grubom silom. Na primjer, prilikom prijave korisnika na web aplikaciju, mogu se uvesti dodatne provjere kako bi se one mogućilo automatizirano slanje zahtijeva. Jedna od takvih provjera je CAPTCHA (engl. *Completely Automated Public Turing test to tell Computers and Humans Apart*). Korisnik prilikom prijave mora očitati određeni niz znakova sa slike. Pozadina slike je namjerno popunjena nasumičnim linijama kako bi se spriječilo računalno otkrivanje znakova na njoj. Odnosno, samo ljudski korisnik će moći ispravno odgovoriti na CAPTCHA provjeru. Time se praktički onemogućuje pogađanje lozinke napadom grube sile jer se vrijeme izvođenja drastično povećava. Dodatno, u sustavima koji zahtijevaju visoku razinu sigurnosti mogu se koristiti dodatni mehanizmi zaštite. Na primjer, nakon određenog broja pogrešnih pokušaja korisnikov račun ili IP adresa se blokiraju na određeno vrijeme. Slika 4. prikazuje primjer CAPTCHA provjere. U nekim primjenama, kao kod kreditnih kartica, pristup se trajno onemogućuje nakon određenog broja pogrešnih pokušaja. Više informacija o napadima grubom silom moguće je pronaći u dodatnoj literaturi pod [12], a poglavlje 5.3. opisuje alate za izvođenje ove metode pogađanja.


***Slika 4. Primjer CAPTCHA provjere***

***Izvor: simple.procoding.net***

| Duljina | Složenost abecede | Vrijeme pogađanja |
|---|---|---|
| 4 | a-z | 1 sekunda |
| 4 | a-z, A-Z, 0-9, posebni znakovi | 4.8 sekundi |
| 5 | a-z, A-Z | 25 sekundi |
| 6 | a-z, A-Z, 0-9 | 1 sat |
| 6 | a-z, A-Z, 0-9, posebni znakovi | 11 sati |
| 7 | a-z, A-Z, 0-9, posebni znakovi | 6 tjedana |
| 8 | a-z, A-Z, 0-9 | 5 mjeseci |
| 8 | a-z, A-Z, 0-9, posebni znakovi | 10 godina |
| 9 | a-z, A-Z, 0-9, posebni znakovi | 1000 godina |
| 10 | a-z, A-Z, 0-9 | 1700 godina |
| 10 | a-z, A-Z, 0-9, posebni znakovi | 91800 godina |

***Tablica 1. Vrijeme pogađanja lozinki***

[7] Uzeta je namjerno ovako velika snaga kako bi se pokazao utjecaj kvalitetne lozinke na mogućnost pogađanja. U stvarnosti se ovakav sustav postiže umreživanjem više snažnijih računala.

*Izvor: www.oraxcel.com/*

## 4.3.2. Napad rječnikom

U kriptoanalizi i informacijskoj sigurnosti, napad rječnikom označava tehniku pogađanja lozinki pretraživanjem najvjerojatnijih kombinacija znakovnih nizova. Za razliku od napada grubom silom, ne isprobavaju se sve moguće kombinacije. Osnovna razlika je uporaba unaprijed proizvedenog rječnika najvjerojatnijih lozinki. Točnije, rječnik predstavlja iscrpan popis riječi proizvoljne duljine koji je proizveden isključivo s ciljem bržeg pogađanja korisničkih lozinki. Napadi rječnikom su često uspješni jer mnogi korisnici često odabiru lozinke koje su kraće duljine[8] ili se lako predviđaju. Na primjer, često se koriste uobičajene riječi iz rječnika te im se dodaju brojevi vezani uz specifične datume[9]. Međutim, napadi uporabom ovakvih rječnika mogu se otežati dodavanjem nasumičnih znakova u sredini lozinke. Na primjer, ukoliko je naša lozinka *sigurnost233*[10], napad rječnikom može se spriječiti dodavanjem nasumičnog niza koji lozinku mijenja u *sigurnaeost233*.

Većina lozinki se odabire tako da ih korisnik što lakše može zapamtiti. Iako mnoge tvrtke danas provode sigurnosne politike koje korisnike prisiljavaju da odabiru snažne lozinke, oni ih i dalje stvaraju po vlastitim ukusima. Točnije, neovisno o tome koliko stroga pravila tvrtka postavlja, većina lozinki će biti odabrane kako bi se lakše zapamtile. Istraživanje dostupno pod [13] dokazuje kako se ljudski lako pamtljive lozinke mogu pogoditi korištenjem pametnih rječnika, neovisno o duljini lozinke. Pametni rječnici predstavljaju popis lozinki koje su odabrane različitim metodama strojnog učenja, odnosno, umjetnom inteligencijom. Istraživanje je rezultiralo stvaranjem algoritma koji koristi Markovljeve modele[11] kako bi stvorio pametne rječnike. Istraživači su algoritam provjerili nad stvarnom bazom korisničkih lozinki te uspjeli pogoditi 67% lozinki. Ovi rezultati dovode u pitanje uporabu lako pamtljivih lozinki kod osjetljivih korisničkih računa.

Uporaba FPGA sklopovlja koristi se i kod napada rječnikom. Zahvaljujući energetskoj učinkovitosti i velikoj procesorskoj moći, idealne su za paralelizaciju ovakvih zadataka. Istraživanje dostupno pod [14] opisuje FPGA sklopovlje koje radi na frekvencijama od 150 MHz, a omogućuje obradu 510 lozinki u sekundi.

[8] Na primjer, rijetko kada su dulje od 7 znakova.

[9] Kao što su datumi rođenja.

[10] Lozinka je loša jer se sastoji od riječi *sigurnost*, koja je sastavni dio hrvatskog rječnika. Dodavanjem brojeva na kraj povećava se snaga lozinke. No, kvalitetni i opsežni rječnici će predvidjeti ovakvo proširenje. Ukoliko napadač ima neke osnovne informacije o korisniku kojemu pripada lozinka, moći će rječnik prilagoditi toj osobi.

[11] Predstavlja matematički model za reprezentaciju stanja u sustavu. U svakom trenutku sustav može prijeći u neko novo stanje ili ostati u istom stanju. Zahvaljujući ovako općem opisu, moguće ga je primijeniti za velik broj različitih problema.

# 5. Alati za rukovanje lozinkama

Rukovanje lozinkama je iznimno složen i važan problem. Kako je opisano u prethodnim poglavljima, postoji više aspekata u rukovanju lozinkama. Osnovna svrha lozinke je autentifikacija korisnika. Iz tog razloga korisnik mora odabrati lozinku odgovarajuće složenosti kako bi se otežalo pogađanje. Kako se kvalitetne lozinke često sastoje od nasumičnih znakova, korisnicima se otežava njihovo pamćenje. U nastavku poglavlja se opisuju alati koji korisnicima olakšavaju rukovanje lozinkama.

## *5.1. Alati za odabir lozinke*

Odabir lozinke predstavlja prvi korak u rukovanju s lozinkama. Kvalitetna lozinka ima nekoliko svojstava. Ovisno o kvaliteti lozinke, korisnikove identitet će biti sigurniji. Kriteriji za odabir lozinke su opisani u poglavlju 3.1. Kako bi se korisnicima olakšao odabir lozinke, postoje mnogi alati koji predlažu lozinke ili ih ocjenjuju.

Alat Password Meter daje detaljnu ocjenu kvalitete lozinke. Svaki kriterij kvalitete je detaljno objašnjen. Password Meter je dostupan preko [22], a Slika 5. prikazuje primjer ocjene lozinke. Alat je potpuno besplatan te dostupan u obliku jednostavne i pregledne web aplikacije. Informacije o ocjeni lozinke su vidljive trenutno, a namijenjene su kako bi korisniku olakšao odabir kvalitetnije lozinke. Budući da trenutno ne postoji službeni sustav vrednovanja lozinki, alat Password Meter uvodi vlastiti sustav ocjenjivanja. U sustav ocjenjivanja ne ulazi predviđeno vrijeme pogađanja lozinke. Izostavljeno je kao jedan od kriterija jer vrijeme pogađanja lozinki ovisi i o sustavu koji se koristi za probijanje. Kriteriji koji odudaraju od uobičajenih alata za odabir lozinke čine broj ponavljanja znakova, sekvencijalni brojevi ili slova te uzastopna upotreba velikih i malih slova. Svi ovi kriteriji poboljšavaju snagu lozinke. No, ovaj popis ne predstavlja potpun skup kriterija. Password Meter daje subjektivnu ocjenu kvalitete lozinke obzirom na vlastiti sustav ocjenjivanja. Neke lozinke koje se smatraju vrlo sigurnim po procjeni ovog alata, možda se nalaze u rječnicima napadača.

Osim alata za ocjenu lozinki, postoje i alati za proizvodnju kvalitetnih lozinki. Jedan od najpoznatijih alata za proizvodnju lozinki na sustavima UNIX/Linux je pwgen. Alat proizvodi lozinke koje se lako pamte, dok su istovremeno sigurne i kvalitetne. Iako lako pamtljive lozinke nisu jednako kvalitetne kao potpuno nasumične lozinke (opisano u poglavlju 4.3.), pwgen osigurava najveću moguću kvalitetu za takve lozinke. Alat se može koristiti interaktivno ili u drugom alatu ili skripti. Odnosno, ponašanje alata ovisi o tome nalazi li se na standardnom izlazu naredbeni redak ili cjevovod u drugi program. Ukoliko se koristi interaktivno, pwgen će na ekranu prikazati velik broj lozinki odvojene razmakom te obrisati ekran nakon nekog vremena. Ovime se sprječava da zlćudni korisnici preko ramena korisnika ne vide proizvedenu lozinku. Kada se alat ne nalazi u interaktivnom načinu rada, ispisuje samo jednu lozinku. Ovime se olakšava njegova uporaba u skriptama i drugim alatima. Više informacija o ovom alatu može se pronaći u njegovim priručniku za korištenje alata, a inačica za operacijske sustave Windows nalazi se pod [23].

| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | pa$$word123!!! | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | ☐ | |
| Score: | 100% | |
| Complexity: | Very Strong | |

| Additions | | Type | Rate | Count | Bonus |
|---|---|---|---|---|---|
| ✱ | Number of Characters | Flat | +(n*4) | 14 | + 56 |
| ✕ | Uppercase Letters | Cond/Incr | +((len-n)*2) | 0 | 0 |
| ✱ | Lowercase Letters | Cond/Incr | +((len-n)*2) | 6 | + 16 |
| ✱ | Numbers | Cond | +(n*4) | 3 | + 12 |
| ✱ | Symbols | Flat | +(n*6) | 5 | + 30 |
| ✱ | Middle Numbers or Symbols | Flat | +(n*2) | 7 | + 14 |
| ✓ | Requirements | Flat | +(n*2) | 4 | + 8 |
| **Deductions** | | | | | |
| ✓ | Letters Only | Flat | -n | 0 | 0 |
| ✓ | Numbers Only | Flat | -n | 0 | 0 |
| ! | Repeat Characters (Case Insensitive) | Comp | - | 5 | - 3 |
| ✓ | Consecutive Uppercase Letters | Flat | -(n*2) | 0 | 0 |
| ! | Consecutive Lowercase Letters | Flat | -(n*2) | 4 | - 8 |
| ! | Consecutive Numbers | Flat | -(n*2) | 2 | - 4 |
| ✓ | Sequential Letters (3+) | Flat | -(n*3) | 0 | 0 |
| ! | Sequential Numbers (3+) | Flat | -(n*3) | 1 | - 3 |
| ✓ | Sequential Symbols (3+) | Flat | -(n*3) | 0 | 0 |

*Slika 5. Alat Password Meter*

*Izvor: www.passwordmeter.com*

## 5.2. Alati za pohranu lozinke

Kako bi lakše zapamtili podatke za prijavu, korisnici često odabiru iste lozinke za više različitih računa. Ovo značajno utječe na sigurnost korisnikovog identiteta. Naime, otuđivanjem korisnikove lozinke zloćudni korisnik može dobiti pristup svim ostalim računima korisnika. Kako bi se korisnicima olakšalo pamćenje lozinki razvijeni su posebni alati. Oni pohranjuju korisničke podatke na siguran način. Obično se koriste dobro poznati kriptografski algoritmi za šifriranje kao što su AES (engl. *Advanced Encryption Standard*), Twofish i drugi. Kako je kriptografija široko područje koje nadilazi opseg ovog dokumenta, pojedini algoritmi se ne opisuju. Bitno je napomenuti kako su korišteni kriptografski algoritmi provjereno sigurni i pružaju tajnost podataka. No, njihova moć također ovisi o odabranoj lozinki. Više informacije moguće je pronaći u dodatnoj literaturi pod [4].

Uporabom alata za pohranu lozinke održava se visoka kvaliteta pojedinih lozinki bez da ih korisnik zapisuje na dodatne papire koji se lako otuđuju. U nastavku se opisuju neki od takvih alata, a detaljnija usporedba i ocjena najpopularnijih alata se nalazi pod [3].

### 5.2.1. KeePass Password Safe

KeePass predstavlja jedan od najpopularnijih alata otvorenog koda za pohranu lozinki. Omogućuje pohranu svih korisničkih lozinki u jednu bazu podataka koja je zaključana tajnim ključem. Ovaj tajni ključ je poznat isključivo korisniku i mora se zapamtiti. No, pamćenje jednog tajnog ključa je jednostavnije nego pamtiti velik broj lozinki. Baza podataka se šifrira putem popularnih kriptografskih algoritama. Tajni ključ za pristup svim ostalim lozinkama se ne pohranjuje u izvornom obliku već se koristi sažetak (engl. *hash*) ključa napravljen pomoću algoritma SHA-256. Uporabom različitih transformacija nad tako pohranjenim sažetkom tajnog ključa bitno se otežava pogađanje lozinke (opisano u poglavlju 4.3). Dodatno, sve lozinke su šifrirane za vrijeme rada alata u memoriji. U slučaju kada operacijski sustav pohranjuje proces u privremenim datotekama na disku, one su i dalje šifrirane. Jedna od najznačajnijih funkcionalnosti alata predstavljaju mehanizmi za uređivanje pohranjenim lozinkama. Kada korisnik mijenja ili unosi lozinke u alat, te informacije nisu vidljive u memorijskom prostoru alata. Osim visoke razine sigurnosti, alat pruža dodatne funkcionalnosti. Na primjer, omogućuje proizvodnju kvalitetnih lozinki te proizvodnju pseudonasumičnih brojeva. Slika 6. prikazuje glavni izbornik alata KeePas. Više informacija o ovom alatu moguće je pronaći u dodatnoj literaturi pod [5].


*Slika 6. Glavni izbornik KeePass alata*

*Izvor: keepass.info*

## 5.3. Alati za otkrivanje lozinke

Korisnici često zaboravljaju vlastite lozinke pa ih žele rekonstruirati. Neki sustavi omogućuju rekonstrukciju lozinke različitim mehanizmima. No, omogućavanje rekonstrukcije i otkrivanja lozinke smatra se lošom sigurnosnom politikom. Ukoliko korisnik može otkriti zaboravljenu lozinku, može i zlćudni korisnik. Iz ovog razloga smatra se kako je otkrivanje lozinke vrlo kontroverzna tema. Mnogi se protive alatima koji omogućuju otkrivanje lozinke jer se ti isti alati mogu upotrijebiti za otuđivanje identiteta. Ovisno o sustavu, postoje različiti alati za otkrivanje lozinki. U nastavku poglavlja se razmatraju alati za otkrivanje lozinki na operacijskom sustavu Windows. Dodatno, analizira se uporaba alata za pogađanje lozinki.

### 5.3.1. Ophcrack

Ophcrack predstavlja alat za otkrivanje lozinki na operacijskim sustavima Windows. Namijenjen je korisnicima koji su zaboravili vlastite lozinke ili forenzičarima prilikom prikupljanja informacija. Naravno, može poslužiti bilo kome tko ima fizički pristup računalu pa tako i zlćudnim korisnicima. Naime, Ophcrack je alat koji se pokreće kao LiveCD. Nakon preuzimanja alata sa službenih stranica, potrebno ga je snimiti na CD (engl.

*Compact Disc*). Računalo na kojemu se nalazi ciljani sustav potrebno je staviti CD s alatom te osigurati pokretanje alata s medija. Alat je zasnovan na operacijskom sustavu Linux. Nakon nekog vremena, LiveCD inačica alata će se podići i automatski biti spremna za rad. Kada se jednom pokrene, Ophcrack će samostalno pronaći korisnike na sustavu i početi rekonstrukciju njihovih lozinki. Postupak je potpuno automatiziran, korisnik obično ne mora ništa dodatno raditi. Nakon obrade, alat prikazuje lozinke na zaslonu. Ophcrack je besplatan alat i radi bez dodatnih alata ili postavki, dovoljno je preuzeti LiveCD sa službene stranice. Zbog loše pohrane lozinki u sustavima Winsows inačice XP, alat otkriva korisničke lozinke u nekoliko minuta. Ukoliko se koristi za otkrivanje lozinke na inačicama Vista ili novije, koristi se napad rječnikom. Obzirom da su greške iz inačice XP popravljene u novijim inačicama, ne postoji efikasnija metoda otkrivanja lozinke od napada rječnikom. Alat Ophcrack ima neka ograničenja i nedostatke. Točnije, lozinke veće od 14 znakova nije moguće rekonstruirati. Zbog načina na koji se alat pokreće, korisnik mora preuzeti alat i snimiti ga na CD te pokrenuti u LiveCD načinu rada. Više o ovom alatu može se pronaći na službenim stranicama pod [24].

### 5.3.2. John the Ripper

John the Ripper je alat otvorenog koda namijenjen operacijskim sustavima UNIX/Linux. Zahvaljujući velikoj popularnosti koju je stekao na tim sustavima, prilagođen je za rad na ukupno 15 različitih platformi. Predstavlja jedan od najpopularnijih alata za provjeru i razbijanje lozinki. Njegova visoka funkcionalnosti dolazi iz činjenice da je stvoren uz pomoć velikog broja dopunskih alata. Zahvaljujući tome, moguće ga je upotrijebiti u gotovo svim scenarijima i načinima rada. Podržava pogađanje lozinki uporabom metode napada grubom silom i napada rječnikom (opisani u poglavlju 4.3.).

Prilikom napada rječnikom, alat samostalno radi određene permutacije i varijacije trenutne lozinke kako bi proširio rječnik prilikom izvođenja napada. Alat koristi višedretvenost kako bi paralelizirao postupak otkrivanja lozinki i time skratio vrijeme izvođenja. Dodatno, zahvaljujući velikoj zajednici korisnika, alat se često ažurira kako bi se osigurala najveća moguća pokrivenost podržanih algoritama. Trenutno postoje različiti moduli koji ubrzavaju vrijeme otkrivanja lozinke za najmodernije kriptografske algoritme. Na primjer, zahvaljujući raznim istraživanjima pronađene su tehnike koje ubrzavaju obradu DES šifrata te sažetke MD5 i SHA algoritmom. Dodatno, postoje razni dodatci koji ubrzavaju rad s popularnim AES algoritmom. Više informacija o ovom alatu moguće je naći na službenim stranicama pod [25].

# 6. Zaključak

Rukovanje lozinkama je zahtijevan zadatak. Zbog velike uloge lozinki u autentifikaciji korisnika, postoji velik pritisak na ispravno izvođenje cijelog procesa rukovanja. Samim time se stvara niz mogućih propusta koje zloćudni korisnik može upotrijebiti kako bi otkrio lozinku drugog korisnika. Autentifikacija lozinkom nije idealna metoda provjere identiteta korisnika. Vidljivo je da postoji niz mogućih nedostataka koje zloćudni korisnik može iskoristiti kako bi otuđio identitet drugog korisnika. Prvi nedostatak se odnosi na odabir same lozinke. Postoji velik broj istraživačkih radova koji ukazuju na različite nedostatke lozinki, posebice na njihov odabir. Naime, korisnici često ne mare za sigurnost vlastitih identiteta. Koriste što jednostavnije lozinke kako bi ih lakše zapamtili. Takve lozinke se lako mogu otkriti metodama pogađanja. Postoje različite metode pogađanja lozinki, a napadač ih bira obzirom na sustav i očekivano vrijeme koje je potrebno za obradu. Najopćenitija metoda napada je napad grubom silom. U ovom napadu, zloćudni korisnik pokušava sve moguće kombinacije znakova kako bi pronašao lozinku. Ukoliko postoji prevelik broj mogućih kombinacija, moguće je upotrijebiti metodu napada rječnikom. Ova metoda ne osigurava pronalazak lozinke, ali se izvodi znatno brže. Dodatno, posebnim algoritmima umjetne inteligencije moguće je stvoriti izrazito kvalitetne rječnike za napad. Čak i kod složenih lozinki korisnici često koriste određene fraze ili algoritme koje se lako pamte. Takve znakovni nizovi se obično lako pogađaju.

S druge strane, dugačke i složene lozinke se teško pamte te ih korisnici zapisuju na papir ili ih pak zaboravljaju. Iako se takve lozinke teško mogu pogoditi, zbog složenosti se često otkrivaju napadima socijalnim inženjeringom. Iskorištavanje ljudskih ranjivosti omogućuje zloćudnim korisnicima otuđivanje lozinki legitimnih korisnika. Kao najčešći oblik napada društvenim inženjeringom, *phishing* je najefikasnija metoda za otuđivanje korisnikovog identiteta. *Phishing* čini skup aktivnosti kojima napadač pokušava korisnike uvjeriti da otkriju svoje osobne podatke.

Zbog tako velike uloge u autentifikaciji korisnika, lozinkama je potrebno na ispravan način upravljati. Rukovanje lozinkama obuhvaća niz radnji. Točnije, rukovanje podrazumijeva odabir kvalitetne lozinke, njihovu sigurnu pohranu i reprodukciju prilikom autentifikacije. Unatoč brojnim nedostatcima, autentifikacija korisnika lozinkom je najčešći oblik provjere identiteta. Očekuje se da će se lozinke i dalje koristiti još neko vrijeme. Za većinu sustava je trošak prelaska na drugi oblik autentifikacije prevelik. No, zahvaljujući brojnim napredcima na području autentifikacije očekuje se razvoj prikladnijih metoda provjere identiteta korisnika.

# 7. Leksikon pojmova

**AES (Advanced Encryption Standar)**

Kriptografski standard zasnovan na algoritmima sa simetričnim ključem, što znači da svaka strana u komunikaciji mora imati tajni ključ kako bi pročitala i poslala poruku. Standardom se opisuju tri blokovske šifre AES-128, AES-192 i AES-256. Svaki koriste blokove veličine 128 bitna, te ključeve veličine 128, 192 i 256 bita ovisno o algoritmu. Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael. - Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael - Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael.

http://www.quadibloc.com/crypto/co040401.htm

**ARP trovanje (Napad ARP trovanjem)**

ARP trovanje je napad na protokol ARP koji iskorištava nedovoljnu provjeru primljenih ARP odgovora. Slanjem posebno oblikovanog ARP odgovora, napadač može prisluškivati mrežni promet, izvesti DoS (eng. Denial of Service) ili MITM (eng. man-in-the-middle) napad.

http://www.watchguard.com/infocenter/editorial/135324.asp

**Autentikacija (Autentikacija je proces potvrđivanja identiteta podatka ili osobe)**

Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Najčešći primjeri su: uz korištenje kartice na bankomatu i upisivanje PIN-a, ili upisivanje (korisničkog) imena i zaporke.

http://searchsecurity.techtarget.com/definition/authentication

**Brute-force napad (Napad grubom silom)**

U kriptografiji napad grubom silom podrazumijeva strategiju pronalaska tajnog ključa ili lozinke koja se, u teoriji, može iskoristiti protiv svakog kriptografskog algoritma. Podrazumijeva sistematično isprobavanje svih mogućih ključeva ili lozinki dok se ne otkrije ispravan. U najgorem slučaju mora se proći kroz cijeli prostor ključeva.

http://www.computerhope.com/jargon/b/brutforc.htm

**CAPTCHA (Potpuno automatizirani Turingov test)**

Način metoda ovjere korisnika koja se koristi kada se želi osigurati da odgovor daje osoba a ne računalo. Proces ovjere uključuje jedno računalo poslužitelj koje traži korisnika da izvede jednostavnu provjeru. Sigurnost ovjere se temelji na pretpostavci da računalo nije u stanju u konačnom vremenu dati odgovor na zadanu provjeru.

http://webtrends.about.com/od/gettingstarted/f/spam_filter.htm

**DES (DES algoritam šifriranja)**

Vrlo popularan kriptografski standard, danas zamjenjen standardom AES. - Vrlo popularan kriptografski standard, danas zamjenjen standardom AES. Tajni ključ za šifriranje podataka sastoji se od 56 bita, što znaći da postoji ukupno 2^56 (više od 72,000,000,000,000,000) mogućih kombinacija. Za šifriranje poruke se koristi jedan od ključeva iz velikog broja kandidata. Algoritam je simetričan, što znaći da obadvije strane moraju imati tajni ključ kako bi mogli komunicirati. http://nvl.nist.gov/pub/nistpubs/sp958-lide/250-253.pdf

**DNS lažiranje (Lažiranje DNS priručne memorije)**

Kod napada lažiranjem DNS priručne memorije, napadač šalje posebno oblikovani DNS odgovor DNS poslužitelju s namjerom da lažna informacija u DNS odgovoru bude pohranjena u priručnu memoriju DNS poslužitelja. Ovisno o informaciji u lažnom DNS odgovoru, moguć je DoS (eng. Denial of Service) ili MITM (eng. man-in-the-middle) napad.

http://www.networkworld.com/news/tech/2008/102008-tech-update.html

**Društveni inženjering (Oblik zavaravanja osoba, umjesto računala)**

Društveni inženjering je oblik zavaravanja ljudi (a ne računala) kako bi obavili određene radnje ili izdali povjerljive informacije. Glavni cilj društvenog inženjeringa je prikupljanje informacija pomoću kojih će napadač lakše napasti informacijskih sustav ili ostvariti neovlašten pristup. http://searchsecurity.techtarget.com/definition/social-engineering

**HTTP (HyperText Transfer Protocol)**

Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtijeve na određenom mrežnom komunikacijskom priključku (tipično priljučak 80), čekajući da klijent inicira komunikaciju. - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtijeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju. http://hr.wikipedia.org/wiki/HTTP http://www.w3.org/Protocols/

**IP (Internet Protocol)**

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

**Kriptoanaliza (Umijeće razbijanja kriptografskih algoritama)**

Kriptoanaliza je znanstvena disciplina koja se bavi razbijanjem kriptografskih algoritama i šifri bez uporabe tajnih informacija kao što su ključ ili lozinka za šifriranje.

http://www.webopedia.com/TERM/C/cryptanalysis.html

**Kriptologija (Znanost o kriptiranju i dekriptiranju)**

Znanost koja obuhvaća pojmove kritpografije i kriptoanalize. Kriptografija je umješnost izmišljanja šifri, dok je kriptoanaliza umješnost njihova probijanja.

http://searchsecurity.techtarget.com/definition/cryptology

**MAC protokol ( Komunikacijski protokol za pristup mediju)**

Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao Medium Access Control protokol (protokol upravljanja pristupom mediju). On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.

http://ahyco.ffri.hr/ritehmreze/teme/mac.htm

**MD5 (Message-Digest 5 algoritam)**

Jedan od najpopularnijnih hashing algoritama, korišten za generiranje sažetaka poruka. Kao izlaz daje 128-bitni sažetak dobiven miješanjem 512-bitnih blokova. - Jedan od najpopularnijnih hashing algoritama, korišten za stvaranje sažetaka poruka. Kao izlaz daje 128-bitni sažetak dobiven miješanjem 512-bitnih blokova.

http://os2.zemris.fer.hr/algoritmi/hash/2002_fabris/index.htm

**MITM napad (Napad ubacivanjem posrednika)**

Napad na sigurnost pri kojem se zlonamjerni napadač umiješa u komunikaciju na način da se postavi između sugovornika te čita i izmjenjuje poruke. https://www.owasp.org/index.php/Man-in-the-middle_attack

**Napad rječnikom (Metoda pogađanja lozinke)**

U kriptografiji napad rječnikom predstavlja metodu pogađanja lozinke (ili tajnog ključa) isprobavanjem svih mogućih riječi iz određenog popisa koji se zove rječnik. Za razliku od napada grubom silom gdje se isprobavaju sve moguće kombinacije znakova, kod napada rječnikom isprobavaju se samo one kombinacije koje su statistički vjerojatnije.

http://www.webopedia.com/TERM/D/dictionary_attack.html

**Phishing (Napad na računalni sustav)**

Phishing je način prikupljanja nekih osjetljivih informacija, kao što su korisnička imena, lozinke i detalji kreditnih kartica, zamaskiravanjem u pouzdan entitet elektroničkih komunikacija. http://www.webopedia.com/TERM/P/phishing.html

**PKI (Infrastruktura javnih ključeva)**

PKI je sustav poslužitelja koji služi kao središnji autoritet koji povezuje javne ključeve s njihovim vlasnicima.
http://searchsecurity.techtarget.com/definition/PKI

**Salt (Salt dodatak)**

Kriptografska metoda koja se koristi za otežavanje napada rječnikom prilikom pogađanja lozinke. Nasumični niz bitova se dodaje lozinki prije nego što se proizvede sažetak (koristeći SHA1, MD5 ili neki drugi algoritam). Napadač mora postojeći rječnik ponovno proizvesti sa odgovarajućom salt vrijednošću (spomenuti nasumični niz bitova) što produljuje vrijeme potrebno za otkrivanje lozinke. http://www.ucertify.com/article/salt-cryptography.html

**SHA-1 (Secure Hash Algorithm)**

Jedan od najpopularnijnih hashing algoritama, korišten za generiranje sažetaka poruka. Kao izlaz daje 160-bitni sažetak dobiven miješanjem 512-bitnih blokova. - SHA-1 je jedan od najpopularnijih hashing algoritama, a služi za provjeru autentičnosti datoteka ili poruke prilikom prijenosa između pošiljaoca i primatelja. Koristi se za generiranje sažetaka poruka, kao izlaz daje 160-bitni sažetak dobiven miješanjem 512-bitnih blokova. SHA-1 je nasljednik MD-5 i koristi se u raznim sigurnosnim programima ili u protokolima kao što su: TLS, SSL, PGP, SSH, S/MIME, i IPsec. - SHA-1 je jedan od najpopularnijnih hashing algoritama, a služi za provjeru autentičnosti datoteka ili poruke prilikom prijenosa između pošiljaoca i primatelja. Koristi se za generiranje sažetaka poruka, kao izlaz daje 160-bitni sažetak dobiven miješanjem 512-bitnih blokova. . SHA-1 je nasljednik MD-5 i koristi se u raznim sigurnosnim programima ili u protokomima kao što su: TLS, SSL, PGP, SSH, S/MIME, i IPsec.
http://www.zemris.fer.hr/predmeti/os2/SHA-1.html

**SIM (Subscriber Identity Module)**

Čip tehnologija koja se koristi u mobilnim uređajima, a sadrži podatke i aplikacijsku logiku za pristup uslugama koje nudi davatelj. Sadrži jedinstveni identifikator IMSI koji identificira pretplatnika kojem pripada kartica. Koristi se u GSM mrežama, a danas je zamijenjena USIM i 3G karticama. http://www.tech-faq.com/subscriber-identity-module-sim.html

**SQL injection napad (Napad injekcijom SQL naredbe)**

Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika. - Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web programa bazi podataka. Na taj način moguće je ugroziti sigurnost web programa koji konstruira SQL upite iz podataka koje su unijeli korisnici.

https://www.owasp.org/index.php/SQL_Injection

**TCP (Transmission Control Protocol)**

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

http://www.webopedia.com/TERM/T/TCP.html

**TLS (Transport Layer Security)**

TLS je kriptografski protokol koji pruža sigurnu komunikaciju Internetom. TLS šifrira dijelove iznad transportnog sloja koristeći simetrične kriptografske ključeve i autentikacijski kod poruka. TLS je nasljednik SSL protokola.

http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

**Twofish (Simetrični kriptografski algoritam za šifriranje blokova podataka)**

Simetrični kriptografski algoritam za šifriranje blokova podataka veličine 128 bita. Koristi ključ veličine 256 bita, predstavlja pobpoljšanu verziju alogiritma Blowfish.

http://searchsecurity.techtarget.com/definition/Twofish

**Usmjeritelj (Uređaj koji usmjerava pakete između računalnih mreža)**

Usmjeritelji su uređaji koji imaju barem dva sučelja na različitim mrežama, a usmjeravaju pakete do njihovog odredišta. Na svom putu, paketi prolaze kroz nekoliko usmjeritelja, a svaki zasebno određuje put kojim će ga dalje slati. http://www.webopedia.com/TERM/R/router.html

# 8. Reference


[1] S. Gaw, E. W. Felten, Password Management Strategies for Online Accounts, Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA

[2] A. Adams, M. A. Sasse, Users are not the enemy, Commun. ACM, 42(12):40-46, 1999.

[3] Password Management Software Product Comparisons, 2012., http://password-management-software-review.toptenreviews.com/

[4] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Wiley, 1996.

[5] KeePass Password Safe, 2012., http://keepass.info/

[6] J. Bonneau, S. Preibusch, R. Anderson, A birthday present every eleven wallets? The security of customer-chosen banking PINs, Computer Laboratory University of Cambridge, 2012.

[7] D. Florencio, C. Herley, A large-scale study of web password habits, ACM Press, 2007.

[8] R. Morris and K. Thompson. Password security: a case history, ACM, 1979.

[9] E. Spafford. Observations on Reusable Password Choices, Proceedings of the 3rd USENIX Security Workshop, 1992.

[10] D. Todorov, Mechanics of User Identification and Authentication: Fundamentals of Identity Management, Auerbach Publications, 2007.

[11] Authentication in an Internet Banking Environment, http://www.ffiec.gov/pdf/authentication_guidance.pdf

[12] M. Shema, C. Davis , Anti-Hacker Tool Kit, Third Edition, Chapter 8, Password Cracking / Brute-Force Tools, McGraw-Hill Osborne Media, 2006.

[13] A. Narayanan, V. Shmatikov, Fast dictionary attacks on passwords using time-space tradeoff, Proceedings of the 12th ACM conference on Computer and communications security CCS 05, 2005.

[14] Y. S. Dandass, Using FPGAs to Parallelize Dictionary Attacks for Password Cracking, Proceedings of the 41st Annual Hawaii International Conference on System Sciences HICSS, 2008.

[15] P. Burkholder, SSL Man-in-the-Middle Attacks, SANS Institute InfoSec Reading Room, 2002.

[16] Y. Joshi, D. Das, S. Saha, Mitigating Man in the Middle Attack over Secure Sockets Layer, Internet Multimedia Services Architecture and Applications, 2009.

[17] K. Evans, Advanced Tutorial: Man in the Middle Attack Using SSL Strip – Our Definitive Guide, 2010.

[18] ARP Poisoning In Practice, 2012., http://www.infosecwriters.com/text_resources/pdf/ARP_Poisoning_In_Practice.pdf

[19] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer, Social phishing, Communications of the ACM, 2007.

[20] G. Ollmann, The Phishing Guide, Next Generation Security Software Ltd., 2008.

[21] D. Forte, The death of MD5, Network Security, 2009.

[22] The Password Meter, 2012., http://www.passwordmeter.com/

[23] PWGen for Windows - Generator of cryptographically-strong passwords, 2012., http://pwgen-win.sourceforge.net/

[24] Ophcrack alat, 2009., http://ophcrack.sourceforge.net/

[25] John the Ripper password cracker, 2012., http://www.openwall.com/john/