Iluzija privatnosti na internetu

Ilija Tešić
student prvog ciklusa studija
Elektrotehnički fakultet
Istočno Sarajevo, Bosna i Hercegovina
ilija.tesic@gmail.com

Sadržaj—**Cilj ovog rada je da pokaže koliko su obični korisnici računara i interneta, zbog svojih ili tuđih grešaka, svakodnevno izloženi opasnostima koje se tiču sigurnosti i privatnosti njihovih podataka. Pomenute su neke metode pomoću kojih može biti narušena privatnost i sigurnost korisnika, kao i neki česti propusti samih korisnika kojih mnogi nisu ni svjesni. Takođe su pomenute neke moguće metode zaštite od najčešćih uzroka narušene privatnosti i sigurnosti korisnika na internetu.**

Ključne riječi-privatnost korisnika; sigurnost podataka; zaštita privatnosti i sigurnosti

I. UVOD

Potpune privatnosti na Internetu nema. U svakom trenutku veliki broj zainteresovanih strana sakuplja podatke o „običnim ljudima“. Sakupljaju se lični podaci o stvarnim ljudima, njihova imena, adrese, brojevi telefona, sakupljaju se podaci o njihovim navikama na internetu, proizvodima koje kupuju, stranicama koje posjećuju, kao i podaci o navikama iz stvarnog života. Ovu veliku količinu podataka neki sakupljaju zbog zaštite državne bezbjednosti, neki da preciznije plasiraju marketinšku kampanju za svoj proizvod, a neki zbog lične koristi ili zadovoljstva. Koji god razlozi bili, narušavanje nečije privatnosti ne može i ne treba biti opravdano. Svijest prosječnog korisnika računara o narušavanju sopstvene sigurnosti i privatnosti nije ni približna stvarnoj situaciji. Osnovna greška prosječnog korisnika računara je pretpostavka da on nema šta da krije i da samim tim nije interesantan ljudima koji bi mogli da iskoriste njegove sigurnosne propuste i da naruše njegovu privatnost. Druga velika greška koju prosječan korisnik pravi je što ima apsolutno povjerenje kompanijama kojima daje svoje lične podatke. To povjerenje kod korisnika stvara iluziju potpune privatnosti i sigurnosti sistema koji koristi pa ni ne preduzima dodatne mjere da bi se zaštitio nego samo konzumira uslugu koja mu je ponuđena u osnovnom obliku, bez ličnih prilagođenja iste. Čak i onaj mali broj ljudi koji su donekle zabrinuti za svoju privatnost i trude se da je na bilo koji način zaštite, veoma često prave velike sigurnosne propuste. Oni tih propusta možda nisu ni svjesni, ali zlonamjerni napadač itekako jeste, i veoma lako ih može iskoristiti i time narušiti sigurnost i privatnost korisnika. Ako bi svaki korisnik znao da je prosječnom poznavaocu računara potrebno od 15 do 30 minuta da uđe u čitav njegov virtuelni život, koji se poklapa sa stvarnim životom u sve većoj mjeri, mnogo bi više bio zabrinut za sopstvenu sigurnost i uložio bi mnogo više truda da je zaštiti.

II. PERCEPCIJA PRIVATNOSTI

Mnogi korisnici žive u iluziji da je njihova privatnost u njihovim rukama i da su svi podaci koje su oni stavili na internet vidljivi samo onima za koje su namjenjeni. Mnogi nisu ni svjesni da bilo koji sajt na internetu može da vidi njihovu lokaciju pomoću IP adrese, sa kog su sajta došli, i mnoge druge informacije, koje korisnik nije eksplicitno dao. Velike internet kompanije svakodnevno skupljaju ogromne količine podataka o svojim korisnicima, bilo da su korisnici svjesni toga ili ne. Pamte se lični podaci korisnika, njegove navike, istorija korištenja određenog servisa ili usluge, obično radi unapređenja proizvoda i pružanja bolje i optimizovanije usluge. Neke kompanije skupljaju podatke o svojim korisnicima isključivo u marketinške svrhe (*Facebook*), da bi im plasirali odgovarajuću reklamu ili proizvod koji bi mogao da ih zanima, ili te podatke dalje prosleđuju drugim kompanijama. Ugovor o uslovima korištenja EULA (*End-User License Agreement*), koji je korisnik dužan da prihvati da bi koristio bilo koji softverski proizvod, određuje, između ostalog, na koji način će informacije o njemu biti korištene, i u koje svrhe. Ti ugovori su obično predugi i napisani nekim stručnim jezikom koji je nerazumljiv većini korisnika, tako da je mali broj ljudi koji to čitaju prije nego sto prihvate navedene uslove. Ugovori o uslovima korištenja su prečesto komplikovani sa jednim razlogom, da daju dobar izgovor velikim kompanijama za mnoge propuste koje imaju nenamjerno ili pak namjerno, sa ciljem iskorištenja korisničkih podataka u neke svrhe na koje korisnici inače ne bi pristali. Velike korporacije koriste svoju poziciju i uticaj na tržištu da primoraju korisnike da se dobrovoljno odreknu svoje privatnosti ako žele da koriste neke od njihovih usluga. Takva narušavanja privatnosti su obično opravdana unapređenjem usluga koje se pružaju korisniku i poboljšanje doživljaja određenog proizvoda. Konkretan primjer je Facebook aplikacija za Android platformu koja od korisnika traži pristup kameri uz mogućnost da u bilo kom trenutku, bez znanja korisnika, koristi kameru, fotografiše i snima video. Drugi primjer je Google-ov email servis Gmail koji od korisnika traži broj telefona da bi mogao nesmetano koristiti njihov servis. Ukoliko se koristi Google pretraživač dok je korisnik prijavljen na svoj Google nalog istorija cjelokupnog pretraživanja će biti zapamćena. Google pretražuje sve elektronske poruke svojih korisnika i na osnovu njih im prikazuje reklame, u zavisnosti od njihovih interesa. To su

samo neki od primjera očiglednog narušavanja privatnosti korisnika, na koja korisnici dobrovoljno i svjesno ali često i nesvjesno pristaju. Ako teoretski isključimo mogućnost da će korisnički podaci biti zloupotrebljeni od stane kompanije koja ih prikuplja, opasnost od narušavanja privatnosti i sigurnosti korisnika nije ni približno otklonjena. Nelegalan pristup korisničkim podacima koje je prikupila neka kompanija ili podacima koje korisnici svakodnevo dijele sa globalnom mrežom, od strane trećeg lica, predstavlja mnogo veći problem. Privatnost i sigurnost korisnika može biti narušena na nekoliko mjesta u cjelokupnom sistemu, ali to se najčešće radi na korisnikovom računaru i u lokalnoj mreži, te na serveru koji nudi određenu uslugu odnosno na internetu.

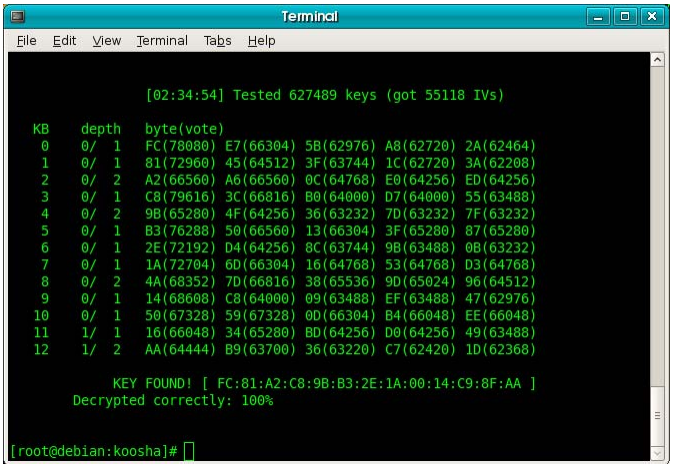
III. LOKALNA MREŽA

Lokalna mreža je često najranjivija tačka i u njoj se može doći do najveće količine podataka. Većina lokalnih mreža nema niakvu zaštitu i omogućuje napadaču da pristupi skoro svim komunikacijama unutar mreže i sa internetom. Lokalne mreže ipak imaju određen stepen zaštite pa napadač mora biti blizu da bi bio povezan na mrežu da bi koristeći sigurnosne propuste došao do osjetljivih podataka. Ako je u pitanju lokalna mreža koja je realizovana pomoću fizičkih veza, odnosno kablova, onda se podrazumjeva da napadač mora imati fizički pristup mrežnoj infrastrukturi. Ta činjenica pruža određen stepen sigurnosti, jer vrlo često napadač nema pristup mreži. Ukoliko je u pitanju kućna ili neka druga manja mreža, vlasnik ili administrator mreže zna ko je priključen na njegovu mrežu i može da predpostavi da li neki od korisnika mreže predstavlja prijetnju za sigurnost i privatnost drugih korisnika. Ako je u pitanju bežična mreža tu je sigurnost na mnogo manjem nivou. Bilo da je riječ o ličnoj kućnoj mreži ili nekoj javnoj bežičnoj mreži u nekom lokalu ili instituciji, bežična mreža je veoma često nikako ili nedovoljno zaštićena. Bilo koji korisnik mreže može veoma lako da „osluškuje“ mrežu i da pristupa kompletnom saobraćaju, uključujući osjetljive podatke kao što su lozinke, podaci o korisniku, bankovni računi i slično.

A. Wireless cracking

Bežične mreže koje su zaštićene WEP zaštitom ili MAC filterom su praktično otvorene. WEP (*Wireless Encryption Protocol*) je standard u kojem je nedugo nakon početka korištenja otkrivena slabost koja omogućava napadaču da vrlo lako razbije enkripciju i pristupi kompletnoj mreži. A MAC adresu je veoma lako maskirati i klonirati neku od adresa legitimnih korisnika mreže. Nedostaci WEP zaštite su uglavnom uzrokovani lošom implementacijom RC4 kriptoalgoritma i CRC-32 kontrolnih suma. [2] Šifrovanjem toka podataka, kratki ključ se proširuje na beskonačni, pseudoslučajni ključ. Pošiljalac podataka korištenjem tog ključa izvršava XOR operaciju nad otvorenim podacima i tako ih šifruje. Primalac podataka generiše isti pseudoslučajni ključ pomoću istog kratkog ključa i primjenom XOR operacije dešifruje šifrovane podatke. Napadač može iskoristiti ovaj nedostatak presretanjem saobraćaja, promjenom određenih bitova i vraćanjem nazad u mrežu. Ukoliko napadač presretne dva paketa sa istim pseudoslučajnim ključem i inicijalizujućim vektorom (*IV*) korištenjem statističkog napada može doći do originalnih podataka pa i do samog ključa. [3] Istraživanje zaštite bežičnih mreža u nekoliko stambenih blokova je pokazalo da su kućne bežične mreže veoma loše zaštićene i vrlo često bez ikakve zaštite. Od ukupno 86 skeniranih mreža, 28 je imalo WEP zaštitu a čak 7 je bilo bez ikakve zaštite. Ovi podaci su zabrinjavajući jer pokazuju koliko obični korisnici ne brinu o svojoj sigurnosti ili nisu ni svjesni kolikom su riziku izloženi. Neke kompanije koje se bave pružanjem usluga u BiH uz ADSL priključak daju bežične rutere koji su podešeni sa WEP zaštitom i najčešće matičnim brojem korisnika kao lozinkom. Administratorski podaci za ruter su fabrički i oni zavise od proizvođača, ali se vrlo lako dolazi do njih. Ovo veliki broj korisnika ne zna, a kompanija koja im pruža tu uslugu im ne govori kolikoj su opasnosti izloženi. WEP zaštita se probija za prosječno 10 minuta, zavisno od dužine ključa. Kao primjer, mreža koja je zaštićena WEP zaštitom biće testirana pomoću alata koji dolaze preinstalirani u Linux distribuciju BackTrack 5 [4]. Prije nego što se počne ikakvo testiranje na mreži korisno je maskirati MAC adresu wireless adaptera. To se postiže korištenjem programa *macchanger* koji maskira stvarnu MAC adresu nekom proizvoljnom. Najprije je potrebno prikupiti neke osnovne podatke o mreži koja se testira. Ti osnovni podaci su ESSID (*Extended Service Set Identification*), BSSID (*Basic Service Set Identification*), kanal i enkripcija. Da bi mrežni adapter bio u mogućnosti da vidi saobraćaj koji nije namjenjen njemu, uključujući i navedene podatke, mora da se prebaci u monitoring mod. Kada adapter radi u ovom modu on vidi sve mreže oko sebe i mnoge podatke o njima, pakete podataka koji emituje neka mreža u okolini, a takođe omogućava da se uspostavi komunikacija sa bilo kojom pronađenom mrežom. Paket *Aircrack-ng* sadrži nekoliko programa koji omogućavaju veoma lako pristupanje loše zaštićenim mrežama. Prebacivanje adaptera u monitoring mod se postiže korištenjem programa *airmon-ng* a program *airodump-ng* omogućava čitanje informacija o okolnim mrežama i prikupljanje paketa iz istih. *Airodump-ng* se podešava tako da prikuplja sve pakete vezane za mrežu koja se testira i snima ih u određanu datoteku. Da bi bilo moguće razbiti WEP zaštitu i time saznati ključ, potrebno je sakupiti određen broj paketa sa podacima u kojima se, u nezaštićenom dijelu, nalaze inicijalizujući vektori. Kada se sakupi dovoljan broj inicijalizujućih vektora moguće je doći do ključa kojim je saobraćaj šifrovan. Program *aircrack-ng* vrši statističke analize sakupljenih paketa i na taj način veoma brzo dolazi do korištenog ključa. Ukoliko na mrežu koja se testira nije spojen ni jedan klijent, program *aireplay-ng* omogućava da se ubace određeni paketi u komunikaciju te da se pristupna tačka (*Access Point*) prevari i da počne da generiše pakete sa inicijalizujućim vektorima koji će poslužiti za otkrivanje ključa. Kada napadač pristupi lokalnoj mreži postoji nekoliko načina da pristupi mnogin podacima određenog korisnika koje on dijeli sa mrežom. Napadač može nesmetano da osluškuje saobraćaj u mreži i da čita pakete koji vrlo često nose

informacije koje vlasnik ne bi svojevoljno objavio. Od tog trenutka napdač je u mogućnosti da vodi virtuelni život umjesto korisnika koji toga vjerovatno nije ni svjestan dok ne postane kasno. Najbolja zaštita za kućne bežične mreže koja danas postoji je WPA2. [5] Takođe je pametno isključiti WPS funkcionalnost čija ranjivost omogućava lako zaobilaženje bilo kakve zaštite na ruteru. Fabrička lozinka na ruteru treba da se promjeni i da se podesi firewall da bi se onemogućio neovlašten pristup ruteru iz lokalne mreže i sa interneta, a to veliki broj običnih korisnika ne zna. Kada napadač pristupi određenoj mreži postoji nekoliko načina da pristupi svim podacima određenog korisnika iste mreže. Veoma poznat napad je takozvani MITM (*Man In The Middle*), koji se zasniva na tome da napadač „stane“ u sredinu, između korisnika i sledeće tačke u mreži, odnosno da preusmjeri ciljani saobraćaj u mreži oponašajući gateway. Tada je napadač u mogućnosti da čita i filtrira sav saobraćaj koji ostvaruje žrtvin računar, da briše ili mjenja pakete. Ukoliko žrtvina veza sa internetom nije zaštićena, napadač je u mogućnosti da osluškuje cjelokupnu komunikaciju, sajt koji trenutno posjećuje, mail koji šalje, pa i lozinke sajtova na koje se žrtva prijavljuje.



Slika 1. Primjer razbijanja WEP ključa korištenjem aplikacije Aircrack-ng

B. ARP spoofing

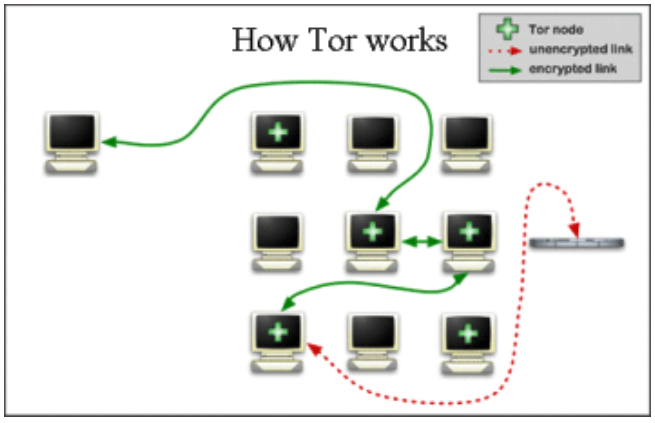
Ovaj napad je najčešći MITM napad i veoma se lako izvodi uz pomoć programa *Ettercap* na Linux platformi ili *Cain&Abel* na Windows platformi. Zasniva se na tome da napadač konstantno šalje lažni ARP (*Adress Resolution Protocol*) paket u mrežu. Cilj je da zatruje ARP keš ciljanog hosta i da poveže svoju MAC adresu sa IP adresom nekog drugog hosta u mreži, najčešće gateway-a. Na taj način, svaki paket koji se pošalje prema gateway-u prolazi kroz napadačev računar i dalje se prosljeđuje na pravi gateway. Napadač je u mogućnosti da pročita ili izmjeni sadržaj paketa prije nego što ga proslijedi na pravu IP adresu ili da prosto zaustavi saobraćaj.

C. DNS spoofing

DNS (*Domain Name System*) server povezuje IP adrese servera sa imenima koja su razumljiva ljudima. DNS spoofing je napad koji povezuje ime, odnosno ljudima razumljivu adresu, sa IP adresom koju napadač postavi i time žrtvu šalje na pogrešnu adresu. Ovaj napad se takođe vrlo lako izvodi pomoću programa *Ettercap* i omogućava izvođenje phishing napada, o kojima će biti riječi kasnije.

D. Session hijacking

Jedna vrlo zgodna tehnika, koja omogućava napadaču da preuzme žrtvin identitet na internetu, a da ne mora da zna ni korisničko ime ni lozinku, je session hijacking. Pošto svaki sajt čuva sesiju prijavljenog korisnika, a ID sesije se čuva u kolačiću (*Cookie*), napadač može koristiti žrtvine privilegije na nekom sajtu samo ako ukrade i iskoristi žrtvin kolačić. U nezaštićenim i loše zaštićenim komunikacijama je krađa kolačića izuzetno laka. Napadač prvo treba da pokrene MITM napad da bi bio u mogućnosti da čita podatke sa mreže. Ako je željeni saobraćaj preusmjeren preko napadača onda on uz pomoć programa *Wireshark* može da čita pakete i u njima da pronađe željeni kolačić. Kada pronađe žrtvin kolačić napadač može iskoristiti plug-in za Firefox *Cookies Manager* pomoću kojeg ubacuje žrtvin kolačić u svoj računar. To omogućava napadaču da koristi određen servis sa svim privilegijama koje ima žrtva sve dok se neko od njih dvoje ne odjavi. Postoji program koji se zove *Faceniff*, za Android platformu, koji ovaj posao mnogo olakšava. Dovoljno je samo da se napadač priključi na istu bežičnu mrežu na kojoj je žrtva i da ukrade sesije većine popularnih servisa, potpuno automatski. Pristup korisničkim podacima u mreži na navedene i mnoge druge načine nije uopste težak jer postoji veliki broj alata koji olakšavaju čitav proces. Postoji čak nekoliko distribucija Linux operativnog sistema koje u sebi imaju veliki broj alata za testiranje sigrunosti mreže i iskorištenje propusta u istoj. Jedna od poznatijih takvih Linux distribucija je već pomenuta Back Track. Svaki korisnik bi trebao biti svjestan mogućeg rizika dijeljenja prevelikog broja ličnih i osjetljivih informacija na internetu. Taj rizik je ogroman, a još je veći ukoliko korisnici nisu svjesni istog i prave sigurnosne propuste koji dodatno izlažu njihove podatke riziku. Postoje mnogobrojne sigurnosne mjere koje se mogu preduzeti sa ciljem zaštite privatnosti, koje u nekoj mjeri smanjuju rizik od nelegalnog narušavanja iste. Najbolja zaštita od prisluškivanja mreže je korištenje sigurne konekcije (*HTTPS*) sa sajtovima koji to omogućavaju. Na žalost veliki broj sajtova koji imaju sigurnu konekciju nemaju je na svim stranicama nego samo na stranicama za prijavljivanje. Takođe, većina sajtova ne primorava korisnika da koristi HTTPS nego korisnik mora ekplicitno navoditi protokol https:// kada unosi adresa stranice. Ovaj problem rješava plug-in za Firefox i Chrome koji se zove *HTTPS Everywhere* [6] koji forsira sigurnu konekciju na svakom sajtu koji to omogućava. Ako je potrebna veća sigurnost i privatnost onda je poželjno koristiti VPN (*Virtual Private Network*) ili aplikaciju Tor Browser [7], koja obezbjeđuje visok stepen privatnosti na internetu.



Slika 2. Primjer rada aplikacije Tor

IV. INTERNET

Pojavom interneta i naglim širenjem njegove popularnosti i upotrebe počele su da se mjenjanu navike ljudi i načini komunikacije i interakcije među njima. Internet je mnogo olakšao komunikaciju među ljudima, kao i dijeljenje i pristup mnogim informacijama koje su do tada bile privilegija manjeg dijela populacije. Većina ljudi nije ni svjesna koliko količinu podataka dijeli sa cijelim svijetom. Kada je u pitanju zaštita sopstvene sigurnosti i privatnosti oslanjaju se na druge ljude ili kompanije, koje bi trebale da zastupaju i štite njihove interese. Sve kompanije zastupaju sopstvene interese, koji su, na žalost, veoma često u suprotnosti sa željama i interesima većine korisnika. Neki korisnici prihvate činjenicu da im je privatnost narušena pravdajući se da nemaju šta da kriju, a drugi nemaju dovoljno znanja da se zaštite. Najveći uzrok narušene privatnosti i sigurnosti na internetu je nepažnja ili neznanje korisnika. Često svojom nepažnjom korisnik instalira neki maliciozni softver, facebook aplikaciju koja stupa u interakciju sa njegovim prijateljima i tako se širi, unese svoje podatke na phishing sajt koji izgleda kao neki drugi i tako svoje podatke preda napadaču… Postoji veliki broj grešaka koje obični korisnici prave na internetu i veliki broj opasnosti za sigurnost i privatnost. U ovom radu će biti opisane neke od najčešćih.

A. *Phishing*

Jedan od načina da se ukradu login podaci od nepažljivih korisnika je phishing stranica. [8] To je obično samo jedna web stranica koja izgleda isto kao neki legalni servis, kao što su facebook ili gmail, i traži od korisnika da se prijavi. Kada se korisnik prijavi na tu stranicu njegovi podaci se zabilježe u bazu podataka ili u neku datoteku, a korisnik se proslijedi na pravi sajt. Phishing stranice se prave vrlo lako. Potrebno je da se snimi HTML stranica zajedno sa pratećim CSS i JavaScript fajlovima, i da se postavi na neki host. Zatim se izmjeni link fajla kojem se prosleđuju podaci login forme i stavi se lokalni fajl koji će te podatke da snimi u bazu. Nakon uspješnog snimanja podataka nepažljivi korisnik se prosleđuje na pravu adresu. Korisnik vrlo često nije ni svjestan da je lično dao svoje podatke napadaču, koji ih može kasnije iskoristiti na razne načine. Phishing napad je vrlo lako izvesti u lokalnoj mreži, mjenjanjem DNS zapisa, ali na internetu je to malo teže. To se obično postiže preko email-a koji je navodno poslat od strane administracije određenog sajta i u kojem se od korisnika traži da se prijavi na link koji mu je poslat, a koji je u stvari phishing sajt. Ove napade je vrlo lako izbjeći ukoliko korisnik gleda da li je adresa sajta koji mu traži podatke legitimna. Svaki moderni internet pretraživač pokazuje na koju adresu vodi link, prije nego što korisnik klikne na njega. Ako link ne vodi na adresu za koju se predstavlja onda je vrlo moguće da se radi o phishing stranici.

B. *Maliciozni softver*

Kreatori ili distributeri malicioznog softvera koriste različite tehnike da privuku pažnju korisnika sa ciljem da istog prevare da pokrene ili na svoj računar instalira neki maliciozni kod. Time mogu omogućiti napadaču pristup svim svojim podacima pa i kompletnom sistemu. Postoje razni maliciozni programi, od onih kojima je jedina svrha da naprave štetu, bez nekog posebnog cilja, do onih kojima je cilj prikupljanje informacija o korisniku računara. Špijunski maliciozni programi skupljaju različite informacije, najčešće lozinke ili informacije o bankovnim računima, ali često skupljaju i navike korisnika na internetu ili prilikom korištenja računara. Najčešći primjeri malicioznog softvera koji se koristi u ove svrhe su keyloggeri. To su programi koji bilježe sve sto je uneseno sa tastature i prosleđuju trećem licu. Drugi programi čekaju samo lozinke ili brojeve kreditnih kartica, pa samo njih šalju napadaču. Postoje i oni programi koji na žrtvinom računaru otvore neki sigurnosni propust i time omoguće napadaču nesmetan pristup ili pak oni koji napadaču daju potpunu kontrolu nad žrtvinim računarom nakon što se intaliraju. Ovakvi programi se najčešće distribuiraju zajedno sa nekim zanimljivim sadržajem kao što su skrinsejveri ili setovi ikonica, koji su obično primamljivi neiskusnijim korisnicima računara. Malo iskusniji korisnici obično instaliraju neki maliciozni kod koji je spakovan u nelegalan softver. Zaštita od malicioznih programa se vrši dobrim antivirusnim alatom i povećanom opreznošću prilikom skidanja određenih tipova datoteka koje bi mogle da sadrže maliciozni kod. Takođe je veoma bitno izbjegavati nelegalan softver jer vrlo često sadrži ugrađene različite maliciozne kodove.

C. *Socijalne mreže*

Socijalne mreže su, nakon pojave interneta, najviše uzdrmale percepciju privatnosti osobe, u ovom slučaju korisnika interneta. Korisnici socijalnih mreža se sve više navikavaju da dijele svoje privatne podatke sa velikim brojem ljudi, a da toga nisu ni svjesni. Prihvatanjem nepoznatih osoba za prijatelje na socijalnim mrežama korisnik rizikuje da njegovi lični podaci, koje dijeli samo sa prijateljima, budu iskorišteni u različite svrhe. Privatni podaci kao što je email adresa mogu dospjeti na spam liste, podaci mogu biti proslijeđeni nekoj kompaniji koja će ih dalje iskoristiti u marketinške svrhe, kriminalci mogu iskoristiti te podatke da

saznaju više podataka o potencijalnoj žrtvi i slično. Posjećivanjem sumnjivih linkova na facebooku koji se zovu „Ko ti gleda profil“, „Promjeni boju facebooka“, „Dislike button“ i slično dovodi korisnika u rizik da se zarazi nekim malicioznim softverom, da izloži sve svoje podatke nekome ili da pokrene skriptu koja će spamovati sve njegove prijatelje i tako se dalje širiti. Svako ko je pročitao uslove korištenja Facebook-a zna da ne postoje slične mogućnosti i neće učiniti ovakvu grešku. Stavljanje fotografija na facebook ili druge servise, bez prethodne obrade, može da predstavlja veliko narušavanje privatnosti. Većina modernih foto aparata ili pametnih telefona uz fotografiju čuva Exif (*Exchangeable image file format*) tagove. Ovi tagovi mogu da sadrže mnoge informacije o uređaju kojim je fotografija napravljena, a ako uređaj ima GPS prijemnik, uz fotografiju su zabilježene i tačne koordinate lokacije na kojoj je fotografija napravljena. Mnogi korisnici pamte lozinke u pretraživaču ili e-mail klijentu, a to predstavlja veliki sigurnosni propust, jer su takve lozinke veoma slabo zaštićene. Postoje mnogo bolja rješenja koja omogućavaju da se lozinke čuvaju na sigurnom. Jedno od boljih rješenja je *Roboform*, a veoma dobre besplatne alternative su *KeePass* i *LastPass.* [9]

V. ZAKLJUČAK

Potupunu privatnost na internetu nije moguće ostvariti ali uz preduzimanje nekih mjera je moguće zadržati privatnost na prihvaljivom nivou. Veoma je bitno da korisnik kontroliše koje informicije dijeli sa internetom i da je svjestan toga. Sigurnost i zaštita privatnosti korisnika interneta u najvećoj mjeri zavisi od njih samih, od njihove edukacije i interesovanja da se zaštite. Ni jedan korisnik interneta ne želi da njegovi privatni podaci budu kompromitovani ali većina smatra da su sigurni, da nisu interesantni ili da se to njima nikako ne može dogoditi. Podizanje svijesti o važnosti, a istovremenoj izloženosti sopstvene privatnosti je prvi korak ka zaštiti iste.

LITERATURA

[1] http://thehackernews.com

[2] https://www.lugons.org/Uputstva/Opste/wep-cracking

[3] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[4] http://www.backtrack-linux.org/

[5] http://www.pcworld.com/article/130330/article.html

[6] https://www.eff.org/https-everywhere

[7] https://www.torproject.org/

[8] http://en.wikipedia.org/wiki/Phishing

[9] https://lastpass.com/

ABSTRACT

The aim of the paper is to show the amount in which regular Internet and computer users are exposed to all kinds of danger regarding their safety and privacy of their data on daily basis. Certain methods which can endanger privacy and safety of the users are mentioned, through some common mistakes many users are not even aware of. Also, certain methods of protection against most common causes of violated privacy and security of users are also mentioned.

ILLUSION OF PRIVACY ON THE INTERNET

Ilija Tešić