NASLOV SMISLITI

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Đaković Branko, Krčmarević Mladen,
Petrović Ana, Spasojević Đorđe
brankodjakovic08@gmail.com, mladenk@twodesperados.com,
pana.petrovic@gmail.com, djordje.spasojevic1996@gmail.com

3. april 2019

Sažetak

TODO napisati apstrakt (na kraju)
Ovde pišemo opis ukratko svega što smo radili. Na ovoj strani mora da bude naslov, ovaj apstrakt i sadržaj - SVE MORA DA STANE

Sadržaj

1 Uvod

U martu 2018. godine bivši zaposleni firme Kembridž Analitika (eng. *Cambridge Analytica*) je otkrio javnosti da je ova firma kupila od društvene mreže Fejsbuk privatne podatke barem 50 miliona korisnika bez njihove saglasnosti [6]. Podaci su prikupljeni uz pomoć aplikacije na Fejsbuku koja je bila namenjena prikupljanju podataka u akadamske svrhe. Međutim, ova aplikacija je, osim za one korisnike koji su na to pristali, uzimala podatke i svih njihovih prijatelja. Na osnovu ove velike količine podataka pravljeni su profili koji su služili za ciljano oglašavanje tokom predsedničke kampanje Donalda Trampa, kao i tokom perioda referenduma o članstvu Ujedinjenog Kraljevstva u Evropskoj uniji. Politika platforme Fejsbuk izričito zabranjuje prodaju ili korišćenje podataka korisnika u svrhe oglašavanja, što je učinilo ovaj slučaj jednim od najvećih slučaja kršenja privatnosti podataka na Internetu. Iako je Trampov kabinet porekao korišćenje ovih podataka u cilju pribavljanja glasača, ova vest je otvorila diskusije o tome ko i u kolikoj meri ima pristup našim podacima na Internetu.

Uzimajući u obzir da društvene mreže kao što je Instagram imaju milijardu korisnika na mesečnom nivou [8], količina privatnih podataka koje oni ostavljaju na ovoj platformi, a koji se kreću od uzrasta i lokacije, do interesovanja i hobija, je ogromna. Uz to, ove kompanije najčešće ne traže dozvolu da čuvaju podatke korisnika, ili kada je traže, to rade na netransparentan način. Povrh svega toga, pojedinci najčešće nisu ni svesni da sve što ostave na internetu, kasnije može biti iskorišćeno na načine koji bi u nekim slučajevima mogli da idu i na njihovu štetu.

TODO: U prvom odeljku bla bla, drugom, trećem .... bla bla bla (kad oderedimo struktru)

2 Šta je privatnost?

Pravo na privatnost se često smatra za jedno od najjasnijih i najvrednovanijih ljudskih prava, ali je privatnost koncept koji je teško definisati [25]. Jedan od problema u definisanju privatnosti leži u širini i neodređenosti ovog pojma, koji obuhvata zaštitu od ispitivanja i nedozvoljenih pretraga, kontrolu nad sopstvenim telom i privatnim informacijama, pa čak i pravo na slobodu mišljenja i govora. Ključni pojam u raspravama o tome šta je privatnost je koncept pristupa, bilo u kontekstu fizičke bliskosti nekoj osobi, bilo u kontekstu posedovanja znanja o toj osobi [22]. Pristup podrazumeva da jedna osoba ima pravo da ograniči ili zabrani pristup sebi u najširem smislu te reči, dok sa druge strane, on takođe podrazumeva i pravo drugih da ostvare pristup određenoj osobi. Upravo je sukob između ova dva ono u čemu leži suština privatnosti. Taj sukob se najviše reflektuje u suprotstavljanju privatnog i javnog, i onoga što bi trebalo da bude privatno i javno. Sa jedne strane, svaki pojedinac ima pravo da ograniči informacije o sebi koje su deo javnog znanja, međutim, preveliko ograničenje pristupa može dovesti do zloupotrebe i do loših posledica po društvo. Upravo zato privatnost predstavlja ključan problem slobode i demokratije [25]. Zbog toga ni ne čudi što se ogroman broj zakona i ustavnih prava odnosi upravo na privatnost. Pri tome, često se sprovođenje ovih zakona i odredbi dovodi u pitanje usled nedefinisanosti pojma. jedan od mogućih načina da definišemo privatnost je da je konceptualizujemo kao društveni ugovor koji dozvoljava pojedincu da ima određen nivo kontrole nad time ko i u kojoj meri ima pristup ne samo njegovim podacima, već i njegovom telu [22].

2.1 Privatnost na Internetu

Sa razvojem Interneta, problem shvatanja privatnosti se dodatno komplikuje i činjenica da veliku većinu dana provodimo na Internetu donosi nove aspekte problemu privatnosti. Svakog dana, korišćenjem interneta za različite potrebe, svaka osoba ostavlja za sobom elektronski trag svojih aktivnosti, koje mogu biti takve da otkrivaju i identitet pojedinca. Uz to, ostavljanje privatnih podataka može imati i određene prednosti, kao što su personalizovane poruke ili na primer, popusti, te je pojedinac suočen sa odlukom da li da propusti ove prednosti, ali očuva privatnost ili da ostavi svoje podatke na internetu, koji kasnije mogu biti zloupotrebljeni [19].

Povrh ovih informacija koje sami voljno ili nevoljno ostavljamo, danas su i informacije koje su deo javnih informacija (kao što su podaci o rođenju ili bračnom statusu pojedinca) kompjuterizovane, što ih čini daleko dostupnijim. Sa jedne strane, ovo ima svoju jasnu prednost, ali ovo podrazumeva da su i ove informacije daleko pristupačnije i onima kojima možda ne bismo želeli da budu [22]. Kapacitet prikupljanja podataka svakim danom sve više raste, što dovodi do mnogo lakšeg prepoznavanja pojedinca i korišćenja podataka o njemu u različite svrhe. Iako često mi sami odlučujemo da podelimo neke privatne informacije na internetu, često pojedinac nije ni svestan kada daje dozvolu nekoj privatnoj kompaniji da koristi njegove informacije i najčešće su pojedinci zbunjeni oko toga šta su tačno njihova prava na privatnost na internetu [19].

2.2 Percepcija privatnosti

Bitan aspekt razmatranja privatnosti na internetu je koncept percipirane privatnosti. Odnosno, problem privatnosti ne ostaje samo na tome da li ona postoji ili ne, već se širi i na to da li pojedinac vidi svoju privatnost kao problem i ako da, u kojoj meri. Percepcija privatnosti dalje određuje ponašanje pojedinca na internetu, utoliko što će pojedinci biti spremniji da koriste određene veb stranice ukoliko smatraju da je njihova privatnost zaštićena i obrnuto. Povrh toga, pokazuje se da, kada postoji uverenost da je privatnost pojedinca zaštićena, oni su spremni da je se vrlo lako odreknu, radi ispunjenja nekih potreba (kao što je na primer kupovina).

Percepciju privatnosti na internetu oblikuju različiti faktori, od kojih se neki vezuju za samog pojedinca, neki za same stranice koje korisnici posećuju, a neki za datu situaciju. Tako, shvatanje privatnosti može zavisiti od pola ili uzrasta, ali i obrazovanja pojedinca, prethodnog iskustva na internetu kao i od toga da li je osoba prethodno iskusila narušavanje privatnosti na internetu. Isto tako, to da li će pojedinac biti zabrinut za svoju privatnost na određenom sajtu može zavisiti od poznatosti brenda tog sajta, opaženog integriteta ili opaženog rizika tog sajta. Na kraju, to kako percipiramo trenutnu pretnju po privatnost može da zavisi i od toga kakvo je poklapanje između traženih informacija i usluge koju dobijamo i da li nam je ona smislena, ili od trenutne percepcije toga koliko je određeni podatak koji ostavljamo na internetu osetljive prirode [19]. Dakle, percepcija privatnosti na internetu je širok problem, koji je pod uticajem mnogih faktora, a koji povratno utiče na ponašanje svakog pojedinca na internetu, koje ponovo dovodi do narušavanja ili očuvanja privatnosti na internetu, te je stoga ovaj problem veoma relevantan za razumevanje privatnosti na internetu danas.

3 Država i privatnost(promeniti naslov)

Kada se govori o privatnosti na internetu, treba pomenuti i odnos države i državnih institucija prema privatnosti pojedinca. Kroz istoriju je bio čest slučaj da su države narušavale privatnost pojedinaca kako bi ostvarile određene interese, rešile probleme ili u borbi protiv terorizma. Slučajeva u kojima su američka administracija i službe kršile privatnost građana ima puno, od prodaje podataka službenika tajnih službi novinarima i privatnim detektivima, do ilegalnog prisluškivanja američkih i stranih državljana od strane FBI.

Neki od tih slučajeva su zloupotreba popisnih spiskova od strane američke vojske u Prvom i Drugom svetskom ratu, korišćenje policijskih dronova, kao i televizijske kamere zatvorenog kruga (eng. *closed-circuit television - CCTV*) - stanovnik Velike Britanije bude uhvaćen na kameri u proseku 300 puta dnevno [22, 23]. Prisluškivanje razgovora i postavljanje bubica je aktom američkog kongresa iz 1934. godine zabranjeno bez sudskog naloga. Međutim, FBI je nastavio to da radi ilegalno, čak i tokom Drugog svetskog rada uz dozvolu predsednika Ruzvelta [28]. Nakon rata, nacionalna sigurnosna agencija - NSA (eng. *National Security Agency*), FBI i druge bezbednosne službe nastavile su sa kršenjem zakona o privatnosti pojedinaca, što su kasnije i proširili na druge vidove komunikacije, pa i na internet.

3.1 Legalno narušavanje privatnosti na internetu

Usled pretnje po bezbednost SAD-a, donošeni su zakoni koji su službama dali veća ovlašćenja i dozvoljen im je upad u privatnost pojedinaca. U narednim odeljcima, biće navedeni neki zakoni kojima administracija dozvoljava narušavanje privatnosti na internetu.

3.1.1 Zakon o nadzoru stranih službi

Američka administracija je 1978. godine donela zakon o nadzoru stranih službi - FISA (eng. *Foreign Intelligence Surveillance Act*), kojim se dozvoljava tajni nadzor inostranih vlada i njihovih službi. Ovim zakonom američki predsednik je mogao da odobri elektronski nadzor stranih državljana na jednu godinu, pod uslovom da se time ne krši privatnost državljana Amerike. U suprotnom, administracija bi morala da dobije sudski nalog za prisluškivanje. Nakon što je 2013. godine Edvard Snouden, bivši zaposleni u NSA i FBI, obelodanio na hiljade tajnih dokumenata američkih tajnih službi, među kojima se našao i projekat PRISM, koji je dozvoljavao NSA pristup svim serverima i informacijama, pa čak i nadzor video poziva bez sudskog naloga [10]. U odeljku 3.2 detaljno će biti obrađen projekat PRISM.

3.1.2 Zakon o skladištenoj komunikaciji

Zakon o skladištenoj komunikaciji (eng. *Stored Communication Act*) predstavlja deo zakona o privatnosti pri elektronskoj komunikaciji (eng. *Electronic Communication Privacy Act*) iz 1986. godine i odnosi se na privatnost kolekcija elektronske pošte. Po ovom zakonu administraciji nije potreban sudski nalog kako bi od dobavljača internet usluga (eng. *Internet provider*) dobila mejlove starije od 180 dana. Problem sa ovim zakonom nastaje usled činjenice da sve više korisnika koriste klaudove internet provajdera, tako da sada nije jedina funkcija provajdera samo

prenos elektronske pošte, već sve više ljudi koriste servere internet provajdera da čuvaju stvari koje bi inače čuvali na privatnim računarima. Usled proširenja skladištenog prostora i funkcija provajderskih servera, skoro pedeset kompanija i organizacija koje smatraju da administracija ne bi smela da dobavlja privatne informacije korisnika sa klauda bez sudskog naloga, udružilo se u organizaciju pod nazivom Digital Due Process, kako bi zahtevali od administracije da unapredi ovaj zakon [24].

3.2 PRISM

Kada je Edvard Snouden u junu 2013. godine obelodanio na hiljade tajnih dokumenata NSA i FBI, među njima su se našli i dokumenti vezani za program PRISM, tajni program korišćen za nadzor aktivnosti na internetu. Program je započet 2007. godine i u narednih nekoliko godina sve velike kompanije su dale saglasnost za nadzor njihovih servera: Majkrosoft 2007., Jahu 2008., Gugl, Fejsbuk i PalTalk 2009., Jutjub 2010., Skajp i AOL 2011. i Epl 2012. godine. Sve navedene kompanije tvrdile su da nikada nisu čuli za PRISM i negirale bilo kakvo učešće u ovom programu [10].

Prema FISA zakonu, NSA je imala pravo da uz sudski nalog traži podatke o pojedincu od internet kompanije. Međutim, kako su u NSA smatrali da ceo taj proces predugo traje i da su potrebni nalozi za oba učesnika internet konverzacije, program PRISM je bio idealno rešenje tog problema. Agencija je imala direktan pristup serverima i mnogo veću slobodu u nadzoru i prikupljanju podataka, pa čak i praćenju poziva uživo preko interneta. NSA ovo i navodi u svojim dokumentima, gde ovaj program nazivaju "jednim od najvrednijih, jedinstvenih i najproduktivnijih pristupa koji NSA ima"[10]. U jednom od dokumenata koje je Snouden otkrio, može se videti tabela sa podacima koje je NSA mogla da prikuplja i prati pomoću PRISM programa. Mejlovi, razgovori, video pozivi, slike, čuvani podaci, video konferencije, istorije pretraživanja korisnika, samo su neki od podataka u koje je NSA imao uvid.

Pored sudskih naloga, FISA je predstavljao problem za NSA jer nisu mogli da prate komunikaciju između dva strana državljanina ukoliko ona ide preko servera koji se nalaze u SAD-u. Kako je većina servera velikih internet kompanija locirano u SAD-u, 2007. godine donet je zakon o zaštiti Amerike - PAA (eng. *Protect America Act*), koji je omogućio NSA da pokrene program PRISM i da zloubotrebljava ovlašćenja data ovim zakonom kako bi prikupljali i pratili komunikaciju na internetu [13]. Iako su sve kompanije umešane u ovaj program negirale bilo kakvu povezanost, kasnije su izlazile sa izveštajima gde navode da je američka administracija zahtevala od njih nadzor i pristup podacima svojih korisnika. U izveštaju kompanije Jahu, oni navode da im je administracija pretila i kaznom od 250 hiljada dolara godišnje ukoliko ne budu sarađivali [3].

4 Rizici za pojedinca na internetu (promeniti naslov)

TODO: uvod, uvod, uvod...

4.1 Društvene mreže

Oko dve trećine korisnika interneta koristi društvene mreže, te je samim tim problem privatnosti upravo na društvenim mrežama sve aktuelniji [15]. Mnoge društvene mreže nude različita podešavanja privatnosti, te se čini da je odluka o tome da li i u kojoj meri želi da podeli informacije o sebi ipak na korisniku. I zaista, istraživanja pokazuju da ljudi sve češće i više preduzimaju korake da ograniče pristup svojim privatnim informacijama. Tako je pokazano da je broj korisnika koji su obrisali komentare drugih ili skinuli svoje ime sa slika na kojima su označeni u porastu u odnosu na 2006. godinu. Više od polovine korisnika ima privatne profile, što ograničava broj ljudi koji mogu da vide njihov sadržaj samo na one koje oni odaberu. Pri tome, žene češće imaju privatne profile, što znači da su one više zabrinute za svoju privatnost u odnosu na muškarce.

Uzimajući u obzir da su najaktivniji korisnici društvenih mreža mladi ljudi, ne čudi što se veliki broj istraživanja fokusira upravo na mlade. Podaci pokazuju da su tinejdžeri 2012. godine bili daleko spremniji da podele informacije o sebi nego što su to bili tinejdžeri 2006. godine [16]. Tako 53 posto njih je podelilo svoju imejl adresu naspram njih 29 posto 2006. godine, dok je procenat onih koji su podelili svoj broj telefona na društvenim mrežama skočio sa 2 na 21 posto. Oko 60 procenata mladih ima privatne profile, dok je ponovo ovaj broj viši za žene nego za muškarce (70 posto naspram 50 posto). Uz to, mladi su samouvereni u svoju sposobnost da kontrolišu broj informacija koje drugi mogu da vide o njima.

Međutim, postavlja se pitanje da li zaista korisnik ima toliku kontrolu nad informacijama koje drugi vide o njemu, uprkos samouverenosti da to kontroliše. Istraživanja pokazuju da bez obzira na to koliko neko odluči da deli informacija, to šta njegovi prijatelji odluče da dele takođe igra značajnu ulogu [9]. Ne samo da prijatelji mogu nenamerno ili namerno podeliti informacije o pojedincu, već se pokazuje da čak iako neko nije na društvenim mrežama, karakteristike ljudi sa kojima se ta osoba druži mogu vrlo lako da predvide i njegove sopstvene karakteristike. Prema tome, sa pojavom društvenih mreža problem privatnosti je postao daleko difuzniji i nejasniji nego što je bio do tada i moguće je postaviti pitanje da li izostanak sa društvenih mreža uopšte garantuje privatnost i da li ona u digitalnom dobu uopšte postoji.

4.2 Krađa identiteta

Uzimajući u obzir prethodno pomenutu količinu informacija koju su ljudi spremni da podele na internetu, kao i činjenicu da ona raste, dolazi do porasta fenomena krađe identiteta. Krađa identiteta je u porastu poslednjih godina, s obzirom da svaki profil na društvenoj mreži pruža dovoljan broj informacija za prisvajanje nečijeg identiteta, makar površno. Spam mejlovi su jedan od popularnijih načina na koji je se uzimaju informacije o nekoj osobi, pa je tako slanje masovnih mejlova sa lažnim linkovima ka određenim sajtovima veoma često, te da postoji oko 30 ovakvih napada dnevno, koji potencijalno mogu da oštete hiljade ljudi [7]. Međutim, postoje i procesi koji su velikom većinom automatski, te samim tim veoma efikasni u dostizanju velikog broja ljudi, što može imati dalekosežne posledice [4]. Tako postoje simulacije koje demonstriraju koliko je lako klonirati nečiji profil i preuzeti njegov identitet, a zatim poslati zahteve drugim ljudima koji prihvatanjem postaju nove žrtve. Uz to, postoje i mogućnosti da se kloniranjem profila na jednoj mreži uspostavi lažni profil osobe na nekoj mreži na kojoj oni ni ne poseduju profil, a da se zatim taj profil

iskoristi da bi se kontaktirali stvarni prijatelji te osobe, na osnovu liste prijatelja sa mreže sa koje je profil ukraden. Ovo omogućava uverljivu simulaciju identiteta neke osobe, a lakoća sa kojom je moguće ovo izvršiti je zabrinjavajuća. Ipak, to nije najopasniji oblik krađe identiteta.

Kako napreduje tehnologija, tako se načini na koje je moguće ukrasti nečiji identitet usložnjavaju i pružaju više opcija za zloupotrebu. Jedna od takvih opcija je dipfejk (eng. *deepfake*) sadržaj i tehnologija. Korišćenje algoritama za mašinsko učenje i open source koda, postoji mogućnost da se manipuliše video sadržajem, tako da je moguće njegovo menjanje da sadrži lice bilo koje osobe [2]. S obzirom da većina korisnika ima veliku količinu svojih slika na internetu, ne čudi što je javni diskurs bogat raspravama o dipfejku, do te mere da postoji predlog zakona u Americi da se ova tehnologija zabrani. Dipfejk video zapisi otvaraju sasvim novo polje za krađu identiteta, koje nije tako lako prepoznati i čije je posledice teško ispraviti. Ovi video sadržaji bi tako mogli da prikazuju političke lidere ili druge značajne ličnosti kako govore ili rade bilo šta, što može imati izuzetno nepovoljne posledice po širu javnost. Iako se čini da je maliciozni potencijal ove tehnologije veliki, ipak ne postoji mnogo potencijalno opasnih sadržaja ove vrste [5]. Ipak, oni se koriste u svrhe sajber nasilja, što znači da ih ne treba ignorisati i da treba imati na umu da privatnost na internetu može biti narušena i na ovaj način, kao i da privatne informacije korisnika mogu biti zloupotrebljene u različite svrhe.

4.3 Kolačići

Prilikom upotrebe pretraživači veba na računar korisnika smeštaju kolačiće (eng. *cookies*) [1]. Kolačići su male tekstualne datoteke koje čuvaju informacije o veb sajtovima kao što su informacije o prijavi korisnika, sadržaj korpe prilikom kupovine, jezik i ostale informacije koje čine korišćenje interneta jednostavnijim. Kolačići se sastoje od tri dela: imena(koriste ga sajtovi da identifikuju kolačić), vrednosti(služi za prepoznavanje korisnika) i atributa. U zavisnosti od trajanja postoje sesijski kolačići koji bivaju izbrisani prilikom gašenja pretraživača i trajni kolačići koji imaju rok trajanja, te se čuvaju na računaru do isteka tog roka. U okviru trajnih, kolačići se dele na kolačiće prve strane i kolačiće treće strane. Kolačići prve strane se koriste samo od strane veb sajtova koji su ih napravili i prvenstveno se koriste za poboljšanje korisničkog iskustva. Kolačiće treće strane (nazivaju se i kolačići za praćenje) koriste sajtovi koji ih nisu napravili. To omogućava subjektima koji su napravili kolačić da dobiju informacije svaki put kada korisnik poseti neku stranicu na kojoj dati subjekti poseduju resurse. Obično je korisno da veb sajtovi pored sadržaja koji je napravio vlasnik koriste resurse drugih sajtova kako bi dodali određene funkcionalnosti. Najčešće su baš ti resursi oni koji vrše praćenje na internetu.

Najzastupljeniji resursi koji koriste kolačiće za praćenje su reklame, vidžeti (programčići/aplikacije) društvenih mreža kao što su "podeli" I "sviđa mi se" i veb analitike. Ako ne postoje, i kolačići prve i treće strane se prave prilikom učitavanja sajta, a ukoliko postoje šalju vlasniku kolačića. To znači da nije neophodno da se pritisne na reklamu ili dugme društvene mreže da bi vlasnik resursa dobio kolačić za praćenje, a time i informacije o sajtu koji je korisnik posetio a često i sajtu sa koga je došao do trenutnog. Informacije koje kolačići za praćenje mogu da čuvaju obuhvataju istoriju pretraživanja, kupovine, lokacije, informacije o uređajima, kada i gde je viđena prethodna reklama, linkovi na koje je korisnik kliknuo i slično.

Postoji više načina za zaštitu od kolačića. Jedan od načina je korišćenje pretraživača u privatnom režimu rada. Međutim to onemogućava i kolačiće prve strane koji mogu biti korisni. Drugi način koji omogućava da se isključe samo kolačići treće strane je da se obrišu kolačići, a zatim onemogući čuvanje kolačića u podešavanjima pretraživača.

4.3.1 Onlajn kupovina

U svetlu toga da je retko šta zapravo privatno na internetu, treba razmotriti i oblast kupovine na internetu, s obzirom da je ovo jedan od delova interneta gde je narušavanje privatnosti naročito neočigledno i netransparentno. Korišćenje kolačića omogućava sajtu da zapamti informacije o osobi (kao što su imena, šifre ili kreditne kartice), što ima svoje prednosti, ali istovremeno podrazumeva odricanje privatnosti zarad pogodnosti, što dovodi korisnika u nepovoljan položaj. Kako kolačići omogućavaju i drugim sajtovima pristup informacijama, tako korisnici mogu videti oglase koji su povezani sa njihovim prethodnim kupovinama, iako nisu pristali direktno da te informacije podele sa tim konkretnim sajtom. Sama praksa kolačića je do skoro bila implicitna, odnosno zahtevala je od korisnika da sam isključi opciju kolačića, umesto da privatnost bude pretpostavka od koje se polazi. Od skoro je ovaj problem i zakonski regulisan, te sada svi sajtovi moraju da obaveste korisnika da prikupljaju informacije o njima putem kolačića i moraju da dobiju pristanak samog korisnika da to urade. Međutim, uprkos ovoj praksi, kao i postojanju prakse stavljanja natpisa da je privatnost podataka zagarantovana, većina ispitanika to ne prepoznaje kao pozitivno i kao nešto što uliva sigurnost [27]. Naprotiv, korisnici često izveštavaju da im nisu jasne politike privatnosti, koje retko čitaju, kao ni načini na koje je njihova privatnost zagrantovana.

Podaci pokazuju da što je veće iskustvo sa kupovinom na internetu i internetom uopšte, to je percipirani rizik od gubljenja privatnosti manji i kupovina češća [20]. Međutim, uprkos tome, ljudi kao jednu od najvećih briga prilikom kupovina na internetu navode upravo brigu oko privatnosti. Dakle, bez obzira na izveštavanje o postojanju zabrinutosti pri kupovini na internetu, čini se da ona ne sprečava ljude da zapravo kupuju preko interneta.

Ipak, istraživanja pokazuju da ako se ispitanicima da procena privatnosti podataka nekih sajtova, oni će uvek birati one sa visokim nivoom procenjene privatnosti i čak bi potencijalno bili spremni da plate da im privatnost bude zagarantovana [27]. Implikacije ovih nalaza su da je ljudima stalo do privatnosti, ali najverovatnije ne razumeju kako da je obezbede. Prema tome, jedan od velikih problema kupovine na internetu i privatnosti na internetu uopšte jeste upravo činjenica da je ovaj koncept korisnicima nejasan i nedovoljno objašnjen, zbog čega treba tražiti nove načine da se svima obezbedi pre svega razumevanje prava na privatnost koje im je zagarantovano.

5 Zaštita privatnosti

TODO: uvod !

5.1 Enkripcija

Internet je otvoren sistem. Svi podaci se kroz više uređaja, deljenih konekcija, ili čak bežično šalju kako bi stigli do željene destinacije. Ovaj

sistem omogućava komunikaciju između uređaja koji mogu biti udaljeni više hiljada kilometara, ali zbog ključnog mehanizma koji to dozvoljava pravi i jedan od najvećih problema. Svaki uređaj koji se nalazi između početnog i krajnjeg odredišta može videti šta je poslato. Svaka elektronska pošta, ukucana lozinka i broj kreditne kartice mogu biti pročitani od strane nekoga u sredini. Da bi se ovo sprečilo koristi se enkripcija.

Enkripcija je mehanizam kojim se bilo kakva informacija šifruje, tj. prebacuje iz čitljivog oblika u naizgled nasumične karaktere, koji se uz pomoć odgovarajućeg ključa mogu vratiti u svoj prvobitan oblik [14]. U upotrebi je od pre više hiljada godina, kada je Cezar slao šifrovane poruke vojsci koje neprijatelj ne bi mogao da razume. Cezarova šifra (eng. *Caesar's cipher*) je prilično jednostavna i zasniva se na zameni svakog karaktera za karakter koji je pomeren u abecedi za nekoliko mesta. Jedina potrebna informacija za šifrovanje je ključ koji označava broj pozicija za koji je karakter pomeren, a za dešifrovanje primalac samo treba da iskoristi negativnu vrednost ključa. Ovu enkripciju bi bilo koji čovek mogao da dešifruje vrlo brzo, tako da nije primenljiva u domenu računara, ali daje osnovu za razumevanje kompleksnijih algoritama koji se koriste pri upotrebi veb pregledača, elektronske pošte ili prilikom onlajn kupovine.

Cezarova šifra primer je simetrične enkripcije. Simetrična enkripcija se koristi u situacijama kada već postoji siguran kanal za komunikaciju, te je potreban samo jedan ključ. Još jedan primer ove vrste enkripcije je AES (eng. *Advanced Encryption Standard*), koji se koristi kod virtuelnih privatnih mreža (o kojima će biti reči u odeljku 5.2), za enkripciju hard diska, kompresiju (WinZip, RAR), kod alata koji se koriste za čuvanje šifara i za enkripciju poruka koje se šalju putem društvenih mreža kao što je Fejsbuk. Do sada nije zabeležen uspešan napad na AES, ali to ne znači da je u potpunosti siguran. Postoje takozvani šide-channel"napadi (tajming ili elektromagnetni napadi koji) koji su bazirani na poznavanju informacija o fizičkom načinu implementacije algoritma, okruženju ili samom sistemu na kome se izvršava [18].

Na internetu se uglavnom koristi asimetrična enkripcija. Ona podrazumeva da svako ko učestvuje u komunikaciji ima svoj javni i privatni ključ, za razliku od simetrične. Par ključeva kod asimetrične enkripcije se generiše po matematičkim principima, tako da ako se nešto šifruje uz pomoć javnog ključa, može se dešifrovati privatnim i obrnuto. Javni ključ pojedinca je poznat svima, a privatni ključ zna i koristi samo osoba koja ga poseduje. Pri slanju poruke, pošiljalac je najpre šifruje sa javnim ključem primaoca, a zatim svojim privatnim ključem. Kada primalac dobije poruku, on je dešifruje uz pomoć javnog ključa pošiljaoca i nakon toga sopstvenim privatnim ključem. Ovim je obezbeđena komunikacija tako da niko sa strane ne može da pročita niti promeni prosleđenu poruku, a da se to ne detektuje. Najpopularniji primer asimetrične enkripcije je RSA (eng. *Rivest–Shamir–Adleman*) [12]. Ona se obično ne koristi za enkripciju čitavih poruka ili fajlova, već se koristi u kombinaciji sa drugim šemama enkripcije ili kao digitalni potpis za dokazivanje autentičnosti i integriteta poruke. Fajlovi se obično enkriptuju nekom simetričnom enkripcijom, a zatim se njihovi ključevi enkriptuju pomoću RSA. Pošto za razliku od AES, RSA može biti razbijena faktorizacijom celih brojeva, ključevi moraju biti duži. Nacionalni Institut za Standarde i Tehnologiju predlaže korišćenje ključa dužine 2048 bitova. RSA je prisutna kod pretraživača veba, imejlova, VPN usluga, četova i drugih komunikacionih kanala.

5.2 Virtuelne privatne mreže (VPN)

Virtuelne privatne mreže (eng. *virtual private network*) nastale su usled potrebe da se biznisi, organizacije, vlade i slični subjekti koji poseduju osetljive informacije zaštite od hakovanja i gubitka podataka u slučajevima kada je potrebno da im udaljeni korisnici ili satelitske kancelarije pristupe, kao i radi smanjenja telekomunikacionih troškova efikasnijim korišćenjem infrastrukture. VPN su privatne mreže koje rade preko deljene javne infrastrukture kao što je internet [26]. Virtuelna je zato što ne postoji odvojena fizička infrastruktura za datu mrežu, već koristi već postojeću javnu infrastrukturu. Privatna je zato što omogućava bezbednu upotrebu uz garanciju da će samo članovi mreže moći da vide poslate informacije [17]. VPN omogućavaju privatnost podataka korišćenjem sigurnosnih procedura(enkripcija) i protokola tuneliranja(IPsec, PPTP, L2TP). VPN napravi "tunel"između korsinika pri čemu se podaci enkriptuju na strani pošiljaoca, šalju kroz tunel i zatim dekriptuju na strani primaoca. Pored podataka mogu se kriptovati i polazna i završna adresa radi veće sigurnosti [11].

VPN "od lokacije do lokacije"(eng. *site-to-site*) je tip mreže koja omogućava uspostavljanje bezbedne komunikacije između više poslovnica na različitim lokacijama preko javne infrastrukture, i time se podaci sa jedne lokacije stavljaju na korišćenje zaposlenima na drugoj. Drugi osnovni tip ovih mreža je VPN za udaljen pristup (eng. *remote access VPN*), koja omogućava pojedincima da uspostave bezbednu vezu sa udaljenom mrežom i pristupe njenim resursima kao da su direktno povezani na dati server.

Iako prvobitno nisu bile namenjene za to, usled skorašnjih otkrića o velikim projektima za nadzor i ograničenja koje određene vlade nameću svojim građanima sve više raste upotreba VPN usluga za zaštitu privatnosti pojedinaca, zaštitu od cenzurisanja kao i za pristup sadržaju koji je geografski ograničen [21]. Još jedan od razloga za povećano korišćenje je porast upotrebe javnih mreža koje je prouzrokovano širenjem mobilne industrije. Ovo je dovelo do stvaranja uslova za napade kao što su krađa akreditiva, presretanje paketa i krađa sesija, što vodi do toga da neki korisnici koriste VPN za zaštitu svojih interakcija. Mnoge VPN usluge nude mogućnost izbora izlaznih tačaka tako da korisnici mogu da dobiju IP adrese u različitim državama.

Iako do nekog stepena VPN provajderi pružaju navedene usluge, dovodi se u pitanje njihova sposobnost da očuvaju anonimnost i privatnost. Privatnost se kod ovih mreža ne odnosi na privatnost krajnjih korisnika već na povezivanje više privatnih mreža. Zbog lakoće korišćenja, velikih performansi i jakog marketinga postoji velika privlačnost prema ovim mrežama, iako neinformisanost korisnika dovodi do problema.

5.2.1 Rizici za korisnike VPN

Iako veliki broj pružalaca VPN usluga tvrde da pružaju robusne i sigurne infrastrukture uz obezbeđivanje bezbedonsti korisnika tako što ne loguju podatke, ne postoje alati i istraživanja koji te tvrdnje proveravaju. Pored toga neki provajderi su poznati po tome što prodaju podatke korisnika i manipulišu saobraćajem. Takmičenje između provajdera zajedno sa nedostatkom objektivnih mera kvaliteta dovodi do zavarivanja klijenata. Usled nedostatka nezavisnih ocena VPN usluga korisnici su primorani da se o tome informišu sa blogova ili veb sajtova. Ti sajtovi su većinom podržani od strane VPN partnerskog marketinga i usluga, pa se od njihovih ocena ne može očekivati nepristrasnost. To se odnosi na neke

od najbolje rankiranih sajtova za ocenjivanje VPN usluga. Pored curenja saobraćaja zbog loše bezbednosti oko 10% VPN servisa presreću i/ili manipulišu saobraćajem stim što su mogući načini za nadziranje saobraćaja koji su teški da se otkriju. Takođe, VPN servisi obično obećavaju veliki broj različitih geografskih lokacija koje korisnici mogu da izaberu kao izlazne čvorove, ali oko 10% njih daje netačne informacije. Između 5 i 30 procenata tih čvorova nalazi se na potpuno drugim lokacijama od onih koje su predstavljene. Čak postoje provajderi koji tvrde da imaju lokacije u preko 190 država, a u stvarnosti se serveri nalaze u ne više od 10 centara podataka [21].

6 Zaključak

Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak.

Literatura

[1] D. Anon. How cookies track you around the web and how to stop them. 2018. on-line at: https://privacy.net/stop-cookies-tracking/.

[2] H. Baker. Making a 'deepfake': How creating our own synthetic video helped us learn to spot one. *Reuters*, 2019.

[3] R. Bell. Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case. *Yahoo Global Public Policy*, 2014.

[4] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. pages 551–560, 01 2009.

[5] R. Brandom. Deepfake propaganda is not a real problem. *The Verge*, 2019.

[6] C. Cadwalladr and E. Graham-Harrison. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 2018. on-line at: https://www.theguardian.com.

[7] N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell. Client-side defense against web-based identity theft. 01 2004.

[8] T. Clarke. 22+ Instagram Stats That Marketers Can't Ignore This Year. *Hootsuite*, 2019. on-line at: https://blog.hootsuite.com.

[9] D. Garcia. Leaking privacy and shadow profiles in online social networks. 2017.

[10] G. Greenwald and E. MacAskill. NSA Prism Program Taps In to User Data of Apple, Google and Others. *The Guardian*, 2013. on-line at: https://www.theguardian.com.

[11] K. Grewal, R. Kajal, and D. Saini. Virtual Private Network. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012. on-line at: www.ijarcsse.com.

[12] J. Lake. What is RSA encryption and how does it work? *comparitech*, 2018. on-line at: https://www.comparitech.com/blog/information-security/rsa-encryption/.

[13] T. B. Lee. How Congress unknowingly legalized PRISM in 2007. *The Washington Post*, 2013.

[14] N. Lord. What Is Data Encryption? Definition, Best Practices & More. *Digital Guardian*, 2019.

[15] M. Madden. Privacy management on social media sites. *Pew Research Center*, 2012.

[16] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton. Teens, Social Media, and Privacy. *Pew Research Center*, 2013.

[17] V. Marijanović. Virtuelne privatne mreže, 2011.

[18] J. Mason. Advanced Encryption Standard (AES). 2017. on-line at: https://thebestvpn.com/advanced-encryption-standard-aes/.

[19] R. Mekovec. Online privacy: overview and preliminary research. *Journal of Information and Organizational Sciences*, pages 195–209, 2010. on-line at: https://bib.irb.hr/datoteka/495673.JIOS2010.pdf.

[20] A. D. Miyazaki and A. Fernandez. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs*, 2005.

[21] V. Perta. A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients. 2015.

[22] M. J. Quinn. *Ethics for the Information Age*, chapter Information Privacy, Privacy And The Government, pages 227–314. Addison-Wesley Professional, Boston, 2014.

[23] J. Roth. Bloomberg in London to Study Security System, 2010. on-line at: https://abc.go.com/wabc.

[24] R. Singel. Google, Microsoft Push Feds to Fix Privacy Laws. *Wired*, 2010. on-line at: https://www.wired.com.

[25] D. J. Solove. *Understanding Privacy*, chapter Privacy: A Concept in Disarrey, pages 1–12. Harvard University Press, Cambridge, Massachusetts, 2008.

[26] W. T. Strayer. Privacy Issues in Virtual Private Networks. *Computer Communications*, 2004.

[27] J.Y. Tsai, S Egelman, L. Cranor, and A. Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, pages 254–268, 2011.

[28] D. Whitfield and S. Landau. *Privacy on the Line: The Politcs of Wiretapping and Encryption*. MIT Press, Cambridge, Massachusetts, 1998.