Privatnost na Internetu

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

27. mart 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 [2]. 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 [3] , 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 prvoj sekciji bla bla, drugoj, trecoj .... 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 [12]. 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 [9]. 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 [12]. 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 [9].

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 [7].

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 [9]. 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 [7].

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 [7]. 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 [9, 10]. 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 [14].Nakon rata, FBI, NSA 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 (eng. *Foreign Intelligence Surveillance Act - FISA*), 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. U ovaj tajni program su bile uključene sve velike kompanije, pa je tako NSA imao pristup serverima Majkrosofta, Jahua, Gugla, Fejsbuka, Jutjuba i Epla [4]. 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 [11].

3.2 PRISM

djoletov drugi deo

4 Zaštita privatnosti

TODO: uvod

4.1 Enkripcija

TODO literatura

Internet je otvoren sistem. Svi podaci se kroz vise uređaja, deljenih konekcija, ili čak bežicno 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. 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 onlajn kupovine.

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, kod koje je potreban samo jedan ključ te se ona koristi u situacijama kada već postoji siguran kanal za komunikaciju. 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.

NASTAVAK

4.2 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 [1]. VPN su privatne mreže koje rade preko deljene javne infrastrukture kao što je internet [13]. 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 [6]. 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 [5].

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 [8]. 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.

4.2.1 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 pri-

morani 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 [8].

5 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. Ovde pišem zaključak.

Literatura

[1] The History of VPN, 2018. on-line at: https://www.le-vpn.com/history-of-vpn/.

[2] 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.

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

[4] 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.

[5] 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.

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

[7] 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.

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

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

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

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

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

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

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

A Dodatak

Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe.