SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2015./16.

Borna Kuri

Privatnost i sigurnost na Internetu

završni rad

mentor Vjera Lopina

Zagreb, 2016.

Borna Kuri

bkuri@ffzg.hr

1 Sadržaj

2 Sažetak

Ovaj rad istražuje sigurnost i privatnost korisnika na današnjem Internetu. Kako bi to postigao, rad pokušava oslikati današnje stanje na Internetu. Kroz rad se obrađuje više tema, od enkripcije na Internetu, do raznih sigurnosnih prijetnji.

3 Ključne riječi:

Internet Sigurnost Privatnost Enkripcija

4 Uvod

Broj uređaja svakodnevno spojenih na Internet je teško točno odrediti. Dok razne studije spominju stotine milijuna i desetke milijarda naprava s konstantnom vezom na Internet, jedna je stvar sigurna. Internet je važniji nego ikad. Danas više ne govorimo o Internetu samo kao ljudskom pomagalu, već kao i mreži vitalnoj samim uređajima za preuzimanje podataka, te dopunjavanje funkcionalnosti.[1] Međusobno spojenih preko njega, na Internetu je 2010. godine komuniciralo oko dvanaest i pol milijarda raznih uređaja. Do 2020. godine predviđa se rast od preko 400%. Studije zaokružuju taj broj na 50 milijardi. [2][3][4]

Kako bi se prilagodile vremenu, te bile prve u svom polju, velike korporacije nude razne modele internetskog poslovanja. Nerijetko, te ideje zvuče radikalno, no s obzirom na osebujan, brz i neočekivan razvoj Interneta, teško je reći što je pretjerivanje, a što vizionarski potez. Sve češće se mogu čuti pozivi od vodećih svjetskih ekonomista i raznih političara na ukidanje fizičkog novca, te prelazak na digitalni novac.[5][6] U posljednjih par godina su se pojavile decentralizirane digitalne kripto-valute poput Bitcoina.[7] Umjesto da propadnu kao što su mnogi očekivali, održale su se godinama.[8]

Novčane transakcije preko Interneta, isto kao i broj uređaja, svakodnevno rastu. U velikom biznisu danas se posluje gotovo ekskluzivno digitalnim transakcijama. S rastom vrijednosti digitalnih transakcija, također rastu i sigurnosni problemi njihovog izvođenja. Svakodnevno se enkripcija na Internetu povećava kako bi se hakerima onemogućila krađa privatnih podataka, bili ti podatci novac, državne tajne ili obični razgovor malog čovjeka na

[1] Fell, Mark. Roadmap for the Emerging Internet of Things – Its Impact, Architecture and Future Governance. 2014. URL: http://carre-strauss.com/documents/IoT_Roadmap.pdf (16.9.2016.)
[2] Evans, Dave. The Internet of Things. 2011. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (16.9.2016.).
[3] Westberg, Hans. 50 BILLON CNNECTIONS 2020. 2010. URL: http://hugin.info/1061/R/1403231/357583.pdf (16.9.2016.)
[4] 'INTERNET OF THINGS' CONNECTED DEVICES TO ALMOST TRIPLE TO OVER 38 BILLION UNITS BY 2020. 27.8.2015. URL: http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020 (16.9.2016.)
[5] Denmark proposes cash-free shops to cut retail costs. 6.5.2015. URL: http://www.reuters.com/article/denmark-cash-idUSL5N0XX2ZQ20150506 (16.9.2016.)
[6] Kelly, Lorcan Roche. Citi Economist Says It Might Be Time to Abolish Cash. 10.4.2015. URL: https://www.bloomberg.com/news/articles/2015-04-10/citi-economist-says-it-might-be-time-to-abolish-cash (16.9.2016.)
[7] Matonis, Jon. Bitcoin 101. // White Paper. 26.5.2013. URL: http://www.trssllc.com/wp-content/uploads/2013/05/White_Paper_Bitcoin_101.pdf (16.9.2016.)
[8] Maltese, Marco E. G. Bitcoin: Left For Dead Hundreds Of Times - Still Alive And Kicking. 25.11.2015. URL: https://cointelegraph.com/news/bitcoin-left-for-dead-hundreds-of-times-still-alive-and-kicking (16.9.2016.)

Facebooku. I dok s jedne strane u umu ljudi raste svjesnost potrebe za enkripcijom, s druge strane se mogu čuti pozivi iz FBI-a i raznih lobija za zabranom snažne enkripcije i predavanjem ključeva za otvaranje kriptiranih poruka kako bi se svi podatci mogli analizirati. [9]

Danas se Internet nalazi u centru pažnje, jer se većina digitalnih interakcija i transakcija odvija na njemu. Ipak, razne institucije i grupe razvijaju alternativne, još sigurnije i decentralizirane protokole kako bi zaustavile kontrolu i preglednost Interneta i drugih digitalnih mreža.

Kriptografi se konstantno nadmudruju, nove enkripcije svakodnevno nastaju, otkrivaju se godinama previđene rupe u softveru, a nove tehnologije nastaju a da nitko nije siguran koja je prava moć Interneta i tehnologije.

Koje opasnosti vrebaju prosječnog korisnika na Internetu? Vrijede li one također i za internacionalne kompanije? Što se radi kako bi se podatci zaštitili? U ovom radu ću pokušati oslikati pejzaž modernih borbi za sigurnost i enkripciju na Internetu, te ukazati na nove smjerove kud se Internet kreće.

[9] Masnick, Mike. FBI Quietly Removes Recommendation To Encrypt Your Phone. 26.3.2015. URL: https://www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml (16.9.2016.)

5 Prijetnje

Kako je rastao broj Internet korisnika, te važnost neposredne povezanosti, osim zloćudnih programa, izmišljen je velik broj tehnika i strategija za prisluškivanje i iskorištavanje korisnikovih podataka preko Interneta. kako državne agencije za sigurnost i hakeri, tako i kompanije. Bile internacionalne ili manje, informacija je u današnjem svijetu zlata vrijedna, te naučiti što više o navikama korisnika je uvijek potrebno radi budućih poslovnih odluka.

Ako provedemo malo vremena na Internetu, lako ćemo mozaik ljudskih strahova povezati u jednu strahovitu priču. Nepoznati haker vreba nad našom bežičnom mrežom kod kuće i na poslu.[10] Istovremeno, Skype bilježi sve naše poslovne razgovore.[11] Istovremeno Facebook prati sve privatne razgovore koje vodimo s prijateljima, te stvara profil nas kao osobe.[12] Zatim te podatke oboje prodaju raznim kompanijama i agencijama za nepoznate svrhe. Kad se ti podatci kreću mrežom, NSA zapisuje sve što prolazi kroz servere pod njihovim nadzorom.[13] To se sve zapisuje, te nikad neće nestati ni biti zaboravljeno.

Do prije par godina takva bi slika izazivala podsmijeh, te bi se lako odbacila kao nabujala mašta. I dok je ova slika zbilja uvećana, kroz zadnjih par godina se velikim djelom pokazala stvarnom. Nakon informacija koje je iznio Edward Joseph Snowden 2013. godine[14], te periodičnog otkrivanja raznih dokumenata od strane Wikileaks[15], više ne možemo nijekati da nas na Internetu špijuniraju razne tvrtke i državne agencije – američke, europske, kineske. Pitanje inherentne važnosti privatnosti je etičko i moralno pitanje, te je zbog toga izvan opsega ovog rada, no smatram da barem pitanje sigurnosti naših osobnih računa – kreditnih kartica i lozinki – nije kontroverzno, te da vrijedi proučiti problem sigurnosti radi njih, ako ničega drugoga.

Bilo da se radi o prisluškivanju bežične mreže kod kuće, servera na Internetu ili ako vaš pružatelj internetskih usluga predaje Vaše podatke, glavni problem ostaje isti – kako zamaskirati podatke da ih neželjene stranke ne bi mogle pročitati.

[10] Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003

[11] Greenwald, Glen; MacAskill Ewen; Ackerman Spencer; Rushe Dominic. Microsoft handed the NSA access to encrypted messages. 12.7.2013. URL: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (16.9.2016.)

[12] Data Policy. URL: https://www.facebook.com/policy.php (16.9.2016.)

[13] Gellman, Barton; Poitras, Laura. US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program. 7.6.2013. URL: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (16.9.2016.)

[14] Szoldra, Paul. This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. 2016. URL: http://www.businessinsider.com/snowden-leaks-timeline-2016-9 (16.9.2016.)

[15] Spy Files. Wikileaks. URL: https://wikileaks.org/spyfiles/ (16.9.2016.)

5.1 Zloćudni programi

Nedugo nakon što je nastao ARPANET, projekt iz kojeg se naposljetku razvio Internet, počeli su se pojavljivati prvi virusi. I dok su virusi činjenica života na Internetu, oni ne ovise o njemu. Dapače, računalni virusi – trojanski konji, malware, adware, spyware - i drugi zloćudni programi, mogu se širiti preko instalacijskih datoteka, optičkih diskova, USBa i ostalih medija. Kao takvi, oni čine širi problem računalnog okoliša. Isto tako, kad napadnu računalo, situacije u kojoj antivirusni program neće moći zaštiti korisnika nisu česte, dok se sigurnosni problemi na Internetu ne mogu zaobići jednostavnom instalacijom programa.[16] Zbog toga smatram da su zloćudni programi poput virusa izvan opsega ovog rada.

Ipak, vrijedi spomenuti jednu prijetnju ovog tipa. To su keylogger programi, to jest pamtioci ključeva. Dok korisnik piše po tipkovnici, oni rade u pozadini računala, te bilježe sve što je korisnik utipkao. Zatim to šalju preko Interneta hakeru ili jednostavno čekaju da haker dobije pristup računalu, te sam preuzme zapisane podatke.

Primjer hardverskog keyloggera.

Keyloggeri postoje u više varijanti. Najčešća je softverska varijanta, gdje program bilježi sve podatke, no postoji i hardverska. Hardverska varijanta se sastoji od USB produžetka koji se umetne u USB priključak za tipkovnicu na računalu, te se tipkovnica priključi na njega. Tako on djeluje kao posrednik između računala i tipkovnice, te bilježi sav promet između njih, najčešće na flash memoriju.[17]

Osim na svom računalu, korisnik treba paziti pri korištenju računala na fakultetima i Internet kafićima jer su veoma korišteni, te dostupna velikom broju ljudi. Keylogger je lakano postaviti. U slučaju da su računala u pitanju namještena da vrate svoje stanje na disku nazad

[16] Gralla, Preston; Troller, Michael. How the Internet Works. 8th edition. Que. 2006.
[17] Keyloggers Explained: What You Need to Know. 2014. URL: http://www.howtogeek.com/180615/keyloggers-explained-what-you-need-to-know/ (16.9.2016.)

nakon svakog isključivanja, te je stoga softverska verzija beskorisna, lako može postaviti hardverski keylogger kupljen za malu cijenu online.

5.2 Prije izlaska na Internet

Za izlazak na Internet, korisnik treba osigurati svoj ruter.[18] Taj posao obično obavlja Internet operater koji korisniku pruža pristup Internetu. No, ukoliko korisnik ima lokalnu mrežu koja spaja više računala ili mu je nepraktično spojiti računala žičanom vezom, može se odlučiti za korištenje vlastitog rutera. Preko tog rutera može imati veću kontrolu nad lokalnom mrežom i konektivnosti računala.

Pri kupnji rutera potrebno je paziti koji se model nabavlja, te dati nekome tko zna da postavi sigurnosne postavke. To uključuje postavljanje moderne WPA2 enkripcije na bežičnu vezu ili jedne od rjeđe korištenih, no sigurnijih alternativa.[19]

Ukoliko se želimo zaštititi od rupa u osiguranju rutera koji koristimo, trebamo paziti koje proizvođače i modele koristimo. Od 2010. godine je poznato da NSA redovito zahtijeva promjene na računalnom hardveru za spajanje na Internet proizvedenom u Sjedinjenim Američkim državama kako bi mogli nadzirati uređaje[20]. Zbog toga je sigurnost svih rutera i drugih mrežnih uređaja proizvedenih u Sjevernoj Americi pod upitnikom. I dok američka vlada ugrađuje sigurnosne rupe u domaće uređaje, istovremeno optužuju kineske proizvođače za istu stvar, te se zalažu za blokiranje Kineskih kompanija koje proizvode mobitele poput ZTE i Huawei.[21][22]

Isto tako, 2015. godine se dogodio skandal kad je otkrivena nesigurnost u vatrozidu Juniper Networksa. Juniper Networks je multinacionalna kompanija koja proizvodi rutere i vatrozide za kompanije, te im je prihod 2014. godine iznosio 4.63 milijarde dolara. Naime, pronađene su dvije rupe u njihovom softveru. Jedan od tih propusta je dozvoljavao napadaču da dekriptira promet koji prolazi kroz uređaj. Pri istraživanju problema, otkriveno je da je vjerojatni krivac američka NSA. Čak ako i nisu direktno stvorili rupu, propust je rezultat njihovih poteza. Naime, Dual_EC enkripcija je označena sigurnom, makar je postojala rupa poznata američkoj NSA. U Dual_EC postoji slabost koju je NSA potencijalno strateški ostavila

[18] Gralla, Preston; Troller, Michael. How the Internet Works. 8th edition. Que. 2006.
[19] Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003
[20] Zetter, Kim. Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. 18.12.2015. URL: https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ (20.9.2016.)
[21] Exclusive: Obama sharply criticizes China's plans for new technology rules. 3.3.2015. URL: http://www.reuters.com/article/us-usa-obama-china-idUSKBN0LY2H520150303 (20.9.2016.)
[22] Greenwald, Glen. How the NSA tampers with US-made internet routers. 12.5.2014. URL: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (20.9.2016.)

u slučaju potrebe prisluškivanja. Pri tome nisu uzeli u obzir mogućnost da će itko drugi otkriti propust, te ga iskoristiti u vlastite svrhe.[2324]

5.3 Windows i sigurnost

Malware je kategorija koja se možda sastoji od velikog broja zlućudnih programa, no na sreću prevencija od svih je jednaka, a zaštita vrlo slična.

Ako koristimo Windows, kako ne bismo zarazili računalo, potrebno je koristiti antivirusni program. Na primjer, popularni besplatni Avast Software ili profesionalni i visoko cjenjeni Kaspersky Anti-Virus.[25]

Ipak, uvijek postoji mogućnost da će naše računalo biti napadnuto novim virusom ili biti probijeno kroz novu sigurnosnu rupu. Ako pitamo profesionalnog programera ili web administratora, često ćemo dobiti odgovor da je borba protiv virusa utrka u kojoj su tvorci virusa uvijek prvi, a pogotovo na Microsoft Windowsu, te da bi bilo bolje preći na Linux platformu.

Linux entuzijasti već deset godina željno isčekuju i rade prema tome da njihova platforma počne parirati Windowsu. Što se tiče web servera, tu su definitivno pobijedili.[26] Svakodnevni korisnici? Nisu još tamo. U posljednje vrijeme velike kompanije od kojih je najistaknutiji Valve predvode pokušaje da se video igre počnu proizvoditi za Linux platformu kako bi potakli sto milijuna gamera koji kod njih kupuju na prelazak. Hoće li to uspjeti još nije sigurno, no potencijalnim prelaskom na Linux platformu bi se smanjio broj sigurnosnih rupa koje hakeri i malware mogu iskoristiti protiv prosječnog korisnika.[27]

Vrijedi spomenuti da postoje još sigurniji operacijski sustavi poput BSD i Plan 9, no oni se koriste za specifične namjene, te nisu za širu publiku kojoj je i Linux previše zahtjevan.[28]

---

[23] Zetter, Kim. Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA. 22.12.2015. URL: https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/ (20.9.2016.)

[24] Goodin, Dan. NSA official: Support of backdoored Dual_EC_DRBG was "regrettable". 14.1.2015. http://arstechnica.com/security/2015/01/nsa-official-support-of-backdoored-dual_ec_drbg-was-regrettable/ (20.9.2016)

[25] Rubenking, Neil J.. The Best Antivirus Protection of 2016. 20.6.2016. URL http://www.pcmag.com/article2/0,2817,2372364,00.asp (20.9.2016.)

[26] Usage of operating systems for websites. 20.9.2016. URL: https://w3techs.com/technologies/overview/operating_system/all (20.9.2016.)

[27] Steam'd Penguins. 12.6.2012. URL: http://blogs.valvesoftware.com/linux/steamd-penguins/ (20.9.2016.)

[28] Macintire, Tim. Take a closer look at OpenBSD. 8.8.2006. URL: https://web.archive.org/web/20070127231412/http://www-128.ibm.com/developerworks/aix/library/au-openbsd.html (20.9.2016.)

5.4 Zaštita na mreži

No ni najsigurniji operacijski sustav ne može zaštititi korisnika na Internetu. Internet se može opisati kao veliki trg na kojem svačiji tragovi ostaju i kamere snimaju korisnike. Nikakvo diskretno ponašanje niti želja za privatnošću neće pomoći. Podatci koji bi se eventualno mogli iskoristiti protiv korisnika ostaju.[29]

Postoji velik broj faktora koji su važni pri zaštiti identiteta i osobnih podataka na mreži, no većina njih je iznad razine znanja prosječnog Internet korisnika. Prva stvar koju korisnik treba napraviti je koristiti web browser s dobrom sigurnosnom zaštitom. Na primjer, Firefox, čiji programeri planiraju u bliskoj budućnosti zabraniti nezaštićene HTTP veze. Korištenjem sigurnijih HTTP veza možemo relativno lagano zaštititi naše podatke od većine znatiželjnih, a zbog same količine prometa na Internetu, velike agencije poput NSA će možda ignorirati enkripciju podataka jednog korisnika i okrenuti se većim metama.[30][31]

Kako bi onemogućio da znatiželjnici vide gdje je sve bio, revni korisnik također može redovito čistiti svoju internetsku povijest kako razne web stranice kod njega ne bi ostave svoje kolačiće, te time obilježile njegovu Internet prošlost. Ipak, ako ciljamo na pravu privatnost, ni to nikako nije dovoljno. Za prosječnog korisnika, ovdje leži linija preko koje ne žele ići jer uloženi trud postaje prevelik.

6 Privatnost na Internetu

HTTP i HTTPS

Do nedavno je prijenos podataka na Internetu funkcionirao većinom preko HTTP protokola. Punog imena HyperText Transfer Protocol, HTTP je nastao 1965. godine kao dio Xanadu projekta. I dok projekt nikad nije zaživio, HTTP se pokazao korisnim.[32]

U svijetlu nedavnih skandala zbog prisluškivanja Internet prometa pokazao se vrlo nesiguran široj javnosti, nešto što su stručnjaci već dugo upozoravali. Time se pojavila potreba za prelazak na bolji protokol. Iz tog razloga se u posljednjih par godina naglo povećao broj web stranica koje koriste sigurniju verziju HTTP protokola – HTTPS. [33]

---

[29] Gustafson, Karl E.; Black, Ryan J.;Groom, Sharon E.; Tam, Michele. The Internet Never Forgets: Google Inc.'s "right to be forgotten" EU ruling and its implications in Canada. 2014. URL: http://www.mcmillan.ca/The-Internet-Never-Forgets-Google-Incs-right-to-be-forgotten-EU-ruling-and-its-implications-in-Canada (20.9.2016.)

[30] Gralla, Preston; Troller, Michael. How the Internet Works. 8th edition. Que. 2006.

[31] 'NSA totally dysfunctional – too much data to detect threats' – whistleblower. 5.5.2016. URL: https://www.rt.com/op-edge/341905-nsa-us-leaks-terrorism/ (20.9.2016.)

[32] Berners-Lee, Tim. HyperText Transfer Protocol. URL: https://www.w3.org/History/19921103-hypertext/hypertext/WWW/Protocols/HTTP.html (20.9.2016.)

[33] HTTPS usage statistics on top websites. 29.8.2016. URL: https://statoperator.com/research/https-usage-statistics-on-top-websites/ (20.9.2016.)

Nastao 1994. godine, HTTPS je u početku koristio SSL protokol za enkripciju, no s mijenjanjem standarda SSL je zamijenjen za TLS protokol 2000. godine. To znači da HTTPS zahtijeva od Internet preglednika da se standardni HTTP kôd zamaskira dodatnom razinom TLS enkripcije.[34]

Preglednici znaju kad smiju vjerovati web stranici da je njihova implementacija protokola važeća time što svaka web stranica koja koristi protokol treba dobiti poseban certifikat od provjerene kompanije ili udruge. U slučaju da taj certifikat nedostaje ili je nevažeći, preglednik će prekinuti vezu.[35]

Ispitivanje u travnju 2016. godine je pokazalo da 41.7% od 141 tisuće najpopularnijih web stranica imaju sigurnu implementaciju HTTPS protokola.[36] Očekujući brzi rast korištenja HTTPS protokola, Mozilla korporacija koja stoji iza Firefox preglednika je 2015. godine najavila kako planiraju ukinuti potporu za HTTP protokol kako bi sav promet na Internetu postao kriptiran. Na tu se vijest broj entuzijasta otvorenog softvera i vlasnika malih Internet stranica pobunio jer su smatrali kako je dobivanje HTTPS certifikata problematično i financijski zahtjevno. No od tad se, iako je prošla tek godina dana, proces dobivanja certifikata automatizirao, ubrzao i olakšao.[37][38]

I dok HTTPS veza štiti protiv većine znatiželjnika, zahvaljujući Snowdenu znamo da čak i s HTTPS vezom američka NSA može razbiti enkripciju u velikom broju slučaja.[39] Više godina se nije znalo kako im uspijeva, no 2015. godine je napokon otkriven jedan od načina. Problem je bio u implementaciji Diffie-Hellmanovog algoritma koji se koristi za generiranje ključeva kod virtualnih privatnih mreža, elektroničke pošte, HTTPS protokola i drugog. Naime, zbog česte loše implementacije algoritma, ključ korišten za kriptiranje velikom je broju slučajeva jedan od nekoliko istih standardiziranih ključeva, te je NSA probila nekoliko najčešćih ključeva čime je bez problema otvarala velik broj poruka.[40]

6.1 Kolačići i reklame

Ponekad na web stranicama trošimo više vremena, te želimo koristiti šire polje opcija koje web stranica nudi. To može biti želja da ostanemo ulogirani u naš osobni račun ili da web stranica zapamti naše želje kako prikazati razne elemente. U takvim slučajevima, web stranica

[34] Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003

[35] Gralla, Preston; Troller, Michael. How the Internet Works. 8th edition. Que. 2006

[36] Jackson, Brian. What is the Difference Between HTTP and HTTPS?. 20.7.2016. URL: https://www.keycdn.com/blog/difference-between-http-and-https/ (20.9.2016.)

[37] Barnes, Richard. Deprecating Non-Secure HTTP. 30.4.2015. URL: https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/ (20.9.2016.)

[38] Eckersley, Peter. Launching in 2015: A Certificate Authority to Encrypt the Entire Web. 18.11.2014. https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web (20.9.2016.)

[39] Halderman, Alex; Heninger, Nadia. How is NSA breaking so much crypto?. 14.10.2015. URL: https://freedom-to-tinker.com/2015/10/14/how-is-nsa-breaking-so-much-crypto/ (20.9.2016.)

[40] Khandelwal, Swati. How NSA successfully Broke Trillions of Encrypted Connections. 16.10.2015. URL: https://thehackernews.com/2015/10/nsa-crack-encryption.html (20.9.2016.)

i naš preglednik zapišu malu tekstualnu oznaku na naše računalo. Ona služi da bi web stranica prepoznala naše želje sljedeći put. [41]

Sami po sebi, kolačići su bezopasni, ali oni ipak spremaju neke osobne podatke. Sami ih ne stvaraju, već bivaju zapisani ovisno o korisnikovim unosima u web stranicu. Nažalost, razne kompanije su našle načine da pomoću vlastitih kolačića prate korisnika kroz razne web stranice, sve na kojima se njihove reklame prikazuju.[42]

Dok većina kolačića traje samo jednu sesiju, dok korisnik ne zatvori preglednik, također postoje kolačići koji se mogu namjestiti da traju i po dvadeset godina – efektivno do kraja života računala. Ipak, takve je moguće lako izbrisati. [43]

Ukoliko korisnik ima uključen Adobe Flash, rječi, ali vrlo pametni programeri će omogućiti stvaranje LSOa, to jest Local shared objecta. Lokalni podijeljeni objekt na hrvatskom, je tip kolačića koji može trajati zauvijek, a Internet preglednik ga ne može sam izbrisati. Njih moramo obrisati sami ili koristiti ekstenziju za Internet preglednik, poput Better Privacy za Firefox.[44]

Na kraju krajeva, bilo tko koga je briga za sigurnost ipak ne bi trebao koristiti programe poput Java i Adobe Flash, zbog dobro dokumentiranih sigurnosnih problema u oboje. Ukoliko ih korisnik ne može izbjeći, tada bi barem trebao namjestiti u postavkama Internet preglednika da pita korisnika prije negoli dopusti dotičnim programima da se uključe.

Što se tiče samih kolačića, korisnici koji žele biti sigurni da ih se ne prati, među ostalim stvarima, ne smiju koristiti niti dozvoliti svojem pregledniku korištenje kolačića.

6.2 VPN – virtualna privatna mreža

U strahu od gubitka privatnosti ili zbog sve strožeg nadziranja copyrighta na Internetu, korisnici sve češće traže novi način kako bi zamaskirali vezu. Isto tako u nekim državama, od kojih se najviše ističu Sjedinjene američke države, pružatelji Internet usluge redovito nadziru veze korisnika kako bi ih usporili ukoliko korisnici preuzimaju podatke od web stranica koje stvaraju veliki promet, poput Netflixa.[45] Korisnici pogođeni ovom neetičnom praksom ponekad traže način kriptiranja veze kako njihovi pružatelji usluge ne bi mogli detektirati s kojeg izvora

[41] Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003

[42] Vries, Lloyd. CIA Caught Sneaking Cookies. 20.3.2002. URL: http://www.cbsnews.com/news/cia-caught-sneaking-cookies/ (20.9.2016.)

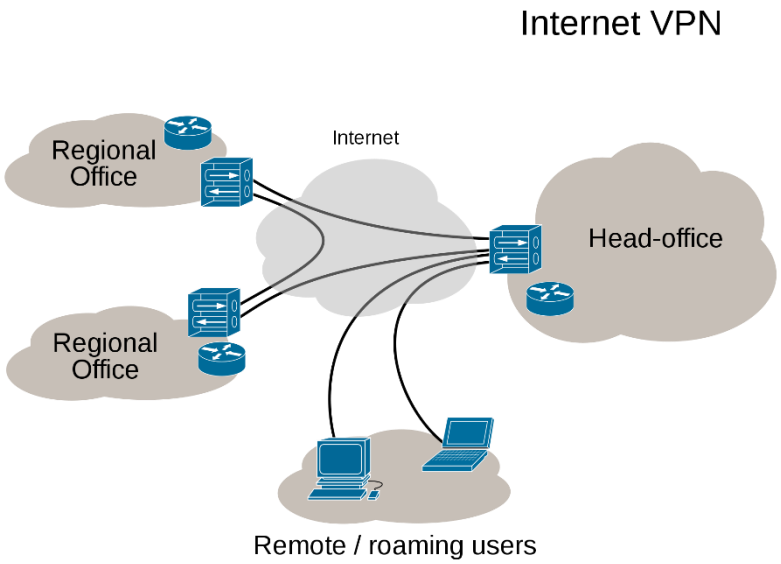
[43] Reilly, Richard. Here's how Facebook, Google, and Apple are tracking you now. 6.10.2016. URL: http://venturebeat.com/2014/10/06/the-cookie-is-dead-heres-how-facebook-google-and-apple-are-tracking-you-now/ (20.9.2016.)

[44] Kirk, Jeremy. Study: Adobe Flash cookies pose vexing privacy questions. 11.8.2009. URL: https://web.archive.org/web/20090813161926/http://www.networkworld.com/news/2009/081109-study-adobe-flash-cookies-pose.html (20.9.2016.)

[45] Epstein, Adam. Netflix launched this handy speed test so you can go shame your internet provider. 19.5.2016. URL: http://qz.com/688033/netflix-launched-this-handy-speed-test-so-you-can-go-shame-your-internet-provider/ (20.9.2016.)

dolazi njihov promet, te time zaobišli usporavanje veze. Obje grupe se sve češće odlučuju za isto rješenje.

VPN, ili virtualna privatna mreža je tip privatne mreže na koje se korisnik može spojiti preko Interneta. Time korisnik može preko Interneta primati podatke iz te mreže uz dodatnu enkripciju. To je današnjim korisnicima Interneta atraktivno zato što pri preuzimanju podataka, virtualna privatna mreža dodatno kriptira podatke prije nego li ih šalje korisniku. Tako bilo tko tko prisluškuje promet gotovo sigurno neće moći odrediti s kojim web stranicama korisnik ima interakciju niti koje podatke prenosi, već će vidjeti samo promet između ta dva izvora. [46]



Primjer VPN mreže korištene u kompaniji

Kako bi veza između VPNa i korisnikovog računala ostala sigurna, najčešće se koristi podatkovni protokol zvan tunneling. Jedan od razloga je to što taj protokol dozvoljava korisniku da koristi druge protokole koje korisnikova standardna mreža ne podupire. Kao primjer toga možemo uzeti činjenicu da velik broj virtualnih privatnih mreža koriste IPv6 Internet protokol, dok velik broj pružatelja Internet usluga još omogućava samo stariji IPv4. No, drugi, puno važniji razlog je zaštita privatnosti.[47]

Kako bi se podatci zaštitili, pri tunnelingu se paketići podataka koji nam trebaju pakiraju zajedno s meta podatcima u kojima su specificirani protokoli i adrese gdje se prvobitni paketići šalju. Nekome tko promatra sa strane, ti drugi paketići izgledaju kao normalan Internet promet umjesto konstantne veze s privatnom mrežom.[48]

[46] Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003

[47] Virtual Private Networking: An Overview. 4.9.2001. URL: https://technet.microsoft.com/en-us/library/bb742566.aspx (20.9.2016.)

[48] Tanenbaum, Andrew S. Computer Networks. New Jersey: Pearson Education, 2003.

Naravno, postoji mogućnost da takva veza bude dekriptirana, te se podatci radi veće sigurnosti trebaju kriptirati na još jednoj razini već na serverima VPNa prije nego li su poslani postupkom tunnelinga prema korisniku. Kakva enkripcija se koristi ovisi o tome tko održava mrežu.

Također treba imati na umu da kompanija koja održava VPN mrežu uvijek može odati identitet svojih korisnika, te čak i vrijeme i imena servera koje je koristio ako zakon tako nalaže. Zbog tog razloga, velik broj VPN kompanija ističe praksu uništavanja svih zapisa – tko je koristio koje servere i kad – nakon tjedan ili mjesec dana.

7 Drugačije paradigme

Tražeći sigurnost i privatnost, od nastanka World Wide Weba bilo je jasno da sustav nije u potpunosti siguran. Koristeći istraživanja iz ranih dana ARPANETa, početkom 21. stoljeća su počeli nastajati razni projekti s novim, radikalnim idejama kako stvoriti sigurnu mrežu. Umjesto da vezu korisnika i web stranice osiguraju standardnim protokolima, novi projekti su počeli modificirati protokole. Odskačući od tud, nastao je novi softver s drugačijim standardima kako bi se stvorile mreže sasvim drugačije strukture koje će maksimalno zaštititi korisnika, te ostati nepristupačne standardnim Internet preglednicima. Postoji barem desetak poznatijih mreža ovog tipa, od kojih su najpoznatiji Freenet, Tor i i2p.[49]

Korištenjem ovih alata moguće je pristupiti dark webu i darknetu, to jest mračnoj mreži i mračnom netu. Mračna mreža je specifičan dio world wide weba koji je nepristupačan korisnicima standardnog softvera, no koristi istu infrastrukturu. S druge strane tamni net označava računalne mreže izolirane od Interneta koje samo ponekad koriste isti softver kao i tamne mreže.[5051]

7.1 Tor

Tor mreža je skupina servera održavanih od strane volontera koja je nastala kako bi korisnik mogao povećati svoju sigurnost na Internetu. Istovremeno, Tor označava i specijaliziran otvoreni softver koji se koristi kako bi omogućio anonimno komuniciranje s drugim korisnicima tog softvera. Tor koristi modificirani Firefox Internet preglednik kako bi korisniku omogućio pristup web stranicama. Za razliku od velikog broja drugih softvera slične namjene, Tor dozvoljava izlazak na „normalan“ web. Ipak, koristeći Tor softver, korisnik može

[49] Anonymity Networks. Don't use one, use all of them!. 2012. URL: http://null-byte.wonderhowto.com/news/anonymity-networks-dont-use-one-use-all-them-0133881/ (20.9.2016.)
[50] Wood, Jessica.. "The Darknet: A Digital Copyright Revolution. 2010. URL: http://jolt.richmond.edu/v16i4/article14.pdf (20.9.2016.)
[51] Greenberg, Andy. Hacker Lexicon: What is The Dark Web?. 19.11.2014. URL: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (20.9.2016.)

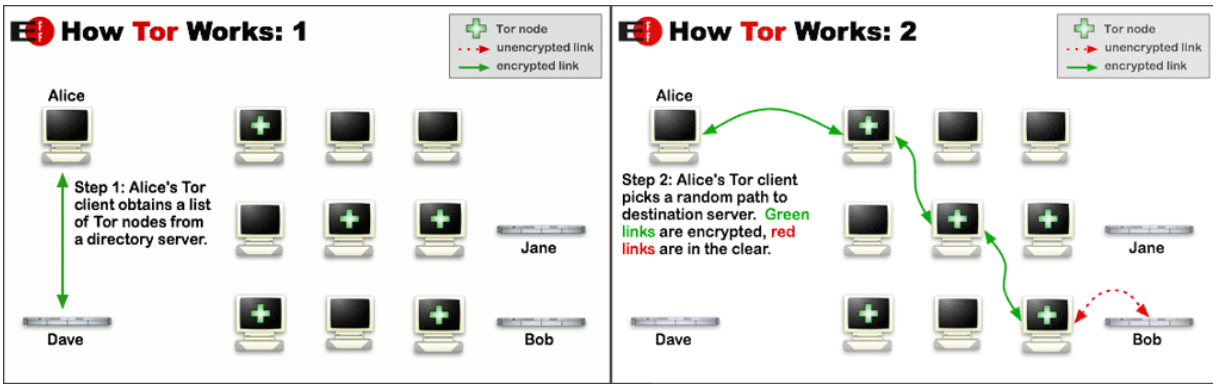
pristupiti stranicama koje koriste poseban model enkripcije i komuniciranja nazvan onion routing.[52][53]

Rani koraci u stvaranju onoga što je na kraju postalo Tor su se dogodili u laboratorijima za vojna istraživanja u Americi sredinom 1990. Cilj je bio stvoriti protokol koji će zaštititi državnu komunikaciju na Internetu. Iz tog rada je nastao onion routing. Kasnije je ideja razvijana u DARPAi, prije nego li su rezultati istraživanja početkom novog tisućljeća postali javni. [54]

Vidjevši potencijal u tome, 2002. godine je nekoliko računalnih znanstvenika izdalo prvu verziju Tora. Par godina kasnije je utemeljena istoimena neprofitna organizacija. Od tad je najveći dio prihoda za održavanje projekta došao od američke vlade, iako se Tor često našao u sukobu interesa s američkom vladom, pogotovo kad se radilo o pitanju dekriptiranja podataka.[55]

Tor je prilično efikasan pri zaustavljanju prisluškivanja prometa Internet korisnika. Ako znamo tko s kime razgovara na Internetu, to jest odakle i kamo idu informacije, to nam dozvoljava da pratimo korisnikove interese i ponašanje. Čak i ako korisnik kriptira sadržaj onoga što šalje, javni dio poslanog paketa sadrži podatke poput destinacije, odakle dolazi i kad je poslan. Tor je posebno dizajniran kako bi otežao praćenje tih paketića po Internetu.

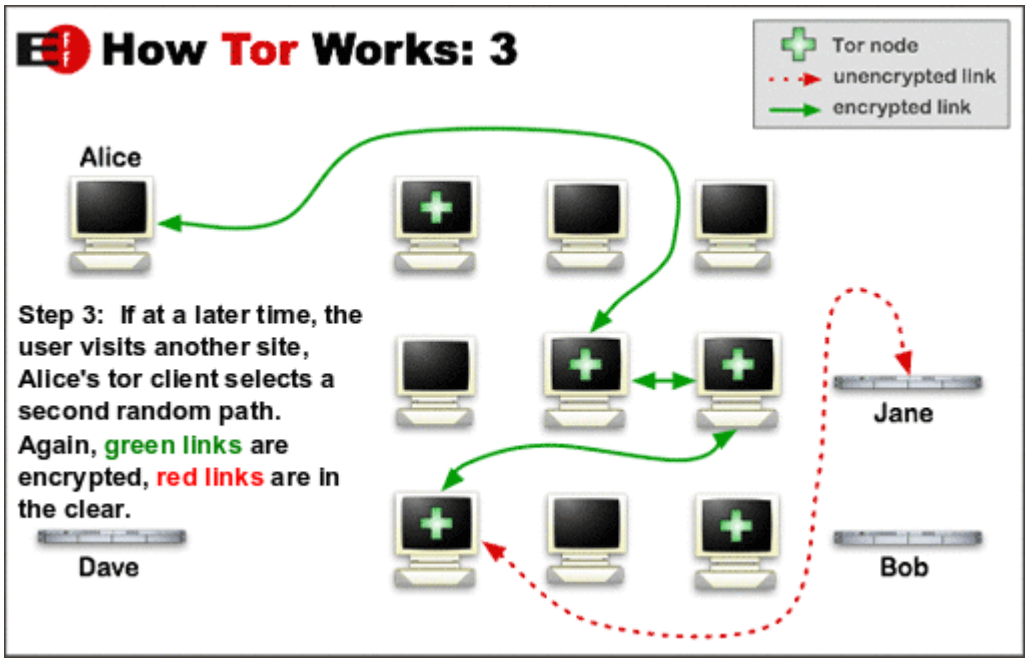
Kako bi Tor smanjio rizik identifikacije korisnika s sadržajem, Tor stvara kriptiranu vezu među više računala pri slanju podataka. Time se računalo korisnika koji pokušava pratiti tuđe informacije lakše zagubi jer zbog postojanja više posrednika, ne zna tko kome šalje podatke. Drugim riječima, umjesto da se podatak pošalje direktno, Tor stvara dinamičnu mrežu koja se sastoji od velikog broja korisnika mreže koji će slati poruku međusobno prije nego li poruka ode do finalnog cilja. Zbog toga praćenje poruke postaje mnogo teže.



Kako Tor šalje podatke

[52] Tor: Overview. URL: https://www.torproject.org/about/overview.html.en (20.9.2016.)
[53] What is the Tor Browser? URL: https://www.torproject.org/projects/torbrowser.html.en (20.9.2016.)
[54] Fagoyinbo, Joseph Babatunde. The Armed Forces: Instrument of Peace, Strength, Development and Prosperity. 28.5. 2013. AuthorHouse.
[55] Levine, Yasha. Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government. 16.6.2016. URL: https://pando.com/2014/07/16/tor-spooks/ (20.9.2016.)

Svaki korisnik koji se nalazi na putu zna samo za identitet korisnika koji je njemu poslao podatke i onoga koji šalje. Nitko nije svjestan cijelog puta, niti sadržaja poslanih podataka. Naravno, korištenjem Tora, svaki korisnik postane posrednik te šalje dalje podatke nevezano za vlastito pretraživanje mreže. Radi efikasnosti Tor zadržava istu liniju komunikacije deset minuta prije nego li promijeni rutu radi sigurnosti.[56]



Promjena puta podataka kroz Tor mrežu

Ipak, Tor ima nekoliko poznatih mana. Jedna mana koju Tor projekt niti ne pokušava riješiti je špijuniranje izlaznih čvorišta.[57] Ukoliko želimo izaći iz tamne mreže na Internet, dio podataka će biti vidljiv, te Tor ne može ništa učiniti kako bi to promijenio. Isto tako, ako upravljamo s jako velikim brojem servera u Tor mreži, možemo identificirati paketiće, te ih uspješno pratiti po mreži. Dugo poznata kao potencijalna slabost, ova slabost mreže je dokazana kad su izašli podatci koji pokazuju da FBI održava velik broj Tor čvorišta.[58] Ipak, istraživanja su pokazala da i uz tu slabost, Tor je prosječno mnogo sigurniji od virtualnih privatnih mreža. S druge strane, teško je odrediti koliko je FBI uspješan u dekriptiranju podataka, te je sigurnost Tor mreže ipak pod upitnikom.[59]

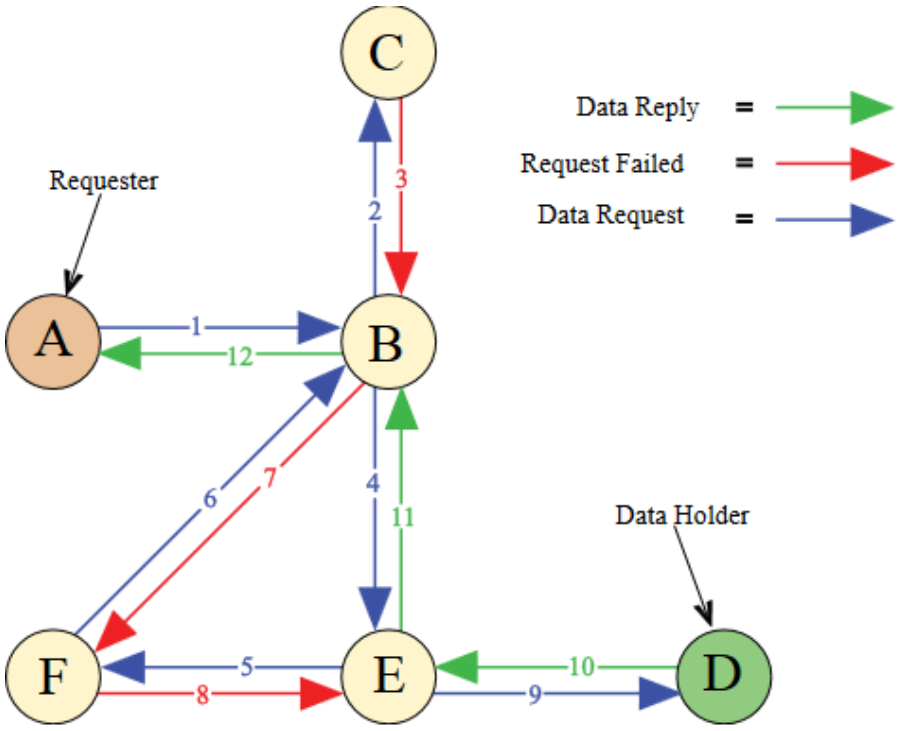
[56] Tor: Overview. URL: https://www.torproject.org/about/overview.html.en (20.9.2016.)
[57] One cell is enough to break Tor's anonymity. 2009. URL: https://blog.torproject.org/blog/one-cell-enough (20.9.2016.)
[58] Khandelwal, Swati. Warning: Over 100 Tor Nodes Found Designed to Spy On Deep Web Users. 26.6.2016. URL: https://thehackernews.com/2016/07/tor-deep-web-spying.html (20.9.2016.)
[59] Murdoch, Steven J. How Tor's privacy was (momentarily) broken, and the questions it raises. 10.20.2015. URL: http://phys.org/news/2015-12-tor-privacy-momentarily-broken.html (20.9.2016.)

7.2 Freenet

Nastavši 2000. godine, Freenet je platforma koja je nastala kako bi riješila problem cenzure na Internetu. Platforma se bazira na peer-to-peer arhitekturi kako bi decentralizirano spremala podatke, dok istovremeno daje korisniku veliku razinu anonimnosti.[60][61]

Kad korisnik koristi Freenet, sam program od njega zahtijeva da na svojem računalu odvoji dio hard diska kako bi program mogao tamo spremiti podatke koji su uploadani na Freenet mrežu. Ta mreža koristi vlastite protokole, te se ne može čitati na standardan način. Ovisno o popularnosti podatci koje program sprema na korisnikov hard disk se brišu ili čuvaju duže vrijeme. Budući da su podatci kriptirani, korisnik ne zna što je u njima, niti ih može otvoriti, zbog čega nije odgovoran za informacije koje se nalaze unutra.[62]

Zbog ovog sistema, kad korisnik postavi web stranicu ili razne podatke na Freenet, ti podatci su izvan njegove kontrole, te se sami šire uokolo. Drugim riječima, podatci više nisu u rukama korisnika, te ih je nemoguće uhvatiti i izbrisati. S druge strane, ako nema interesa, podatci se s vremenom mogu fragmentirati, raširiti između više korisnika te nestati djelomično ili čak potpuno u nekim slučajevima.



Kako Freenet traži podatke na mreži

[60] Freenet: About. https://freenetproject.org/about.html (20.9.2016.)
[61] FAQ. https://wiki.freenetproject.org/FAQ (20.9.2016.)
[62] Freenet: Understand. https://freenetproject.org/documentation.html#understand (20.9.2016.)

Kako se cijela mreža ne bi mogla ušutkati, dizajnirana je da bude otporna i samostalna. Ne postoje centralni serveri. Pošto se sve informacije šire uokolo po mreži, te su kriptirane, teško je znati tko ima koje informacije, te tko traži koje podatke dok ne znamo točno što tražimo.

Budući da je puno poznatiji, većina pokušaja probijanja softvera koji štiti korisnike na tamnoj mreži se fokusira na Tor. Zbog toga se puno manje zna o pravoj otpornosti Freeneta. Navodno je bio probijen od strane anonimnih korporacija u kontaktu s američkom vladom, no detalji nisu objavljeni, te je pravo sigurnosno stanje Freeneta pod upitnikom.[63]

7.3 Budućnost

Tor i Freenet nisu jedini projekti koji su kroz godine pokušali na Internetu stvoriti mreže gdje korisnik može biti anoniman. Drugi, manji projekti, poput I2p[64] i GNUnet[65] također postoje, te pokušavaju slične stvari. No, kakvo god bilo njihovo stanje, čak i da prijeđemo preko problema često spore veze, na kraju je vidljiva jedna činjenica. Oni nisu zamjena za Internet kakav je, već samo dopuna u specifičnim situacijama. Često su sporiji od Interneta na koji je generalna populacija naviknuta, te dolaze s vlastitim problemima.

Pitanje glasi, možemo li promijeniti Internet na način kako bi korisnik mogao svoje podatke učiniti potpuno privatnima? Očiti odgovor, isto kao i s postojanjem virusa, glasi ne. No, pitanje ne završava ovdje. Ono se mijenja i nadovezuje na druga pitanja poput, je li moguće napraviti enkripciju dovoljno kompliciranu kako nitko ne bi imao vremena niti moć procesuiranja da otključa enkripciju kod značajnog broja Internet korisnika? Koristeći standardnu svjetski široku mrežu u obliku kakav ima danas, odgovor je definitivan ne. Ali, u slučaju da dovoljan broj korisnika prijeđe na alternativne mreže – Torov Onion net ili Freenet – u tom slučaju ne znamo. Velik problem leži prvenstveno u nepraktičnosti te tehnologije, u njenoj sporosti, te u nezainteresiranosti prosječnog korisnika da se navikne na tako ezoteričnu tehnologiju.

Ipak, to ne znači da će Internet zauvijek ostati takav kakav je, niti da neće biti promjena paradigme. U pokušaju decentralizacije Interneta kako bi učinilo cenzuru nemogućom, te praćenje korisnika težim, novi perspektivni projekti nastaju. Neki od njih uz potporu milijunaša iz Silikonske doline, poput Urbita[66] koji obećava revoluciju u razini decentralizacije i načinu na koji Internet funkcionira. Što će takvi projekti donijeti i hoće li išta donijeti, još je nepoznato.

[63] Volpenheim, Sarah. Police in online struggle. 18.11.2015. URL: http://www.thedickinsonpress.com/news/north-dakota/3885239-predators-police-online-struggle (20.9.2016.)
[64] https://geti2p.net/en/
[65] https://gnunet.org/
[66] https://www.urbit.org/

8 Upozorenje: Heartbleed

I tako, dok se velik broj programera bavi krpanjem sigurnosnih propusta, amateri izmišljaju vlastita rješenja, a hakeri objavljuju svoje najnovije uspjehe, često zaboravimo koliko ozbiljni sigurnosni propusti mogu biti. Zapitajmo se; što ako postoji nepoznat, ali fatalni propust u samom srcu softvera koji koriste ne samo mali korisnici, već gotovo cijeli Internet, uključujući velike multinacionalne kompanije? Banke, tehnološki divovi, Vlade. Većina korisnika Interneta, čak i neki informatičari neće znati niti jedan primjer takve situacije. Ipak, postoji relativno nedavan slučaj gdje se takva situacija odigrala. Sigurnosna rupa u pitanju je dobila ime Heartbleed.[67]

Kako bismo razumjeli situaciju, potrebno je početi s OpenSSLom. OpenSSL je popularna implementacija široko korištenih kriptografskih protokola na transportnom sloju Interneta. On služi kako bi zaštitio vezu između dva računala od prisluškivanja s treće strane. OpenSSL je dostupan na velikom broju platformi, od Windowsa do Linuxa i raznih BSD sustava. Postao je veoma važan za svakodnevni rad Interneta, te je 2014. godine korišten na dvije trećine svih web servera na svijetu.[68]

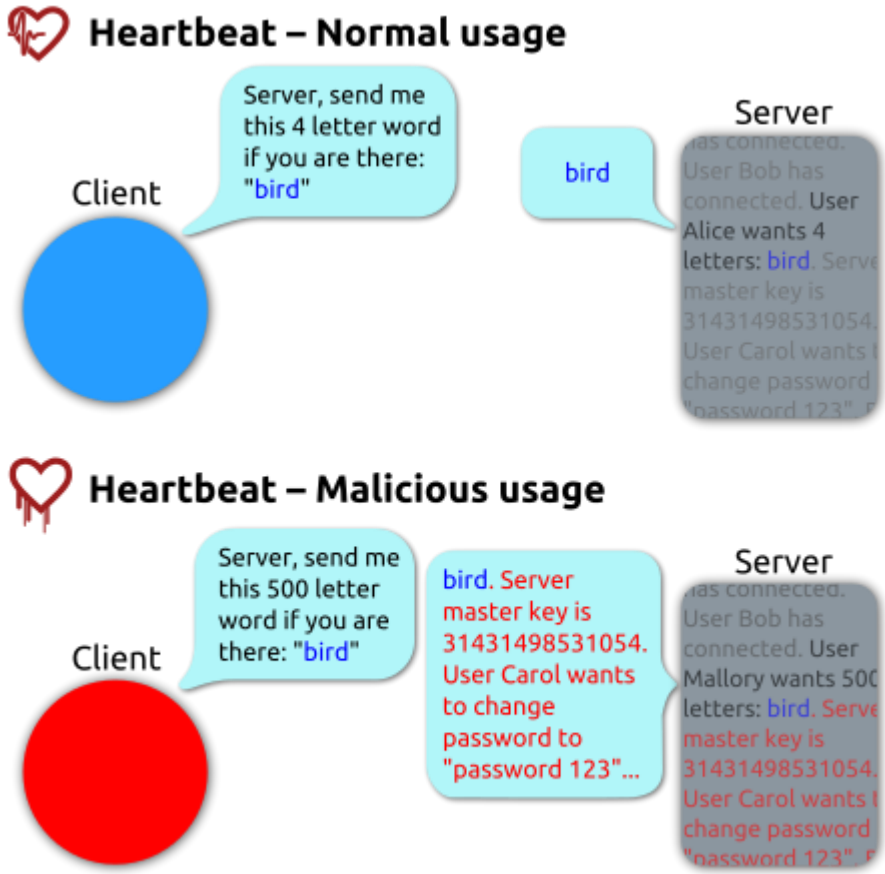
Kako bi testirao vezu između sebe i servera, OpenSSL nalaže računalu na jednoj strani veze da drugoj pošalje molbu za odgovorom. Ta molba se sastoji od paketa koji sadrži neki tekst i broj koji potvrđuje broj znakova u tom tekstu. Na primjer, „Jedanaest slova: informatika“. Kako bi računalo potvrdilo da je paket namijenjen za nj, ono treba moći otvoriti paket, te poslati paket istog sadržaja nazad. [69]

U verzijama OpenSSLa zahvaćenim Heartbleedom, postojala je mana u ovom procesu. Naime, verzija programa u pitanju nije provjeravala je li broj slova u poslanoj poruci jednak broju slova koji je poruka tvrdila da zahtjeva. Zbog toga, ako bi korisnik na jednoj strani poslao poruku s uvećanim cijelim brojem, nešto neočekivano bi se dogodilo. Na primjer, haker bi sa svog računala poslao modificiranu poruku „Devetsto deset slova: informatika“. Potom bi server vratio ne samo sadržaj poruke, nego i ono što se nalazilo u njegovoj memoriji nakon toga, sve dok se ne bi ispunio broj slova koja je korisnik tražio. Time bi privatni podatci nenamijenjeni korisniku bili poslani s servera. Ovom rupom su zahvaćene su sve verzije OpenSSLa od 1.0.1 do 1.0.1f, što znači da je u vrijeme objavljivanja postojanja sigurnosne rupe, ona bila prisutna na velikom broju servera već dvije godine. [70]

OpenSSL je kroz te dvije godine bio korišten posvuda. Razne banke su ga je koristile za milijunske transakcije svakodnevno. Zbog toga, nakon što je u travnju 2014. godine obznanjeno postojanje ove sigurnosne rupe među stručnjacima je izbila panika. Rješenje za

[67] http://heartbleed.com/
[68] Goodin, Dan. Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping. 8.4.2014. URL: http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/ (20.9.2016.)
[69] Hunt, Troy. Everything you need to know about the Heartbleed SSL bug. 8.4.2014. URL: https://www.troyhunt.com/everything-you-need-to-know-about3/ (20.9.2016.)
[70] David, Gary. The Heartbleed Vulnerability: What It Is and How It Affects You. 10.4.2014. URL: https://blogs.mcafee.com/consumer/what-is-heartbleed/ (20.9.2016.)

problem je izdano tjedan dana kasnije, no i dva mjeseca nakon toga 300.000 stranica je ostalo ranjivo. Sveukupno, da se sigurnost nebrojenih Internet stranica nanovo testira, vjerojatno je utrošeno više od 500 milijuna dolara.[71]



U mjesecima nakon saniranja rupe bilo je dosta diskusije na temu prave štete nanesene ovom sigurnosnom rupom. Postavljalo se pitanje točnog broja hakera koji su dotičnu grešku iskoristili kako bi ukrali podatke. No, zbog nedostatka načina da se lako i točno utvrdi napad ovog tipa, statistika nije poznata.

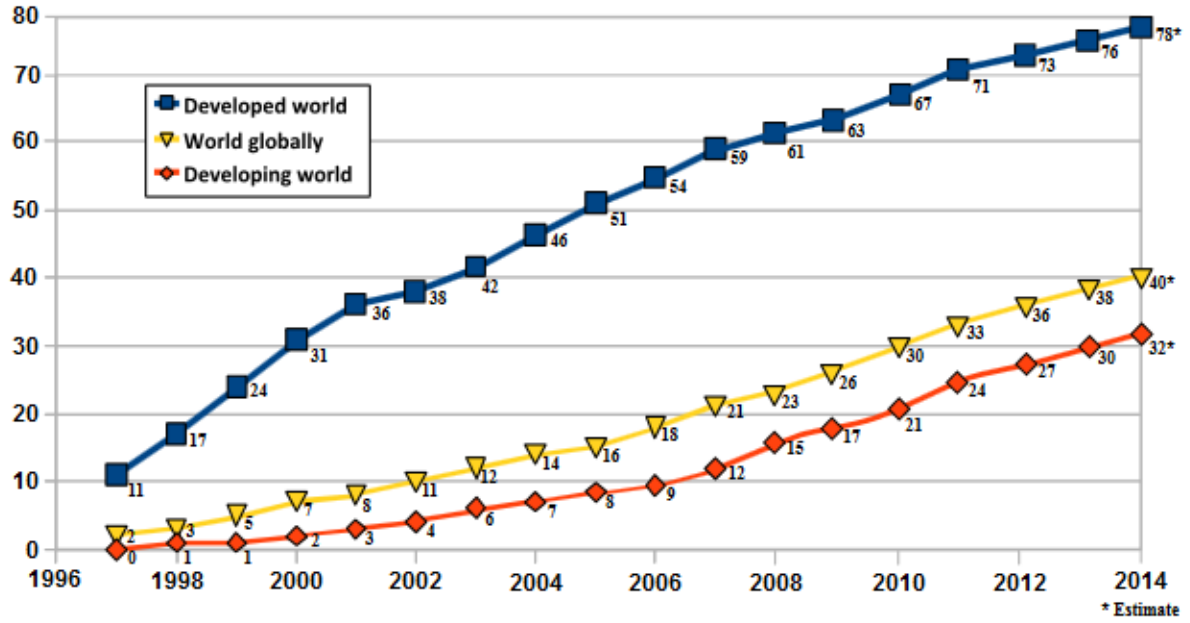
9 Nadziranje građana

9.1 Rast i važnost Interneta

Iako povijest Interneta počinje 50ih godina 20. stoljeća, u akademiji se počeo širiti tek 80ih godina, a šira javnost je dobila lagan pristup tek 90ih. U sljedećih 20 godina korištenje

[71] Kerner, Sean Michael. Heartbleed SSL Flaw's True Cost Will Take Time to Tally. 19.4.2014. URL: http://www.eweek.com/security/heartbleed-ssl-flaws-true-cost-will-take-time-to-tally.html (20.9.2016.)

Interneta je raslo nevjerojatnom brzinom, te je u danas preko 46% svjetskog stanovništva imalo pristup Internetu.[72][73]



Rast korisnika interneta[74]

U Hrvatskoj, redovit pristup Internetu ima preko 70% stanovnika. Po najnovijim procjenama iz 2016. godine broj Internet korisnika u Hrvatskoj je oko 3,1 milijun. To nas smješta na 45. mjesto na svjetskoj ljestvici po postotku.[75]

9.2 Nadzor Interneta

Zbog rasta korištenosti Interneta u životu velikog broja ljudi, počela je rasti važnost Interneta kao izvora informacija i vijesti, mjesto za kupovinu, komunikaciju, te razne druge aktivnosti. Time se pojavila želja za njegovom cenzurom i špijuniranjem. Bili razlozi politički (poput kritiziranja vlade), moralni (npr. Internet kockanje) ili sigurnosni (zaustavljanje terorista), mnoge stranke pokušavaju uspostaviti kontrolu nad Internetom. [76]

[72] http://www.internetlivestats.com/internet-users/
[73] Brief History of the Internet. URL: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (20.9.2016.)
[74] .Individuals using the Internet 2005 to 2014.International Telecommunications Union. URL: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls (20.9.2016.)
[75] Percentage of Individuals using the Internet 2000-2013. International Telecommunications Union. 2015. URL: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls (20.9.2016.)
[76] Dutton, William H.; Dopatka, Anna; Law, Ginette; Nash, Victoria. Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet. Division for Freedom of Expression, Democracy and Peace, United Nations Educational, Scientific and Cultural Organization (UNESCO). Paris, 2011.

Jedan od najočitijih primjera je iranska politika prema Internetu, gdje je u strahu od vanjskih političkih i kulturnih utjecaja, te nemorala, oko 50% od 500 najpopularnijih svjetskih web stranica blokirano.[77] Kako bi se osamostalili, te imali veću kontrolu nad Internetom i bolje zaštitili državne tajne od potencijalnih hakera, Iran je krenuo u razvijanje vlastitog državnog Interneta.[78] Država također otežava pristup proxy serverima i virtualnim privatnim mrežama, iako je to moguće zaobići.

Neki drugi primjeri državne cenzure su Singapur[79] i Sudan[80], radi zaštite tradicionalnih vrijednosti, Turkmenistan[81] i Njemačka[82], radi političke sigurnosti, te Turska[83] radi državne sigurnosti. Naravno, ova lista nije potpuna, već samo primjer jer je nabrajanje svih država koje cenzuriraju, te objašnjavanje razloga velika tema za sebe.

Države nisu jedini entiteti koji mogu cenzurirati Internet ili nadzirati korisnike. Gotovo svaka kompanija koja nudi online usluge može špijunirati korisnika. Zbog svoje masivne veličine, Google je dobar primjer.

Google ostvari preko 40.000 pretraživanja svake sekunde, to jest preko 3 milijarde pretraživanja dnevno.[84] S tim brojkama, Google je najveći pretraživač na Internetu. Google kompanija također posjeduje Gmail, najčešće korišteni besplatni online mail, te Youtube. Pri korištenju njihovog pretraživača, Google u web preglednik stavlja kolačić koji može biti korišten za praćenje korisnika po Internetu. Taj kolačić traje dvije godine, te se obnavlja svaki put kad koristimo Google stranice.[85] Google sprema te podatke, ali briše podatke o korisniku kod kojeg su podatci sakupljeni nakon dvije godine. Pretraživač je također često optužen da manipulira rezultate pretraga, s najstarijim slučajem iz 2002. kad je iz rezultata filtrirano više web stranica koje kritiziraju scijentologiju.[86]

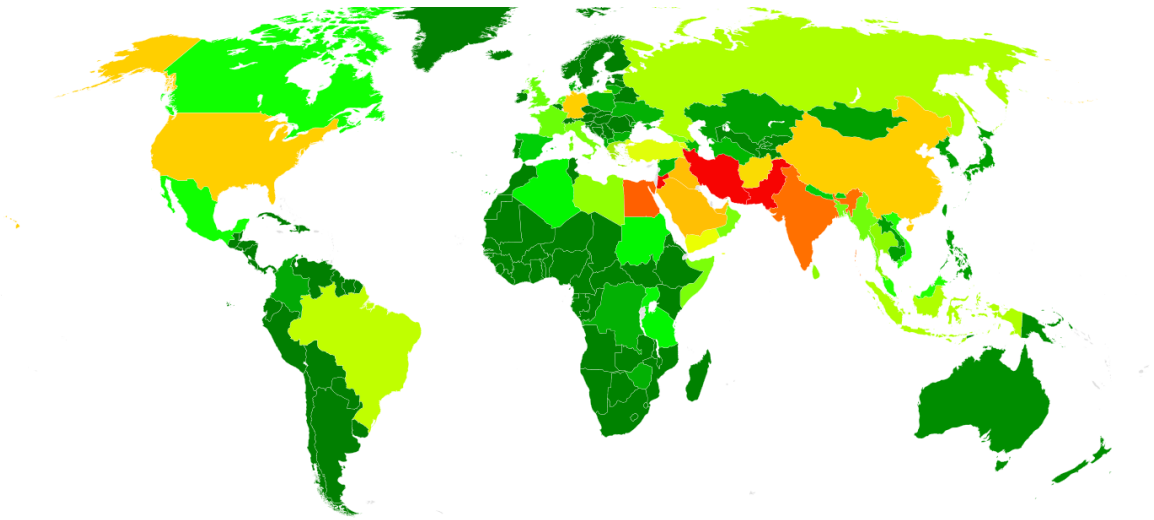
Kako bi građani mogli zaštititi svoju privatnost, Europska unija je stvorila ideju prava na zaborav. Naime, ukoliko se na Internetu mogu naći podatci o nezgodnom događaju iz prošlosti, osoba može zatražiti od Europske unije (ili Argentine, druge države s sličnim zakonom) da Google ili drugi pretraživači uklone spornu web stranicu ili podatke.[87]

---

[77] Shaheed, Ahmed. Layers of Internet Censorship in Iran. 5.7.2014. URL: http://shaheedoniran.org/english/blog/layers-of-internet-censorship-in-iran/ (20.9.2016.)
[78] Iran rolls out domestic Internet. 29.8.2016. URL: http://www.bbc.com/news/technology-37212456 (20.9.2016.)
[79] Singapore bans two porn websites in symbolic move. 23.5.2008. URL: http://www.reuters.com/article/us-singapore-internet-odd-idUSS2322899620080523 (20.9.2016.)
[80] https://opennet.net/research/profiles/sudan (20.9.2016.)
[81] Turkmenistan: News black hole. URL: https://12mars.rsf.org/2014-en/2014/03/10/turkmenistan-news-black-hole-turkmentelekom/ (20.9.2016.)
[82] Sherr, Ian. https://www.cnet.com/news/germany-is-putting-an-end-to-hate-speech-on-the-internet/ (20.9.2016.)
[83] Internet censorship in Turkey. 3.5.2015. URL: https://policyreview.info/articles/analysis/internet-censorship-turkey (20.9.2016.)
[84] http://www.internetlivestats.com/google-search-statistics/ (20.9.2016.)
[85] Privacy FAQ. https://www.google.com/policies/faq/ (20.9.2016.)
[86] GOOGLE, Censorship and Scientology?. 21.3.2003. URL: https://web.archive.org/web/20060515015927/http://www.factnet.org/Scientology/Google_Scientology.html (20.9.2016.)
[87] Factsheet on the "Right to beForgotten" ruling. URL: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (20.9.2016.)

9.3 NSA

NSA je obavještajna organizacija vlade Sjedinjenih američkih država. Ona se bavi globalnim nadziranjem, sakupljanjem i procesuiranjem podataka. Osnovana je 1952. godine od strane jedinice koja je za vrijeme Drugog svjetskog rata razbijala šifre. Danas je najveća američka obavještajna organizacija i po broju zaposlenih i po budžetu. [88][89]



Zeleno: zemlje iz kojih NSA skuplja najmanje podataka; Crveno: najviše[90]

U nedavnoj povijesti, prva veća kontroverza u kojoj se američka NSA našla, se dogodila 2005. godine kad je otkriveno da je agencija prisluškivala telefonske i računalne veze velikog broja Amerikanaca.[91] No pravi skandal je nastao tek 2013. kad je Edward Snowden objavio klasificirane dokumente pokazujući pravi opseg sakupljanja podataka.

Od petog mjeseca 2013. godine klasificirani podatci su počeli izlaziti na vidjelo, te nisu prestali od tad.[92] Među prvima je bila mapa koja opisuje količinu procesuiranih podataka po državi. Zelena boja označava najmanje, a crvena najviše špijuniranja.

---

[88] Howe, George F. The Early History of NSA. URL: https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/early_history_nsa.pdf (20.9.2016.)

[89] Gellerman, Barton; Miller Greg. 'Black budget' summary details U.S. spy network's successes, failures and objectives. 29.8.2014. URL: https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (20.9.2016.)

[90] Greenwald, Glen; MacAskill, Even. Boundless Informant: the NSA's secret tool to track global surveillance dana. 11.6.2013. URL: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (20.9.2016.)

[91] Greenwald, Glen. NSA collecting phone records of millions of Verizon customers daily. 6.6.2013. URL: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (20.9.2016.)

[92] Global Surveilance. URL: https://www.ub.uio.no/fag/informatikk-matematikk/informatikk/faglig/bibliografier/no21984.html (20.9.2016.)

NSA svakodnevno prati stotine milijuna mobilnih telefona, te je redovito pokazano da ima pristup svim komunikacijama preko Googlea, Microsofta, Skypea, Applea, Yahooa itd. Također redovito traže od raznih američkih ako ne i šire, pružatelja Interent usluga podatke o prometu korisnika. Kompanije koje nude privatne virtualne mreže često koriste tu činjenicu kako bi reklamirali svoje usluge. I dok je istina da je teže razbiti enkripciju virtualne privatne mreže, znano je da u barem nekim slučajevima NSA može i to postići.[93]

Također je objavljeno je da su uspješno razbili enkripciju Googleovog Gmaila, te da su imali pristup svim mailovima više godina. Pošto je ovaj podatak postao poznat, Google je brzo reagirao u pokušaju da zaštiti korisnike, no nije poznato je li uspio.[94]

Počevši s 2000. godinom, NSA je uložila stotine milijuna dolara kako bi pronašla i stvorila rupe u raznim metodama za enkripciju. Fokusirali su se posebno na SSL, virtualne privatne mreže, te 4G vezu za mobilni Internet.[95]

9.4 Kineski vatrozid

Jedan od najpoznatijih sustava za špijuniranje Internet korisnika i cenzuru je takozvani Veliki kineski vatrozid. Projekt je pokrenula kineska vlada 2003. godine pod imenom „Projekt zlatnog štita“. Završen je 2006. godine, te ga nadgleda državna policija. Pod njima rade civili koji pregledavaju Internet sadržaj odabran od strane softvera koji kontrolira Internet komunikaciju.[96]

Glavni prioritet vatrozida je pregledavanje domaćih web stranica i emailova kako bi se pronašli politički nepodobni sadržaji i zaustavili potencijalni protesti. Također se pregledavaju i online igrice, te se zaustavljaju ilegalni sadržaji.[97]

Jedan od načina na koji se zaustavlja nepodobni sadržaj je IP blokiranje, to jest, zabrana komuniciranja s web stranicama koje dolaze s određenih servera i mjesta na svijetu. Isto tako, određeni URLovi su blokirani, te promet između korisnika i te web stranice zaustavljen. Oba se slučaja daju izbjeći korištenjem proxy servera i dodatne enkripcije, no veoma je moguće da bi i taj server mogao biti blokiran, te da bi enkripcija mogla privući pažnju.[98]

---

[93] Perlroth, Nicole; Larson, Jeff; Shane, Scott. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. 5.9.2013. URL: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=1 (20.9.2016.)

[94] Leswing, Kif. What it looks like when the NSA hacks into your Gmail and Facebook. 15.8.2016. URL: http://www.businessinsider.com/nsa-prism-target-had-gmail-and-facebook-hacked-2016-8 (20.9.2016.)

[95] Gillum, Jack. Report: NSA cracked most online encryption. 9.5.2013. URL: http://phys.org/news/2013-09-british-spy-agencies-web-encryption.html (10.9.2016.)

[96] The Great Firewall of China: Background. 1.5.2011. URL: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/ (20.9.2016.)

[97]

[98] VPNs & Internet in China: Everything you need to know. 7.12.2014. URL: https://vpnreviewer.com/internet-vpn-china (20.9.2016.)

U slučaju da paketići koje računalo šalje ili prima sadrži zabranjene ključne riječi, promet može biti zaustavljen, te korisnik analiziran. Ovo zahvaća više protokola, no najviše zahvaća web pretraživače.

U nekim slučajevima kineski serveri zaustave promet, pregledaju sadržaj, te ga pošalju korisniku, praveći se kao da se ništa nije dogodilo. Tako će, ukoliko korisnici na dva kraja razgovaraju, državni server moći špijunirati razgovor. Ovaj tip napada na korisnika je čest i među hakerima, te se zove čovjek u sredini („man in the middle“) napad.

Kako bi korisnici zaobišli cenzuru, najčešće se koriste proxy serveri izvan Kine. No, bez veze sigurne barem kao HTTPS, mogućnost da će vatrozid uspjeti detektirati i cenzurirati vezu je velika.

Od ranije spomenutih sigurnijih Internet i darknet sistema, Tor i Freenet mogu zaobići barem neke filtere, no Tor nije pouzdan. Isto tako i virtualne privatne mreže mogu pomoći. Ipak, Kineski vatrozid se redovito ažurira, te među ostalim detektira i blokira Tor te redovito zabranjuje raspon IP adresa u kojima se nalaze razne virtualne privatne mreže. I dok VPN proizvođači ne mogu napraviti ništa osim promjene svojih serverskih centara, programeri Tora se redovito nadmudruju s vatrozidom. Ispitivanjem puta kojim paketići putuju uspjeli su otkriti da je svo filtriranje podataka u Kini centralizirano umjesto na razini provincija i da se filtri najviše fokusiraju na aplikacijski i transportni protokol. Ti podatci su timu bili vrlo važni pri odlučivanju kamo dalje s razvojom Tor softvera. Igra mačke i miša, privatnosti i enkripcije, cenzure i širenja podataka se nastavlja.[99][100]

[99] Learning more about the GFW's active probing system. 14.9.2015. URL: https://blog.torproject.org/category/tags/china (20.9.2016.)
[100] Freenet FAQ. URL: Blocked: https://freenetproject.org/help.html#blocked (20.9.2016.)

10 Zaključak

Kako bih oslikao stanje u kojem se nalaze korisnici Interneta u današnjem svijetu, obradio sam više tema, te sam se dotaknuo velikog broja specijaliziranih polja. Kroz rad sam se potrudio dotaknuti osnovne problematike u svakoj od njih kako bih predočio širi pejzaž tog polja u današnjem svijetu.

Kroz gotovo cijeli rad se ponavlja ime jedne agencije, američke NSA. I to ne samo kroz rad, već je njihovo ime postalo poznato i često na Internet portalima, u novinama, socijalnim mrežama, čak i televiziji, do te mjere da ih je spomenuti postao klišej. NSA je postala toliko eksponirana da često zaboravimo kako nije jedina. Postoje mnogi državni aparati s sličnim ciljevima. U programima za globalno nadziranje sudjeluju i agencije mnogih drugih zemalja. Kad bi im i vjerovali, Internet ostaje pun hakera i zloćudnih programa.

Možemo li učiniti svoju vezu sigurnom u ovakvom svijetu? Hoće li doći vrijeme kad će svi podatci na Internetu zauvijek ostati dostupni i dekriptirani? Hoće li Internet postati centraliziran i pasti pod upravu nacionalnih ili međunarodnih vlada?

Ako pitamo velik broj programera, njihov odgovor možemo naći u standardima i aplikacijama koje stvaraju. Mozilla i Google nam to pokazuju svojim žarkim zalaganjem za HTTPS protokol. Različite grupe nam daju svoj odgovor kroz Tor, Freenet i slične projekte. Čak i kompanije prepoznaju želju za sigurnošću kroz sve veću ponudu virtualnih privatnih mreža.

Niti jedno od ovih rješenja nije savršeno, te softver ide dalje u oba smjera. Standardi za enkripciju se povisuju, a broj računala korištenih za razbijanje istoga raste. Hoće li doći do promjene paradigme koja će izmijeniti dinamiku ovog sukoba? Možda, no rješenje zasigurno još nije stiglo.

Uz pojavljivanje Bitcoina se otvorila nova Pandorina kutija. Iako Bitcoin nije postao konkurent pravom novcu, definitivno je otvorio nova polja istraživanja kao decentralizirana digitalna kripto-valuta. Vlade brine pomak komunikacije iz kafića koji se može nadzirati u novi svijet Interneta. Isto tako i banke brine ideja novca kojim ne mogu upravljati. U oba slučaja, lagano rješenje je u kontroli i transparentnosti digitalnog prometa.

I dok se veliki igrači bore za budućnost Interneta, mali hakeri pokušavaju upasti korisnicima na bežičnu vezu, te virusi čekaju posvuda na Internetu za naivnog korisnika da ih pokrene.

Smatram da je važno holistički procijeniti situaciju u kojoj se nalazimo jer to na kraju pomaže korisniku da razumije povijesni kontekst vremena koje protječe, potencijalno neočekivane rezultate i preokrete u tehnologiji koja se razvija i koristi, te možda za korisnika i najvažnije, pomogne mu pri „surfanju“ Internetom.

Dok etička i pravna borba na tu temu traje, a kriminalci otkrivaju nove „industrije“, jedino što korisniku preostaje je pobrinuti se za vlastitu sigurnost.

11 Literatura

1. Anonymity Networks. Don't use one, use all of them!. 2012. URL: http://null-byte.wonderhowto.com/news/anonymity-networks-dont-use-one-use-all-them-0133881/ (20.9.2016.)
2. Barnes, Richard. Deprecating Non-Secure HTTP. 30.4.2015. URL: https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/ (20.9.2016.)
3. Berners-Lee, Tim. HyperText Transfer Protocol. URL: https://www.w3.org/History/19921103-hypertext/hypertext/WWW/Protocols/HTTP.html (20.9.2016.)
4. Brief History of the Internet. URL: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (20.9.2016.)
5. Data Policy. URL: https://www.facebook.com/policy.php (16.9.2016.)
6. David, Gary. The Heartbleed Vulnerability: What It Is and How It Affects You. 10.4.2014. URL: https://blogs.mcafee.com/consumer/what-is-heartbleed/ (20.9.2016.)
7. Denmark proposes cash-free shops to cut retail costs. 6.5.2015. URL: http://www.reuters.com/article/denmark-cash-idUSL5N0XX2ZQ20150506 (16.9.2016.)
8. Dutton, William H.; Dopatka, Anna; Law, Ginette; Nash, Victoria. Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet. Division for Freedom of Expression, Democracy and Peace, United Nations Educational, Scientific and Cultural Organization (UNESCO). Paris, 2011.
9. Eckersley, Peter. Launching in 2015: A Certificate Authority to Encrypt the Entire Web. 18.11.2014. https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web (20.9.2016.)
10. Epstein, Adam. Netflix launched this handy speed test so you can go shame your internet provider. 19.5.2016. URL: http://qz.com/688033/netflix-launched-this-handy-speed-test-so-you-can-go-shame-your-internet-provider/ (20.9.2016.)
11. Evans, Dave. The Internet of Things. 2011. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (16.9.2016.).
12. Exclusive: Obama sharply criticizes China's plans for new technology rules. 3.3.2015. URL: http://www.reuters.com/article/us-usa-obama-china-idUSKBN0LY2H520150303 (20.9.2016.)
13. Factsheet on the “Right to beForgotten” ruling. URL: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (20.9.2016.)
14. Fagoyinbo, Joseph Babatunde. The Armed Forces: Instrument of Peace, Strength, Development and Prosperity. 28.5. 2013. AuthorHouse.
15. FAQ. https://wiki.freenetproject.org/FAQ (20.9.2016.)
16. Fell, Mark. Roadmap for the Emerging Internet of Things – Its Impact, Architecture and Future Governance. 2014. URL: http://carre-strauss.com/documents/IoT_Roadmap.pdf (16.9.2016.)
17. Freenet: About. https://freenetproject.org/about.html (20.9.2016.)
18. Freenet FAQ. URL: Blocked: https://freenetproject.org/help.html#blocked (20.9.2016.)
19. Freenet: Understand. https://freenetproject.org/documentation.html#understand (20.9.2016.)
20. Gellerman, Barton; Miller Greg. ‘Black budget’ summary details U.S. spy network’s successes, failures and objectives. 29.8.2014. URL: https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (20.9.2016.)
21. Gellerman, Barton; Poitras, Laura. US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program. 7.6.2013. URL: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (16.9.2016.)
22. Gillum, Jack. Report: NSA cracked most online encryption. 9.5.2013. URL: http://phys.org/news/2013-09-british-spy-agencies-web-encryption.html (10.9.2016.)
23. Global Surveilance. URL: https://www.ub.uio.no/fag/informatikk-matematikk/informatikk/faglig/bibliografier/no21984.html (20.9.2016.)
24. Goodin, Dan. Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping. 8.4.2014. URL: http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/ (20.9.2016.)
25. Goodin, Dan. NSA official: Support of backdoored Dual_EC_DRBG was “regrettable”. 14.1.2015. http://arstechnica.com/security/2015/01/nsa-official-support-of-backdoored-dual_ec_drbg-was-regrettable/ (20.9.2016)
26. GOOGLE, Censorship and Scientology?. 21.3.2003. URL: https://web.archive.org/web/20060515015927/http://www.factnet.org/Scientology/Google_Scientology.html (20.9.2016.)

27. Gralla, Preston; Michael Troller. How the Internet Works. 8th edition. Que. 2006.
28. Greenberg, Andy. Hacker Lexicon: What is The Dark Web?. 19.11.2014. URL: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (20.9.2016.)
29. Greenwald, Glen. How the NSA tampers with US-made internet routers. 12.5.2014. URL: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (20.9.2016.)
30. Greenwald, Glen; MacAskill, Even. Boundless Informant: the NSA's secret tool to track global surveillance dana. 11.6.2013. URL: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (20.9.2016.)
31. Greenwald, Glen. NSA collecting phone records of millions of Verizon customers daily. 6.6.2013. URL: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (20.9.2016.)
32. Greenwald, Glen; MacAskill Ewen; Ackerman Spencer; Rushe Dominic. Microsoft handed the NSA access to encrypted messages. 12.7.2013. URL: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (16.9.2016.)
33. Gustafson, Karl E.; Black, Ryan J.;Groom, Sharon E.; Tam, Michele. The Internet Never Forgets: Google Inc.'s "right to be forgotten" EU ruling and its implications in Canada. 2014. URL: http://www.mcmillan.ca/The-Internet-Never-Forgets-Google-Incs-right-to-be-forgotten-EU-ruling-and-its-implications-in-Canada (20.9.2016.)
34. Halderman, Alex; Heninger, Nadia;. How is NSA breaking so much crypto?. 14.10.2015. URL: https://freedom-to-tinker.com/2015/10/14/how-is-nsa-breaking-so-much-crypto/ (20.9.2016.)
35. Howe, George F. The Early History of NSA. URL: https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/early_history_nsa.pdf (20.9.2016.)
36. https://geti2p.net/en/
37. https://gnunet.org/
38. http://heartbleed.com/
39. https://opennet.net/research/profiles/sudan (20.9.2016.)
40. HTTPS usage statistics on top websites. 29.8.2016. URL: https://statoperator.com/research/https-usage-statistics-on-top-websites/ (20.9.2016.)
41. http://www.internetlivestats.com/google-search-statistics/ (20.9.2016.)
42. http://www.internetlivestats.com/internet-users/
43. https://www.urbit.org/
44. Hunt, Troy. Everything you need to know about the Heartbleed SSL bug. 8.4.2014. URL: https://www.troyhunt.com/everything-you-need-to-know-about3/ (20.9.2016.)
45. Individuals using the Internet 2005 to 2014.International Telecommunications Union. URL: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls (20.9.2016.)
46. Internet censorship in Turkey. 3.5.2015. URL: https://policyreview.info/articles/analysis/internet-censorship-turkey (20.9.2016.)
47. 'INTERNET OF THINGS' CONNECTED DEVICES TO ALMOST TRIPLE TO OVER 38 BILLION UNITS BY 2020. 27.8.2015. URL: http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020 (16.9.2016.)
48. Iran rolls out domestic Internet. 29.8.2016. URL: http://www.bbc.com/news/technology-37212456 (20.9.2016.)
49. Jackson, Brian. What is the Difference Between HTTP and HTTPS?. 20.7.2016. URL: https://www.keycdn.com/blog/difference-between-http-and-https/ (20.9.2016.)
50. Kerner, Sean Michael. Heartbleed SSL Flaw's True Cost Will Take Time to Tally. 19.4.2014. URL: http://www.eweek.com/security/heartbleed-ssl-flaws-true-cost-will-take-time-to-tally.html (20.9.2016.)
51. Khandelwal, Swati. How NSA successfully Broke Trillions of Encrypted Connections. 16.10.2015. URL: https://thehackernews.com/2015/10/nsa-crack-encryption.html (20.9.2016.)
52. Khandelwal, Swati. Warning: Over 100 Tor Nodes Found Designed to Spy On Deep Web Users. 26.6.2016. URL: https://thehackernews.com/2016/07/tor-deep-web-spying.html (20.9.2016.)
53. Kirk, Jeremy. Study: Adobe Flash cookies pose vexing privacy questions. 11.8.2009. URL: https://web.archive.org/web/20090813161926/http://www.networkworld.com/news/2009/081109-study-adobe-flash-cookies-pose.html (20.9.2016.)
54. Kelly, Lorcan Roche. Citi Economist Says It Might Be Time to Abolish Cash. 10.4.2015. URL: https://www.bloomberg.com/news/articles/2015-04-10/citi-economist-says-it-might-be-time-to-abolish-cash (16.9.2016.)
55. Keyloggers Explained: What You Need to Know. 2014. URL: http://www.howtogeek.com/180615/keyloggers-explained-what-you-need-to-know/ (16.9.2016.)

56. Larson, Jeff; Perlroth, Nicole; Shane, Scott. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. 5.9.2013. URL: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=1 (20.9.2016.)
57. Learning more about the GFW's active probing system. 14.9.2015. URL: https://blog.torproject.org/category/tags/china (20.9.2016.)
58. Levine, Yasha. Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government. 16.6.2016. URL: https://pando.com/2014/07/16/tor-spooks/ (20.9.2016.)
59. Leswing, Kif. What it looks like when the NSA hacks into your Gmail and Facebook. 15.8.2016. URL: http://www.businessinsider.com/nsa-prism-target-had-gmail-and-facebook-hacked-2016-8 (20.9.2016.)
60. Macintire, Tim. Take a closer look at OpenBSD. 8.8.2006. URL: https://web.archive.org/web/20070127231412/http://www-128.ibm.com/developerworks/aix/library/au-openbsd.html (20.9.2016.)
61. Maltese, Marco E. G. Bitcoin: Left For Dead Hundreds Of Times - Still Alive And Kicking. 25.11.2015. URL: https://cointelegraph.com/news/bitcoin-left-for-dead-hundreds-of-times-still-alive-and-kicking (16.9.2016.)
62. Masnick, Mike. FBI Quietly Removes Recommendation To Encrypt Your Phone. 26.3.2015. URL: https://www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml (16.9.2016.)
63. Matonis, Jon. Bitcoin 101. // White Paper. 26.5.2013. URL: http://www.trssllc.com/wp-content/uploads/2013/05/White_Paper_Bitcoin_101.pdf (16.9.2016.)
64. Murdoch, Steven J. How Tor's privacy was (momentarily) broken, and the questions it raises. 10.20.2015. URL: http://phys.org/news/2015-12-tor-privacy-momentarily-broken.html (20.9.2016.)
65. 'NSA totally dysfunctional – too much data to detect threats' – whistleblower. 5.5.2016. URL: https://www.rt.com/op-edge/341905-nsa-us-leaks-terrorism/ (20.9.2016.)
66. One cell is enough to break Tor's anonymity. 2009. URL: https://blog.torproject.org/blog/one-cell-enough (20.9.2016.)
67. Percentage of Individuals using the Internet 2000-2013. International Telecommunications Union. 2015. URL: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls (20.9.2016.)
68. Privacy FAQ. https://www.google.com/policies/faq/ (20.9.2016.)
69. Reilly, Richard. Here's how Facebook, Google, and Apple are tracking you now. 6.10.2016. URL: http://venturebeat.com/2014/10/06/the-cookie-is-dead-heres-how-facebook-google-and-apple-are-tracking-you-now/ (20.9.2016.)
70. Rhee, Man Young. Internet Security: cryptographics principles, algorithms and protocols. 1st edition. Wiley, 2003
71. Rubenking, Neil J.. The Best Antivirus Protection of 2016. 20.6.2016. URL http://www.pcmag.com/article2/0,2817,2372364,00.asp (20.9.2016.)
72. Singapore bans two porn websites in symbolic move. 23.5.2008. URL: http://www.reuters.com/article/us-singapore-internet-odd-idUSS2322899620080523 (20.9.2016.)
73. Shaheed, Ahmed. Layers of Internet Censorship in Iran. 5.7.2014. URL: http://shaheedoniran.org/english/blog/layers-of-internet-censorship-in-iran/ (20.9.2016.)
74. Sherr, Ian. https://www.cnet.com/news/germany-is-putting-an-end-to-hate-speech-on-the-internet/ (20.9.2016.)
75. Steam'd Penguins. 12.6.2012. URL: http://blogs.valvesoftware.com/linux/steamd-penguins/ (20.9.2016.)
76. Szoldra, Paul. This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. 2016. URL: http://www.businessinsider.com/snowden-leaks-timeline-2016-9 (16.9.2016.)
77. Spy Files. Wikileaks. URL: https://wikileaks.org/spyfiles/ (16.9.2016.)
78. Tanenbaum, Andrew S. Computer Networks. New Jersey: Pearson Education, 2003.
79. The Great Firewall of China: Background. 1.5.2011. URL: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/ (20.9.2016.)
80. Tor: Overview. URL: https://www.torproject.org/about/overview.html.en (20.9.2016.)
81. Turkmenistan: News black hole. URL: https://12mars.rsf.org/2014-en/2014/03/10/turkmenistan-news-black-hole-turkmentelekom/ (20.9.2016.)
82. Usage of operating systems for websites. 20.9.2016. URL: https://w3techs.com/technologies/overview/operating_system/all (20.9.2016.)
83. Virtual Private Networking: An Overview. 4.9.2001. URL: https://technet.microsoft.com/en-us/library/bb742566.aspx (20.9.2016.)

84. Volpenheim, Sarah. Police in online struggle. 18.11.2015. URL: http://www.thedickinsonpress.com/news/north-dakota/3885239-predators-police-online-struggle (20.9.2016.)
85. VPNs & Internet in China: Everything you need to know. 7.12.2014. URL: https://vpnreviewer.com/internet-vpn-china (20.9.2016.)
86. Vries, Lloyd. CIA Caught Sneaking Cookies. 20.3.2002. URL: http://www.cbsnews.com/news/cia-caught-sneaking-cookies/ (20.9.2016.)
87. Westberg, Hans. 50 BILLON CNNECTIONS 2020. 2010. URL: http://hugin.info/1061/R/1403231/357583.pdf (16.9.2016.)
88. What is the Tor Browser? URL: https://www.torproject.org/projects/torbrowser.html.en (20.9.2016.)
89. Wood, Jessica.. "The Darknet: A Digital Copyright Revolution. 2010. URL: http://jolt.richmond.edu/v16i4/article14.pdf (20.9.2016.)
90. Zetter, Kim. Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA. 22.12.2015. URL: https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/ (20.9.2016.)
91. Zetter, Kim. Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. 18.12.2015. URL: https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ (20.9.2016.)