FBIM Transactions
DOI 10.12709/fbim.02.02.02.07

INTERNET SIGURNOST U SVETLU OTKRIĆA EDVARDA SNOUDENA

INTERNET SECURITY IN LIGHT OF EDWARD SNOWDEN'S REVELATIONS

Zoran Čekerevac
"Union" Univerzitet – Fakultet za poslovno industrijski menadžment, Beograd, Srbija

Zdenek Dvorak
University of Žilina, Faculty of Special Engineering, Žilina, Slovakia

Petar Čekerevac
Libek, Beograd, Srbija

JEL category: **L86, L96**

Apstrakt

Internet je danas glavni komunikacioni kanal za sve privatne i poslovne komunikacije, a pored njega u stalnom usponu je i upotreba mobilnih komunikacija. Svi ovi vidovi komunikacija su izloženi mnogim opasnostima, a integritet i tajnost podataka su ugroženi kako pri prenosu tako i pri skladištenju. Sigurnost i tajnost komunikacija na Internetu ugrožavaju brojni napadači, od pojedinačnih hakera pa sve do najviših državnih institucija.

S jedne strane izvanredno brz razvoj informacionih tehnologija omogućava njihovu sve efikasniju zaštitu, ali s druge strane i nove mogućnosti za prisluškivanje i špijunažu. „Višak" računarskih kapaciteta na strani napadača omogućava im da usmere pažnju ne samo na velike i značajne, već praktično na sve korisnike interneta uključujući i MSP i pojedince. Čak i u situacijama primene najsavremenije zaštite postoje načini da se neopaženo pristupi podacima. Tema postaje značajnija kada se imaju u vidu nedavni događaji vezani za aferu sa prisluškivanjem internet poruka od strane NSA koje je u časopisu The Guardian juna 2013 obelodanio Edward Snowden i koji su izazvali burne diskusije na ovu temu koje su potvrdile da se mnoge (ako ne sve) države bave prisluškivanjem telekomunikacionih kanala, a da je NSA imala „nesreću" da bude prva otkrivena. Pored prikupljanja podataka sa elektronske pošte, posebno su interesantni i tokovi novčanih transakcija. Objavljeni tajni podaci o razmerama špijuniranja komunikacionih kanala su nakratko poremetili i odnose među najmoćnijim državama, ali su doprineli da ova problematika dođe u žižu pažnje i da se kreiraju nova pravila i propisi. U ovom radu se razmatra trenutno stanje u internet poslovanju i posebno zaštita elektronske pošte.

Autor zadužen za korespodenciju:
Petar Čekerevac
petar@cekerevac.eu

Ključne reči: *internet, kreditne kartice, mobilne komunikacije, Edward Snowden, projekat Muscular, Windstop, tempora, Patriot Act*

Abstract

Modern communication and modern business are linked to the massive use of the Internet and mobile communications. However, use of Internet and mobile communications can compromise the integrity and confidentiality of data during both their transmission and their storage. Attackers can be a single hacker, but also the highest government institutions.

Remarkably rapid development of IT allows more efficient data protection, but also gives new opportunities for eavesdropping and spying. "Excess" of computing capacities on the attackers' side enables them to cover virtually all Internet users, including individuals. Even in situations with the latest protection there are ways to access data unnoticed. The topic becomes more significant when one considers the recent events related to an affair with wiretapping of internet posts by the NSA, which Edward Snowden revealed in The Guardian in June 2013. The publication of these secrets launched a flood of discussions that have confirmed that many (if not all) countries tapped telecommunication channels, and that the NSA only had the "misfortune" to be discovered first. In addition to collecting data from e-mails, of particular interest are flows of financial transactions. This information has contributed that this problem came to the focus of attention and that new rules and regulations will be created. This paper discusses the current state of the Internet business, and in paricular the protection of electronic mails.

Keywords: *Internet, credit card, mobile communications, Edward Snowden, Project Muscular, Windstop, Tempora, Patriot Act*

1 UVOD

Savremena komunikacija među ljudima i savremeno poslovanje vezani su za masovnu upotrebu Interneta. Internet je danas glavni komunikacioni kanal za elektronske novčane transakcije kreditnim i debitnim karticama, prenos elektronske pošte, međunarodne govorne i video komunikacije, a pored njega u stalnom usponu je i upotreba mobilnih komunikacija. Bez ovih komunikacija privredni subjekti danas praktično ne mogu da obavljaju svoju delatnost. Međutim, ovi vidovi komunikacija su izloženi mnogim opasnostima. Integritet i tajnost podataka su ugroženi kako pri prenosu tako i pri skladištenju. Izvanredno brz razvoj informacionih tehnologija omogućava njihovu sve efikasniju zaštitu, ali i povećane rizike od prisluškivanja i špijunaže, jer se danas praktično svako bez većih ograničenja može baviti neovlašćenim prikupljanjem podataka. „Višak" računarskih kapaciteta na strani napadača omogućava im da mogu da usmere pažnju ne samo na velika i značajna preduzeća, već praktično na sve korisnike interneta uključujući i MSP i pojedince. Čak i u situacijama primene najsavremenije zaštite postoje načini da se neopaženo pristupi podacima. Tema prisluškivanja i zaštite postaje značajnija kada se imaju u vidu nedavni događaji vezani za aferu sa prisluškivanjem Internet poruka od strane NSA (Nacionalna Siguronosna Agencija SAD) koju je u časopisu The Guardian juna 2013 obelodanio Edward Snowden i koji su izazvali burne diskusije na ovu temu koje su potvrdile da se mnoge (ako ne sve) države bave prisluškivanjem telekomunikacionih kanala, a da je NSA imala „nesreću" da bude prva otkrivena.

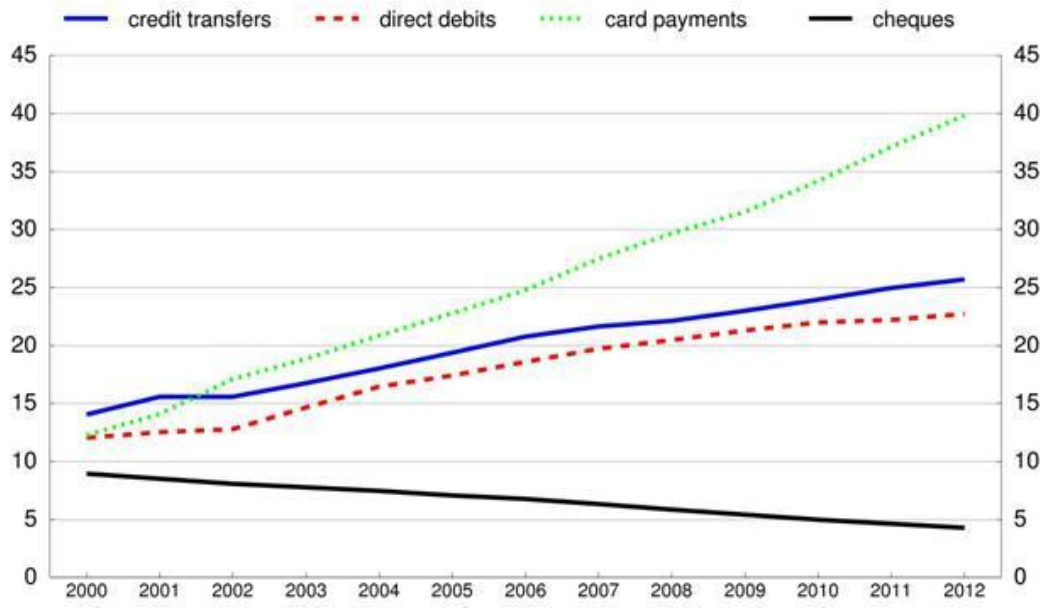
2 SAVREMENO INTERNET POSLOVANJE

Savremeno poslovanje je vezano za masovnu upotrebu elektronskih komunikacija, za elektronske novčane transakcije, kreditne i debitne kartice, plaćanja putem Interneta, prenos elektronske pošte, upotrebu mobilnih komunikacija i drugih informacionih tehnologija. Štaviše, savremeno poslovanje se bez njih praktično ni ne može realizovati. Prema godišnjem izveštaju Evropske Centralne Banke (ECB) u pogledu bezgotovinskih plaćanja, u 2011-oj godini zabeležen je porast od 4,6%, na 90,6 milijardi EUR, u odnosu na prethodnu godinu. Plaćanje kreditnim karticama je obuhvatilo 41% svih transakcija. (European Central Bank, Payment Statistics for 2011, 2012) U 2012-oj godini porast bezgotovinskih plaćanja u odnosu na prethodnu

godinu iznosio je 4,2% i dostigao 95,5 milijardi EUR, a plaćanje karticama je dostiglo 42%. (European Central Bank, 2013)

Na slici 1 prikazan je broj transakcija u milijardama EUR u periodu 2000-2012 godina.

Prema rezultatima Osterman Research (Symantec, 2013), 74% intelektualne svojine organizacija boravi u elektronskoj pošti ili kao tekst ili kao prilog. Na osnovu izveštaja The Radicati Group, Inc. Prikazanih u Tabeli 1 može se videti da se procenjuje da je u 2013-oj godini funkcionisalo nešto manje od četiri milijarde računa (adresa) elektronske pošte i da će taj broj u naredne četiri godine porasti za preko milijardu novih računa. Od svih računa, približno četvrtinu predstavljaju računi koji se koriste isključivo u poslovne svrhe. Sigurno je da se i veliki broj privatnih računa takođe koristi u poslovne svrhe.



Slika 1 Broj transakcija u milijardama EUR u periodu 2000-2012 godina (procenjene vrednosti) Izvor: ECB (Payment statistics for 2012, 2013)

Tabela 1 Privatni i poslovni e-mail računi 2013-2017 g.

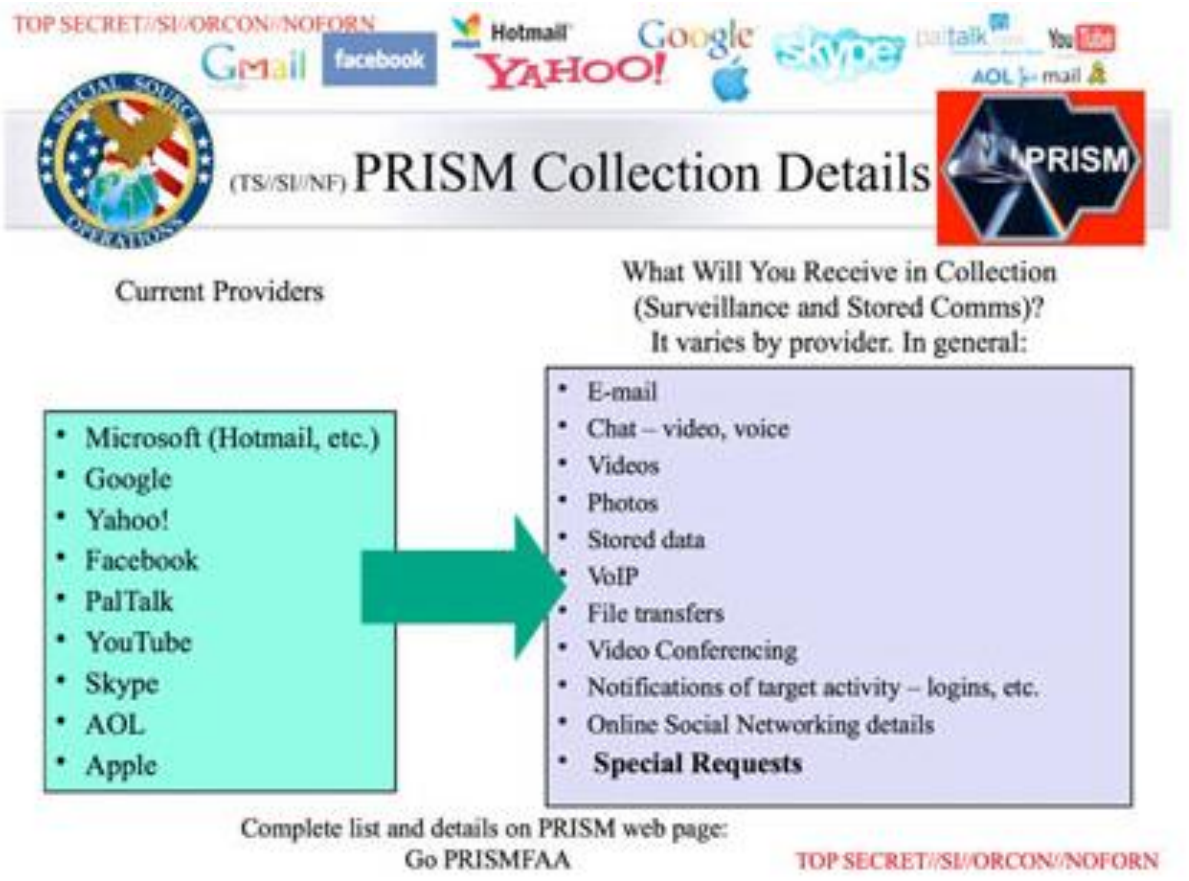
	2013	2014	2015	2016	2017
Ukupni broj e-mail računa u milijardama	**3,899**	**4,116**	**4,353**	**4,626**	**4,920**
Broj poslovnih e-mail računa u milijardama	**0,929**	**0,974**	**1,022**	**1,078**	**1,138**
% Poslovnih e-mail računa	24%	24%	23%	23%	23%
Privatnih e-mail računa u milijardama	**2,970**	**3,142**	**3,331**	**3,548**	**3,782**
% Privatnih e-mail računa	76%	76%	77%	77%	77%

Izvor (Radicati & Levenstein, 2013)

Mobilne komunikacije su danas vrlo popularan, ako ne i najmasovniji vid komunikacija. Broj aktivnih mobilnih telefona će prevazići svetsku populaciju u 2014-oj godini. (Pramis, 2013) Očekuje se da će do kraja 2013. godine biti aktivno 6,8 milijardi mobilnih telefona. (Betakit, 2013) Na osnovu statističkih podataka Svetske banke (The World Bank, 2013) prema broju mobilnih telefona na 100 stanovnika listu predvodi Makao SAR, Kina sa 284, a sledi Hong Kong SAR, Kina sa 228. Na dnu liste su Erirteja sa 5,4, Somalija sa 6,7, Severna Koreja sa 6,9 i Mijanmar sa 11,1 mobilnih telefona na sto stanovnika. Odgovarajući broj mobilnih telefona je u SAD 98,1, u Velikoj Britaniji 130,75, u Srbiji 92,8, a u Nemačkoj 131,3.

Imajući u vidu navedene podatke lako je sagledati bogatstvo informacija koje se svakodnevno prenosi komunikacionim kanalima. Sigurno je da su mnogi zainteresovani za prikupljanje podataka sa komunikacionih kanala u cilju njihove upotrebe ili kasnije upotrebe. Svaki korisnik interneta, kreditne kartice ili mobilnog telefona lako je mogao da pretpostavi da je osim toga što je korisnik usluge istovremeno i objekat posmatranja, ali je malo onih koji su bili svesni veličine resursa i obima špijunaže komunikacija. Polovinom 2013. godine naglo se digla bura oko bezbednosti elektronske pošte i podataka koji cirkulišu elektronskom poštom. (Čekerevac, Čekerevac, & Vasiljević, 2013) Iako se veruje da je primenom desktop računara, gejtveja i enkripcije prenos elektronske pošte bezbedan čak i u oblaku, Edward Snowden (Snowden, 2013) je pokazao da to i nije slučaj, da se elektronska pošta, i ne samo ona, aktivno prati i prisluškuje. Na osnovu The Guardian serijala „O bezbednosti i slobodi“ (Greenwald & MacAskill, 2013) Agencija za nacionalnu bezbednost (NSA) ima direktan pristup sistemima Google, Facebook, Apple i drugih američkih Internet giganata. U strogo poverljivom dokumentu čiji su sadržaj autori objavili, NSA pristup je deo ranije neobjavljenog programa pod nazivom Prizma, koji omogućava službama da prikupljaju materijal uključujući istorije pretraživanja, sadržaj e-pošte, prenošenje datoteka i razgovora uživo. Dokument tvrdi da se podaci prikupljaju direktno sa servera glavnih američkih provajdera Internet usluga. Zakonska osnova za prikupljanje podataka leži u USA Patriot Act (2001), Protect America Act of 2007 (2007), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (2008).

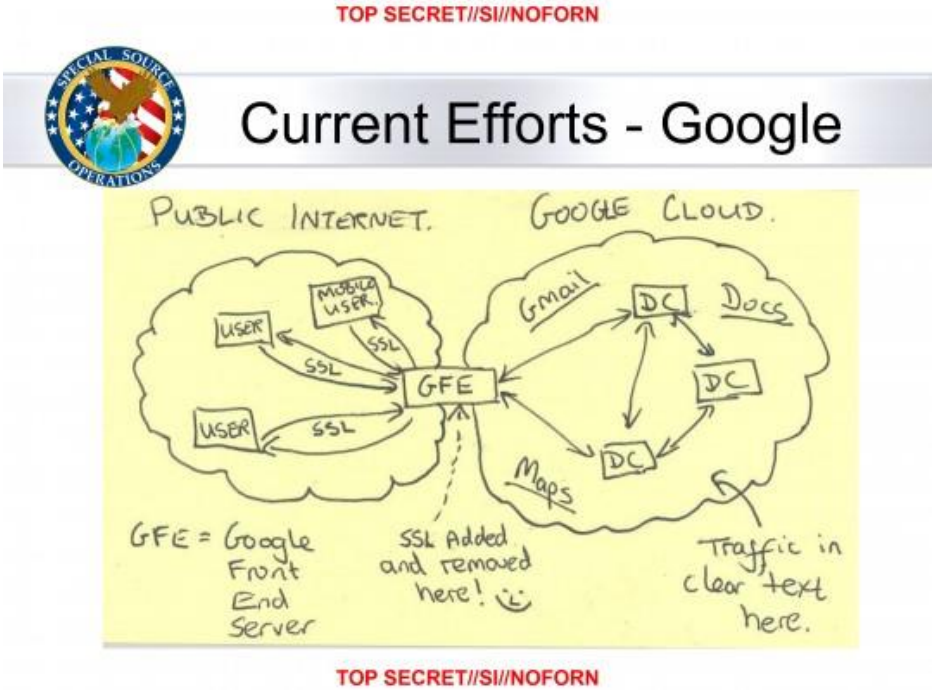
Na slici 2 prikazani su neki detalji prikupljanja podataka po projektu Prizma.



Slika 2 Detalji prikupljanja podataka po projektu Prizma (Izvor: (Greenwald & MacAskill, 2013))

U skladu sa pomenutom zakonskom regulativom, u program prisluškivanja su postepeno uključivani najveći svetski internet provajderi počev od Microsft-a (2007. god.), preko Yahoo-a (2008. god.), Google, Facebook i PalTalk (2009.), YouTube (2010.), Skype i AOL (2011.) i Apple (2012.) (Izvor: (Greenwald & MacAskill, 2013)) Lako je pretpostaviti da novi učesnici u

prisluškivanju nisu bili oduševljeni kada su od dobili NSA zahtev za preuzimanje korisničkih podataka, iako je on bio sudski odobren. Međutim, to sigurno nije ništa u odnosu na trenutak kada su saznali da je NSA, iza njihovih leđa, tajno preuzimala znatno veće količine podataka. (Oremus, 2013) Slika koju je objavio Washington Post 30. oktobra 2013. (v. sliku 3) bacila je novo svetlo na obim i vrstu prikupljanja podataka.



Slika 3 Prikaz napada na komunikaciju između Google i njegovih korisnika (Izvor (Gellman, 2013))

Na osnovu slike 3, tvrdnji Edwarda Snowdena i tzv. dobro obaveštenih izvora, Agencija za nacionalnu bezbednost (NSA) je tajno provalila u veze Yahoo-a i Google-a širom sveta. Prisluškivanjem tih linija, agencija je dobila mogućnost da prati rad više stotina miliona korisničkih računa što joj je otvorilo neslućene obaveštajne mogućnosti. Na osnovu poverljivih podataka objavljenih u The Washington Post-u (2013) aktivnosti su sprovođene u okviru tajnog projekta „Muscular“ namenjenog za presretanja saobraćaja sa privatnih linkova povezanih sa Yahoo i Google serverima. Kao glavni razlozi za uvođenje projekta „Muscular“ navode se (Nautiyal, 2013):

1. Mnogo rudarenja podataka obavlja se van teritorije SAD, gde su mehanizmi za praćenje slabije razvijeni i gde FISC (Foreign Surveillance Intelligence Court) nema jurisdikciju; i
2. Ovakav način prikupljanja podataka je znatno manje vidljiv kompanijama Internet provajderima koje su poslednjih godina postajale sve transparentnije u pogledu podataka koje dostavljaju državnim organima SAD.

Pristupna tačka poznata kao DS-200B nalazi se izvan teritorije SAD, kod za sada nepoznatog provajdera telekomunikacionih usluga. Kada se pročulo o programu „Muscular“ Google i Yahoo su ubrzali svoje aktivnosti na potpunom kriptovanju svojih mreža. (Galagher, 2013) Sličnu nameru je pokazao i Microsoft, koji je zbog sumnji da su i njihove linije nadgledane najavio da je ušao u proces enkripcije unutrašnjeg saobraćaja. (Wilking, 2013) Ovakve Microsoftove najave bi trebalo da kompenzuju činjenicu da je Microsoft pomagao NSA u premošćavanju mehanizama za zaštitu podataka miliona korisnika. (Piermon, 2013) U sličnim problemima se našao još jedan svetski gigant Cisco. U svom izveštaju novembra 2013 kompanija je najavila dve važne stvari: Kompanija se uključuje u oblast Interneta u nameri da na Internet poveže skoro svaki objekat na Zemlji i da pokreću nove tehnologije u tom smeru. Druga važna informacija je bila pad tražnje svog hardvera na tržištima u razvoju zbog strahova korisnika da NSA koristi američki hardver da špijunira ostali svet. Cisko je u to vreme beležio

pad narudžbina za 25% u Brazilu i 25% u Rusiji. Umesto očekivanog rasta prodaje od 6% Cisko je zabeležio pad od 12%. Objavljivanje informacija o prisluškivanju od strane NSA ugrozilo je poslovanje mnogih američkih kompanija okrenutih internet tehnologijama u ranoj fazi naglog uspona razvoja Interneta i da će se na duže staze otvoriti dodatni prostor za neameričke kompanije. (Mims, 2013)

Interesantno je da je u projekat prisluškivanja uključena i Velika Britanija preko zajedničkog programa „Windstop“. Sa strane Velike Britanije za projekat je nadležan Glavni komunikacioni centar (General Communications Headquarters – GCHQ). Na taj način, a imajući u vidu da Velika Britanija jedan od glavnih centara (ako ne i glavni centar) za Internet saobraćaj, ovim dvema službama je omogućeno da nesmetano prate skoro celokupni Internet saobraćaj.

Međutim, iako se sva pažnja skoncentrisala na prisluškivanja i prikupljanje podataka od strane američkih kompanija i obaveštajnih službi, postoje dokazi da su i nemačke kompanije sarađivale sa obaveštajnim službama SAD, ali i sa drugim obaveštajnim službama. U svojoj izjavi Savezni poverenik za zaštitu podataka Peter Schar je poimence naveo „Vodafon Deutschland“ i „Deutsche Telekom“. (Jungholt, 2013). Juna 2013 je objavljeno da je i Velika Britanija uspostavila svoj program monitoringa („Tempora“) koji treba i da nadmaši projekat Prizma. (Franceschi-Bicchierai, 2013). Sasvim je sigurno da slični projekti postoje i u drugim zemljama, npr. Italija, Indija i Kanada. (Mirani, 2013)

Na to da se stanje u ovoj oblasti neće poboljšavati posredno ukazuje izjava Michaela Hajdena (direktor NSA od 1995 do 2005) u kojoj je praktično opisao sve one koji su zabrinuti zbog projekta Prizma i koji žele transparentnost u upravljanju državom kao: „nihiliste, anarhiste, Lulzseke, Anonimuse, dvadesetogodišnjake koji sa suprotnim polom nisu kontaktirali pet ili šest godina.“ (Ackerman, 2013) (Moore, 2013)

3 ZAŠTITA ELEKTRONSKE POŠTE

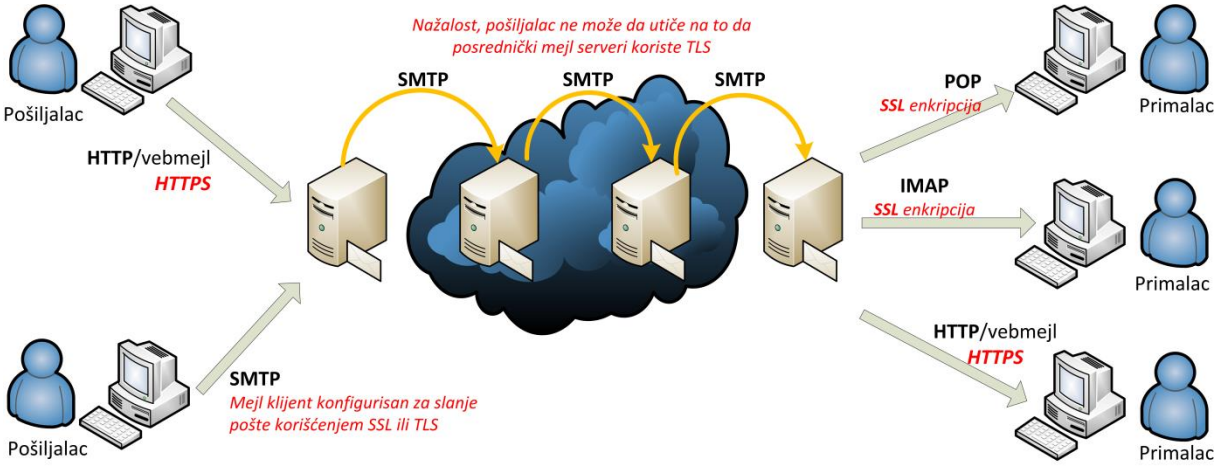
Šifrovanje elektronske pošte danas, još uvek, nije široko rasprostranjeno. Većina i-mejl poruka neke tipične organizacije i dalje se šalje u obliku čistog teksta što omogućava da poruke budu lako presretnute. U 2013-oj godini manje od jedne polovine, 44% organizacija omogućava korisnicima manuelnu enkripciju, a nešto više od jedne trećine, 35% organizacija ima mogućnost da u zavisnosti od sadržaja poruke i vrste podataka poruku šifruje. Situacija je bila još nepovoljnija u prethodnoj godini kada su odgovarajući procenti bili 40 i 27. (Osterman Research, 2013)

Da bi se obezbedio šifrovani prenos podataka između korisnika i Internet servis provajdera (ISP) potrebno je podesiti Secure Socket Layer (SSL) i Transport Layer Security (TLS) enkripciju. SSL konekcija se može aktivirati na veb pretraživaču ili na imejl programu. Poruke se mogu (i trebaju) šifrovati pri prenosu, ali da bi to bilo moguće, potrebno je da to bude urađeno i kod pošiljaoca i kod primaoca.

Za šifrovanje imejl poruka mogu da se koriste funkcije ugrađene u uslugu e-pošte, ili može da se preuzme softver za šifrovanje ili klijent dodaci (kao što su oni koji koriste OpenPGP (Constantin, 2011)). U slučaju nužde, mogu se koristiti Veb-bazirani servisi za šifrovanje e-pošte kao Sendinc ili JumbleMe, mada taj način primorava korisnika da veruje trećoj strani, određenoj kompaniji. (Geier, 2012)

Na slici 4 prikazana je ilustracija opšteg slučaja kretanja elektronske pošte od računara pošiljaoca do računara primaoca, kao i protokoli koji se koriste u određenim fazama. Crvenom bojom (*italik*) su naznačeni mogući tipovi enkripcije u pojedinim fazama. Za šifrovani prenos pošte potrebno je da mejl server pošiljaoca podržava SMTP preko TLS. Kao što se na slici 4 može videti, iako je sve učinio da poveća bezbednost, pošiljalac ne može da utiče na trasu i na način rada posredničkih mejl servera.

Najčešći oblici enkripcije podataka, uključujući S/MIME (Secure/Multipurpose Internet Mail Extensions) i OpenPGP, podrazumevaju instalisanje bezbednosnog sertifikata na korisnički računar primaoca poruke i davanje pošiljaocu poruke niza karaktera, javnog ključa. Mnogi imejl klijenti, kao i dodaci za veb pretraživače podržavaju S/MIME standard. Moguće je kupiti i kompletna softverska rešenja za potpuno šifrovano prenošenje poruka od pošiljaoca do primaoca.



Slika 4 Ilustracija tipičnog prenosa elektronske pošte od pošiljaoca do primaoca u varijantama bez kriptovanja (crna boja) i sa kriptovanjem (crvena boja) (izvor: adaptirana verzija slike objavljene u (Čekerevac, Čekerevac, & Vasiljević, 2013) *i* (Anon, 2013)*)*

U slučaju korišćenja prenosnih uređaja, tableta, notbukova, telefona i drugih mobilnih uređaja, za zaštitu elektronske pošte pogodno je koristiti šifrovanje preuzete pošte, ali je još preporučljivije kriptovati ceo uređaj i sve podatke kako bi ostali zaštićeni i u slučaju gubitka uređaja. Uz kriptovanje poruka treba i definisati odgovarajuću politiku brisanja podataka, kako bi se racionalno koristili raspoloživi resursi.

Pri enkripciji elektronske pošte moguće je koristiti:

- Enkripciju „s kraja na kraj" (End-to-end encryption),
- Server-server enkripciju i
- Klijent-server enkripciju.

Sigurno je da se najbolji rezultati mogu očekivati od s kraja na kraj enkripcije, pa će ovde biti detaljnije razmotrena.

Šifrovanje e-pošte s kraja na kraj, tj. od pošiljaoca do primaoca, je uvek bilo teško, iako su sredstva za postizanje ove vrste enkripcija sve bolja i lakša za korišćenje. Pretty Good Privacy (PGP) i njegov rođak besplatna verzija GNU Privacy Guard (GnuPG) danas su standardni alati za ovu svrhu. Oba ova programa mogu da obezbede zaštitu imejla u tranzitu, a takođe štite i sačuvane podatke. Glavni imejl klijenti, kao što su Mozilla Thunderbird i Microsoft Outlook mogu da se konfigurišu tako da nesmetano rade sa softverom za šifrovanje i omogućavaju pošiljaocu da jednim klikom potpiše, potvrdi, šifruje i dešifruje imejl poruke.

Iako naizgled jednostavno, korišćenje GnuPG i/ili PGP podrazumeva da i pošiljalac i primalac koriste isti softver, što je sada redak slučaj. Ako jedna od strana ne podržava GnuPG/PGP nema ni šifrovanog prenosa poruke s kraja na kraj.

Drugi preduslov je da pošiljalac mora da poseduje i verifikuje javne ključeve primalaca kojima se poruka namenjena. Tu je bitno i da pošiljalac poruke ne upadne u zamku poznatu po imenu „čovek u sredini" (eng. „man in the middle") kojom prisluškivači mogu da navedu pošiljaoca da koristi pogrešni javni ključ. Čovek u sredini napad se obično bazira na znatiželji, lakovernosti ili nepažnji korisnika koji svoje podatke čini dostupnim napadaču, kao što je objašnjeno u radu Srđana Nikića (2010) ili npr. u prikazu Margaret Rouse (2007) ili detaljnije u (Admin, 2011).

4 ZAKLJUČCI

Otkrića Edwarda Snowdena izazvala su buru na polju komunikacija. Pokazalo se da nema potpuno zaštićenih ni osoba ni institucija. Na površinu su isplivale veze i institucije uključene u sisteme prisluškivanja. Pokazalo se kako se ponašaju i najveći svetski internet provajderi. Sve to je znatno uzdrmalo internet provajdere locirane u SAD. Mnogi korisnici su prebacili svoje poslovanje na evropske servere. Da bi povratili poverenje američki provajderi su najavili kriptovanje svojih mreža. Prema navodima časopisa Ars technica, Google je već više godina imao plan da kriptuje svoju mrežu, ali je ta ideja ubrzana tek posle objavljivanja podataka o projektu „Prism".

Microsoft, svetski gigant u proizvodnji softvera i usliga „u oblaku“, iako je prethodno pomagao NSA u nelegalnim aktivnostima prisluškivanja, takođe je objavio da će svoju mrežu zaštiti kriptovanjem. Razlog ovakvih izjava je, najverovatnije, želja da se pospeši prodaja novih Office paketa namenjenih za rad u oblaku. Malo je verovatno da neko dobije želju da drži podatke na MS serverima i da koristi MS programe, ukoliko su mu ti podaci poverljivi. Verovatno je i da će tokom vremena pritisak na korisnike da koriste računarstvo u oblaku postati sve veći, pre svega zbog naplate pretplate na te usluge, a u pozadini će se vrlo verovatno vršiti i nadzor tih informacija. Na takav zaključak navodi i postepeno gašenje podrške za MS desk top aplikacije. S jedne strane to može da bude i dobro za korisnike open source Open Office paketa. Tako je moguće da monopolista ugrozi samog sebe. U pogledu elektronske pošte se najverovatnije ništa bitnije neće promeniti, osim što će broj kriptovanih poruka narasti. Samo kriptovanje će doprineti zaštiti sadržaja od napada amatera, ali ne i zaštiti od državnih i sličnih institucija. Verovatno je da će razmenjivači važnih poruka biti prinuđeni da se vrate starim oprobanim tehnologijama ili da pokušaju da pronađu nove vidove enkripcije.

CITIRANI RADOVI

Ackerman, S. (2013, 08 06). *Former NSA chief warns of cyber-terror attacks if Snowden apprehended.* Retrieved from theguardian: http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden

Admin, J. (2011, 07 2). *Man In The Middle Attack Using Ettercap.* Retrieved from Hackaholic: http://www.101hacker.com/2011/03/man-in-middle-attack-using-ettercap.html

Anon. (2013, 08 01). *Email.* Retrieved from Surveillance Self-Defense: https://ssd.eff.org/tech/email

Betakit. (2013, 10 29). *Number of cell phone plans expected to surpass world's population in early 2014.* Retrieved from Betakit: http://www.betakit.com/number-of-cell-phone-plans-expected-to-surpass-worlds-population-in-early-2014/

Constantin, L. (2011, 11 21). *OpenPGP JavaScript Implementation Allows Webmail Encryption.* Retrieved from PCWorld: http://www.pcworld.com/article/244406/openpgp_javascript_implementation_allows_webmail_encryption.html

Čekerevac, Z., Čekerevac, P., & Vasiljević, J. (2013, 09 07). *Internet safety of SMEs regarding the security of electronic mail.* Retrieved 09 19, 2013, from FBIM Transactions: http://www.meste.org/fbim/fbim_srpski/FBIM_najava/III_Cekerevac.pdf

European Central Bank. (2012, 09 10). *Payment Statistics for 2011.* Retrieved 12 02, 2013, from European Central Bank: http://www.ecb.europa.eu/press/pr/date/2012/html/pr120910.en.html

European Central Bank. (2013, 09 19). *Payment statistics for 2012.* Retrieved from European Central Bank: http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html

FISA. (2008, 07 09). *H.R. 6304(110th): FISA Amendments Act of 2008.* Retrieved from govtrack.us: https://www.govtrack.us/congress/bills/110/hr6304/text

Franceschi-Bicchierai, L. (2013, 06 22). *Revealed: British Spy Agency Secretly Taps Global Communications.* Retrieved from Mashable: http://mashable.com/2013/06/21/gchq-spy-agency-taps-global-internet/

Galagher, S. (2013, 11 06). *Googlers say "F*** you" to NSA, company encrypts internal network.* From Ars Technica: http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/

Geier, E. (2012, 04 25). *How to encrypt your email.* Retrieved from PCWorld: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html

Gellman, B. (2013, 10 30). *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say.* Retrieved from The Washington Post: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-

data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Greenwald, G., & MacAskill, E. (2013, 06 07). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved 08 04, 2013, from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Jungholt, T. (2013, 08 03). FDP-Minister will "Datenuntreue" bestrafen. *Die Welt*. Retrieved 09 20, 2013, from http://www.welt.de/politik/deutschland/article118648774/FDP-Minister-will-Datenuntreue-bestrafen.html

Mims, C. (2013, 11 14). *Cisco's disastrous quarter shows how NSA spying could freeze US companies out of a trillion-dollar opportunity.* From Quartz: http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity/

Mirani, L. (2013, 06 11). *Think U.S. Snooping Is Bad? Try Italy, India or Canada.* Retrieved from Mashable: http://mashable.com/2013/06/11/nsa-privacy-italy-india-canada/

Moore, A. (2013, 08 07). *Former NSA boss compares PRISM critics to Al Qaeda.* Retrieved from deathandtaxes: http://www.deathandtaxesmag.com/203430/former-nsa-boss-compares-prism-critics-to-al-qaeda/

Nautiyal, A. (2013, 11 18). *Google Encrypts Its Network to Counteract NSA Surveillance.* From JOLT digest: http://jolt.law.harvard.edu/digest/privacy/google-encrypts-its-network-to-counteract-nsa-surveillance

Nikić, S. (2010, 03 05). *Najčešće metode napada cyber kriminalaca i kako se odbraniti.* Retrieved from IT Veštak: http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf

Oremus, W. (2013, 10 30). *To celebrate spying on Google users, the NSA drew a smiley face.* Retrieved from Future tense: http://www.slate.com/blogs/future_tense/2013/10/30/nsa_smiley_face_muscular_spying_on_google_yahoo_speaks_volumes_about_agency.html

Osterman Research. (2013, 07). *Why Should You Encrypt Email and What Happens if You Don't?* Retrieved from Osterman Research White Paper: http://www.ostermanresearch.com/whitepapers/orwp_0194.pdf

PAA. (2007, 08 05). *Protect America Act of 2007.* Retrieved from U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm

Piermon, E. (2013, 07 12). *Microsoft helped the NSA bypass encryption, new Snowden leak reveals.* From RT - Russia Today: http://rt.com/usa/microsoft-nsa-snowden-leak-971/

Pramis, J. (2013, 02 28). *Number of mobile phones to exceed world population by 2014.* Retrieved from Digital trends: http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014/

Radicati, S., & Levenstein, J. (2013, 04). *Email Statistics Report, 2013-2017.* Retrieved from The Radicati Group, Inc.: http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

Rouse, M. (2007, 06). *Man in the middle attack (fire brigade attack).* Retrieved from SearchSecurity: http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack

Snowden, E. (2013, 06 23). *Edward Snowden News*. Retrieved from Edward Snowden News: http://edward-snowden.net/category/edward-snowden/

Symantec. (2013, 03 13). *Symantec Encryption Solutions for Email, Powered by PGP Technology.* Retrieved 08 01, 2013, from Symantec: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-solutions-for-email.pdf

The Washington Post. (2013, 10 30). *How the NSA's MUSCULAR program collects too much data from Yahoo and Google.* Retrieved from The Washington Post - National Security: http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p1/a129319

The World Bank. (2013). *Mobile cellular subscriptions (per 100 people).* Retrieved from The World Bank: http://data.worldbank.org/indicator/IT.CEL.SETS.P2

USA Patriot Act. (2001, 10 24). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.* Retrieved 08 03, 2013, from epic.org: http://epic.org/privacy/terrorism/hr3162.html

Wilking, R. (2013, 11 27). *Suspicious of NSA spying, Microsoft moves to encrypt internet traffic - report.* From RT - Russia Today: http://rt.com/usa/microsoft-encryption-nsa-spying-358/

Datum prve prijave: 25.02.2014.
Datum prijema korigovanog članka: 08.04.2014.
Datum prihvatanja članka: 08.05.2014.

Kako citirati ovaj rad?

*Style – **APA** Sixth Edition:*
Čekerevac, Z., Dvorak, Z., & Čekerevac, P. (2014, 07 15). Internet sigurnost u svetlu otkrića Edvarda Snoudena. (Z. Čekerevac, Ed.) *FBIM Transactions, 2*(2), 68-78. doi:10.12709/fbim.02.02.02.07

*Style – **Chicago** Fifteenth Edition:*
Čekerevac, Zoran, Zdenek Dvorak, and Petar Čekerevac. 2014. "Internet sigurnost u svetlu otkrića Edvarda Snoudena." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 2 (2): 68-78. doi:10.12709/fbim.02.02.02.07.

*Style – **GOST** Name Sort:*
Čekerevac Zoran, Dvorak Zdenek and Čekerevac Petar Internet sigurnost u svetlu otkrića Edvarda Snoudena [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - [s.l.] : MESTE, 07 15, 2014. - 2 : Vol. 2. - pp. 68-78.

*Style – **Harvard** Anglia:*
Čekerevac, Z., Dvorak, Z. & Čekerevac, P., 2014. Internet sigurnost u svetlu otkrića Edvarda Snoudena. *FBIM Transactions,* 15 07, 2(2), pp. 68-78.

Style – **ISO 690** Numerical Reference:
Internet sigurnost u svetlu otkrića Edvarda Snoudena. **Čekerevac, Zoran, Dvorak, Zdenek and Čekerevac, Petar.** [ed.] Zoran Čekerevac. 2, s.l. : MESTE, 07 15, 2014, FBIM Transactions, Vol. 2, pp. 68-78.