INTERNET SIGURNOST U SVETLU OTKRIĆA EDVARDA SNOUDENA

INTERNET SECURITY IN LIGHT OF EDWARD SNOWDEN'S REVELATIONS

Zoran Čekerevac [1], Zdenek Dvorak [2], Petar Čekerevac [3]

Rezime

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 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. U ovom radu se razmatra trenutno stanje u internet poslovanju i posebno zaštita elektronske pošte. 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.

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, 2012) U 2012-0j 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)

[1] Fakultet za poslovno industrijski menadžment, Univerzitet Union, Beograd

[2] Faculty of special engineering, University of Žilina, Žilina

[3] Libek, Beograd

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. (Radicati & Levenstein, 2013) procenjuje se da u 2013-oj godini funkcioniše nešto manje od 3,9 milijardi e-mejl računa i da će taj broj u 2017-oj godini porasti za preko milijardu novih računa, na 4,92 milijarde. 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.

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 i Severna Koreja sa 6,9 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 (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) i nekoliko drugih zakona predviđenih za borbu protiv terorizma.

Detalje prikupljanja podataka po projektu Prizma dali su Greenwald i MacAskill (2013), a prikaz napada na komunikaciju između Google i njegovih korisnika prikazali su Naughton (2013), Gellman (2013) i mnogi drugi.

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. bacila je novo svetlo na obim i vrstu prikupljanja podataka.

Na osnovu 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. Pristupna tačka poznata kao DS-200B nalazi se izvan teritorije SAD, kod za sada nepoznatog provajdera telekomunikacionih usluga. 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 je 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)

Na osnovu u radu prikazane analize može se zaključiti da ne postoji apsolutna zaštita poruka iako se sve čini da poruka bude zaštićena „s kraja na kraj". Čak i u tim situacijama pošiljalac i primalac poruke moraju da veruju kompaniji koja im je prodala softver za enkripciju. Zbog toga pošiljalac i primalac poruke moraju da budu veoma obazrivi pri komunikaciji o važnim pitanjima.

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

Summary

Modern communication and modern business are linked to the massive use of the Internet. However, use of Internet can compromise the integrity and confidentiality of data during both their transmission and their storage. Remarkably rapid development of IT allows more efficient data protection, but also new opportunities for eavesdropping and spying. "Excess" of computing capacities on the attackers' side enable them to cover virtually all Internet users, including

individuals. Even in situations with the latest protection there are ways to access data unnoticed. This paper discusses the current state of the Internet business, and the protection of electronic mail. 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.

Mobile communications are now very popular, if not the most massive form of communication. The number of active mobile phones will surpass the world population in the year 2014. (Pramis, 2013) It is assumed that at the end of 2013 there were 6.8 billion active cell phones. In view of these data it is easy to perceive the wealth of information that is transmitted daily over the communication channels. Every user of the Internet, credit card or mobile phone could have guessed easily that in addition to be the service user, at the same time, he was the object of observation, but only a few were aware of the size and scope of resources for espionage of communications. Based on The Guardian series, "Glenn Greenwald on security and liberty" (Greenwald & MacAskill, 2013) National Security Agency (NSA) has direct access to systems like Google, Facebook, Apple and other U.S. internet giants. NSA access was a part of the previously undisclosed program called Prism, which allows the departments to collect material, including browsing history, content of e-mails, file transfer and live chat. Details of data collection under the project Prism were given by Greenwald and MacAskill (2013), and the explanation about the attacks on the communication between Google and its users was presented by Naughton (2013), Gellman (2013) and many others.

In the wiretapping program, there were gradually included the world's largest internet service providers starting from Microsft's (2007) and ending with Apple (2012).

Based on the claims of Edward Snowden and so called "well-informed sources", the NSA has secretly invaded the links of Yahoo and Google all over the world. By eavesdropping these lines, the agency got the opportunity to follow the work of hundreds of millions of users' accounts. On the basis of confidential information published in The Washington Post (2013) activities are conducted within the secret project "Muscular" intended to intercept traffic from private links associated with Yahoo and Google's servers. It is interesting that in the project was also included the United Kingdom through a joint program "Windstop". This way, bearing in mind that the UK is one of the main centers for the Internet traffic, these two services are able to smoothly follow almost the entire Internet traffic.

Although all the attention is concentrated on the interception and data collection by U.S. companies and intelligence services, there are evidences that German companies also cooperated with U.S. intelligence agencies, and with other intelligence agencies. In his statement, the Federal Commissioner for Data Protection Peter Schar cited by name "Vodafone Deutschland" and "Deutsche Telekom". (Jungholt, 2013). In June 2013 it was announced that the United Kingdom established its monitoring program ("Tempora") which should outperform the Prism project. It is certain that similar projects exist in other countries, eg. Italy, India and Canada.

Based on the analysis presented in the paper, it can be concluded that there is no absolute protection of messages even when one did everything to protect message "from end to end." Even

in these situations, the sender and the recipient have to trust the company that sold them the software for encryption. Therefore, the sender and the recipient, both have to be very cautious when communicating about important issues.

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