SOME RISKS IN DATA EXCHANGE WHILE USING THE INTERNET

Zoran Čekerevac[1], Petar Čekerevac[2], Zdeněk Dvořák[3]

ABSTRACT
Use of the 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. Rapid development of IT allows more efficient data protection, but also gives new opportunities for eavesdropping and spying. Even in cases of latest protection there are ways to access data unnoticed. The topic becomes more significant when one considers the recent events related to the wiretapping of Internet posts by the NSA, which Edward Snowden revealed in The Guardian in June 2013. This paper discusses the current state of the Internet business, and risks in data exchange while using the Internet.

Key words:
Internet, communications, Snowden, Muscular, Windstop, Tempora, Patriot Act

APSTRAKT
Upotreba Interneta i mobilnih komunikacija može da dovede do ugrožavanja integriteta i tajnosti podataka kako pri njihovom prenošenju, tako i pri njihovom skladištenju. Napadači mogu da budu pojedinačni hakeri, ali i najviše državne institucije. Brz razvoj informacionih tehnologija omogućava sve efikasniju zaštitu podataka, ali i nove mogućnosti za prisluškivanje i špijunažu. Čak i kod primene najsavremenije zaštite postoje načini za neopažen pristup 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. U ovom radu se razmatraju trenutno stanje u Internet poslovanju i rizici u razmeni podataka koji pri tom nastaju.

[1] Dr. Zoran Čekerevac, Associate Professor, "Union" University - Faculty of Business and Industrial Management, Venizelosova 31, 11000 Belgrade, zoran@cekerevac.eu
[2] MSc Petar Čekerevac, Kutpoint, Akademska 20, 11080 Belgrade-Zemun, petar@cekerevac.eu
[3] prof. Ing. Zdeněk Dvořák, PhD., FŠI ŽU v Žiline, 1.Mája 32, 010 26 Žilina, zdenek.dvorak@fsi.uniza.sk

Key words:
Internet, komunikacije, Snowden, Muscular, Windstop, Tempora, Patriot Act

1 INTRODUCTION

Modern communication between people and modern business are linked to the massive use of the Internet and mobile communications. The Internet is now the main communication channel for electronic money transactions by credit and debit cards, for electronic mail transmission, international voice and video communications. Many of these activities are performed by mobile communications. However, all these forms of communication are exposed to wide range of risks. The integrity and confidentiality of data are vulnerable during transmission, but also in storage. Extraordinarily rapid development of information technology allows their more efficient protection, but also an increased risk of eavesdropping and espionage, because nowadays virtually everyone, without major restrictions, may engage own resources in unauthorized data collection. "Excess" of computing capacity on the side of the attackers enables them to be able to focus attention not only on the big and important companies, but virtually on all Internet users, including individuals. Even in situations with the latest protection there are ways to access data unnoticed. Eavesdropping and protection becomes more important when one takes into account recent events related to the scandal of wiretapping Internet messages by NSA (USA National Agency of Secured), which was published in The Guardian in June 2013 by Edward Snowden and have provoked numerous discussions on this topic that confirmed that many (if not all) countries are tapping telecommunications channels, and that the NSA had an "accident" to be first detected. The case of e-mails is detailed explained in [1], and here will be paid attention on risks that follow Internet business.

2 RISKS OF MODERN INTERNET BUSINESS

According to the annual report of the European Central Bank (ECB) in respect of non-cash payments, in 2011 there was an increase of 4.6% to EUR 90.6 billion, compared to the previous year. Credit cards included 41% of all transactions. [2] In 2012, the growth of non-cash payment in comparison to the previous year was 4.2% and reached 95.5 billion Euros, and credit card's payment has reached 42%. [3]

According to the Osterman Research [4], 74% of intellectual property of organizations resides in electronic mail as a text or as an attachment. According to the The Radicati Group, Inc. report, shown in the Table 1, it can be seen that it is estimated that in 2013 worked a little less than four billion e-mail accounts and that its number will increase by over a billion new accounts during the next four years. Almost a quarter of all accounts represents accounts that are used solely for business purposes. It is certain that a large number of private accounts is also used for business purposes.

Table 1 Private and business e-mail accounts from 2013 to 2017 year *Source* [5]

	2013	**2014**	**2015**	**2016**	**2017**
The total number of e-mail accounts in billions	**3.899**	**4.116**	**4.353**	**4.626**	**4.920**
Number of business e-mail accounts in billions	**0.929**	**0.974**	**1.022**	**1.078**	**1.138**
% of Business e-mail account	24%	24%	23%	23%	23%
Private e-mail accounts in billions	**2.970**	**3.142**	**3.331**	**3.548**	**3.782**
% of private e-mail accounts	76%	76%	77%	77%	77%

Mobile communications are now very popular, if not the most massive form of communications. The number of active mobile phones will surpass the world population in 2014. [6] Based on the list of statistical data of the World Bank [7] the number of mobile phones per 100 inhabitants, on the list led Macao SAR, China with 284, followed by Hong Kong SAR, China with 228. At the bottom of the list there are Eritrea with 5.4, Somalia 6.7, North Korea 5.9, and Myanmar with 11.1 mobile phones per hundred residents. Adequate numbers of mobile phones are in Serbia 92.8, the U.S. 98.1, UK 130.75, and in Germany 131.3.

In light of these data it is easy to perceive the wealth of information that is transmitted daily by communication channels. It is certain that many are interested in collecting data from the communication channels in order of their (mis)use. Every user of the Internet, credit card or mobile phone easily could have guessed that in addition to the role of service user at the same time is the object of observation, but there were only a few who were aware of the size and scope of resources of communications espionage. In mid-2013 suddenly arose up storm about security of e-mail and data circulating by e-mail. Although it is believed that, by use of a desktop computers, gateways and encryption, transmission of e-mail is safe even in the cloud, Edward Snowden [7] showed that this is not the case, that e-mail, and not only e-mail, was actively monitored and eavesdropped. Based on the series of The Guardian, "Glenn Greenwald on security and liberty" [8] National Security Agency (NSA) has direct access to systems like Google, Facebook, Apple and other U.S. Internet giants. In strictly confidential documents whose content was published by authors, NSA access was part of the earlier unpublished program called "Prism", which allows the departments to collect material including browsing histories, e-mail contents, file transfers and live chats. The document states that the data were collected directly from the servers of major U.S. Internet service providers. The legal basis for data collecting is the USA Patriot Act [9], Protect America Act of 2007 [10], Foreign Intelligence Surveillance Act of 1978 - Amendments Act of 2008 **[**11].

In accordance with the aforementioned legislation, in the eavesdropping program were gradually included the world's largest Internet service providers ranging from Microsoft (2007), over Yahoo (2008), Google, Facebook and PalTalk (2009), YouTube (2010), Skype and AOL (2011) to Apple (2012). [8] It is easy to assume that new entrants in the wiretapping were not delighted when they received the NSA requests for user data takeover, even though it was court approved. However, it certainly is nothing compared to the moment when they learned that the NSA, behind their backs, secretly took much larger amounts of data. [12]

Based on the claims of Edward Snowden and "well-informed sources", the National Security Agency (NSA) has secretly invaded the links of Yahoo and Google all over the world. Eavesdropping of these lines gave the agency the opportunity to follow the work of hundreds of millions of user accounts and opened up immense intelligence capabilities. On the basis of confidential information published in The Washington Post [13] activities were conducted within the secret project "Muscular". The main reasons for the implementation of the "Muscular" were cited as [14]:

1. Many data mining is performed outside the United States, where monitoring mechanisms are poorly developed and where the FISC (Foreign Intelligence Surveillance Court) has no jurisdiction; and
2. This method of data collection is much less visible to companies, Internet service providers, which in recent years have become more transparent in terms of information that they submitt to U.S. government agencies.

When word got out about the "Muscular", Google and Yahoo have accelerated their activities in full encryption of their networks. A similar intent was demonstrated by Microsoft, which due to suspicions that they and their lines are supervised announced that it has entered into a process of encryption of internal traffic. [15] These Microsoft announcements should compensate the fact that Microsoft helped the NSA in bridging mechanisms aimed to protect data of millions of users. [16] Similar problems have been experienced in another global giant Cisco, which in its report of November 2013 revealed two important things: the Company aims to expand in the Internet market in order to connect to the Internet almost every object on the planet Earth and to initiate new technology in this direction. Another important information was a drop in demand of their hardware in some markets because of users' fears that the NSA uses American hardware to spy the rest of the world. Cisco at that time noted the drop in orders by 25% in Brazil and 25% in Russia. Instead of the expected sales growth of 6% Cisco has seen a decrease of 12%. Publication of information about eavesdropping has endangered the operations of many American companies, producers of internet technologies at an early stage of the Internet boom, and in the long run opened additional space for non-US companies. [17]

It is interesting that in the project of wiretapping was included also the United Kingdom through a joint program "Windstop". On the UK side, for the project is responsible General Communications Headquarters (GCHQ). In this way, bearing in mind that the UK is one of the main (if not the main) centers of Internet traffic, these two services were able to smoothly follow almost the entire Internet traffic.

Despite all the attention is concentrated on tapping and collection of data from U.S. companies and intelligence services, there are evidences that also the German companies cooperated with U.S. intelligence agencies, and with other intelligence agencies. In its statement, the Federal Commissioner for Data Protection Peter Schar cited by name "Vodafone Deutschland" and "Deutsche Telekom". [18] In June 2013 it was announced that the United Kingdom established its program оф monitoring ("Tempora") which should outperform the Prism project. [19] It is certain that similar projects exist in other countries, e.g. Italy, India and Canada. [20]

That the situation in this area will not be better indirectly suggests the statement of Michael Hayden (Director of the NSA from 1995 to 2005), in which described all who are concerned about the Project Prism and want transparency as "nihilists, anarchists, activists, Lulzsec, Anonymous, twentysomethings who haven't talked to the opposite sex in five or six years". [21]

3 CONCLUSIONS

Edward Snowden caused a storm in the field of communication. He has shown that there are no fully protected persons or institutions. On the light came institutions involved in wiretapping systems and their relationships. All this has greatly shaken the internet service providers located in the United States. Many users have switched their business to the European servers. In order to regain the trust of their users American providers, as Google, have announced encrypting of their networks. Microsoft, the world's giant in production of "in the cloud" software and services, although previously assisted in the NSA illegal wiretapping activities, also announced that it will encrypt its network. The reason probably lay in intentions to encourage Office users to use it in the cloud. It is unlikely that someone gets the desire to keep the information on the MS servers and to use the MS "in the cloud" software, if such data are confidential. It is likely that pressure on users to use cloud computing will grow, primarily due to the collection of subscriptions to cloud services, but it is very likely that in the background a control of the information will be to also performed. This conclusion is based on phasing out of support for some desk top applications. This may be good for users of open source the Open Office package. So it is possible that the monopolists endanger themselves. In e-mails probably nothing significant will be changed, except that the number of encrypted messages will grow. Encryption can protect the contents from attacks by amateurs, but not from state and related institutions. It is likely that the exchangers of important messages will be forced to return to the old proved technologies, or to try to find new forms of encryption.

REFERENCES

[1] ČEKEREVAC, Z, ČEKEREVAC, P AND VASILJEVIĆ, J.: Internet safety of SMEs regarding the security of electronic mail. *FBIM Transactions.* [Online] 09 07, 2013. [Cited: 09 19, 2013.] http://www.meste.org/fbim/fbim_srpski/FBIM_najava/III_Cekerevac.pdf.

[2] EUROPEAN CENTRAL BANK: Payment Statistics for 2011. *European Central Bank.* [Online] 09 10, 2012. [Cited: 12 02, 2013.] http://www.ecb.europa.eu/press/pr/date/2012/html/pr120910.en.html.

[3] —. Payment statistics for 2012. *European Central Bank.* [Online] 09 19, 2013. http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html.

[4] SYMANTEC: Symantec Encryption Solutions for Email, Powered by PGP Technology. *Symantec.* [Online] 03 13, 2013. [Cited: 08 01, 2013.] http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-solutions-for-email.pdf.

[5] RADICATI, S. AND LEVENSTEIN, J.: Email Statistics Report, 2013-2017. *The Radicati Group, Inc.* [Online] 04 2013. http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.

[6] PRAMIS, J.: Number of mobile phones to exceed world population by 2014. *Digital trends.* [Online] 02 28, 2013. http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014/.

[7] SNOWDEN, E**.** Edward Snowden News. *Edward Snowden News.* [Online] 06 23, 2013. http://edward-snowden.net/category/edward-snowden/.

[8] GREENWALD, G. AND MACASKILL, E.: NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* UK, 06 07, 2013.

[9] USA PATRIOT ACT.: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. *epic.org.* [Online] H.R. 3162, 10 24, 2001. [Cited: 08 03, 2013.] http://epic.org/privacy/terrorism/hr3162.html.

[10] PAA.: Protect America Act of 2007. *U.S. Government Printing Office.* [Online] 08 05, 2007. http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm.

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

[12] OREMUS, W.: To celebrate spying on Google users, the NSA drew a smiley face. *Future tense.* [Online] 10 30, 2013. http://www.slate.com/blogs/future_tense/2013/10/30/nsa_smiley_face_muscular_spying_on_google_yahoo_speaks_volumes_about_agency.html.

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

[14] NAUTIYAL, A.: Google Encrypts Its Network to Counteract NSA Surveillance. *JOLT digest.* [Online] 11 18, 2013. http://jolt.law.harvard.edu/digest/privacy/google-encrypts-its-network-to-counteract-nsa-surveillance.

[15] WILKING, R.: Suspicious of NSA spying, Microsoft moves to encrypt internet traffic - report. *RT - Russia Today.* [Online] 11 27, 2013. http://rt.com/usa/microsoft-encryption-nsa-spying-358/.

[16] PIERMON, E.: Microsoft helped the NSA bypass encryption, new Snowden leak reveals. *RT - Russia Today.* [Online] 07 12, 2013. http://rt.com/usa/microsoft-nsa-snowden-leak-971/.

[17] MIMS, C.: Cisco’s disastrous quarter shows how NSA spying could freeze US companies out of a trillion-dollar opportunity. *Quartz.* [Online] 11 14, 2013. http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity/.

[18] JUNGHOLT, T.: FDP-Minister will "Datenuntreue" bestrafen. *Die Welt.* 08 03, 2013.

[19] FRANCESCHI-BICCHIERAI, L.: Revealed: British Spy Agency Secretly Taps Global Communications. *Mashable.* [Online] 06 22, 2013. http://mashable.com/2013/06/21/gchq-spy-agency-taps-global-internet/.
[20] MIRANI, L.: Think U.S. Snooping Is Bad? Try Italy, India or Canada. *Mashable.* [Online] 06 11, 2013. http://mashable.com/2013/06/11/nsa-privacy-italy-india-canada/.
[21] ACKERMAN, S.: Former NSA chief warns of cyber-terror attacks if Snowden apprehended. *theguardian.* [Online] 08 06, 2013. http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden.

Článok recenzovali dvaja nezávislí recenzenti.