OVERVIEW OF WEB ANONYMIZATION

Tomáš Sochor[1], Cyril Klimeš[1]

[1] *Mendel University in Brno, Czech Republic*

EUROPEAN JOURNAL OF BUSINESS SCIENCE AND TECHNOLOGY

Volume 3 Issue 2
ISSN 2336-6494
www.ejobsat.com

ABSTRACT

Web anonymization tools have been used for a long time, primarily by the users afraid of possible undesirable consequences of their on-line activity on the web. The paper analyzes both historically proven anonymization tools like TOR and newer tools, namely JAP/JonDo and CyberGhost VPN that are based on slightly modified technological principles. The primary focus is given to the measurement and evaluation of the latency increase and the transmission speed decrease in comparison to normal (non-anonymized) web browser operation. Results show that all anonymization tools being subject of the analysis provide relatively moderate latency increase. On the opposite, the transmission speed decrease was more significant, especially for JonDo. This confirms the conclusions of previous studies resulting that no anonymization tool is suitable for daily web browsing. On the other hand, in the case when higher anonymity is required, their use can be reasonably comfortable from the point of view of latency increase. However, their usefulness for downloading larger files is always disputable.

KEY WORDS

world wide web, anonymization in communication, onion routing, cascade mix, TOR, JAP, JonDo, I2P, CyberGhost VPN, latency, transmission speed

JEL CODES

L86, A100

1 INTRODUCTION

World-wide web seems to be almost omnipresent application service in present networks. Due to the fact that www service is used by a huge number of users – e.g. according to Statista.com (2017), there were almost 3.6 billion of Internet users in 2017 – usually on daily basis, not only the security of the communicated contents and resiliency against

SOCHOR, Tomáš, and KLIMEŠ, Cyril. 2017. Overview of Web Anonymization. *European Journal of Business Science and Technology,* 3 (2): 96–105. ISSN 2336-6494, DOI http://dx.doi.org/10.11118/ejobsat.v3i2.101.

breaches of various types (for details about current threats, see e.g. Zuzčák and Sochor, 2017) is an issue. There are situations when the client identification should not be disclosed to the server, too. This is because the client IP address is often closely related to the place of residence of workplace of the user. In situations when the user's activity does not follow the rules enforced in the specific state, they usually try to conceal their location. Such situations were not anticipated when the Internet (and its key protocol, namely Internet Protocol – IP) was designed. Thus, special tools that are able to "anonymize" the Internet communication are applied in such situations. In most cases, such tools concentrate on www traffic anonymization.

It should be emphasized here that the term "anonymization" means solely the anonymization for the sake of keeping the communication private (including, and primarily, the communication metadata, namely the identification of the parties hereof). This comment seems to be particularly important in the present context of ICT where the same term "anonymization" is more frequently used in the context of removing or hiding a part of data files (or their replacement with e.g. symbolic names – that should be called "pseudonymization"). This different meaning for "anonymization" increases its popularity because of recent increase of attacks against private data in various data stores and new rules aimed to prevent such attacks (e.g. GDPR).

Sometimes, anynomization is confused with encryption. However, encryption, which is widely available for www communication via https protocol (that is, in fact, just ordinary http protocol with encryption using SSL or TLS protocols added), cannot provide anonymity for a user. While the contents of the communication is encrypted and therefore (if implemented properly) unreadable for any third party, the sole fact of communication with a specific www server is not hidden using https. Therefore different tools have been designed to disguise even the IP addresses.

1.1 Anonymization Principles

To avoid the client's IP address disclosure, various tools for web anonymization have been developed. Virtually all of them focus on concealing the client's IP address because concealing the other, server side IP address seems infeasible due to the properties of addressing schemes used in the Internet (primarily DNS service). The basic principle of anonymization tools is illustrated in Fig. 1.

Among anonymization tools, The Onion Routing project (abbreviated as TOR) described in Dingledine et al. (2017) is one of the oldest and best-known ones. While the original idea behind TOR was to help people living in states with authoritative government, its availability also helped criminals to improve their ability to hide their activities from the police (Glenny, 2012). Some other tools have emerged later, namely I2P (see I2P, 2017) and JAP/JonDo (see JAP, 2017). Also, new approaches (namely the application of virtual private networks – or VPN) appear in anonymization tools that is demonstrated by CyberGhost VPN (for details see CyberGhost, 2017).

The anonymization techniques have been studied recently, both from the point of view of general properties of anonymity tools (e.g. in Bagai and Hu, 2016), and more specifically, from the point of view of the onion routing principle (Feigenbaum et al., 2012) and from the point of view of the efficiency of various anonymization tools (e.g. Liška et al., 2010; Sochor, 2012; Sochor, 2013; Kapusta, 2016).

All of the above mentioned anonymization tools are based on a certain type of usage of intermediate nodes where either cascading or encapsulation happen. Completely different approach is implemented in a newer tool called CyberGhost VPN where the anonymity is obtained by replacing a real client with the VPN server address. The latter approach seems to be constrained somehow by the fact that the VPN server (or servers) present a single point of failure and for its applications e.g. in countries where the majority of the Internet traffic is under governmental control it could be easier to block the traffic from the VPN servers'

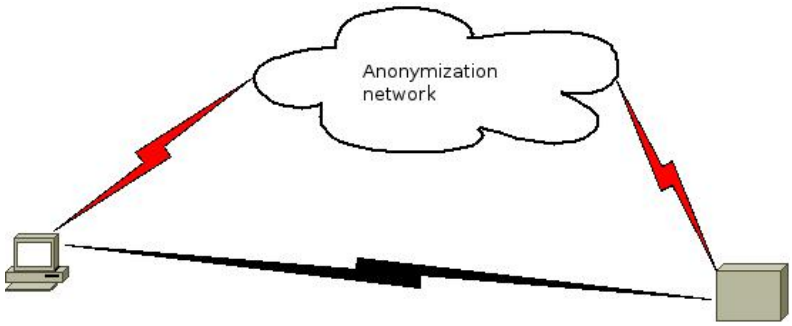

Fig. 1: Comparison of ordinary www traffic (lower part direct from the client to the http server) to the anonymized traffic (upper part when the traffic passes through the network of anonymization nodes)

IP addresses rendering the service useless. On the opposite, distributed tools relying on users' engagement (by providing their own resources to the cascade or onion network, e.g. TOR) is much more resilient in such a situation. CyberGhost VPN was added in the older set of tools to measure in order to investigate its efficiency and to compare with traditional tools. Nevertheless, the above mentioned weakness of this tool is a factor to consider in choosing the appropriate tool in the context of the network where it should be used.

The majority of the studies mentioned above focused on free tools, like TOR and I2P, and a free part of JAP/JonDo services. The prevailing approach was to examine the anonymization tool behavior from the users' perspective. This is the approach applied in this paper, too.

The contribution of the paper is the significant update of the findings obtained in older studies, whose part was initiated by the author hereof, as well as including newly emerged tools into the set of evaluated anonymization tools.

2 ANALYSIS OF ANONYMIZATION TOOLS

During the history of the internet usage, various anonymization techniques emerged. Some of them (e.g. using private GRE tunnels or later private VPNs) has not proven to be secure enough and they are not used any more (at least for anonymization) while others, more successful ones, have been implemented in various anonymization tools, both commercial and freely available. There is a technique used for anonymization for quite a long period that is called *onion routing*. This is implemented in the most traditional anonymization tool called The Onion Routing (abbreviated as TOR).

2.1 The Onion Routing – TOR

As mentioned above, TOR is the oldest and the most frequently used tools among anonymization ones. TOR operation is based on a list of available nodes throughout the world called onion routers. Most of the onion routers are operated by TOR users. When sending a web request, a client automatically forms a way through 3 onion routers. On each of the onion routers, a cryptographic encapsulation is formed. The third (i.e. last) onion router decapsulates the http request and sends the request in a standard way to the target web server on behalf of the client.

No onion router in the network knows more that its direct predecessor and its direct successor. Moreover, thanks to the encryption, the intermediate onion router even cannot interfere into the payload of the packets being transmitted. This ensures the non-disclosure of the client's IP address. This procedure is called "onion routing" because of the subsequent encapsulation. As a result, every packet is "wrapped" in multiple layers of encapsulation thus resembling the onion bulb.

2.2 Invisible Internet Project – I2P

I2P approach to concealing the source IP address is so-called "garlic routing." This approach has been partly inspired by TOR's onion routing and tries to improve it. Garlic routing's improvement (in comparison with onion routing where the request is encrypted repeatedly layer-by-layer and those layers are removed on the way through onion nodes) consists in optional chaining of multiple requests inside a single encrypted layer. However, because of technical problems in long-term usage of I2P that made obtaining the complete set of measurement using I2P very difficult, I2P was finally not included in the set of anonymization tools to measure for this study.

2.3 JAP/JonDo

JonDo (sometimes called JonDonym, formerly JAP) has started as a free tool at the University of Dresned (Germany). It has been changed into partially paid service later but certain (limited) part of the service remained free of charge. JonDo operation is based on so-called cascade-mix. Cascade-mix is a special routing method differing from onion or garlic routing. In this case, a network of special nodes (called mixes) is formed and used. The JonDo client connects to the selected starting node in the cascade mix. Then, the client sends a packet (e.g. a web request) that is encrypted on the first mix-node and subsequently sent to another mix-node. The set of mix-nodes used for sending a single packet is called a cascade. Individual packets are sent through different cascades up to the target server. During transmission, packets can be intentionally delayed, or re-shuffled, in various cascades. Even the data from various clients using the same cascade could be merged to make the reverse decoding even more complex task this improving the anonymity.

2.4 CyberGhost VPN

CyberGhost VPN is a relatively new tool, it started in 2011. The basic available for free (after a free registration) while so-called premium service (offering higher speed) is commercial. The principle of the client's IP address anonymization is based on connection to the selected VPN server provided by the service (their number is claimed to exceed 1000) and subsequent communication passed by the server on behalf of the client. One of the main advantage CyberGhost VPN is its multiplatformness (the native client is available not only for Windows and MacOS but for mobile OS Android and iOS, too).

2.5 Special Operating Systems for Anonymity

In addition to specific application providing anonymity as described above, there are some specialized operating systems designed so that they support better integration of anonymization tools into the operating system services thus providing even better protection for users' anonymity. Most of such systems are built on various Linux distributions and two of them are briefly introduced in this subsection. Nevertheless, this subsection is included here rather to provide a complex overview. The operating systems described here were not incorporated into the anonymization efficiency measurements. The primary reason for this decision was the fact that both of them employs TOR system for anonymity that is already included in the measurements

2.5.1 Tails

Tails stands for the acronym of The Amnesic Incognito Live System[1]. This is, as indicated in its title, a "live" system whose very first emphasis is the users' privacy and anonymity protection. Tails is a free software based on Debian Linux. The system can be executed from a USB disk (either flash or hard drive), CD, DVD or SD card. The system can be run on virtually any PC. Thanks to the fact that this is a "live" system, there are almost no tracks

[1] Tails is available at `https://tails.boum.org`.

remained on the PC disk after finishing its operation. Tails redirects all networks requests through TOR service that is described earlier. The operating system includes several applications supporting anonymous traffic, namely web browser, instant messaging client, e-mail client, office suite, sound and graphic editors and others.

2.5.2 Whonix

Whonix is also a GNU Debian/Linux-based operating system[2]. Unlike Tails, this is not a live system and therefore is cannot be executed from a removable medium. Its basic approach to anonymity is splitting the operating system into several (usually two) separate virtual machines (VM). The first VM is working part that is allowed to communicate exclusively through the second VM that is configured so that it communicates via TOR. Like Tails, Whonix includes a bunch of preinstalled applications for anonymous operations in the Internet.

3 WEB ANONYMIZATION EFFICIENCY EVALUATION

The main goal of the presented study was to verify and/or update older results that evaluated the efficiency of web anonymization tools as the latency increase and transmission speed decrease resulting from anonymization. As shown by previous measurements (Liška et al., 2010; Sochor, 2012; Sochor, 2013), the latency increase as well as transmission speed decrease were significant, sometimes much worse that by the factor of 10.

However, due to the fact that anonymity services develop and the bandwidth capacities of ordinary residential and SMB Internet connections increase (supposing that free anonymization services are primarily used by residential users while corporations tend to look for commercial solutions) as well, it is expected that the situation can change rapidly from the point of view of anonymization tools, too.

The proven approach applied in earlier papers consisting in repeated measurements of the anonymized web traffic using different tools and their comparison with the traffic to the same websites without anonymization is applied here, too. Nevertheless, a wider variety of web pages and files and higher number of measurements was used. Moreover, more detailed statistical assessment of measured data was performed here.

4 MEASUREMENT SETUP

The measurement setup design bore in mind the results of earlier measurements (mainly Sochor, 2013) that have demonstrated that the the anonymization requirements to local computing resources are low. Therefore, the decision was made to perform all measurements on an ordinary laptop (namely a PC laptop with Intel Pentium running at 1.5 GHz, 4 GB RAM running 64-bit Windows 10 Home operating system). The Internet connection has been facilitated using a Qualcomm Atheros WiFi interface supporting IEEE 802.11b/g/n communication modes.

4.1 Specification of the Internet Connection used for Measurements

All the measurements analyzed here have been performed in the end of 2016 on a small residential local network connected to the Internet via an Internet Service Provider using 2.4 GHz WiFi connection. There were no explicit limitations applied to the connection to the Internet, and a fixed public IP address was assigned to the client's router (NAT was used here, supposed having no influence to

[2]Whonix is freely downloadable at `https://www.whonix.org`

Tab. 1: List of www pages for measurement

ID	Title (abbr.)	Size (kB)	IP address	Country	Pict.	CSS	Scr.
1	Stormware contacts	2946.1	217.198.115.210	CZ	18/1	3	7
2	Think Ostrava	1066.5	81.91.222.110	CZ	13/3	5	5
3	Fares – City transport Praha	511.84	194.228.3.208	CZ	35/13	4	8
4	Brno airport	3054.7	62.168.14.114	CZ	19/7	4	10
5	Facebook Log In	479.4	31.13.84.36	IRL	4/84	8	2
6	Who we are | UNICEF	412.76	23.64.15.26	NL	24/10	12	15
7	BBC – Local – BBC Local	1119.6	212.58.246.80	UK	6/172	10	18
8	About Us – LEGO.com	2421.0	171.20.53.203	DK	13/0	0	5
9	Google	344.51	216.58.201.227	USA	3/0	0	0
10	NHL Hockey Tickets	329.12	104.90.155.82	USA	76/0	3	1
11	Ebay Online Customer Service	219.05	66.135.223.16	USA	2/26	5	5
12	Official Apple Support	2983.9	104.90.164.244	USA	10/25	4	17
13	AirAsia | Check-In	618.1	54.169.4.245	SGP	5/0	4	4
14	Univ. of Tokyo	2180.2	210.152.135.178	JP	15/95	7	3
15	TOYOTA EAST JAPAN	449.83	203.211.201.139	JP	13/0	0	3
16	A.I.Corp. | Embed. Software	436.35	153.122.124.217	JP	77/26	2	5
17	Africa Universities	2079.1	41.203.16.58	SA	9/41	1	12
18	Lagos University	129.43	195.45.48.50	NGA	40/2	2	1
19	About Us	106.44	164.97.249.110	AUS	3/31	1	2
20	Austral. animals | Perth Zoo	3303.5	119.252.89.140	AUS	30/9	12	36

Tab. 2: URL of www pages for measurement

ID	URL
1	`http://www.stormware.cz/kontakty/`
2	`http://thinkostrava.cz/cs/`
3	`http://www.dpp.cz/jizdne-na-uzemi-prahy/`
4	`http://www.brno-airport.cz/sluzby-na-letisti/mapa-terminalu/`
5	`ttps://www.facebook.com/`
6	`http://www.unicef.org/about/`
7	`http://news.bbc.co.uk/local/hi/default.stm`
8	`http://www.lego.com/en-us/aboutus`
9	`https://www.google.cz/`
10	`https://www.nhl.com/tickets`
11	`http://ocsnext.ebay.com/ocs/home?`
12	`http://www.apple.com/support/`
13	`https://checkin.airasia.com/`
14	`http://www.u-tokyo.ac.jp/en/about/history.html`
15	`http://www.toyota-ej.co.jp/index_top.html`
16	`http://www.aicp.co.jp/`
17	`http://africauniversities.org/`
18	`http://www.unilag.edu.ng/pages.php?page=contact-details`
19	`https://www.border.gov.au/about`
20	`http://perthzoo.wa.gov.au/animals-plants/australia`

the connection performance). The averaged measured downstream speed was 42 Mbps and 9 Mbps for upstream while ISP's declared parameters were 100/10 Mbps.

4.2 Objects Selected for Measurements

The measurements were performed using two custom-made sets, the first one composed of 20 www pages, and the other set was composed of 8 Windows executable files accessible via http protocol.

4.2.1 WWW pages

Web pages for testing have been selected so that only pages with fixed file size (i.e. pages with unfrequent changes). The exact page size was measured using the Web Page Analyzer tool (version 0.98)[3] providing detailed statistics about the web page components (number, type, size, download time etc.).

Among a broader set of such www pages, a subset was selected so that a wide geographical spread (from the point of view of server location) is obtained. As one can see in the Tab. 1, server from all five continents were incorporated in the selection. The geographic location of servers was determined using Flagfox plug-in to Mozilla Firefox (version 5.1.8). The final set of 20 web pages is listed in Tab. 1. As one can see, four servers were located in the US, another four together in Africa and Australia, four in Asia, four in Europe excluding the Czech Republic and the remaining four in the Czech Republic. Also the number of pictures (headed by "Pict."), style files (CSS) and scripts ("Scr." heading) are displayed. URL information about all www pages is listed in the following Tab. 2.

Before the measurements has started, all pages were tested for correct download and displaying. The results of testing was almost faultless. More specifically, both JAP and CyberGhost displayed all pages correctly, while TOR did not display the single page from Australia (`http://www.seek.com.au/`) that was subsequently replaced and it is not listed in the Tab. 1 and 2.

4.2.2 WWW Files

Files used for testing the download speed were chosen almost randomly but files available from web (http) distributing servers with throttling the download speed for intentional transmissions were excluded. All selected files are freely available Windows executables (*.EXE) without any explicit download speed limit. Downloading was tested in all anonymization tools before commencing the measurements, and the test result was 100% positive. The final selection of 8 files is listed in the Tab. 3.

5 MEASUREMENT METHODOLOGY

Before every measurement start, all other applications communicating with the Internet (which could potentially distort the measurement results) were stopped. In addition, common applications running on ordinary computers, which could affect the computer performance (e.g. checking for updates), were stopped. All measurements were done using web browser Mozilla Firefox 44.0.2. The web browser cache was emptied before measurements and their use during measurement was disabled in order to avoid measurement distortion.

5.1 Measurement of Web Page Latency and Download Speed

The latency of web page download (here, the round-trip time – or both-sided latency) is defined as the time difference between sending the first byte of the web request, and the reception of the first byte of the response. The latency was measured using the Performance-Analyzer 1.1.6.1 plugin. This plugin measures both the www page total loading time and the loading times of individual www page items.

[3] Available at `http://www.websiteoptimization.com/services/analyze/` for free.

Tab. 3: List of files for measurement

ID	File name	Size [MB]	IP address	Country
1	NetBeans IDE 8.1	214.02	137.254.56.26	USA
2	WireShark 2.0.2	45.33	104.25.10.6	USA
3	PSPad 4.6.0	3.98	81.0.235.28	Czech Rep.
4	ThunderBird 38.6.0	32.4	104.16.40.2	USA
5	Avast 11.1.2253	4.97	104.90.180.145	USA
6	Zoner Photostudio 18	66.1	217.198.122.22	Czech Rep.
7	BS.Player 2.70	10.06	212.18.44.40	Slovenia
8	Gimp 2.8.2	24.3	209.132.180.179	USA

Tab. 4: Files for measurement – URLs

ID	URL
1	`http://download.netbeans.org/netbeans/8.1/final/bundles/netbeans-8.1-windows.exe`
2	`https://1.eu.dl.wireshark.org/win64/Wireshark-win64-2.0.2.exe`
3	`http://pspad.poradna.net/release/pspad460inst_cz.exe`
4	`http://download.cdn.mozilla.net/pub/thunderbird/releases/38.6.0/win32/cs/Thunderbird\%20Setup%2038.6.0.exe`
5	`http://files.avast.com/iavs9x/avast_free_antivirus_setup_online.exe`
6	`https://www.zoner.cz/download/stazeni-souboru.aspx`
7	`http://download3.bsplayer.com/download/file/mirror1/bsplayer270.setup.exe`
8	`http://saimei.acc.umu.se/pub/gimp/gimp/help/windows/2.8/2.8.2/gimp-help-2-2.8.2-en-setup.exe`

In addition, the plugin produced graphical processing of results as well.

The two-sided latency (RTT) was expressed as Time To First Byte (TTFB) value measured in the plugin, i.e. time from sending the request till the first byte of response arrival to the web browser. The transmission speed was calculated as a ratio of the total size of the web page divided by the cumulative time of the web page download.

5.2 Measuring File Download

Measurements of file download times were performed using Download Status Bar 13.4.4.2 plugin into Firefox. This plugin can measure both current and average transmission speed, download total time, file size, etc.

6 MEASUREMENT RESULTS

Both for web pages and files, the four anonymization modes were measured.

- No anonymization,
- Anonymization using TOR (in default configuration),
- Anonymization using CyberGhost VPN,
- Anonymization using Jap/Jondo.

6.1 Results of Web Page Anonymization

Measurements of anonymization of web pages were performed in 10 measurement for every web page in the web page set as listed above. Each measurement was performed in every of four anynomization modes listed below (in fact, three modes using different anonymization tool, and one mode without anonymization). This totals in 40 (4 modes, 10 measurements)

Tab. 5: Latency and transmission speed averaged values and standard deviations for web page download

Anonymiz. mode	Lat. [ms]	Incr. [%]	Std. dev.	Speed [kbps]	Drop [%]	Std. dev.
No anonymization	488		128	5,471		783
CyberGhost VPN	777	59%	208	2,536	54%	285
TOR	788	61%	256	2,888	47%	421
JonDo	702	44%	141	2,793	49%	221

values of both latency and download time (later converted to download speed) were measured for every single web page in the set. Each single measurement started from the same web page displayed in the web browser.

The results were averaged (10 measurements) and the standard deviation was calculated as well. The summary results for web pages download (for both latency and transmission speed) are listed in Tab. 5. In addition to the measured results, the ratios of latency increase and transmission speed are displayed in order to get a better overview of how anonymization worsens the parameters of www communication. The results are used for the overall comparison of the measured results to older measurements as described in Section 6.3.

6.2 Results of File Download Anonymization

The file download was measured in 5 sets, i.e 20 values was measure for every single file in the set described above in Tab. 3. Again, the download always started from the www browser home page. The summarized results (averages and standard deviations) for file download are listed in Tab. 6.

Tab. 6: Transmission speed averaged values for file download

Anonymization mode	Speed [kbps]	Speed drop [%]	Std. dev.
No anonymization	40.29		2.54
CyberGhost VPN	13.14	67%	1.46
TOR	15.15	62%	1.27
JonDo	2.843	93%	1.26

Like in the case of www pages, the file download speeds are listed together with speed drop percentages and standard deviations.

6.3 Comparison with Previous Results

The measured results roughly conform to the previous results cited above. According to Sochor (2012), the latency increase factor for TOR was 3.1 while 2.2 for JAP. The present measurements demonstrated that the latency increase is still significant but the increase ratii are significantly lower, just around 1.5 as shown by the "Incr." column in the Tab. 5. This difference was partly caused by the use of a broader range of ages for measurement (among the measured pages, there are specific cases where the latency increase factor is significantly bigger than 2, still), and partly because of the overall decrease of latency in www service due to the increased bandwidth.

Regarding the transmission speed decrease, it was almost 40% for TOR and 2% for JAP for web pages while 5% for TOR and 20% for JAP for file download according to the previous study. As one can see from the current results in Tab. 5 and 6 above, the present results in transmission speed decrease seem to be much worse that they used to be in the past. However, when looking to results closely, it is obvious that the greater differences are observed for newer anonymization tools like JonDo and CyberGhost. On the other hand, the measured results for TOR remained rather similar (37% decrease in 2012 and 47% in 2016). More significant differences for JonDo could be cause by the fact that the "free" part of JonDo service was tested and it is not documented whether the parameters of this free services have remained the same since 2012. The significant worsening seem to indicate that the transmission speed could be intentionally throttled by the JonDo network operators in order to maximize the difference between the free and commercial service.

7 DISCUSSION AND CONCLUSIONS

The results of measurements shown above confirm the main conclusions of previous works as declared in the introduction, i.e. all the anonymization tools subject to the measurement caused a significant latency decrease and transmission speed increase. Therefore, it cannot be recommended to use anonymous web browsers for a daily use unless special circumstances justify doing so, especially for downloading bigger amounts of data (that is almost inevitable in the present web where the average sizes of ordinary pages increase quite rapidly).

On the other hand, the latency increase is relatively favorable for using the anonymous web browsing, especially to smaller web pages. Downloading bigger files using anonymous web browsing can be quite lengthy, nevertheless.

Bearing in mind the fact that situation among anonymization tools changes quite rapidly, it seems reasonable to perform more detailed investigation in this field. There are some other reasons for that, primarily the fact that the transmission speed decrease measured here is bigger that it used to be earlier.

8 REFERENCES

Bagai, R. and Lu, H. 2016. Measuring Client-Server Anonymity. In: Gaj, P., Kwiecień, A. and Stera, P. (eds.). *Computer Networks: Proceedings of 23rd Int. Conf., CN 2016*, pp. 96–106.

CyberGhost. 2017. *CyberGhost VPN*. [online]. Available at: `http://www.cyberghostvpn.com/en`. [Accessed 2017, October 25].

Dingledine, R., Mathewson, N. and Syverson, P. 2017. *Tor: The Second-Generation Onion Router*. [online]. Available at: `https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf`. [Accessed 2017, October 25].

Feigenbaum, J., Johnson, A. and Syverson, P. 2012. Probabilistic Analysis of Onion Routing in a Black-box Model. *ACM Transactions on Information and System Security*, 15 (3).

Glenny, M. 2012. *DarkMarket: How Hackers Became the New Mafia*. London: Vintage Books.

I2P. 2017. *The Invisible Internet Project*. [online]. Available at: `https://geti2p.net/en/`. [Accessed 2017, October 25].

JAP. 2017. *Anonymity & privacy*. Project AN.ON Anonymity Online. [online]. Available at: `http://anon.inf.tu-dresden.de`. [Accessed 2017, October 25].

Kapusta, L. 2016. *Nástroje a techniky anonymní www komunikace*. Bachelor thesis.

Liška, T., Sochor, T. and Sochorová, H. 2010. Comparison Between Normal and TOR-anonymized Web Client Traffic. *Procedia – Social and Behavioral Sciences*, 9, 542–546.

Sochor, T. 2012. Anonymization of Web Client Traffic Efficiency Study. In: Gaj, P., Kwiecień, A. and Stera, P. (eds.). *Computer Networks: Proceedings of 19th Int. Conf., CN 2012*, pp. 237–246.

Sochor, T. 2013. Automatic Control of Configuration of Web Anonymization. *International Journal of New Computer Architectures and Their Applications (IJNCAA)*, 3 (2), 1–10.

Statista.com. 2017. *The Statistics Portal*. [online]. Available at: `https://www.statista.com/`. [Accessed 2017, November 1].

Zuzčák, M. and Sochor, T. 2017. Behavioral Analysis of Bot Activity in Infected Systems Using Honeypots. In: Gaj, P., Kwiecień, A. and Sawicki, M. (eds.). *Computer Networks: Proceedings of 24th Int. Conf., CN 2017*, pp. 118–133.

AUTHOR'S ADDRESS

Tomáš Sochor, Department of Informatics, Faculty of Business and Economics, Mendel University in Brno, Zemědělská 1, 613 00 Brno, Czech Republic, e-mail: tomas.sochor@mendelu.cz

Cyril Klimeš, Department of Informatics, Faculty of Business and Economics, Mendel University in Brno, Zemědělská 1, 613 00 Brno, Czech Republic, e-mail: cyril.klimes@mendelu.cz