Introduction to Information Security, INTROSEC 2019.

Autumn Term 2019

Assignment 2A

Task 4: Anonymisation Tools: Keeping Your Information to Yourself

2019 - 12 - 11

Group 21

Justas Narusas, Efstathios Psyllakis

Introduction

It is worth highlighting that anonymization of identity is becoming a major concern in everyday life. Personal data is exposed worldwide and can be compromised at any given time, it just depends on if an individual is interested to acquire information about a user. As a result, testing of anonymization tools was chosen in order to find out if the existing technology is reliable.

Design

ProtonMail

Emails are considered as one of the primary ways of communication nowadays between individuals and many of them care for their anonymity alongside these communication channels with regard to their profession (e.g. journalists), information included (e.g. classified info) etc. As a result, we have chosen to test ProtonMail, a secure email service provider based in Switzerland, and check its services and accountability.

The process of setting up ProtonMail is as easy as using a common email service. A user needs to sign up on their official website by creating a username and password. There are no delays with regard to the usability of the tool. Also, it is stated that you can use Tor browser instead of a regular one in order to improve your anonymity. Usage of a regular browser like Google Chrome, Firefox, etc can be traced back to the user, therefore that can induce a breach of complete anonymity. Furthermore, the identification process of a user is possible to stay anonymous using captcha option rather than email, sms, or donation verification methods which may expose his/her personal data. Former stated methods will keep some personal data, which can become a breach of anonymity. Information about using the tool is clearly stated on their website and it could be understandable even from a naive user.

In addition, ProtonMail is used for encrypting your emails and securing your communication with end-to-end encryption. Furthermore, two-factor authentication with TOTP tokens is available for its login process which can increase the level of security for a user (“ProtonMail,” 2019). Compared to other secure mailing services seems to be one of the most reliable and trustworthy based on their encryption technology, privacy policies and data collecting methods. On the other hand, the tool does not provide the user with complete anonymity. The network administrator will be able to identify the tool's usage if the user connects via regular browser, but the content of emails could not be revealed.

To conclude, there is a possibility of uncovering the anonymized data if the receiver is using a regular email provider as the service can be breached from a third party. ProtonMail provides you with extra symmetric encryption and expiration date options that can protect from data leakage.

ProtonVPN

Virtual Private Networks were developed alongside the Internet and they are used as an extension for users in order to use a private network across a public network. This feature enables them to exchange data across shared or public networks as if they were connected to a private network. Furthermore, VPNs were developed at first for remote users or corporations but nowadays are commonly used from individuals in order to stay anonymous on the Internet ("Virtual private network," 2019). As a result, ProtonVPN was decided to be tested which belongs to the same company as ProtonMail.

Creators of ProtonMail provide users with another great product - ProtonVPN which is a virtual private network software. The installation process is very easy even for a common user and ProtonMail offers a user-friendly UI. The user can use its ProtonMail account (which is already quite anonymous, since it does not require any personal data in order to sign-up) for ProtonVPN.

Furthermore, Virtual Private Network does not give complete anonymity to a user, even though some VPN providers ensure they do. For instance, every time a user connects to a VPN, service provider keeps user's IP address logged. ProtonVPN was chosen with regard to the provided no-logs policy and strong encryption methods (e.g. network traffic is encrypted with AES-256 and key exchange is made with 4096-bit RSA) ("ProtonVPN Service—Privacy Policy," n.d.). The collection of IP addresses connected to the VPN could be a concern, but since the service is located in Switzerland, ProtonVPN is not required to release any of its logs or data, as it is stated on the official website in the *Threat Model* section:

"Under Swiss law, we cannot be forced to log your IP address, and therefore even though we technically have access to your IP addresses, we cannot be legally obligated to log it and turn it over. This is rather unique to Switzerland and one of the reasons we decided to base ProtonVPN in Switzerland." ("Understanding the VPN Threat Model," 2017)

It is worth highlighting that ProtonVPN's free version does not offer full access to advanced services. On the other hand, ProtonVPN seems to be one of the most reliable services compared to other free VPNs. For instance, HolaVPN provides with a completely free service, but log data and personal information are collected in order to maintain its service, which make user's identity not as anonymous as it may be expected by a typical user, (who have common misconceptions of anonymity using virtual private network). In addition, Wikipedia's page about VPN on the section *"Public or Private VPNs"* illustrate clearly a disadvantage of common VPNs which may lead to a breach of user's security:

"Users must consider that when the transmitted content is not encrypted before entering a VPN, that data is visible at the receiving endpoint (usually the public VPN provider's site) regardless of whether the VPN tunnel wrapper itself is encrypted for the inter-node transport." ("Virtual private network," 2019)

To conclude, a user should also take in consideration the fact that connecting to a VPN means that at the same time, relies on the trustworthiness of the provider, as users' activity passes through their servers ("Tor Vs VPN: The Pros and Cons of Each," n.d.).

TorBrowser

Internet is used daily by users around the globe. In order to browse the Internet a browser like Google Chrome, Firefox, Opera, etc. is needed. As a result, Tor browser was chosen to be tested, which allows the user to explore the internet via Tor Network (onion network) without giving away its identity (IP address).

The installation process is straightforward compared to any other browser. User needs to visit Tor Browser's official website to download a compatible version regarding his operating system. The only challenging part of keeping user's maximum available anonymity depends on the privacy & security settings chosen within the browser. Default settings do not offer maximum security, so the user has to modify them manually (security level, history collection, etc.).

All the documentation regarding Tor's use and how it works can be found on the official website. Tor Browser is built for anonymization purposes so regular browsing will keep your identity safe. On the other hand, it will be challenging for a regular user to go through all the documentation because it is complex to understand, requires time and understanding of how network, protocols and Internet itself works.

Tor Browser offers a relay traffic browsing by hiding the location and activity of a user as it works on a distributed network (Tor Network), which is maintained by volunteers all around the world ("The Tor Project | Privacy & Freedom Online," n.d.). The tool hides user's connection and destination, but does not remove personal data, which is a very common misconception among users. For instance, by using Yahoo, Gmail or any other applications, that require personal data, the user exposes his/her information on the exit node of connection. Tor Browser's vulnerabilities are the exit nodes where personal data can be breached and acquired, which can later be traced to the origin of the user, which has been done before. It can also be called a man-in-the-middle attack, which is done by setting up a fully functional exit node and sniffing its traffic ("Tor network exit nodes found to be sniffing passing traffic," n.d.).

Test Protocol

In order to test the aformentioned Anonymization tools, a test protocol which will test their credibility and usability levels on their main features (emails, browsing, secure exchange of data) was formed:

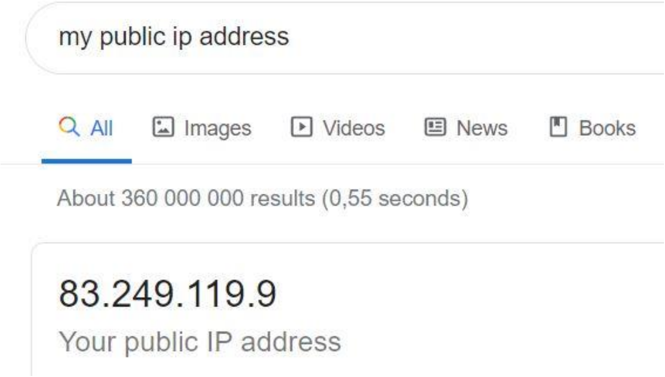
- Setup of tools through downloading and installing them, comparing the followed procedure between the tools.
- Testing them on Windows OS in order to see how they perform and identify possible issues.
- Observe their usability compared to average users.
- Monitor their performance for possible security issues for users.
- Document and analyze all gathered info.

Experiment Results

ProtonVPN

ProtonVPN application was easy to set up. Since an anonymous account for ProtonMail was already created, it was used to log into the application. Application itself is very user-friendly with easy to read user interface and all the information approachable by being one or two mouse clicks away.

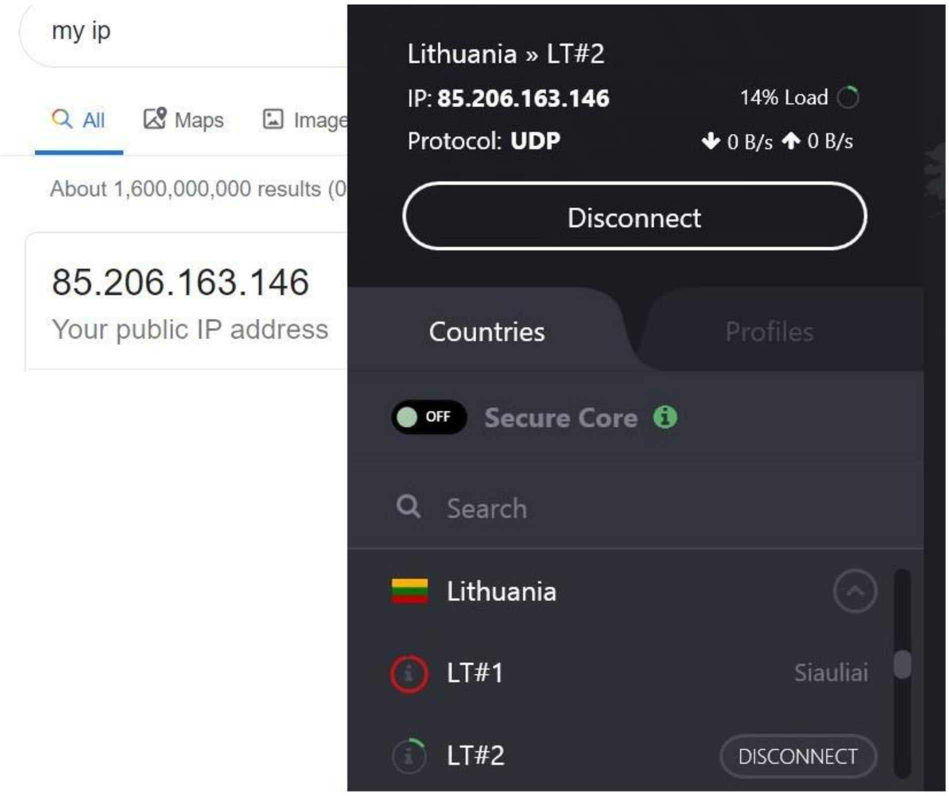
While testing VPN’s usage, our public IP address was acquired by using Google’s help.


my public ip address

About 360 000 000 results (0,55 seconds)

83.249.119.9
Your public IP address

The VPN was tested by connecting it to a Lithuanian VPN server and the IP address was checked again.


my ip

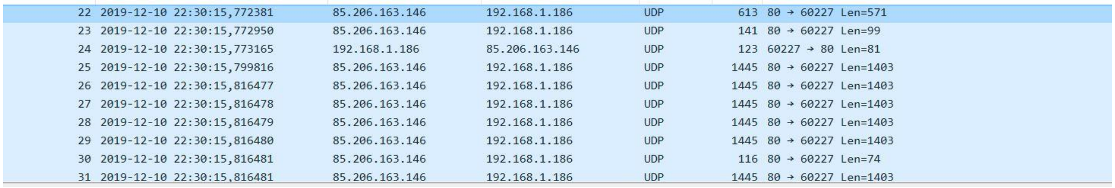
About 1,600,000,000 results (0

85.206.163.146
Your public IP address

Lithuania » LT#2
IP: **85.206.163.146** 14% Load
Protocol: **UDP** 0 B/s 0 B/s

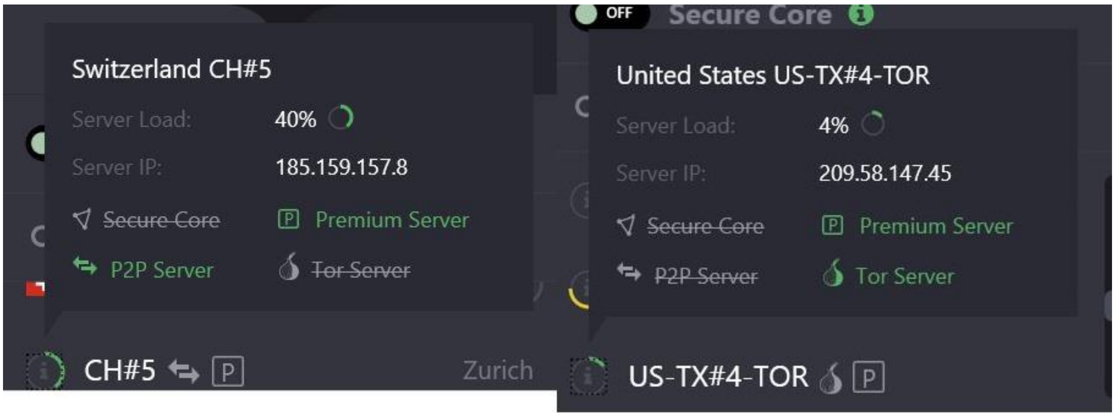
Lithuania
LT#1 Siauliai
LT#2 DISCONNECT

Observing that the VPN provided a Lithuanian public IP, it was decided to test network traffic by visiting some websites while using Wireshark. All the connections seemed to go back and forth between the static IP address and the VPN server in Lithuania. In addition, there were no connections observed to the website IP addresses as it should appear when not using a VPN.



```
22  2019-12-10 22:30:15,772381   85.206.163.146   192.168.1.186    UDP    613  80 → 60227 Len=571
23  2019-12-10 22:30:15,772950   85.206.163.146   192.168.1.186    UDP    141  80 → 60227 Len=99
24  2019-12-10 22:30:15,773165   192.168.1.186    85.206.163.146   UDP    123  60227 → 80 Len=81
25  2019-12-10 22:30:15,799816   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
26  2019-12-10 22:30:15,816477   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
27  2019-12-10 22:30:15,816478   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
28  2019-12-10 22:30:15,816479   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
29  2019-12-10 22:30:15,816480   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
30  2019-12-10 22:30:15,816481   85.206.163.146   192.168.1.186    UDP    116  80 → 60227 Len=74
31  2019-12-10 22:30:15,816481   85.206.163.146   192.168.1.186    UDP   1445  80 → 60227 Len=1403
```

Further information about server’s options and availability can be found by pressing ‘i’ next to the name of the server.



Switzerland CH#5

Server Load: 40%

Server IP: 185.159.157.8

~~Secure Core~~ Premium Server

P2P Server ~~Tor Server~~

CH#5 Zurich

United States US-TX#4-TOR

Server Load: 4%

Server IP: 209.58.147.45

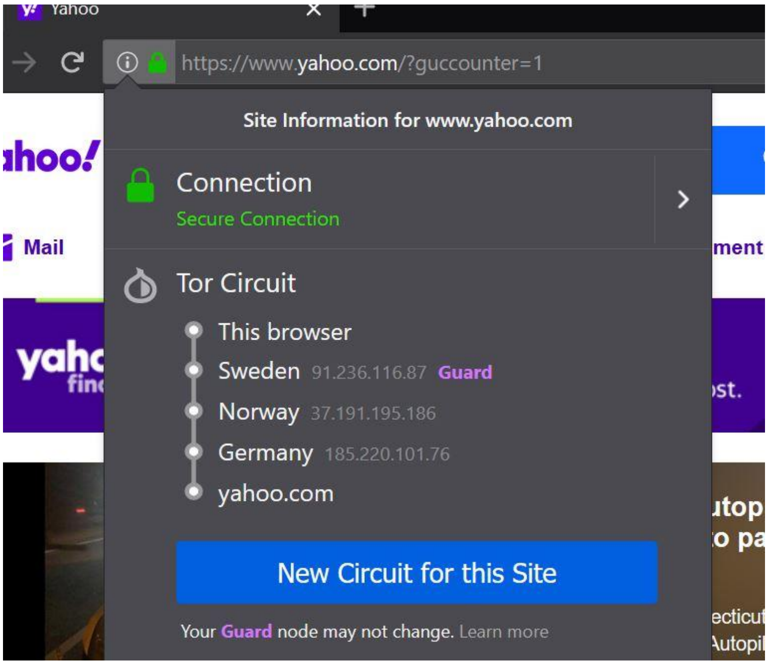
~~Secure Core~~ Premium Server

~~P2P Server~~ Tor Server

US-TX#4-TOR

Tor Browser

After downloading and installing Tor browser its usability was tested, which seemed to be quite easy and straightforward for any regular user. Although, it is noticeable, that more time required to start the browser compared to Google Chrome or Firefox. When browsing the web, the load time is slightly longer between pages, since it has to connect to the network circuit which is displayed at the top left-hand corner of the browser.



Site Information for www.yahoo.com

Connection

Secure Connection

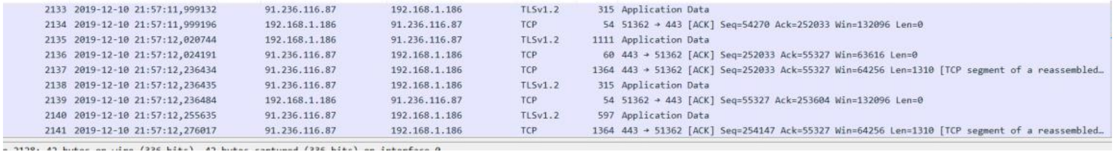
Tor Circuit

- This browser
- Sweden 91.236.116.87 Guard
- Norway 37.191.195.186
- Germany 185.220.101.76
- yahoo.com

New Circuit for this Site

Your Guard node may not change. Learn more

While using Tor Browser, network traffic was tested with Wireshark. In addition, connections were observed only between our static IP address and the Tor Circuit's first layer of network (in this case of Sweden) when a website was visited.



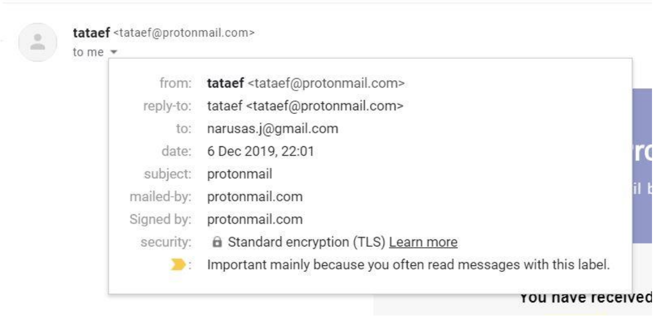
```
2133 2019-12-10 21:57:11,999132   91.236.116.87   192.168.1.186   TLSv1.2    315 Application Data
2134 2019-12-10 21:57:11,999196   192.168.1.186   91.236.116.87   TCP         54 51362 → 443 [ACK] Seq=54270 Ack=252033 Win=132096 Len=0
2135 2019-12-10 21:57:12,020744   192.168.1.186   91.236.116.87   TLSv1.2   1111 Application Data
2136 2019-12-10 21:57:12,024191   91.236.116.87   192.168.1.186   TCP         60 443 → 51362 [ACK] Seq=252033 Ack=55327 Win=63616 Len=0
2137 2019-12-10 21:57:12,236434   91.236.116.87   192.168.1.186   TCP       1364 443 → 51362 [ACK] Seq=252033 Ack=55327 Win=64256 Len=1310 [TCP segment of a reassembled…
2138 2019-12-10 21:57:12,236435   91.236.116.87   192.168.1.186   TLSv1.2    315 Application Data
2139 2019-12-10 21:57:12,236484   192.168.1.186   91.236.116.87   TCP         54 51362 → 443 [ACK] Seq=55327 Ack=253604 Win=132096 Len=0
2140 2019-12-10 21:57:12,255635   91.236.116.87   192.168.1.186   TLSv1.2    597 Application Data
2141 2019-12-10 21:57:12,276017   91.236.116.87   192.168.1.186   TCP       1364 443 → 51362 [ACK] Seq=254147 Ack=55327 Win=64256 Len=1310 [TCP segment of a reassembled…
e 2138: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
```

ProtonMail

Three-step procedure required in order to get started with ProtonMail:

1. Visit official website protonmail.com and click 'Sign Up' at the top right corner of the website.
2. Choose the plan desired and fill in the information required in order to register an account (username and password are the only fields required to keep you anonymity).
3. Enjoy using ProtonMail

Email to a Gmail account received from a ProtonMail account will be displayed as in the screenshot below:

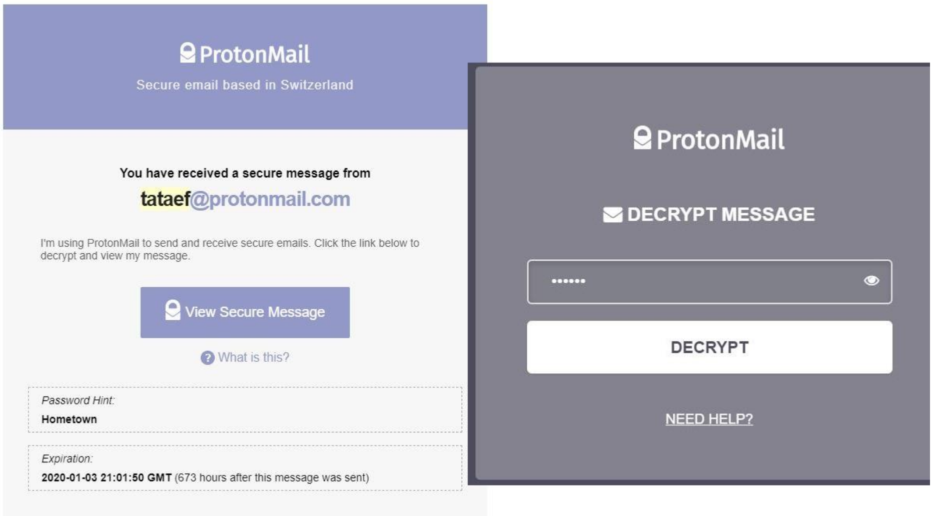


tataef <tataef@protonmail.com>
to me

from: tataef <tataef@protonmail.com>
reply-to: tataef <tataef@protonmail.com>
to: narusas.j@gmail.com
date: 6 Dec 2019, 22:01
subject: protonmail
mailed-by: protonmail.com
Signed by: protonmail.com
security: Standard encryption (TLS) Learn more
Important mainly because you often read messages with this label.

You have received

A message will appear as on the left picture when an encrypted email is received, and after pressing the ‘View Secure Message’ option, it will forward the user to ProtonMail’s website. Afterwards, the user has to type the decryption key, which is hinted in the email received and by entering the password the message will be shown. Note: the email received had an expiration date that the user can set up when sending an email.



ProtonMail
Secure email based in Switzerland

You have received a secure message from
tataef@protonmail.com

I'm using ProtonMail to send and receive secure emails. Click the link below to decrypt and view my message.

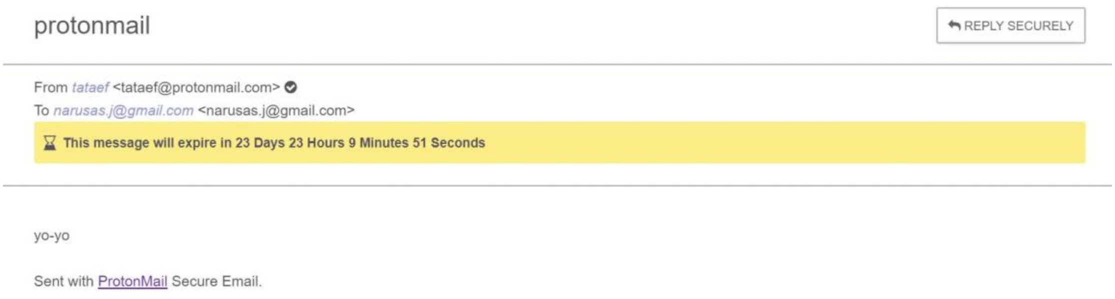
View Secure Message

What is this?

Password Hint:
Hometown

Expiration:
2020-01-03 21:01:50 GMT (673 hours after this message was sent)

The message that was received:



protonmail

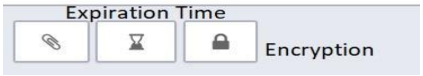
From tataef <tataef@protonmail.com>
To narusas.j@gmail.com <narusas.j@gmail.com>
This message will expire in 23 Days 23 Hours 9 Minutes 51 Seconds

yo-yo

Sent with ProtonMail Secure Email.

When sending an email, the expiration time and encryption of the email could be set by choosing to do so at the bottom:

Sent with ProtonMail Secure Email.



Time Summary

December 5th - preliminary research and discussion with course assistant - 3h

December 6th - research of tools and start of the lab report - 4h

December 7th - researching and writing the lab report - 2h

December 9th - testing of tools and writing of the lab report - 5h

December 10th - finalization of tool testing and the lab report - 6h

Conclusions

User’s data security and anonymity has become a major concern as most of societies live in the digital age. Personal data collection is a power that tech giants such as Facebook or Google have over us, the users. Not only that, hackers always work on acquiring personal information, which can be sold and profited of.

Throughout the experiment, three different anonymization tools were examined with regard to their usability and their services provided to an average user. ProtonMail, ProtonVPN and Tor Browser are one of the most secure and user-friendly tools of their kind compared to others on the market if used correctly. In addition, tested tools’ benefits outweigh the costs, which were discovered during the analysis and experimentation process. As a result, they are highly recommended for users that are concerned about their anonymity online.

Users should consider combining tools’ use, in order to maximize their security, while browsing, communicating with peers or file sharing. Although, misuse of these tools can cause anonymity breaches, just like being online without using them, nothing will be safer than a user itself being cautious of how he uses anything and everything that technology has provided us with. To conclude, education of users about common threats, misconceptions and technology usage is crucial and providing them with the right knowledge should be a priority of societies as the online environment will be safer.

References

ProtonMail. (2019). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=ProtonMail&oldid=930059913

ProtonVPN Service—Privacy Policy. (n.d.). Retrieved December 11, 2019, from ProtonVPN website: https://protonvpn.com/privacy-policy

The Tor Project | Privacy & Freedom Online. (n.d.). Retrieved December 11, 2019, from https://torproject.org

Tor network exit nodes found to be sniffing passing traffic. (n.d.). Retrieved December 11, 2019, from https://www.scmagazineuk.com/tor-network-exit-nodes-found-sniffing-passing-traffic/article/1479106

Tor Vs VPN: The Pros and Cons of Each. (n.d.). Retrieved December 11, 2019, from https://www.hotbot.com/blog/tor-vs-vpn-the-pros-and-cons-of-each/

Understanding the VPN Threat Model. (2017, June 18). Retrieved December 11, 2019, from ProtonVPN Blog website: https://protonvpn.com/blog/threat-model/

Virtual private network. (2019). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=929051104