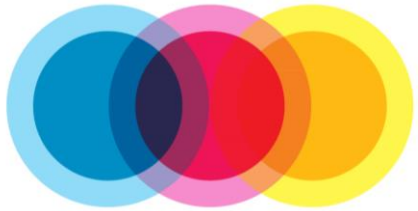


SHARE FOUNDATION

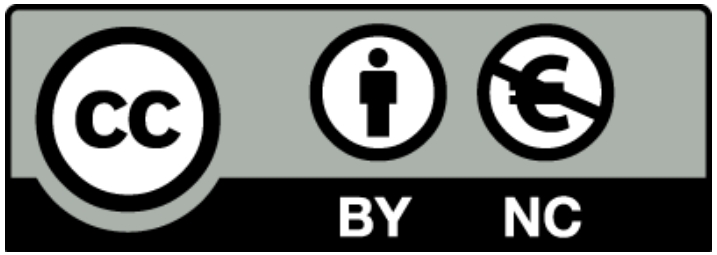
network of young media makers
european youth press

Digital Security

BELGRADE, SEPTEMBER 2015

ANDREJ PETROVSKI, SHARE FOUNDATION

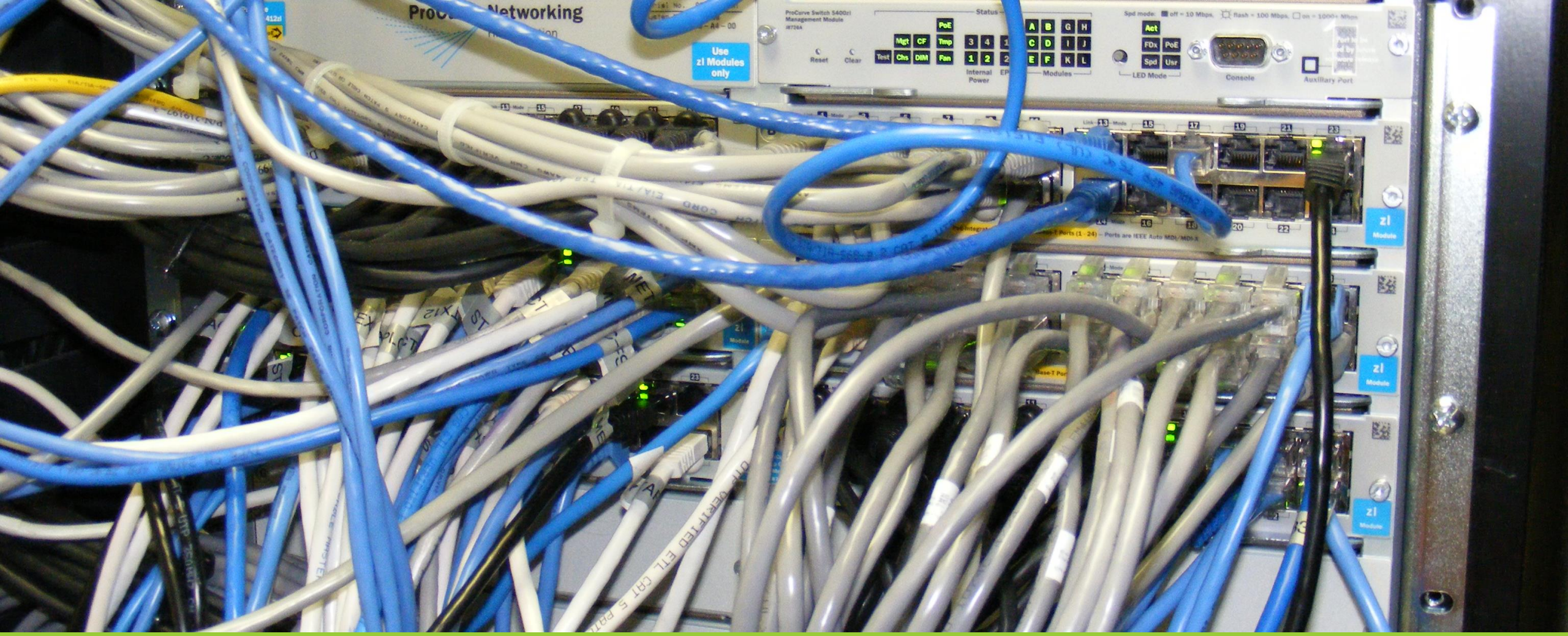
WWW.SHARECONFERENCE.NET



What is the Internet?

The Internet in its essence is not what most people perceive when online. It is an abstract space which gives limitless opportunities, but basically it consists of hardware, millions of servers, routers, cables and other network peripheral devices. Basically, in most cases, there is a physical cable or wireless connection reaching almost every corner of the world and every Internet user. Each and every network device of the Internet infrastructure has its own physical location. Some of them are grouped, which makes their locations a sort of “crossroads” of the Internet.

One of the reasons we seldom discuss the issues of this invisible infrastructure is the fact that the speed of the packets traveling through the network is so big and unnoticeable to us, in most cases we don’t feel a significant difference in whether our packets are traveling just around the corner or to around the world and back.



The physical Internet

Mostly cables, routers and servers.

How does the Internet work?

All the information transmitted through the Internet, between the routers, servers and other hosts, is split into smaller chunks of data known as packets. Every packet consists of a header and content. If we need to explain this by using an analogy, we should think about those packets as a traditional paper envelope where the letter inside is the content and the stamps and the addresses written on the outside are the headers. Without an address written on the envelope, the letter will never reach the intended destination. Similar to a post office, the ISP's router examines the destination address of each packet and determines where to send it. As we said, those "addresses written on the envelope" are called headers and they are one type of metadata.

Nothing to hide?

Article 12 of the UDHR says:

*"No one shall be subjected to arbitrary interference with his **privacy**, family, home or **correspondence**, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

The Right to Privacy in the Digital Age

UN Resolution 68/167** aims to examine the **protection and promotion** of the **right to privacy** in the context of **domestic and extraterritorial surveillance** and/or **interception of digital communications** and **collection of personal data**, **including** on a **mass scale.

Is digital privacy a special category of privacy? If Yes, should it be implemented diferently?

Even the best of laws are not enough.

Activity 1: A day without privacy

Imagine that privacy doesn't exist in the world you live in.

- Everyone can watch you doing your daily routines.
- Everyone will know all your bank accounts, credit card numbers, PIN numbers etc.
- Everyone can listen to your conversation with other people.
- Everyone will know everything about you.

Try to answer the following questions.

- Do you feel "naked"?
- Do you feel violated?
- Have you experienced something similar to this?
- Do you think this scenario is possible?

Activity 2: Trace my shadow

Everyone has a shadow that follows them around all the time. The real shadows, we can control, the digital ones – not so much.

Go to: https://myshadow.org/trace-my-shadow

- Check the boxes that apply to you
- How many traces did you get? (I got 132 :S)

Let's discuss these results.

Fortunately, it’s up to you

In many cases, behavioural patterns that are considered positive in the digital environment can strongly influence the level of online privacy and security.

On the other hand, laziness is privacy’s most dangerous enemy.

Security isn’t magical, it doesn’t come automatically or naturally.

There are quite a few aspects that need to be considered.

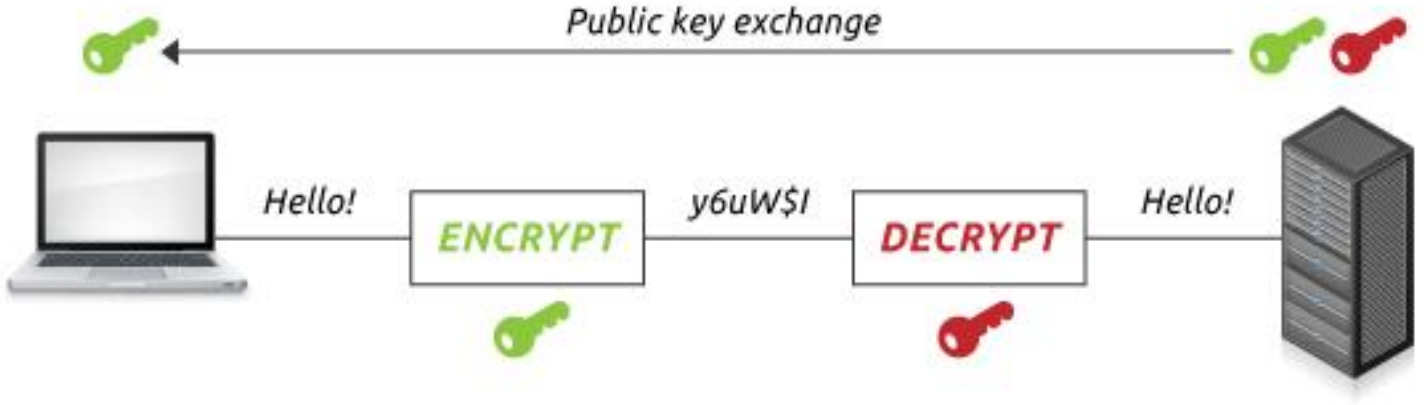
A universal solution doesn’t exist.

Sharing sensitive information

Everyone who is in possession of information that can seriously affect other should consider those information sensitive.

Each and every person comes across that kind of information at some point, and many need to share or forward the information further.

In these situations ***encryption*** plays a key role in securely transferring information from point A to point B.



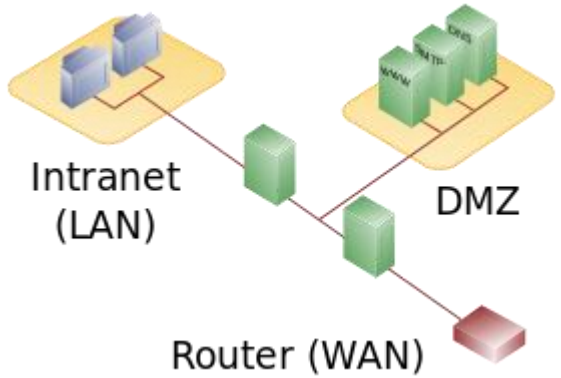
Storing sensitive information

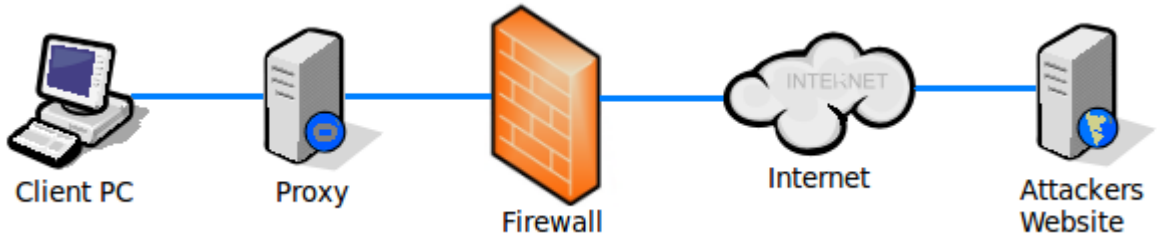
There are situation in which sensitive information that has already been received needs to be stored for further processing or research.

Using an encrypted channel to transfer information between point A and point B doesn't make much sense if point B, i.e. the information receiver isn't properly secured and protected.

That is why, different types of software and hardware are used. Even though hardware can be more efficient, software solutions are cheaper or free and they offer nearly the same features.

These include ***Firewalls, Anti-Virus/Malware software*** etc.



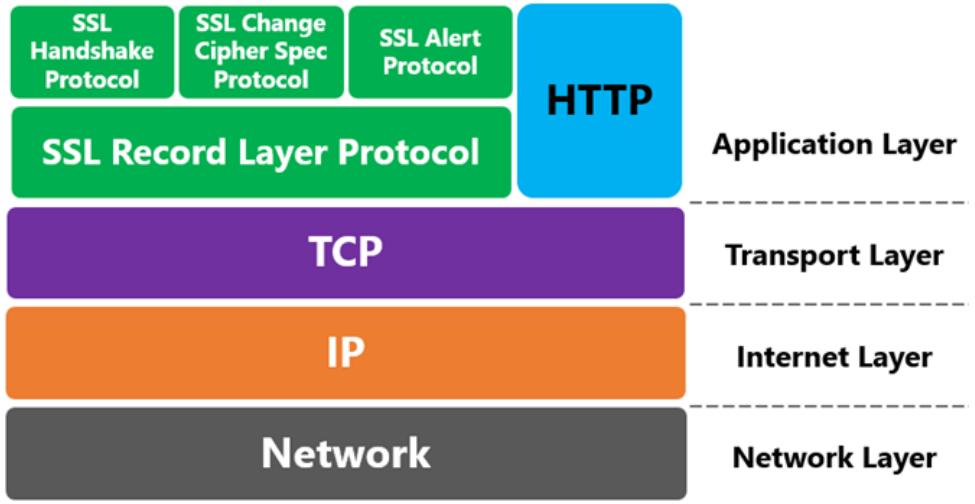


Where and how you connect

While online there are many sensitive information that are transferred between the user and online services, these include, but are not limited to usernames, passwords, personal data etc. That is why it is important to secure the connection.

When using some public network, such as public wi-fi hotspot or a computer in an internet café using a secure connection is obligatory since these systems are quite easy to gain access to in addition to the fact that the connection provider has full control over the data flow and can intercept it.

The safe thing to do is to use ***SSL*** whenever you can.

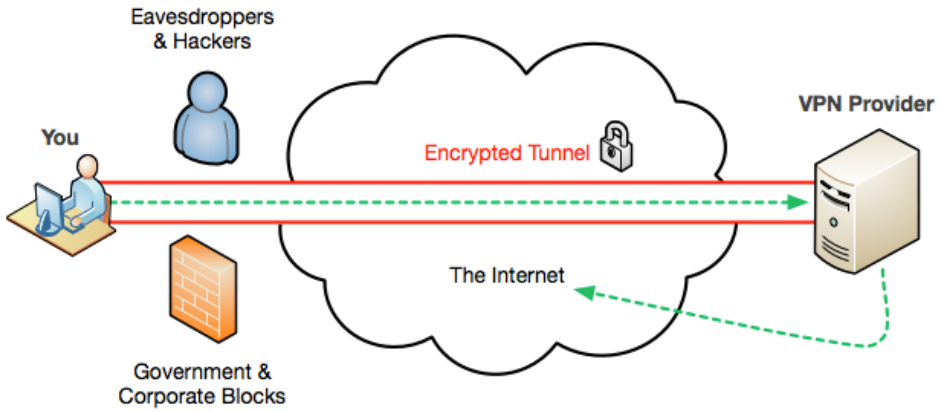


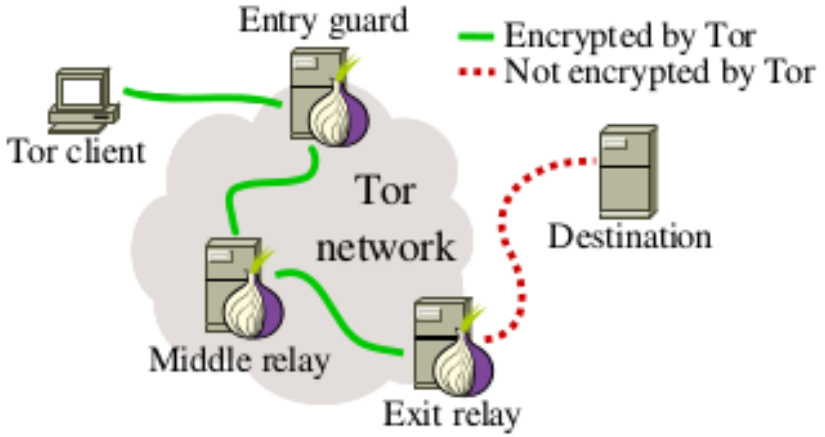
What you do while you are connected

By using a secure connection only the data the user sends trough the network. However, there are many information that are not sent by the user, but by the applications and services he uses.

These data is known as Meta Data. Meta Data in many cases is more important that the actual content the user sent trough the network, because once it's logically mapped Meta Data can show the physical movement of the user, his interactions with other people, information about the devices they used etc.

In cases when the user needs to stay anonymous ***VPN*** or ***TOR*** is used.





Forgetting to install updates

A huge number of new types of malicious software that can corrupt the user's privacy is being developed every day.

Fortunately, new techniques to mitigate different sorts of attacks is being developed on daily basis as well.

Every tool can be configured to get updates automatically. However, it is a smart choice to configure the software what updates to install.

What are the risks?

Dealing with sensitive information can get anyone in trouble, especially in environments in which the basic human rights are being violated.

There are several ways trough which the system can oppress active citizens, mostly the mechanism consists of fines, prison sentences, excommunication, isolation or even more drastic measures.

Besides, there is always the risk that someone can steal and misuse or abuse sensitive data.

Do’s and don’ts

Use strong passwords and store them securely. Change them often.

Install firewall and anti-virus software. Update them on regular basis.

Update the software!!!

Log out of all websites after having finished using them.

Only use trusted connections.

Only use trusted services.

Stay informed about the risks.

Never include birthdays, names or other personal data when creating passwords.

Never install untrusted software, especially when it comes to anti-virus solutions.

Don’t let the system install updates automatically.

Don’t leave the computer unattended when logged on.

Don’t connect to public wi-fi unless properly protected.

Don’t click on any link received via email.

Passwords

Create passwords as complex as possible.

Use pseudorandom passwords:

MdbmaL-T4m18thBd = My dad bought me a Lap-Top for (4) my 18th Birthday

Change passwords every 60-90 days, or in case something happens.

DO NOT WRITE PASSWORDS ON POST-ITS!

Do not use same passwords for multiple accounts.

Store passwords some place safe.

Strong recovery questions are as important as a strong password.

Demonstration 1: KeePass

Easy-to-use tool that securely stores passwords in a database.

The database can be locked in several different ways, including master password and key file.

If the master password gets lost, all the passwords in the database are lost as well.

There are no backdoors for password recovery.

Download: http://keepass.info/download.html

Tutorial on how to use KeePass:

http://keepass.info/help/base/firststeps.html

Demonstration 2: TOR Browser

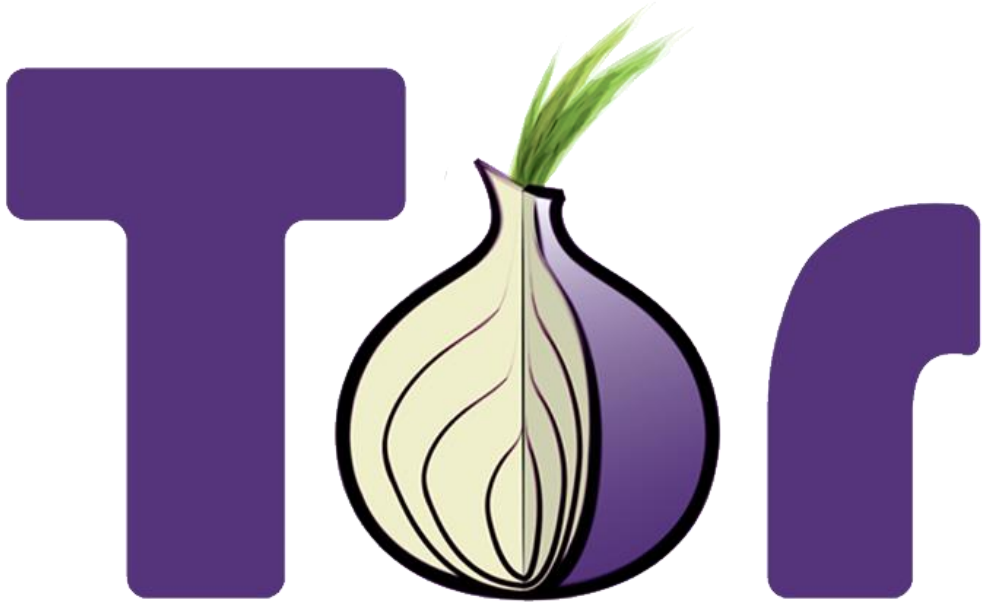
Probably the best tool for online anonymity.

The recent versions are very simple to install.

It comes preconfigured as a web browser, which is in essence a modified Firefox.

Download link:

https://www.torproject.org/download/download



Demonstration 3: PGP

Pretty Good Privacy is a mechanism for encryption of e-mail communication.

It is based on a pair of private and public keys.

Provides end-to-end encryption.

Mozilla Thunderbird:

https://www.mozilla.org/en-US/thunderbird/

A plug in used for PGP is Enigmail.

Demonstration 4:Pidgin

Pidgin is a tool that enables encrypted and private chat communication.

It doesn’t leave plain text copies on servers.

Works with all major chat services.

Best used with the OTR plug in:

https://otr.cypherpunks.ca/

Download link:

https://www.pidgin.im/

Tutorial and other resources:

https://securityinabox.org/pidgin_securechat

Web browsing

Secure web browsing is one of the most important segments of internet privacy.

There are several mechanisms that secure online privacy.

It is best when these mechanisms are combined together.

Web browsers offer Private Browsing mode, which is not really private, but it is a good start.

VPN (Virtual Private Network) services offer fast and private web browsing, but can cost a lot of money.

TOR is slightly slower, but it’s free and has somewhat better level of privacy.

However, none of these mechanisms can really protect the users if not used properly.

Demonstration 5: HTTPS everywhere

It is installed as a plug in to the browser.

Makes the browser request for SSL connection whenever possible.

No configuration necessary.

Download link:

https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en

Anti – virus software

Avira is a free anti – malware tool.

http://www.avira.com/en/avira-free-antivirus

Spybot is a tool that allows it’s users a set of different utilities related to malware management.

http://www.safer-networking.org/

Comodo firewall is a personal firewall.

https://personalfirewall.comodo.com/

Q&A / Discussion

Thank you for your attention!

E-MAIL: A.PETROVSKI@SHAREDEFENSE.ORG

WEB: WWW.SHARECONFERENCE.NET