# h6 Onion

## Hiding Behind the Keyboard: The Tor Browser € (Shaves & Bair 2016)

* Introduction:
  + The Onion Router A.K.A Tor is simply web browser, based on Firefox Internet browser
  + The browser’s idea is to hide user’s sessions etc. by browser modifications
  + Tor is easy to use for anyone without more complexity
  + Only viable internet connection is needed to use it
* History and Intended Use of The Onion Router:
  + Tor allows connections to websites which may be blocked by authorities
  + Ensures privacy between conversations
  + Tor browser gives possibilities to implement crimes with it
  + Initially developed by US government
  + Tor is not currently controlled by anyone, but anyone can improve and test it
* How The Onion Router Works:
  + Tor routes traffic through random relays and uses several layers to hide users’ internet traffic
  + Exit relay does not know where the traffic came from its initial phase
  + The idea of these several layers is to hide the origin of sender
  + Breaking Tor’s anonymity is almost impossible but not fully
  + Tor uses “bridges” to avoid service providers or governments to prohibit the traffic
    - Relays are publicly posted on the internet and prohibition of relays is possible, whereas bridges are not listed publicly
  + The most used anonymous browser
  + In case of countries which censuring is enabled more than usual browsing traffic may be slowed
  + Tor gives channel to criminals change information, files etc. without discover by law enforcement
  + IP addresses are also hided using Tor
  + Tor browser does not keep any browsing history data
    - Shutting down computer after browsing the data will be lost
  + Pretty much only few data are left behind of Tor usage, some cache data and empty files, but nothing from browsing
  + Anyhow, there might have been left some shadow files on a computer the usage of Tor which may reveal use of the tool
* Tracking Criminals Using TOR:
  + Governments are deanonymizing Tor by:
    - Finding criminals and terrorists
    - Prohibiting citizens to access internet
  + Changing Tor browser’s settings may reveal user or make the revealing easier
  + Allowing geolocation or allowing constantly updates and web requests may reveal Tor user’s real IP address
  + IP address is one of the most common way tracking Tor users

## Install [TOR browser](https://www.torproject.org/download/) and access TOR network (.onion addresses). (Explain in detail how you installed it, and how you got access to TOR).

Steps behind installation:

1. Open Linux virtual machine
2. Googling Tor browser website
3. Choosing the correct package to install (Linux version)
4. Extracting files into the VM’s temp folder
5. Launching Tor browsers installation file
6. Open the browser and check settings of it, among other things I check internet connection by the tool

## 

Figure 1. Tor browser

## Browse TOR network, find, take screenshots and comment

## 

Figure 2. Searhing Onion search engine

As warning text points out the connection must be changed to Onion Network to search anonymously

## Kuva, joka sisältää kohteen teksti Kuvaus luotu automaattisesti

Figure 3. Trying to find something to buy

## Kuva, joka sisältää kohteen teksti Kuvaus luotu automaattisesti

Figure 4. The marketplaces filtered

First try gives different kind of results to buy Bitcoins and directs to going to Deepweb and Darnet markets and many other suspicious sites.

## Kuva, joka sisältää kohteen teksti Kuvaus luotu automaattisesti

Figure 5. Tor browser & the marketplace

At first glance seems like there is quite much frauds. The figure 5 indicates that it’s possible buy real money from there.

## Kuva, joka sisältää kohteen teksti Kuvaus luotu automaattisesti

Figure 6. Potential Identity Leak

## 

Figure 7. Price list for social media account hacking services

## 

Figure 8. Forums

It was quite difficult to find any discussion forum or other that kind of sites which actually work and are not blocked. After a while of searching the first site opened was some darknet site.

## In your own words, how does anonymity work in TOR? (e.g. how does it use: public keys, encryption, what algorithms?)

Tor uses ephemeral encryption key with each relay in circuit. Tor’s authentication uses pubic decryption which is called ”onion key” to make “distributed trust” for users (torproject.org 2022). Tor uses different ciphers to hide its connections, for example, RSA and AES ciphers are used. Public keys and hash functions are used thought secret keys are not. Using these aforementioned algorithms and techniques Tor hides user activities and anonymity in its connections using multiple layers and secret channels to make users hidden.

## What kind of the threat models could TOR fit?

List of different threats that could be done using Tor:

* Terrorism
* drug dealing
* conspiracy
* spy
* fraud
* business espionage
* money laundering
* Spoofing

In general level any of the known cyber security threat model or tool could fit to solve issues and threats coming from Tor misuse.

A couple of tools to mention:

* OWASP
* Microsoft Security Development Lifecycle (SDL)
* Cairis
* IriusRisk
* SecuriCAD by Foreseeti

Using these tools is possible avoid uppers list Tor’s misused actions by modelling and designing companies cyber security. Also, other models than these tools could fit the case. Using Cyber Kill Chain, MITRE ATT&CK Framework or other equivalent frameworks could increase cyber security level.

## Sources:

Shaves & Bair, 2016, [Chapter 2. The Tor Browser | Hiding Behind the Keyboard (oreilly.com)](https://learning.oreilly.com/library/view/hiding-behind-the/9780128033524/XHTML/B9780128033401000021/B9780128033401000021.xhtml#s0055) Read: 2.12.2022

Torproject.org, 2022, <https://support.torproject.org/about/key-management/> Read: 3.12.2022