jamk.fi

Tor-Network

Essay

Mikael Romanov

Essay
Marraskuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), tieto- ja viestintätekniikan tutkinto-ohjelma
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisältö

1 Introduction

I wanted to do an essay about Tor network since there was an interesting news article about closing down the Finnish “sipulikanva” by Police and Customs: https://www.aamulehti.fi/uutiset/poliisi-ja-tulli-sulkivat-huumekaupasta-tunnetun-salaisen-keskustelupalstan-200502987/

It was especially interesting since, how and why would you consider to close such site when another pops up merely in days. I wanted to do research and read about the core concept of Tor and how it works. This is an essay about Tor network, what is it, how it works, why it works and who uses it and how to use it.

2 Tor (The onion router)

2.1 History

Tor concept was developed by U.S Navy computer scientists David Goldschlag & Michael G. Reed and mathematician Paul Syverson in the mid 1990’s. The reason for developing Tor was that digitalization brought information sharing over network and agencies realized the value of sharing information over network. So Tor was developed for secure communication over network. Tor was then developed further by Defense Advanced Research Projects Agency (DARPA) in 1997.

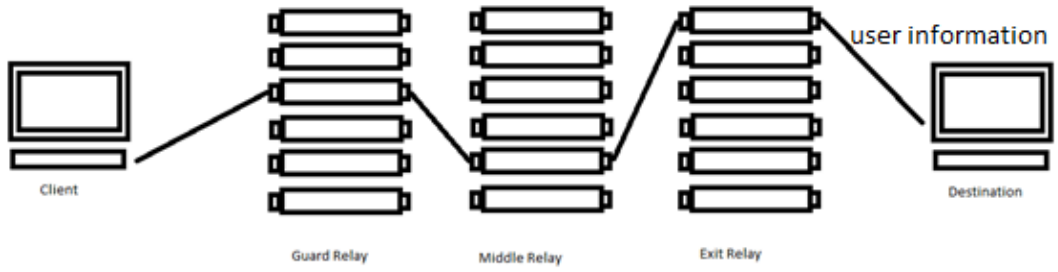
In 20. September 2002 alpha version of Tor was released by Paul Syverson, Nick Mathewson and Roger Dingledine as The Onion Routing Project which then continued and became **The Tor Project, Inc**.

2.2 What is Tor

Tor is an overlay network consisting of volunteer routers which allow people using Tor network to have better privacy and security. The Tor Project is a non profit organization which research and develop online “anonymity” and privacy. Tor is developed for the reason that organizations and governments couldn’t learn users browsing habits or location. The improved privacy and “anonymity” comes from encrypted

traffic and bouncing it through thousands volunteers relays which uses the volunteers bandwidth. Tor network can be reached by any device on the market (Win, Linux, Android, Apple) by downloading Tor Browser. It isn't recommended as an everyday browser, since there are trade-offs using it. Slower speed due to bouncing through volunteer relays and it is depended on the relays bandwidth, Flash and Quicktime plugins don't work. Also many may think that since Tor improves privacy and hides users IP-address it would be possible to download Torrents as an "anonyme", but Torrent applications ignore proxy settings and make direct connection through. Even if the application connects through Tor the application send a tracker GET request with your real IP-address and therefore so called "anonymity ends". It is also frowned upon to download Torrents via Tor since it slow the whole network speed for Tor users.

A side note, if the user uses the same computer and same ISP always while browsing via Tor, it isn't anymore "anonyme" or secure, since internet is built on trusted devices and thus is only a matter of used recourses to track the culprit or a mistake made while using Tor. A simple misconfiguration on the Tor browser itself or an user mistake. As an example the user buys something from Silk Road and uses his own credit card, real name and his home address.



2.3 How Tor works

Computer first connects with Tor Projects directory servers, which are trusted redundant servers that list all of the relays available in the Tor network. Tor proxy the downloads the information of available relays to use to build a circuit. First Tor proxy talks to someone on the Tor network and selects an entry relay(Guard relay). Once the guard relay is selected it will exchange TLS keys with the relay, once the keys are exchanged, connection eshtablished and secured it will build a circuit(Figure 1).

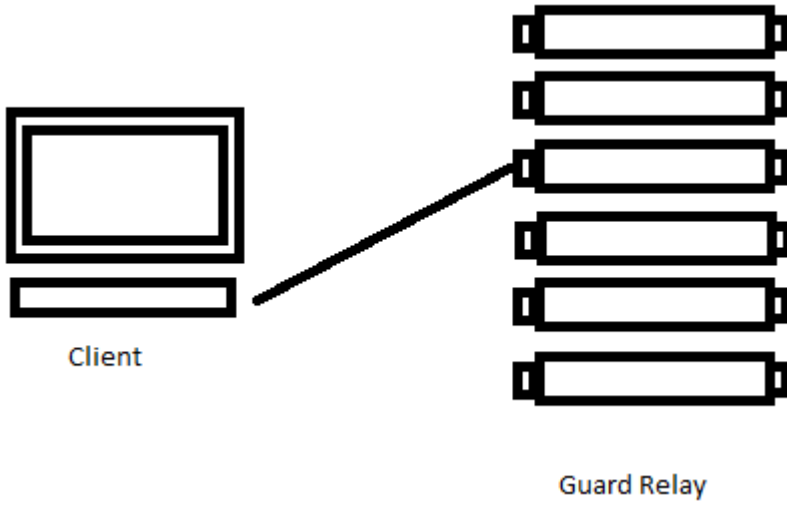


Figure 1 TLS exchange

After the Guard relay circuit has been established, the Tor proxy demands the Guard relay to extend its circuit to the middle relay (Figure 2)

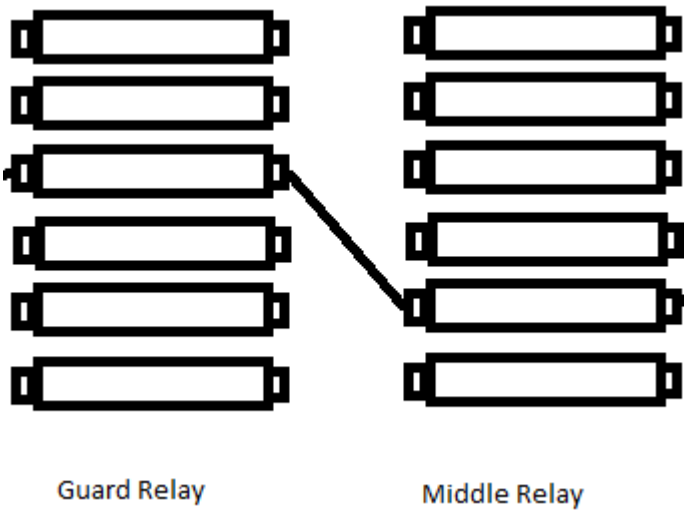


Figure 2 Guard to middle

The guard relay and the middle relay establishes also a TLS connection, then middle relay is instructed to extend to an exit relay and does the same thing as the as the above.(Figure 3)

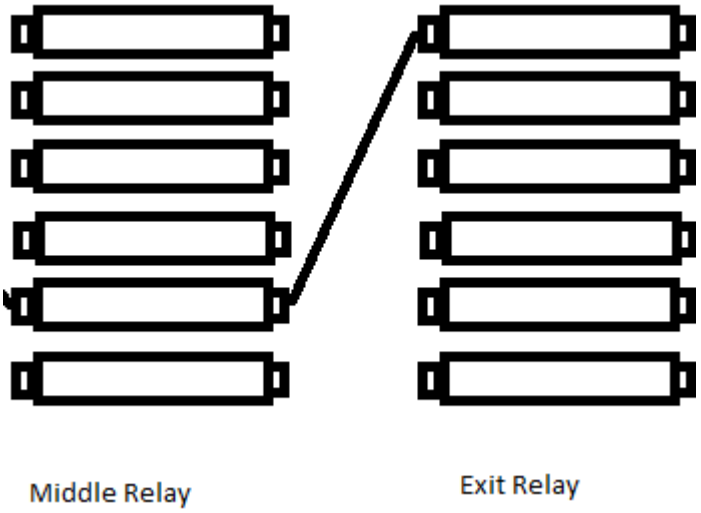


Figure 3 Middle exit circuit

The final product looks like this. The proxy send a request to get to some site, Guard relay unwraps one layer of encryption, send it to middle relay it unwraps one layer of encryption sends it to exit relay and exit relay unwraps once more and sees the wanted request and routes it. (Figure 4)

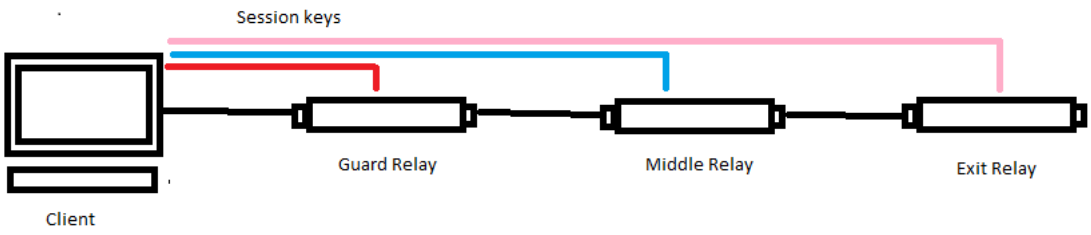


Figure 4 Final circuit complete

As it has said earlier many times, Tor bounces through relays. When using Tor the connection goes through 3 relays.(Guard, Middle, Exit)

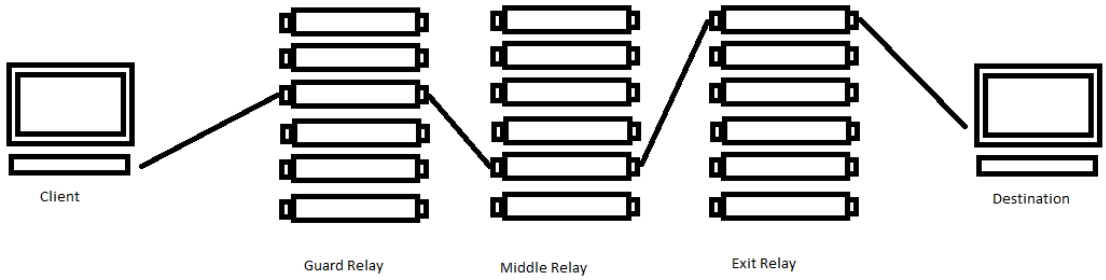


Figure 5 Relay bouncing

Guard Relay are entry point relays which are chosen to serve as guards and are relays that have been in use for a long time, stable and have high bandwidth. Middle relay is only the “middle man” and it is for transferring data from guard to exit relay, it prevents the Guard and Exit to know each other. Exit relay is the exit point where the traffic is routed to the destination.

2.4 Who uses Tor

It is divided into four different groups: normal people, bad people, people who are from countries where there is censorship and people who are concerned about cyberspying. Tor is a good proxy but if the case is that youtube or something else is blocked, its better to use another proxy. The usual scenario is that normal people use for hiding their identity while chatting in forums and searching something that your not supposed. But the biggest benefits of tor is for criminals that sell illegal substances, guns, children, credit cards, assassination and so on. There are plenty of different people to go around especially on the “dark side of the web” (Silk Road, TorDir) but there are also good sites like hackBB and hash party which are intended for black hat hackers, place to learn hacking.

2.5 How to use Tor

Tor proxy can be accessed by downloading Tor bundle from https://www.torproject.org/download/download-easy.html.en or by example making a bootable usb stick with Tails, so you can go anywhere and use Tor on the go.
https://tails.boum.org/

So if you decide to use Tor proxy; the Tor browser or Tails they are pretty much good to go right from the gecko. There are plenty of configurations that can make your browsing more private but the usability lower. There is on the privacy and security settings a slider, that has adjustment for HIGH, MEDIUM HIGH, MEDIUM LOW and LOW Security levels. When using Tor, it should be considered always using only HTTPS version of sites, creating new identity(getting a new IP-address once a while) also it should be noted that DON'T use Google, Yahoo, Bing, DuckduckGo as a search engine. Disconnect.me should be used as a private search engine https://disconnect.me/freeprotection . Don't use torrents, don't enable nor install plugins, don't open downloaded documents via Tor while being online and don't browse with any other browser same time.

3 Thinking

The concept of Tor makes me think that it is secure, but what if the computer using Tor has a virus or keylogger or such. The keylogger can literally send anything you type to a remote server. So spyware and malware are the biggest concerns while using Tor. The second concern is that if the server where you're trying to connect is infected or compromised and tries to read of information of you.

A high security concern is also on the exit relay, which sees the data. A hypothetical scenario but if somebody invests 2 million dollars a year example on router which are configured for exit relays with logging all the traffic and data that goes through.

A thing to consider when using Tor network is that it is possible to have DNS leakage which leads to DNS queries going out locally, even if the traffic is routed through Tor.

There is privacy but no anonymity on online.

4 Sources

https://www.pcworld.com/article/2686467/how-to-use-the-tor-browser-to-surf-the-web-anonymously.html

https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-and-why-do-people-use-it/#1ccd9f517d75

https://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/

https://www.torproject.org/

https://www.huffingtonpost.com/2013/07/18/tor-snowden_n_3610370.html

https://www.expressvpn.com/internet-privacy/tor/history/

https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/

https://en.wikipedia.org/wiki/Tor_(anonymity_network)