International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 08 | Aug - 2021 ISSN: 2582-3930

The Onion Router - Anonymity as a service

GANESHA HEGDE

Co Author – DR. SAMITHA KHAIYUM

Master of Computer Applications

Dayanand Sagar College of Engineering

Abstract

In this paper we are going to study about The Onion Router which is generally considered as the gateway to the Dark Web. Understanding the architecture of The Onion Router, working rules of The Onion Router, benefits of The Onion Router, What are all the basic requirements to use The Onion Router ,the general audience of The Onion Router and difference between The Onion Router and VPN.

.

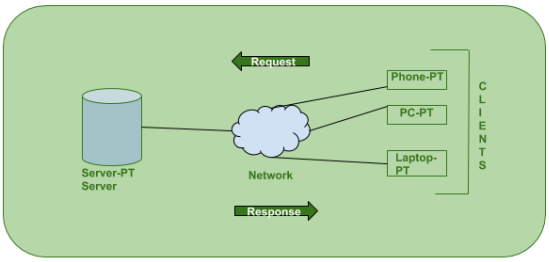
KEYWORDS:

Origin of Tor, Working of Tor, Dark Web ,Entry node, Exit node, Advantage of The Onion Router, Disadvantage of The Onion Router, Usage of The Onion Router.

INTRODUCTION

As we know, we all use the internet.Basically, the web may be a good way to connect with the worldwide population. Most folks use the web as a way to connect with people, sharing Info, sharing files, for entertainment and socializing purposes, and plenty of different things that would be useful to us. The most necessary use is that you just will get data and education from the net. It helps folks learn numerous things and other people get data that they implement in their daily life. But there is a problem with the way we use the

internet. It is easy to track users and their usage and use that information for evil purposes.

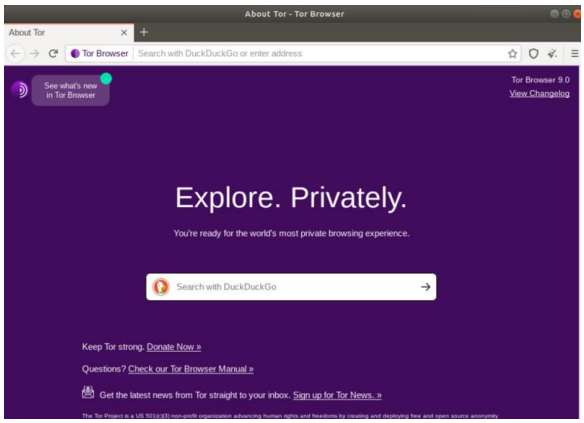


(fig. 1 - client server architecture)

The above diagram shows the workings of client-server architecture of the web. Here data packets are sent using any tcp/ip protocol between two nodes. The data packets consists of 3 parts -

1 Source IP Address
2 Actual Data
3 Destination IP Address

Although the actual data is encrypted, the IP address can be traced. This can be a golden opportunity for a hacker to fulfil their intentions.So to maintain anonymity we can consider using the **Tor** also known as **The Onion Router.**



(fig. 2 TOR browser window)

Origin of Tor

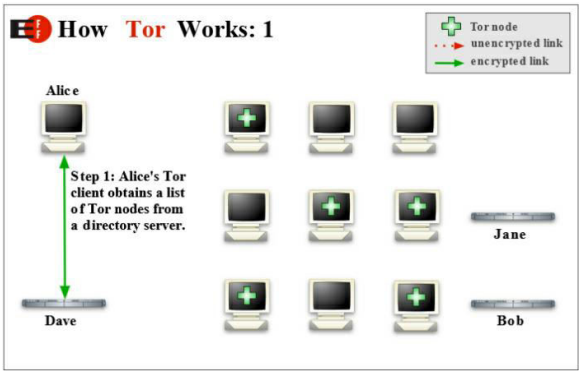
The Onion Router, typically known as Tor is a freeware and open-source offering for anonymous communication by leading web traffic through a free, worldwide, volunteer overlay network consisting of over seven thousand relays so as to hide a user's location and usage from anyone conducting network surveillance or traffic analysis.

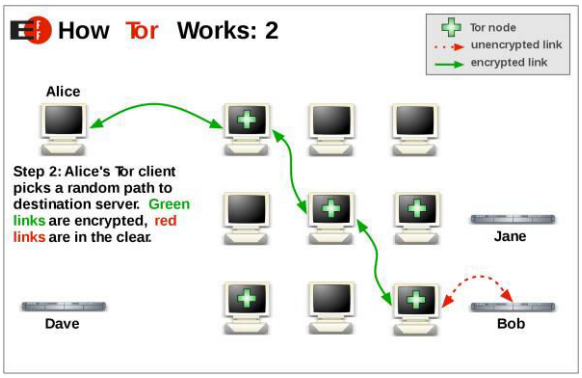
The U.S. Naval Research Lab staff members, mathematician Paul Syverson, and computer scientists Michael G. Reed and David Goldschlag developed the core concept of Tor in the 90s for shielding online communication channels of U.S. intelligence. It was further developed by The Defense Advanced Research Projects Agency in the year of 1997. The alpha version of Tor, developed by Syverson and computer scientists Roger Dingledine and Nick Mathewson so-known as The Onion Routing project (which later simply called "Tor", as an acronym for the previous name), launched on 20th September of 2002. A year later they released it for the general public.

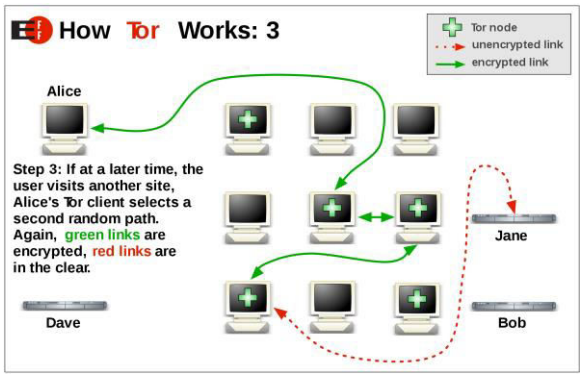
The Tor project may be a non-profit organization that conducts analysis and development into online privacy and obscurity. it's designed to prevent folks – as well as government agencies and companies – from learning your location or pursuit your browsing habits

Working of Tor

Tor Browser routes all of your network footprints inside of the network, making you anonymous. As the images below illustrate, it consists of a three-layer proxy, like layers of an onion. Tor Browser connects arbitrarily to one of the publicly listed entry nodes, bounces that traffic through a arbitrarily selected middle relay, and at last spits out your traffic through the third and final exit node.



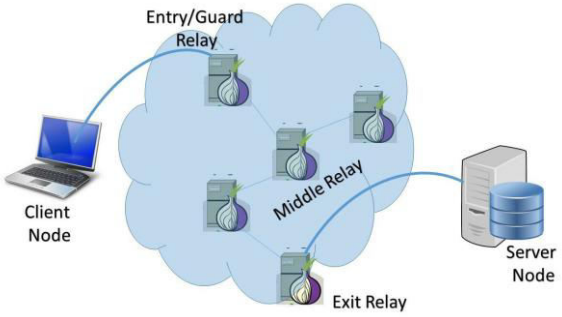




As a result, the service you are attempting to access might welcome the user in a foreign language. These service providers observe your IP address and guess the country and language, however, whilst the use of Tor, is going to often appear to be in a physical region halfway across the globe. Tor does not support UDP, rather it makes use of TCP/IP.

The Three Kind of nodes or relays in Tor are :

1. **Entry Node** : It is the entry point to the Network. Every client will first connect to the guard node meaning they will see the actual IP Address of the client who is trying to connect. The public listing of the Tor network guard nodes is updated almost every minute.
2. **Intermediate Node** : Also known as middle relays cover most parts of the Tor circuit in any given transmission. They consist of relays through which data is passed in an encrypted format and no node knows more than its predecessor and descendant.
3. **Exit Node:** It is the final relay in the Tor network. They are the nodes that send the data info to the destination and are usually thought of as the culprit because the Exit node is perceived as the origin IP Address.



Legal limitations of Tor

The Tor Browser is an application that is free to use. In some countries, however, using the Tor browser is prohibited by national authorities. China has criminalized the use of anonymity services and blocks Tor network traffic from transmitting through the nationwide Firewall. Countries which include Russia, Saudi Arabia, and Iran, are operating hard to prevent citizens from using Tor.It hides your identity but it doesn't mean it is untraceable. If somebody is taking part in such criminal activity and you're the exit relay, the traffic is going to be tracked to you. Governments also are terribly cautious of Tor users and keep an eye on them. Just by being a Tor user, you may be marked as a criminal and have all of your activities monitored.

Who uses Tor?

- **Journalists**: use Tor to shield their resource's identity and themselves whilst they may be following leads on-line.
- **Normal people:** folks who use Tor to keep their internet activities

hidden from websites and advertisers; those concerned about cyberspying; and users evading censorship in certain parts of the world.

- **Terrorists**: these men make use of Tor to mask their real identity from government agencies. They additionally use it to shop for weapons from black markets etc.

Tor additionally cites bloggers, business executives, IT specialists and law enforcement officials as key users when working undercover on-line, or investigating questionable web sites and offerings.

The Dark Web:

Since we are studying about Tor, let's also get acquainted with the Dark web as the majority of Tor users are using it to surf the dark web.

The World Wide Web (also known as WWW OR W3) can be divided into 3 parts:

1 **Surface web** : is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines.

2 **Deep web** : It is a part of the World Wide Web whose contents are not indexed by standard web search-engines. The content of the deep web can be located and accessed by a direct URL or IP address, but may require a password or other security access to get past public-website pages.

3 **Dark web** : The dark web is the World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access.The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

The dark web has flourished due to bitcoin, the cryptocurrency that allows two parties to conduct a trusted transaction while not knowing every other's identity. Nearly all dark web commerce sites conduct transactions in bitcoin or some variant, however, that doesn't mean it's safe to carry out business there.

Advantages of Tor

- **Free of Cost** : The Tor browser is free to download and use.As it is an open source project a person with a good grasp of knowledge of technology can download the project source code and make changes to the code as they would like.

- **Multi-layer encryption :** In the Tor network, your traffic is redirected and encrypted several times to stay totally anonymous.

- **Hides your online activity :** Your browsing history and cookies are automatically reset after each use.

- **Anti-spy protection** : Tor forbids hackers from tracking the websites you visit.

- **Anonymous identity** : Tor tries to make all users look-alike to prevent anyone from identifying you by the characteristics of your browser or devices.

- **Focus on privacy** : The main idea behind Tor is privacy and anonymity as it masks the user's IP Address and does not reveal it to anybody. Anyone from journalists and political rebels to your average user can use this platform to keep their information safe from repressive governments or big corporations.

- **Familiar UI** : The Tor browser is similar to most browsers you've used before. It's accessible to many people and is user-friendly, making it easy to use.

Disadvantages of Tor

- **Slow speed** : Since traffic goes through a lot of relays, there is usually a delay in content. Photos and videos have hassle loading.

- **Service ristriction:** Many larger internet offerings block access to Tor. When visited, these sites display an error message. Others allow access but with some annoyance.

- **Legal issues** : If someone's internet activity is found to be illegal and you are the exit relay, then the traffic will be traced back to you. Governments are very cautious of Tor users and are frequently monitored. Just by being a Tor user, you may be marked as a criminal and have all of your activities monitored

VPN : Tor alternative

While both Tor and VPNs work to mask your online identity, VPNs offer maximum security if used right. Tor Browser is a freeware that will encrypt all your requests, but it's slow, doesn't have access to all websites and you might face legal issues. Meanwhile, VPNs are fast, encrypt all your internet footprint, give you access to any Internet site and put you in control of your intended geographical region.

Mainly Tor uses multiple nodes to protect your identity and the nodes are selected at random, there are at least 3 nodes in the network. VPN uses only 2 nodes and the IP Address of the source is hidden. Also no random nodes are selected for connection.

How to use Tor?

Tor browser can be downloaded from the website www.torproject.org and it is available for almost all platforms such as Microsoft Windows , OS X , LInux, Android and you can also download the source code and compile for your system.
Using Tor is pretty simple and it is well documented.
Alternatively you can use it from your Firefox web browser as the browser supports it.

Using Tor and VPN together might give you extra privacy.

Conclusion

Personal security and privacy are turning more and more necessary as governments, hackers, and even our favorite search engine Google bring even more advanced methods to interrupt our anonymity and track our behavior.
One may use Tor for hiding their identity but their identity can still be traced. We are at an age of rapid evolution in science and technology but ethical/moral implications are ambiguous with the advancement of technology. Tor is an open-source and free software program that is used to encrypt one's online activity, however, it is slower, does not give access to any or all websites, and might probably cause issues with the law.
Though Tor is probably going to charm more sophisticated net users, public concern over government and corporate surveillance and monitoring is probably going to mean it becomes widely used by mainstream internet users. Security specialist Bruce Schneier lately made anonymization tools such as Tor the first step in his advice on "how to remain secure against the NSA". But this kind of technology will not survive in the future, as the attempts to crack it get smarter and more persistent.

REFERENCES

1 What is Tor? A beginner's guide to the privacy tool [https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser]
2 Tor Documentation and Blog[https://www.torproject.org]
3 Using Tor vs. VPN for Anonymous Browsing [https://clario.co/blog/tor-vs-vpn-comparison/#:~:text=The%20key%20difference%20between%20Tor,provide%20a%20secure%20VPN%20tunnel.]
4 Wikipedia [https://en.wikipedia.org/wiki/]
5 How to Access the Dark Web: Guide to Browsing Dark Web using TOR Browser [https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/#:~:text=Despite%20its%20current%20usage%20as,safeguard%20U.S.%20Intelligence%20online%20communication.&text=TOR%20is%20a%20version%20of,to%20browse%20the%20web%20anonymously.]