International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Comparison of Anonymous Communication Networks-Tor, I2P, Freenet

Neelam Negi

MCA Department, Veermata Jijabai Technological Institute, Matunga, Mumbai

---

Abstract - *In the past few years, revelations made my some secret organizations around the world has given rise to an interest in anonymous communication in order to protect the identity of the users and encourage freedom of speech. In order to provide such online anonymity, several software and platforms have emerged in the recent years. These software/platforms enable their users to protect their identity. In this paper, I shall give a brief overview of three well known anonymous networks – Tor, I2P and Freenet, mention their strengths and weaknesses and finally provide a comparison of the three networks.*

Key Words: **Anonymity, Freenet, I2P, Tor, freesites, Darknet**

1. INTRODUCTION

The tremendous advancements in technology in past few decades has given rise to the concern of communication privacy. Reasons for protecting the identity while communicating may differ from one user to other. An individual may want to remain anonymous while performing confidential activities or business transactions. Privacy is of highest value to certain individuals who do not wish to make their activities known to others.

Although encryption mechanisms are one way to secure communication, there might still be certain aspects of communication that are at a risk of exposure such as IP addresses of communication parties. Exposure of IP addresses of individuals may result in severe consequences. An intruder can easily overhear and analyse the communication packets passed and use techniques such as traffic analysis to uncover a number of aspects of the ongoing communication, thereby proving to be a potential threat to an individual's privacy.

In order to overcome all these issues, several techniques/software have been developed, that provide anonymous and safe communication over the internet. The Onion Router (Tor) Project is one such solution to the growing needs of anonymity in communications. Tor was one of the first known solutions to this problem. Overtime, Tor came up some limitations as it was based on a centralized system. To overcome its challenges, one more project emerged known as the Invisible Internet Project (I2P) with an aim of providing even better security and anonymity. One more system called Freenet emerged with the aim of providing distributed, Internet-wide, peer-to-peer overly network that provided platform for censorship-resistant communication and publishing.

2.1 THE ONION ROUTER (TOR)

The Tor network is a platform for enabling anonymous communication. The basic idea on which Tor operates is routing the traffic across an overlay network of routers that operate globally, and are volunteer operated and managed. This routing involves more than over seven thousand relays primarily focused at concealing the user's identity, location and usage pattern. This makes the user less vulnerable to any one observing the network or performing traffic analysis.

A major issue with the public internet is that anyone observing the network can analyze the network and know a great deal of information about the user's activity on the internet, data being transferred, sites visited, etc. Even if the data is encrypted, a lot can be determined from analyzing the network traffic itself. Tor aims to eliminate this problem by directing this network traffic through a network of routers so that your transactions are distributed across various sources in the network and the communication can't be traced back to any single point in the network.

The group of connected routers form a circuit of encrypted connections through relays on the Tor network. No individual resource on this relay path knows the complete path around the circuit or the identity and location of other participants in the circuit. The sender / receiver is allowed only a single hop around this circuit, as a result of which no eavesdropper can use traffic analysis or any other method to track any of the participating resource. Ideally, one such circuit is kept alive for a duration of ten minutes after which the upcoming requests are provided a new circuit.

2.2 THE INVISIBLE INTERNET PROJECT

I2P is also an anonymous communication and overlay network that enables its users to send and receive messages anonymously. I2P is very similar to Tor in terms of features such as providing anonymous access to online content, peer-to-peer routing and multi layered end-to-end data encryption. However, the primary focus of I2P is to create a network within the internet.I2P communication mechanism heavily relies on packet-based routing. Every user in the relay network has two associated "tunnels"- inbound and outbound. A "tunnel" is a sequence of peers that route messages in one direction. A user intending to send a

message passes the message through an outbound tunnel while incoming messages will be received via the inbound tunnel. A user can determine the length of these tunnels, thus making the choice between levels of anonymity and latency.

2.3 FREENET

Freenet is a software platform that enables the users to anonymously browse, share and publish content as well as websites called "freesites". The inspiration behind Freenet was to build a censorship resistant communication network.

Freenet also follows mechanisms used by I2P and Tor whereby communication between nodes are encrypted and routed through other nodes to make it difficult to track down the participating resources and the content being communicated.

Every Freenet user is required to contribute to the network by giving bandwidth and a portion of their hard – drive for the data store. This portion is used to store files, however the user cannot discover the content of those files as they are encrypted. Hence, no user actually knows what's in his data store and hopefully, cannot be held accountable for it. One interesting feature of Freenet is its ability to store only the popular content. Files are automatically kept or discarded depending upon how popular they are. This causes the least popular content to be automatically discarded thus making space for new or popular content.

3. CONCLUSIONS

Tor and I2P are similar in the sense that they both provide anonymous proxy networks whereas freenet is a more of a distributed datastore with provisions of applications built on top of it to enable even more generic and anonymous communication. All of them provide features that help users get anonymity. Here are the observations made comparing various aspects of the functionality provided by each of the three:

Anonymity

Anonymity, being a qualitative measure is difficult to be compared. All the three networks viz. Tor, 12P and Freenet provide fundamentally different functionalities and have their own levels of anonymity.

The Tor Project provides the Tor browser that functions using a network of encrypted tunnels to and between Tor routers. These routers are randomly selected and form a circuit, where no router has any information about anything other than its preceding and successive connections. The Tor browser also has many other inbuilt features that enhance its privacy and security settings such as always-on private browsing feature, restriction of third party cookies, disabling recording of browser history or website data, etc. All these make Tor reasonably anonymous and safe for its users to communicate.

I2P on the other hand, does not come with a browser but has to be manually installed using the RP installer. Nevertheless, l2P also encrypts its data in multiple layers [in total four layers of encryption) and even the end nodes are cryptographic identifiers., so that none of the recipients of the message reveal their lP addresses to third party observers. While Tor's basic intent is to enable its users reach the internet anonymously, l2P focusses on creating its own interact. Hence, the 12P network isn't accessible from a regular computer. After installing the RP software, the computer can join the DP network and act as a router, to start routing the traffic. Thus, this creates a dynamic and decentralized network, which makes it difficult to figure out what is being communicated at each router. Thus, it is safe to assume that 12P does provide a good deal of anonymity.

Free-net stands out completely among the three of these networks being compared. Unlike the two other networks, Freenet is not a proxy service but a highly decentralized peer-to-peer platform. Where I2P and Tor use routers for message communication. Freenet works on the principle of storing encrypted parts of data on every user's hard drive without actually knowing the entire content of it. It has been entirely decentralized in order to reduce the vulnerability to attacks. A user using the Freenet can actually decide which users they want to connect to. Freenet also has a provision of a "dark net" mode. in which a user can decide to connect only to his / her friends;

Speed

The bandwidth utilization of Tor is the least amongst the three. However, when it comes to latency. 12P is slightly better. Freenet loses in both these aspects as every user has to contribute bandwidth that it uses in order to route mesh: across the network. The request is routed across many nodes and as a result, the bandwidth consumption is relatively higher compared to other systems.

Darknet Sites

Again, this a subjective Issue. In case of static content, Freenet stands a clear winner because of its ability to hold content even after a user is offline or has stopped using the platform. Otherwise, I2P is something to look for because of the vast range of hidden services it has to offer such as torrent trackers, iMule [emule client for l2P) and many eepsites.

Popularity

This can be stated undoubtedly that Tor is so far the most popular platform with huge community support, user base

and larger funding. However, this does not mean that I2P and Freenet are less useful. The prime reason for the popularity of Tor is its ease of use as well as reliable anonymous access to the public internet where as l2P creates its own internet, and is also not the easiest platform to learn and use. Same applies to Freenet, it takes a while before you get adapted to its functionality, and even when you do, the platform only promotes storage of a file/content until it stays popular.

Content

The content of the three platforms differs widely due to the difference in their primary objectives. As Tor was designed to ease access to regular internet while being anonymous, the content of Tor is the content of the entire internet. Tor also provides some hidden services.

I2P focusses more on creating its own network within the internet, it has much more hidden services to offer compared to Tor and has more "file sharing" type of content. Freenet boasts of a lot more static content and can hold data even after the publisher is offline or has stopped using the platform. Any content can be held by Freenet as long as it stays popular.

Usage

Though all of these networks provide a good deal of anonymity to the users, the choice of using either of them totally depends on the user, it depends on factors such as what you are using it for, what level of security you desire and who do you want to be anonymous from. Tor is a great option if one intents to surf the internet without exposing their activity on the network. It provides good level of anonymity to users while browsing the regular internet.

However, if hidden services and dark sites are considered, I2P is the one to be considered. I2P undoubtedly provides a lot more darknet services while providing good deal of anonymity. Freenet is something one can use to access static content and when one is highly cautious of not being exposed to strangers. The darknet mode is extremely useful where a user can connect to only people they trust.

Community Support and Related Work

Tor being the most popular network among the three has the largest amount of funding and user base. There are a ton of research papers on Tor and related work on it. I2P also has good documentation on its official website but has relatively less research performed by users. Freenet overall is the least famous among all considering the amount of related work found on it.

On a concluding note, it can be safely stated that no anonymity network is entirely "perfect" and can be assumed to capable of doing everything. If one desires effective anonymity, the best way is to learn to use and adapt to more than just one tool. Every network has their distinct features and respective usages. Though Tor and l2P provide anonymity by protecting the transport of data and routing through a series of nodes, it does not guarantee protection against timing attacks. The user has to act smart while using any of the anonymizing tools. A few smart habits should be inculcated such as refraining to provide your name or any other revealing information while browsing the internet. Be active on the internet during time intervals when you know there will be generally a higher number of users active.

Anonymity networks right now still have a long way to go. As far as the three of these networks are concerned, after analyzing all their features, functionality, efficiency and limitations, I would suggest of use not just one of them but a combination of all the three.

REFERENCES

[1] Tianbo Lu, Zhimin Lin, Lingling Zhao, Yang Li, On Privacy and Anonymity in Freenet System, International Journal of Security and Its Applications, Vol. 10, No. 5 (2016) pp.41-56.

[2] Afzaal Ali, Maria Khan, Muhammad Saddique, Umar Pirzada, Muhammad Zohaib, Imran Ahmad, Narayan Debnath., TOR vs I2P: A Comparative Study , Cecos University of Information Technology and Emerging Sciences, Peshawar, Pakistan,

[3] Gildas Nya Tchabe and Yinhua Xu, Anonymous Communications : A survey on I2P Technische

University of Darmstadt, Theoretische Informatik ,Kryptographie and Computeralgebra Cryptography, Privacy and Security Karolinenplatz 5, 64289 Darmstadt, Germany

[4] What is Freenet? (2017, April 17), Retrieved from https://freenetproject.org/pages/about.html

[5] The Invisible Internet Project (I2P) (2017, April 17), Retrieved from https://www.torproject.org/index.html.en

[6] Tor (2017, April 17), Retrieved from

https://geti2p.net/en/about/intro