Tor network: Architecture, Anonymity and Hidden Services

Mohammed Hamza Javed

***Abstract* - Developed by US Navy employees, Tor networks use advanced encryption techniques and routing to protect their users and serve as the basis for online anonymity. While some may view this as necessary in order to protect their freedom of speech and expression, others may see it as ethically concerning and reckless, due to the illegal activities that could take place. Furthermore, although Tor networks are stated to keep online traffic private and hidden, certain security issues exist that stand to contest this claim. As the concerns for 'the dark web' grow, in this essay I will deconstruct how Tor networks operate, the methods they employ to keep users anonymous and an evaluation of their use in the modern world.**

***Index Terms*—tor, dark web, networks, anonymity, routing, hidden services**

I. Introduction

Tor networks are networks designed for the sole purpose of privacy and anonymity. Through the use of nodes (i.e. routers), a web request can be made that is entirely encrypted, with third parties being unable to identify where the request has originated from or where its final destination is.

Developed in the 1990s, Tor (also known as The Onion Router) was created by Paul Syverson, Michael Reed and David Goldschlag, who were employees of US Naval Research Laboratories. Their goal was to protect private US Government communications and the identities of US Navy agents [1]. In September 2002, however, Tor became publicly available. The idea behind this was to hide US Navy agents in plain sight; if they blend in with the public, they are more difficult to spot. Because Tor is a non-profit which relies partly on government funding to stay active, many people do not have trust in it as they believe that this allows the government to track individuals using the network, despite the concept of onion routing (which will be explained in more depth in section 3).

II. Background

Tor is used to hide a person's online and network activity, their identity, geographical location, as well as the websites that they have visited. This is done by encrypting a web request as it leaves the client's machine and bouncing it around through different nodes, until it reaches a web server that directs it to its destination. As a result, common users of Tor networks include:

- Political activists
- Victims of crime
- Whistleblowers
- Those wanting to hide from aggressive advertising
- Those wanting to hide from the government
- Those wanting privacy, in general

The ability to go untraced online is very important to users of a Tor network as their online activity, or the secrets they reveal, could lead them to prosecution, or in some very serious cases, death.

Not all uses of online anonymity are for noble purposes, however. The misuse of Tor networks allows for malicious activity, such as child abuse, sale of illegal substances, distribution of malware and more [2]. The same concepts that protect those with noble intentions also protects those with malicious intentions, otherwise Tor networks would not be used as a safe space for anonymity. This has sparked many debates about whether protection from criminal activities is more important than anonymity.

Those in favour of Tor networks demand that their online activity should be untraceable as they have strong beliefs in their rights to freedom and privacy. If these were to be impacted, they would have no place to speak their mind without fear of prosecution. Many of these people have a deep mistrust of the government and authority figures and as such require a space where they can be confident that they won't be silenced. On the other hand, those opposed to Tor networks believe that anonymity can lead to irresponsibility and unaccountability for one's actions. Having no trace of a person's activities means that they can participate in illegal activities without facing justice for it. As well as this, online anonymity can cause people to behave in ways that they would not, if their name was attached to their actions. This could include bullying and spreading hate, illegal threats and even fraud [3].

While Tor networks, in the past, have been used for malicious activities, I think it is important to keep in mind the safe space that they provide to those wanting to use their online anonymity for good. From journalists wanting to report on oppressive regimes within their country to victims of a crime seeking justice, without having their identity revealed, you often can't have the good without the bad. As a result, if there

was a possibility for Tor to disband the illegal communities that use their network, it would be a good start, but since the anonymity that protects them also protects those with just intentions, this would be impossible without intervention, which no party would want.

III. Architecture

A. Onion Routing

Anonymity differs from confidentiality. Confidentiality, which is usually associated with encryption, hides a message so that if it is intercepted, a third party cannot read it [17]. This is prominent in TLS certificates and HTTPS. Anonymity, on the other hand, hides the sender so that a third party will not know that a message has been sent at all! This is where onion routing comes in. As mentioned before, Tor networks work through the use of onion routing. This is a technique that uses multiple layers of encryption in order to hide where a request is being sent from and where its destination is, making it critical for online anonymity.

Tor networks consist of three main parts in order to work: a client, a server and multiple nodes (also known as relays or routers). There can be hundreds of nodes for a request to bounce around, but for the sake of simplicity, we will look at three in the following example. When the client makes a web request, the request is encased in three layers of encryption by the client's public keys before being sent to a node. This is done as a failsafe so that if one layer of encryption fails (which is unlikely), there are still two other layers that can protect the data [18]. The request is passed to the first node, called the entry guard, which decrypts the first layer of encryption using its private key, before passing the request to the middle relay. Like before, the middle relay decrypts the second layer of encryption, realizes that the message is still encrypted and passes the request to the exit node. The exit node peels off the last encryption layer, reads the request and sends it to the web server, which redirects it to its destination [4].

The client machine and nodes work together by having corresponding public and private key pairs. These are what are used to encrypt the request before it is sent and to decrypt them when they enter the respective node. Any third party that attempts to intercept the request after it has been encrypted will not be able to read its contents as they will not have access to the private keys [5]. This exchange where two different keys are required is known as asymmetric cryptography and forms the basis of online privacy.

The nodes in a Tor network are what are used to obfuscate the name and location of the sender and the device they are trying to communicate with. To ensure maximum security of the data being sent, all nodes are only authorized to know the minimum amount of information to send the data to the next node in the circuit [19]. In this way, no single node can read the sender IP address and the destination. Similarly, nodes do not know the full path of data or their role in the circuit, i.e. if they are the entry guard, middle relay or exit node [6].

B. Tor vs VPN

When a request reaches the exit node, the final layer of encryption is stripped away so that its contents can be read and passed along to the destination. The request and the client's identity are at the most risk at this point, since there is no more protection surrounding the request, and no encryption between the exit node and the destination. If an attacker controlled both the entry guard and exit node, they could use this opportunity to sniff for network traffic at this exact point and deanonymize the client, removing the entire purpose of Tor networks.

In order for maximum security and privacy, Tor can be used alongside a VPN. A VPN is a Virtual Private Network that is also built for privacy, however it does not use onion routing as Tor does. They are encrypted and can be used to cover the areas in a Tor network that are particularly vulnerable, such as the path from the client to the entry guard, and the path from the exit node to the server. As well as this, through the use of a VPN, the entry guard will become less exploitable as it will only be able to see the VPN's IP address rather than the client's actual IP address [7].

However, there are some downsides to using a VPN alongside Tor. One of which is that any data that is passed through the VPN will be routed through its network and servers, and so a user must ask themselves if they can trust that the VPN provider does not keep track of their activity [20]. Even through the use of Tor, a VPN will be able to view a user's identity, location and visited websites if it is not configured accurately, and therefore, it is recommended by Tor that the user does not use a VPN if they do not know how to set it up correctly.

In my opinion, as long as they understand how to configure it correctly, a user wanting complete anonymity online should use Tor alongside a VPN. This is because many VPN providers, such as ExpressVPN, have been independently scrutinized to prove that they do not keep logs of user data and activity, as well as having no legal obligation to hand over information to authority figures [8]. As well as this, the ability to access online resources through the VPN's IP address (rather than the client's IP address) ensures that attackers will not be able to sniff private information that could lead to them discovering the client's identity. All of these points add an extra layer of protection to the client's data, proving that using Tor over VPN is the way for complete online privacy.

IV. Anonymity

The purpose of Tor is to provide total anonymity and to prevent others from exposing personal information. Some reasons as to why someone could want online anonymity include:

- Freedom to express their views
- Freedom from societal pressures
- To remain untraceable by the government
- To protect themselves and their personal safety
- To prevent data miners collecting their information [9]

These are all reasons for someone to use the Tor network, and if they do so, they expect to remain hidden. Tor employs many techniques to keep their users protected such as onion routing, use of asymmetric cryptography and scrambling of web requests [21]. However, it also offers its own web browser as a user friendly implementation of the network.

As a modified version of Mozilla Firefox, the Tor browser allows for easy accessibility and aims to resolve privacy and security issues that are present in many other common browsers, such as disabling plugins that can leak the client's IP address. Many common browsers allow downloadable extensions that can be untrustworthy and lax in their dealing with security, and as such, these risks are prevented in the Tor browser.

Another useful feature is the incremental changing of Tor's circuit of nodes. This is done so that there is more difficulty for an attacker to trace the path of traffic. Without this, an attacker could constantly sniff an exit node and use this to determine where a client's requests are going.

The Tor browser also strongly encourages the use of websites with TLS Certificates (i.e. HTTPS websites) as these websites encrypt the data that they send back and forth between client and server. Through a TLS Certificate, the server can verify that the data has not been tampered with and can be trusted to be secure.

Finally, Tor browsers allow the use of exit node bridges to help anonymize those who live under a government that is actively blocking access to Tor. These bridges are nodes with a slightly different configuration that are not listed on the public Tor directory. As a government can't block all bridges, their use allows clients to access the network without the risk of being exposed [10].

While there are many advantages of using Tor networks for privacy, there are some downsides too. For example, Tor lends itself easily to end-to-end traffic correlation attacks [22]. These are attacks where, instead of attempting to decrypt the data sent through the network, the attacker looks for patterns in the traffic that match the incoming and outgoing data that is sent. By looking at the size of the data or the time that the data was sent, the attacker can make a prediction for when it will be received by the exit node, and using this information, can attempt to deanonymize the client. Since the exit node decrypts the data, it can be sniffed by the attacker to get a clear view of the contents within [11].

As well as this, while Tor is not illegal to use, it can make the government suspicious as they might think that a client has something to hide. Those with security concerns could be at risk as the government could set a specific surveillance on them, restricting their ability to use the network freely.

After thorough research, it seems as though the security measures that the Tor network takes is proactive in ensuring that users can remain anonymous whilst using it. By using the specially made Tor browser, users can eliminate the risk of identity exposure through the extra features provided, such as disabling insecure plugins and changing the node circuit constantly. Although the unsolvable issue of Tor's lack of end-to-end encryption persists, users can mitigate this by ensuring that they use websites with the HTTPS protocol, as well as using a VPN to remain protected from attackers.

V. Onion Services

Originally called 'hidden services', websites that are exclusive to Tor networks and have a top level domain of '.onion' are now called onion services [23]. These are websites that are made anonymously and can only be accessed via a link provided from the website's host [12]. Onion services are private servers that allow two-way anonymity. This is where the server does not know the IP address of the client, and the client does not know the IP address of the server [13]. Because of this, there is no risk of a Distributed Denial of Service or Man in the Middle attack as the attacker will not know the IP address of the client, and therefore cannot cause them any harm.

An onion service is set up to provide complete privacy and no risk of interception of data. The server will pick three nodes at random to become introduction points for the service and will store the nodes' IP addresses, as well as the server's public key within a 'hidden service descriptor'. The descriptor is then kept within a distributed hash table. When a client searches for the service using the .onion top level domain, they connect to the distributed hash table and receive the node IP addresses and the public key [14]. From there, the client chooses a node to be a rendezvous point, which it encrypts with the server's public key and sends a message to one of the introduction points, asking it to forward the rendezvous point to the server. Once the server receives the message, it decrypts it with its private key and sends another message to the rendezvous point. From here, the onion service has been correctly configured between server and client and they can continue to communicate via the rendezvous point, without knowing each other's IP address. Since it takes three hops from both sides to reach the rendezvous point, in total, it takes six hops for a message to be relayed to both the client and server [15].

VI. Discussion

It is clear that Tor networks have a strong aim to ensure that those who require online anonymity are provided with it. I think that, while there are some downsides of using Tor, overall, there are more positives associated with its use. In the modern world, it is very common and even accepted that most online websites will attempt to steal our data and sell it for their own personal gain, as well as whistleblowers being silenced for leaking enlightening information. Furthermore, dictatorial governments rule with an iron fist and ban any forms of criticism and revelation of topics that they want to keep buried. The users of Tor networks are those who require a safe haven to express their feelings and correct these injustices that are carried out, without the fear of identity exposure or prosecution.

As such, the media paints a picture of Tor networks being used only for wrong, and while there are some issues that stem from anonymity, news articles use these to detract from the good that comes from Tor networks. The overuse of the term, 'the dark web' has led to fearmongering of Tor networks, despite the term simply referring to an anonymous, "hidden collective of sites" [16]. Whilst it would be wrong to not acknowledge that Tor networks can lead to criminal activities, these things, while unjustifiable, are to be expected when it comes to online anonymity. However, I believe the freedom to make these choices is more important to have, than to lose.

The fear of Tor networks stems from the lack of knowledge surrounding them. Going forward, I think it is critical that the public perception of Tor is reevaluated so that those who require the anonymity it provides are able to use it justly.

BIBLIOGRAPHY

[1] Deakin University, "What Lies inside the dark web?," this., 12-Sep-2017. [Online]. Available: https://this.deakin.edu.au/the-dark-web. [Accessed: 27-Oct-2022].

[2] E. Jardine, A. M. Lindner, and G. Owenson, "The potential harms of the Tor anonymity network cluster disproportionately in free countries," Proceedings of the National Academy of Sciences, vol. 117, no. 50, pp. 31716–31721, Nov. 2020.

[3] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.

[4] J. Palme and M. Berglund, "Anonymity on the Internet," People.dsv, 12-Apr-2022. [Online]. Available: https://people.dsv.su.se/jpalme/society/anonymity. [Accessed: 27-Oct-2022].

[5] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," 2005 IEEE Symposium on Security and Privacy (Samp;P'05), 2005.

[6] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[7] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and Onion Routing," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482–494, 1998.

[8] R. Jansen, K. Bauer, N. Hopper, and R. Dingledine, "Methodically Modelling the Tor Network," USENIX, 2012.[Online].Available: https://www.usenix.org/system/files/conference/cset12/cset12-final12.pdf. [Accessed: 28-Oct-2022].

[9] E. Ramadhani, "Anonymity communication VPN and Tor: A Comparative Study," Journal of Physics: Conference Series, vol. 983, p. 012060, 2018.

[10] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[11] Johansen, "How to Use Tor Browser Safely in 2022: A Beginner's Guide," VPNMentor, 2022. [Online]. Available: https://www.vpnmentor.com/blog/tor-browser- work-relate-using-vpn/. [Accessed: 28-Oct-2022].

[12] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.

[13] R. Kang, S. Brown, and S. Kiesler, "Why do people seek anonymity on the internet?," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Apr. 2013.

[14] Tor Project, "What is a bridge?," Tor Project: Support. [Online]. Available: https://support.torproject.org/censorship/censorship-7/. [Accessed: 29-Oct-2022].

[15] Y. Zhu, X. Fu, B. Gramham, R. Bettati, and W. Zhao, Correlation-Based Traffic Analysis Attacks on Anonymity Networks, Jul. 2010.

[16] Tor Project, "How do Onion Services work?," Tor Project — How do Onion Services work? [Online]. Available: https://community.torproject.org/onion- services/overview/. [Accessed: 31-Oct-2022].

[17] M. Lefoane, I. Ghafir, S. Kabir, I. Awan, "Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks", IEEE Transactions on Industrial Informatics, 2023.

[18] K. Rankin, "Tor Hidden Services," Linux Journal, 23-May-2018. [Online]. Available: https://www.linuxjournal.com/content/tor-hidden- services. [Accessed: 30-Oct-2022].

[19] P. Winter, A. Edmundson, L. M. Roberts, A. Dutkowska- Zuk, M. Chetty, and N. Feamster, in How Do Tor Users Interact With Onion Services?, Baltimore, MD: USENIX, 2018, pp. 411–427.

[20] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Usenix Association, 2004. [Online]. Available: https://svn- archive.torproject.org/svn/projects/design-paper/tor-design.pdf. [Accessed: 30-Oct-2022].

[21] Kaspersky, "What is the deep and dark web?," www.kaspersky.com, 2019. [Online]. Available: https://www.kaspersky.com/resource-center/threats/deep- web. [Accessed: 31-Oct-2022].

[22] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[23] M. Yazdi, S. Kabir, M. Kumar, I. Ghafir, F. Islam, "Reliability Analysis of Process Systems Using Intuitionistic Fuzzy Set Theory". In: Garg, H. (eds) Advances in Reliability, Failure and Risk Analysis. Industrial and Applied Mathematics. Springer, Singapore, 2023.