The Onion Router and the Darkweb

Corianna Jacoby Mentor: Ming Chow

December 15, 2016

1 Abstract

The Onion Project is a service that provides anonymized access to the Internet and the onion darknet primarily through obfuscation. It has created a network to route requests through which allows it to obfuscate users when accessing surface websites as well as allowing users to create sites on its darknet which cannot be traced back to the host machine. The darknet is used for a myriad of reasons, some mundane, some criminal, and some protection-based. This paper seeks to provide introductory knowledge about the workings of Tor as well as some of its vulnerabilities.

2 Introduction

Tor provides two services, private and anonymous connections to the Internet and hidden services. Hidden services are websites that are anonymous, like its users. This means that the servers that run the website are hidden and the owner can remain anonymous. These sites can only be found using Tor and end in '.onion' instead of '.com' or an equivalent. These sites, because they can only be accessed through Tor, are considered to be a darknet, which is commonly defined as a suite of hidden internet services that require a specific protocol for access. Other protocols provide access to other darknets. Darknets make up the dark web, which is in turn a small portion of the deep web. The deep web refers to all web content that cannot be accessed through a standard search browser. This is a broad classification as, for instance, online government or university databases and content protected by pay-wall are also considered part of the dark web.[1] It is estimated that the full content of the deep web vastly outweighs that of the surface web, or the web accessible through search engines. But since it is not searchable, it is incredibly hard to estimate the size of the deep web. In the words of Anand Rajaramand, co-founder of Kosmix in 2009, "no one has a really good estimate of how big the deep web is. Five hundred times as big as the surface web is the only estimate I know."[2] Tor itself boasts users from all communities; from whistle-blowers, high-powered individuals hoping to escape scrutiny, criminals, military, law enforcement, regular citizens, to those trying to get around censorship.

1. Author Monica Barratt, *A discussion about dark net terminology*, `http://monicabarratt.net/a-discussion-about-dark-net-terminology/`.

2. Andy Beckett, *The dark side of the internet*, 2009, `https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet`.

3 To The Community

People consider themselves to be anonymous on the internet, that their online persona can be separated from their public one. However, over the last few years it has become increasingly clear that this is not true. Traffic analysis link a person's online habits and allow for targeted profiling. While this is most frequently used for ads and may seem harmless, for many it is a warning of constant surveillance. Beyond traffic analysis, even without sophisticated methods it is surprisingly easy to take a username on one site and link it together with the same user on other sites, as usernames are frequently re-used over multiple websites. This can be used to build a fairly detailed profile, potentially including identifying information, of a specific person. People have not always thought to be careful regarding their personal information on the Internet, so even if their current information is well-protected they have have old links or presence on places where more personal information was revealed.

However, given how integrated the Internet is in everyone's lives it is nearly impossible to remove oneself entirely without removing oneself from society. Therefore, it is imperative that alternatives are clear and accessible. People should have the ability to access information, or share information, anonymously and to be able to do so without a high barrier of entry. However, it is also imperative that people understand what they are doing when they anonymize themselves and the threats they remain vulnerable to and the new threats to very wary of. Tor and other darknet providers are not useful for everyone or even necessary for all online activities of those using it, but everyone should know that they exist and what the services provide and what they do not. For many, the darkweb is simply where drug marketplaces and pedophiles thrive and access to them is the only reason to use a service like Tor. Therefore, this paper aims to introduce the broader community to these services and their potential applications.

4 History

The Onion Router (Tor) began as military project funded by the Defense Advanced Research Projects Agency (DARPA) in the U.S. Naval Research Labs (NRL) in the 1990's. It was initially developed as a method for anonymizing traffic so law enforcement officials could keep their identity secret on the Internet. For instance, undercover agents needed a way to communicate with their handlers without being detecting and officials wanted to be able to look at websites without a government IP address appearing on traffic logs. Paul Syverson, along with two other mathematicians, began working on the concept of onion routing. It worked by camouflaging Internet requests by passing them through several random other IP addresses in the onion routing network before contacting the destination. This would allow a specific user's request to remain unattached to the user. However it would not be unattached from the onion network as the final IP address that the website would see would have to be in the network. So, if all Tor users were law enforcement it would be relatively easy to identify all Tor connections as law enforcement, which defeated the point for most use. Therefore, the project had to be outsourced and expanded to be used by all – those enforcing the law, those breaking it, and those just wanting

an anonymous connection for a myriad of reasons. This allowed users to truly camouflage themselves because a Tor user could be anyone. In 2002, with the help of Roger Dingledine and Nick Mathewson, Tor became a free, open-source project for all to use and began downplaying its government origins to attract all types of users.[3][4][5]

Tor is currently maintained through The Tor Project, a non-profit that is funded by a variety of sponsors including average users, government agencies, corporations, and NGOs.[6] For instance, DARPA has been funding Tor since 2014 to develop a search engine, to be called Memex, that would index darknet sites both for search purposes and analytics.[7][8] Additionally, Tor is currently available for mobile on Android through The Guardian Project, which develops apps to help protect users privacy on mobile.[9] Tor continues to expand across the globe and has a published 'core staff' of more than 60 – some of which are simply identified using a username. This staff works on maintaining Tor, working on new release versions, and continuing research.[10]

5 Functionality

Tor enables clients to access regular websites without the traffic being tied back to them. Encryption on the web prevents attackers from seeing what clients are sending to websites, but does not protect against traffic analysis. Traffic analysis allows an observer to see the source and destination of client data. This is enabled through the way data packets are sent over the Internet. Data packets are made up of two parts; the payload, which contains the data a client is sending to a service, and the header, which contains information about the location of the request and the destination along with other meta information. Secure websites use Transport Layer Security (TLS) to encrypt the payload but the header is not encrypted so that the Internet service provider (ISP) can figure out where to send the request and response. This header is what enables traffic analysis, which can potentially betray a client's location, business affiliation, with certain kinds of use, and allows a profile of the client to be built. Tor aims to provide anonymity by preventing traffic analysis of users from occurring.

5.1 Connections

All that will be discussed in this section is work that is done 'under the hood'. All a user has to do is enter a destination URL and the rest of the work

3. Paul Syverson, *Paul Syverson Home Page*, `http://www.syverson.org/`.

4. David Kushner, *The Darknet: Is the Government Destroying 'the Wild West of the Internet?'*, October 2015, `http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022`.

5. Yasha Levine, *Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government*, July 2014, `https://pando.com/2014/07/16/tor-spooks/`.

6. Inc. The Tor Project, *Tor*, `https://www.torproject.org/`.

7. Kim Zetter, *Darpa Is Developing a Search Engine for the Dark Web*, February 2015, `https://www.wired.com/2015/02/darpa-memex-dark-web/`.

8. Patrick Howell O'Neill, *Tor is building the next-generation Dark Net with funding from DARPA*, April 2015, `http://www.dailydot.com/layer8/next-generation-tor-darpa/`.

9. *Guardian Project – People, Apps and Code You Can Trust*, `https://guardianproject.info/`.

10. Project, *Tor*.

will be done automatically. To do this, Tor routes each request from a user through multiple Tor relay nodes so the path from client to service is hard to follow. Tor relay nodes are simply connections through Tor users that have volunteered bandwidth to Tor for this purpose. This way any request passes through multiple IP addresses and the destination website cannot simply figure out the client by seeing who sent it the packet. The complicated aspect of this is that any relay cannot know where the request originated and it's ultimate destination or any node on the network could trace the path and malicious nodes on the Tor network would be able to easily perform traffic analysis.

Tor addresses this problem using public key encryption and a published list of relay nodes. To walk though the process, we will start with some client. The client contacts a Tor administrative server, of which several exist, to get an updated list of Tor relay nodes. Using this list it constructs a path of nodes from an entry node (referred to as a guard node) and ending at an exit node which will then contact the outside website. It then encrypts the message (the data packet) with the public key of the last node in the path. That message and the address of the last node are then encrypted using the public key of the second to last node in the path. It does this until it reaches the first node in the path, the guard node, at which point it has a message encrypted using the guard node's public key that contains a message encrypted using the second node's public key and the address of the second node, and so on. It then sends the message to the guard node, which decrypts the message using its private key. It will then send the remaining message to the next node, whose address it found by decrypting the message. This will continue down the path until the exit node decrypts the message to find a data packet. The exit node will then contact the destination using a regular Internet connection. This make it appear as if it is sending the request. The default length of a path, also known as a Tor circuit, is three nodes; a guard, a relay, and an exit node. All nodes are required have up-to-date encrypted access to the web, either TLS or Secure Sockets Layer Version 3 (SSLv3). However, it is the client's responsibility to use secure websites so that the payload is not passed in the clear. The response will be sent back using the same path. Paths are maintained for a maximum of 10 minutes before they are changed. This removes some overhead for a client so it doesn't have to create a new path for every request to a site.[11]

Messages are passed using a stream cipher, where bits are passed one at a time between two nodes, using 128-bit Advanced Encryption Standard (AES). Node authentication is done though public-key 1024-bit RSA. Each relay has a long-term identity RSA key that should never be changed and used just for authentication. This comes into play when nodes identify themselves to each other, as they will perform a 'handshake' for authentication so that each node can pass information securely to the other and confirm that the other node is who they think it is. This key will never change, as it is the identifier of this node. Each relay also has a medium-term key it uses to encrypt and decrypt messages – or 'onion skins' as they are termed in Tor.[12] These keys should be changed regularly but do not need to be switched out very frequently. A node must accept its old message key for at least one week after changing it. Exit nodes must also have a short-term key for connections to the web. This key is

11. Project, *Tor*.
12. Ibid.

expected to change at least once a day. Nodes have several other sets of keys, but these are the essential keys to message routing in Tor. The SHA-1 hash function is used for authentication and is the standard hash function in Tor.[13] The newer versions of Tor, 2.4 and above, use elliptic curve cryptography instead of RSA, as it is known that 1024-bit RSA can be brute forced using specialized chips. However, as some distributions of Linux-based operating systems only provide support through version 2.3, it was estimated that only 10 percent of Tor users used 2.3 and above in 2013.[14]

5.2 Hidden Services

Another main Tor service is hidden services. These are services that, like Tor's users, want to maintain an element of anonymity. Therefore these services can only be accessed using a .onion address, which requires the Tor Browser. This method, unlike conventional websites, does not reveal the site's host IP address. Therefore a user can set up a hidden server without worrying that the content will be traced back to them. To ensure this, the hidden service communicates with other nodes using Tor circuits. The hidden service first selects a number of introduction nodes and sets up Tor circuits to them. This allows the introduction points to send a message back to the hidden service without directly knowing its location. Then it must put together a hidden service descriptor so users can find the service, which contains the hidden service's public key and references to the introduction nodes. The hidden service then signs this with its private key and uploads it to the database hash table. This table is distributed, meaning it is hosted on multiple nodes and contains redundancies so data will not be lost if a node goes offline, and creates the .onion address. Hidden service addresses are 16 characters long and generated using the service's public key. Once a hidden service has done this it is set up and can communicate with clients.[15]

A client can then find the hidden service though its .onion address and then get the descriptor from the distributed hash table. This gives the client the introductory nodes. The client then builds a Tor circuit to a random relay node, which acts as a rendezvous point. The client then sends a message, via Tor circuit, to one of the introductory nodes of the hidden service. This message contains the address of the rendezvous node and a one-time secret. This secret is used as authentication between the client and the hidden service. This means that the client can only use this one-time secret once if they want to stay anonymous and must also tell the secret to the rendezvous node. The hidden server will then receive the message through its introductory node and then build a Tor circuit to the rendezvous node in the message and give it the one-time secret. The rendezvous node will then send a message to the client notifying that a connection to the hidden service has been established and authenticated. From there on the hidden service and the client can communicate through the rendezvous point. This is similar to communication with an outside

13. *torspec - Tor's protocol specifications*, `https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt`.

14. Dan Goodin, *Majority of Tor crypto keys could be broken by NSA, researcher says*, September 2013, `http://arstechnica.com/security/2013/09/majority-of-tor-crypto-keys-could-be-broken-by-nsa-researcher-says/`.

15. Project, *Tor*.

service with the rendezvous node essentially functioning as the exit node except instead of using TLS to communicate with the surface web, it sends a message to the client or hidden message respectively using the proper Tor circuit. The encryption standards are the same as above as this method just relies on the encryption and anonymity Tor circuits provide.[16]

6 Vulnerabilities

6.1 Malicious Attacks

As with any other service, malicious attacks can occur against a client. This may either be due to the service used, be it a hidden service or a public website, or through the Tor network itself. It goes without saying that sites with malicious scripts or corrupted downloads can still effect users even if they using Tor as they will receive the data sent from the website and the Tor nodes will not. Hidden services are also subject to the same types of attacks that can affect regular sites such as cross-site scripting, SQL injection, and denial of service attacks.

However, in Tor, given the relay aspect of connections, other nodes can have malicious effects as well. This generally occurs at the exit node, as it is the only node that has access to the data going to and coming from the service. This can include injecting malware into downloaded binaries when the exit node receives them, although this can only be done when the download is not encrypted, so through a HTTP connection.[17] To prevent this encryption, some nodes are known to perform sslstrip, which converts the request for an HTTPS website for its HTTP equivalent which causes payload data to be passed in plaintext. This can allow an attacker to aggregate usernames and passwords or other sensitive data. Malicious nodes have also been known to try to interfere with SSH connections, a connection that allows a user to access a network remotely. This is more difficult since SSH connections are verified through a key that is established the first time a client uses the SSH connection so this attack is limited in functionality unless the malicious node intercepted that first connection.[18]

Tor has a system to combat these malicious exit nodes. All relay nodes have flags to indicate their status. Only certain nodes are configured to be exit nodes, which is denoted by a flag. If a Tor user suspects that their connection has been tampered with they can report the exit node to a directory authority. Directory authorities then vote on the node and if a consensus votes it is malicious it is given a BadExitNode flag. This ensures that the node will no longer be used as an exit node, although it may still be used as a relay node. This flag update is guaranteed to distribute through the whole network within three hours.[19] This is sufficient because relays nodes have much less power since the

16. Project, *Tor*.
17. Gareth Owen, *Tor: Hidden Services and Deanonymisation*, 2014, `https://www.youtube.com/watch?v=-oTEoLB-ses&feature=youtu.be`.
18. Philipp Winter and Stefan Lindskog, "Spoiled Onions: Exposing Malicious Tor Exit Relays," *Privacy Enhancing Technologies Lecture Notes in Computer Science*, January 2014, 304–331, doi:`10.1007/978-3-319-08506-7_16`, `http://www.cs.kau.se/philwint/spoiled_onions/techreport.pdf`.
19. Project, *Tor*.

data to and from the network is encrypted as a part of the Tor system. Furthermore, at each hop from one node to another in the Tor circuit integrity checks are performed so if a relay node modifies the message it will be discovered at the next node and that node will be reported.[20] However, if node is suspected of using a broken version of Tor or of engaging in end-to-end correlation attacks its valid flag may be stripped meaning it will not be used by any user for any reason.[21]

6.2 De-Anonymization

Given that people frequently turn to Tor as a method to protect their privacy and become anonymous, most attacks are intended to de-anonymize users and hidden services. There is general consensus among the community that while it is generally infeasible to discover the identity of a particular user without that user making other mistakes, it is possible to de-anonymize a subset of the Tor community some of the time. To clarify, de-anonymizing a user refers to discovering the IP or MAC address they connected to the Tor network from. IP and MAC addresses give up more information than simply a unique identifier, they also can be looked up to access geolocation and other data. If a user connects to Tor using a VPN or proxy, there will still be additional steps to discover the owner of the machine. However, law enforcement agencies frequently can request this information from providers and then be able to link an IP to its request over VPN or proxy.

Part of Tor's security is that an observer can't track your request because it passes through multiple other computers spread across the world. However, if someone can control all the nodes used in a client's circuit, clearly they can connect the user to the service they are accessing. However, this is difficult in practice given the high number of Tor nodes and the fact that circuits expire. This means that even if someone was able to do this they would likely only being able to collect data during the window that the circuit was used. However, even with only the entry node and exit node, it is possible to use a timing attack and correspond the messages, which allows the attacker to know the originating IP and destination. This is more likely because while it is still fairly unlikely for a user to select an entry and exit node who are both run by a malicious third-party, it is more likely than controlling all the nodes in the circuit. Furthermore, because Tor users keep entry nodes for a period of time, beyond just the 10-minute circuit, if a Tor user is using a malicious entry node there is a larger window of opportunity that an exit node run by the same user will be used.[22]

However there are also attacks that can be used when just the entry node is compromised. Massachusetts Institute of Technology (MIT) researchers have, using simple analytics, built traffic profiles of users that use their entry node based on the traffic pattern of data packets. This profiling allowed them to achieve 88% accuracy in determining the types of services and hidden services a user was accessing.[23] It is worth noting that the entry node for a hidden

20. Owen, *Tor: Hidden Services and Deanonymisation.*

21. Project, *Tor.*

22. Owen, *Tor: Hidden Services and Deanonymisation.*

23. Ryan Whitwam, *MIT researchers figure out how to break Tor anonymity without cracking encryption*, July 2015, `https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption`.

service can always de-anonymize that hidden service.[24] However, this is technique limited by the fact that this analysis can only be done on users using a compromised entry node and only while they use that node.[25]

One area of great concern is what a large agency can do with an entry node. There is evidence to suggest that the National Security Agency (NSA) has the means to decrypt 1024-bit RSA keys exchanged through Diffie-Hellman. This would be possible due to specialized equipment allowing a much faster brute-force attack. There is significant evidence to suggest the NSA has this sort of technology. Because this encryption relies on factoring and large primes and some Diffie-Hellman keys are frequently reused, cracking a single prime allows multiple communications to be cracked. As this is the encryption standard used by Tor, if a user has an NSA node running as its entry node, the NSA could easily decrypt the entire message. This would allow it to know the origin, because it is an entry node, but also the destination. Futhermore, even as a relay node, the NSA could decrypt the remainders of messages and like correlating the forward and back messages to find both ends of the connection. It is worth noting, however, that this simply supports the theory that some Tor users can be identified some of the time. It is also worth noting that the latest versions of Tor use elliptic curve cryptography, which is hypothesized to be harder to brute force than RSA/Diffie-Hellman.[26][27] However since there has been less research of elliptic curve cryptography, it has not been as well proved to be secure as RSA. However, given their relative popularity, decryption efforts can be assumed to have been focused more on RSA than elliptic curve cryptography. This is a double-edged sword as this means that there is more uncertainty that it cannot be cracked but also more unlikely that the NSA has a decryption shortcut because it has not been focused on that area of cryptography.

Some attacks are even possible without any nodes at all. Simply using traffic patterns and monitoring of the Tor network for time correlations can allow for nodes to be identified as a type of node (exit, relay, entry, rendezvous point, etc.) and for users to be connected to their request. However, these types of surveillance generally require a huge amount of resources to monitor enough to be useful.[28] With respect to simple timing attacks, they can be improved by causing users to download large files. This makes the data steam more unique because of the large payload. However, even with these large files, which make it much easier to track the pack the packet takes through the network, false positives are expected. A researcher proposing the method of passing large files estimates a 6% rate of false positives. Roger Dingledine, one of the founders and current co-director of Tor, argues that this rate is simply to high to be useful, given the number of Tor users at any given time.[29]

Another main area for de-anonymization comes from services themselves.

24. Barb Darrow, *Vulnerability could make Tor, the anonymous network, less anonymous*, July 2015, `http://fortune.com/2015/07/29/tor-vulnerability/`.

25. Whitwam, *MIT researchers figure out how to break Tor anonymity without cracking encryption.*

26. Swati Khandelwal, *How NSA successfully Broke Trillions of Encrypted Connections*, October 2015, `http://thehackernews.com/2015/10/nsa-crack-encryption.html`.

27. Goodin, *Majority of Tor crypto keys could be broken by NSA, researcher says.*

28. Owen, *Tor: Hidden Services and Deanonymisation.*

29. Jason Koebler, *How the NSA (Or Anyone Else) Can Crack Tor's Anonymity*, November 2014, `http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity`.

As mentioned earlier services may have malicious scripts causing the user to identify themselves, even on hidden services. For instance, in bringing down Freedom Hosting, thought to be the largest service for hosting hidden services at the time, the FBI took control of the servers and shut down all of the websites with a maintenance message. It also include a script that caused the computer sending the request to send its IP address and an identifier of the website visited to an FBI server. This allowed the FBI to get the IP addresses of people vising child pornography websites hosted by Freedom Hosting.[30] This is why it is recommended that users have JavaScript disabled for all sites.

For servers that run hidden services, the standard attacks that plague regular websites can be additionally dangerous for hidden services as they can cause them to betray their source IP address. For example, SQL injection can be used to dump contents of a site, which can include that site's actual address.[31] It is thought that vulnerabilities in the original Silk Road website, a marketplace that at the time grossed $1.2 billion, leaked the site's host IP address which allowed authorities to gain access to the servers and start to track down the owner of the site.[32]

It is worth mentioning, however, that most people who were identified and arrested for their activities can blame much of this on not being careful enough with their data on the regular web as opposed to Tor vulnerabilities. Ross Ulbricht, who created the original Silk Road, a drug marketplace, was identified because of a post looking for developers, referring them to his Gmail account, which was rossulbricht@gmail.com. The post was made using a handle that was also used to post the first ads for the Silk Road.[33] An Anonymous member was caught because he used Tor inconsistently. The kid who posted about a fake bomb threat at Harvard in 2013 logged onto Tor using Harvard's Internet service, which is monitored. Since the authorities could tell that the message came from the Tor network, they simply looked at who was using Tor on the Harvard internet at the time the email was sent.[34] In short, Tor can anonymize your traffic but it does not prevent you from falling prey to many of the same exploits that exist on the regular web and can introduce some new vulnerabilities. It is also worth mentioning that currently Internet traffic correlation, consistently monitoring that a person is on Tor at the same time as an Internet persona, can be enough for a warrant.[35]

7 Censorship

It is important to acknowledge what the darknets can mean for citizens of governments that believe in censorship. People can use Tor to access blocked areas of the Internet to see the free press or talk with others about their own government without fear. However for these individuals, the risk that comes

30. Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, September 2013, `https://www.wired.com/2013/09/freedom-hosting-fbi/`.

31. Adrian Crenshaw, *Dropping Docs on Darknets: How People Got Caught*, August 2014, `https://www.youtube.com/watch?v=7G1LjQSYM5Q`.

32. Joshuah Bearman, *The Untold Story of Silk Road, Part 1*, May 2015, `https://www.wired.com/2015/04/silk-road-1/`.

33. Ibid.

34. Crenshaw, *Dropping Docs on Darknets: How People Got Caught.*

35. Bearman, *The Untold Story of Silk Road, Part 1.*

with being identified is much higher. For this reason the creators of Tor are careful not to advocate that Tor is a perfect source that will always protect anonymity. Fortunately, it seems that these governments tend to be more focused on blocking Tor access in their countries than tracking down users. This is likely partly due to the high amount of resources that would be needed to sort through all the Tor users looking only for those from their country and the limitation with de-anonymization already discussed. Aside from China, which has expended a large number of resources actively engaging with combatting Tor's influence, most of these countries mainly block Tor using fairly straightforward methods such as using services developed in the United States of America (U.S.) for companies.[36]

Some of the methods used are as simple as as blocking the Tor Project website. This is a 'surprisingly effective' tactic, in the words of Jacob Appelbaum a former Tor employee, because while Tor does not need to be downloaded from the website, copies are available on Github and through email, it prevents people from learning about Tor and about these other methods of installation if they do not know someone who can direct them to these services.[37] This is used in almost every country that is known to censor Tor, including most Middle Eastern countries such as the United Arab Emirates, Saudi Arabia, Iran, and Syria. Some countries have invested in SmartFilter, currently owned by parent company Intel, which looks at HTTP requests and sees if the word Tor appears in the request. Tor has updated their protocols such that their connection looks as indistinguishable as possible and so this is not an effective tactic against recent versions of Tor. Some countries have also simply forced Internet service providers (ISPs) to cut down on the amount of bandwidth that is allocated to SSL requests, effectively slowing Tor requests to an unusable speed. Furthermore, some countries have directly blocked access to Tor entry nodes, as these IP addresses are publicly posted.[38]

This caused Tor to establish bridge nodes. These are nodes whose IPs are not publicly listed but are given out by request to get around this issue. Originally bridge nodes could be provided by request on the Tor website. However after a period of time it was discovered that China had obtained all those IP addresses and had blocked them. So then the Tor Project allowed users to request bridge nodes through email addresses where the IPs offered were tied to the email address used to request them. The intention was that information required to create new email addresses would slow the rate of acquiring IPs down. However, inevitably, it was determined that China had acquired all of those IP addresses as well. Now bridge nodes are usually distributed though social media from humanitarian groups and proponents of Tor to other individuals seeking to use the service directly. China now currently follows up on all SSL connections so if a user connects to an entry node using a secure line, someone will try to connect to the same IP and verify the type of connection. As long as China continues to try to block Tor there will be a continual back and forth between the two, creating new censors and trying to avoid detection. These are some of the ways governments try to filter out Tor from existing in their country.[39]

36. Roger Dingledine and Jacob Appelbaum, *How governments have tried to block Tor*, `https://www.youtube.com/watch?v=GwMr8Xl7JMQ`.
37. Ibid.
38. Ibid.
39. Ibid.

8 Alternative Services

While Tor is likely the most well known darknet provider, it is by no means the only service. Another well-known service is Freenet. Freenet was developed by Ian Clarke in 2000 and works as a distributed peer-to-peer network. What this means is that as a user of Freenet, you list a set of trusted peers in the network and all your requests are routed through them. As every Freenet user stores some portion of the data that Freenet hosts encrypted on their machine, the idea is that between a user's trusted peers and their trusted peers and so on, every user of Freenet will eventually be able to access every piece of data on the darknet. These data stores may run chat relays, freesites (Freenet's version of hidden services), or another service and accessed through keys allowing authentication that the contents have not been tampered with. Freesites are less interactive than on Tor as they are simply data stores and frequently do not have commenting or search capabilities. The peer-to-peer aspect of Freenet is thought to generally provide more security as a user only directly interfaces with other trusted users and requests are quasi-randomly passed to other nodes using some directional rules which ensure that it doesn't take too long to find a request but also ensure a request would be hard to follow. Freenet has its own vulnerabilities but since it only accesses within its darknet some risks are diminished. It is worth noting that Freenet stores data directly on other user's computers and that data can be decrypted, although it is difficult, and might be able to be used by authorities against the user although the thought is that the user should have plausible deniability since they do not know what is stored.[40] Essentially, Freenet is a distributed data store with the build-in capability for communication and some applications build on top to enable other types of services. One benefit that must be noted is that this means that data will be stored after the poster has left the network.[41] This is because there is no way to delete data in Freenet other than for it to become so unpopular that it is never requested and all the caches storing that data have been filled with other data.[42]

I2P is another darknet provider. Like Tor it provides both darknet services and access to the Internet. Much of its anonymity is guaranteed through similar methods as Tor and, like Tor, the object is not to obscure that a user is using I2P but obscure what they are using I2P to do. One major difference is that I2P is fully distributed so all data is stored on user computers and found through the network while Tor uses directories.[43] This system allows I2P to provide peer-to-peer functionality where a user can simply interface with other trusted users and their trusted peers. I2P also uses similar types of message routing as Tor, although it is referred to as 'garlic routing' instead of 'onion routing'. This is in part to distinguish itself but also because I2P will bundle encrypted messages together while passing them through the network.[44] I2P also uses Diffie Hellman key exchange, but with 2048-bit keys and Advanced Encryption Standard (AES) cryptography, which are considered more secure.

40. None, *Freenet - Overview*, `https://freenetproject.org/`.
41. *I2P Compared to Freenet*, `https://geti2p.net/en/comparison/freenet`.
42. None, *Freenet - Overview*.
43. *I2P: A scalable framework for anonymous communication*, `https://geti2p.net/en/docs/how/tech-intro`.
44. *Garlic Routing*, `https://geti2p.net/en/docs/how/garlic-routing`.

Similarly to Tor, the introduction of outproxies, the equivalent of exit nodes in Tor, introduces some vulnerabilities in I2P because of their interface with the regular net. I2P was created after both Tor and Freenet and has benefited from research on both systems, given the peer-to-peer network heuristics and similar routing systems to onion routing. Access to "eepsites", the I2P equivalent of hidden services, is thought to be faster through I2P than through Tor and more integrated.[45]

Both I2P and Freenet benefit in some ways from being smaller than Tor. Crucially, since their membership is small there has been less work done to block them or discover their vulnerabilities. However, on the flip side this is also a detriment to the services in many ways as well. For that exact same reason there has been much less research on the networks proving their strength or finding vulnerabilities that can then be fixed. Additionally, since their networks are smaller, they are easier to analyze as a whole group and identify individuals in the same way that the large number of Tor users provides anonymity to each user. I2P has suffered this to a slightly less degree as many of its organizational structures are similar to Tor and so has benefited from some of the same research. Additionally, I2P and Freenet have not had to do as much on scaling their systems, which has likely caused the systems to work closer to how they work originally designed but also leaves the question of how to scale and if the systems will work once scaled still to be addressed.

9 Tips for Darknet Usage

- Only send sensitive or personal information to trusted sites. Furthermore, only send sensitive information through encrypted access, namely HTTPS connections. Tor only protects your access point – not anything passed to the site directly.
- Use secure websites and connections whenever possible.
- Ensure JavaScript, Flash, and other platforms that can execute code on your computer without your knowledge are disabled.
- Make sure you are using updated browsers and releases to ensure that you have the most up-to-date patches and fixes of vulnerabilities that may have been discovered.
- If you use default configuration of the Tor Browser, make sure you set up DNS requests to be by proxy as this is not set by default. This means that otherwise any DNS lookup will see your IP.[46]
- Connect through Tor via VPN if possible. This will not stop law enforcement from finding you but it does add an extra layer of protection from other things coming through from Tor.
- Given that outgoing nodes have exposed the most vulnerabilities in these systems, check if you can use a hidden website instead of going to the

45. *I2P: A scalable framework for anonymous communication.*
46. Crenshaw, *Dropping Docs on Darknets: How People Got Caught.*

surface net. Several well-known sites have hidden service equivalents, including Duck Duck Go, the search engine that doesn't record traffic information, and Facebook. Their addresses can be looked up using hidden service directories.

10 In Summary

While Tor is not a perfect system, it is still one of the best options for anonymized access to the Internet and a darknet network. Some of this is purely due to the fact that the Tor network is well-known and handles a huge number of users. This helps Tor have a large platform of available knowledge and helps guarantee a stable future for Tor, although nothing can be assured. However, it is important that users are vigilant on Tor and continue to protect their own information during use. It is also of the utmost importance that every user of Tor knows that using Tor does nothing if they are not using Tor properly. It is also important to note, that the anonymity of a hidden service host is not as secure as that of a regular user. However, used correctly, Tor can be a huge boon in allowing users freedom of information, press, and communication in ways that are no longer available on the surface net. Yet, for all Tor does, it cannot stop or rest on its laurels. Clearly, Tor needs to continue evolve to stay secure. This is crucial in avoiding censorship but also in advanced encryption methods, methods for detecting and reporting mal-intentioned nodes in the network, and ensuring its users are up-to date and aware of the vulnerabilities and minimize risk to themselves.

References

Barratt, Author Monica. *A discussion about dark net terminology*. `http://monicabarratt.net/a-discussion-about-dark-net-terminology/`.

Bearman, Joshuah. *The Untold Story of Silk Road, Part 1*, May 2015. `https://www.wired.com/2015/04/silk-road-1/`.

Beckett, Andy. *The dark side of the internet*, 2009. `https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet`.

Crenshaw, Adrian. *Dropping Docs on Darknets: How People Got Caught*, August 2014. `https://www.youtube.com/watch?v=7G1LjQSYM5Q`.

Darrow, Barb. *Vulnerability could make Tor, the anonymous network, less anonymous*, July 2015. `http://fortune.com/2015/07/29/tor-vulnerability/`.

Dingledine, Roger, and Jacob Appelbaum. *How governments have tried to block Tor*. `https://www.youtube.com/watch?v=GwMr8Xl7JMQ`.

Garlic Routing. `https://geti2p.net/en/docs/how/garlic-routing`.

Goodin, Dan. *Majority of Tor crypto keys could be broken by NSA, researcher says*, September 2013. `http://arstechnica.com/security/2013/09/majority-of-tor-crypto-keys-could-be-broken-by-nsa-researcher-says/`.

Guardian Project – People, Apps and Code You Can Trust. https://guardianproject.info/.

I2P: A scalable framework for anonymous communication. https://geti2p.net/en/docs/how/tech-intro.

I2P Compared to Freenet. https://geti2p.net/en/comparison/freenet.

Khandelwal, Swati. *How NSA successfully Broke Trillions of Encrypted Connections*, October 2015. http://thehackernews.com/2015/10/nsa-crack-encryption.html.

Koebler, Jason. *How the NSA (Or Anyone Else) Can Crack Tor's Anonymity*, November 2014. http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity.

Kushner, David. *The Darknet: Is the Government Destroying 'the Wild West of the Internet?'*, October 2015. http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022.

Levine, Yasha. *Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government*, July 2014. https://pando.com/2014/07/16/tor-spooks/.

None. *Freenet - Overview*. https://freenetproject.org/.

O'Neill, Patrick Howell. *Tor is building the next-generation Dark Net with funding from DARPA*, April 2015. http://www.dailydot.com/layer8/next-generation-tor-darpa/.

Owen, Gareth. *Tor: Hidden Services and Deanonymisation*, 2014. https://www.youtube.com/watch?v=-oTEoLB-ses&feature=youtu.be.

Poulsen, Kevin. *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, September 2013. https://www.wired.com/2013/09/freedom-hosting-fbi/.

Project, Inc. The Tor. *Tor*. https://www.torproject.org/.

Syverson, Paul. *Paul Syverson Home Page*. http://www.syverson.org/.

torspec - Tor's protocol specifications. https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt.

Whitwam, Ryan. *MIT researchers figure out how to break Tor anonymity without cracking encryption*, July 2015. https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption.

Winter, Philipp, and Stefan Lindskog. "Spoiled Onions: Exposing Malicious Tor Exit Relays." *Privacy Enhancing Technologies Lecture Notes in Computer Science*, January 2014, 304–331. doi:10.1007/978-3-319-08506-7_16. http://www.cs.kau.se/philwint/spoiled_onions/techreport.pdf.

Zetter, Kim. *Darpa Is Developing a Search Engine for the Dark Web*, February 2015. https://www.wired.com/2015/02/darpa-memex-dark-web/.