**The Tor Network**

**Is Tor the solution to our anonymity concerns?**

**Introduction**

**Goals**

* Present “The Onion Router” (Tor), its history and its uses.
* Discover how Tor functions to preserve anonymity.
* Compare Tor to normal internet browsing.
* Determine whether Tor is worth using for normal internet users.

**Motivation**

Increasing concerns over preserving anonymity drive our research toward “The Onion Router” (Tor). Tor has been used for years as a method of preserving anonymity in an online environment. Recent revelations about the NSA and other government agencies storing personal data and internet browsing habits have many Americans concerned about preserving their anonymity.

Around the world, people share similar anonymity concerns. Secure and anonymous internet usage is important because the internet is designed to be a free and open environment. Discussions and actions on the internet can be hindered if anonymity is not a possibility. Situations where anonymity is important to physical safety can arise when dealing with whistleblowers and political dissidents. In some cases user anonymity can be the difference between freedom and jail (or life and death in extreme cases). Because of these factors, it is important to find a good mechanism for preserving anonymity in an easy and accessible way.

When researching how to preserve anonymity online, most sources refer to Tor as the answer to their anonymity concerns. While Tor can be used to preserve anonymity to an extent, there is no guarantee of anonymity and there are certain limitations to its protection. In this document we will detail how Tor works, how it functions to preserve anonymity, the limitations on its protection and the difference between the security of Tor versus classic internet browsing. Before getting into the details of how Tor works, we will give a brief background of Onion Routing and how it originated.

**History**

The concept of Onion Routing was first developed in 1995 by David M. Goldschlag, Michael G. Reed, and Paul F. Syverson for the Naval Research Laboratory’s Center For High Assurance Computer Systems with funding from The Office of Naval Research (ONR). The first generation of Onion Routing was outlined in the paper ["Hiding Routing Information"](http://www.onion-router.net/Publications.html#or-infohiding) by the 3 researchers mentioned above. In 1997, Onion Routing gained funding from the Defense Advanced Research Projects Agency (DARPA) to develop a more robust Onion Routing network.

An early version generation of Tor was tested in 1998 as a small distributed network with about 13 nodes and a redirector for TCP traffic. The initial tests were promising so further analysis and testing occurred based on the original design. The test network hosted more than one million connections per month in the final months (about 50,000 per day).

After initial testing and continual ONR and DARPA funding, the generation 2 development of the Tor network is released in 2003 as an open source (MIT) project, with it’s lead developers being Roger Dingledine, Nick Mathewson and Paul Syverson.[[1]](#footnote-0)

After 2003, Tor was pursued as a separate project, still with funding from DARPA and ONR (as well as various other sources). The network is currently maintained by The Tor Project, which facilitates the setup of volunteer nodes, the development of the software, the outlining of bugs and known vulnerabilities, distributing of Tor browsing software and securing (and using) funding.[[2]](#footnote-1)

Tor is still very widely used, consisting of approximately 4.5 million connected clients per day as of December 2015[[3]](#footnote-2). It is one of the most highly respected mechanisms for achieving anonymity online. The NSA itself has stated that Tor is “Still the King of high secure, low latency Internet Anonymity” and that “There are no contenders for the throne in waiting”.[[4]](#footnote-3) Now that we have an idea of how Tor originated and how it is used today, we can get into the details of what Tor is and how exactly it works.

**Tor Overview**

**What is Tor?**

Tor is “a group ofvolunteer-operated servers that allows people to improve their privacy and security on the Internet”.[[5]](#footnote-4) Tor uses Onion Routing, which was designed to prevent Traffic Analysis of networks. By using layers of encryption (hence the name “Onion”), Tor can protect a message’s content. The messages are sent through multiple relays before reaching their final destination, which when coupled with the layered encryption preserves the anonymity of the original sender (as well as obfuscating the link between sender and receiver).

Tor network nodes are volunteer based, meaning anyone can go to the Tor Project website and download the software necessary to run a Tor node.[[6]](#footnote-5) Tor maintains a directory of all current Tor nodes which can be retrieved by the Tor Browser (the browser for utilizing the network). When a Tor user sends a message, a random path of Tor nodes is chosen to be the circuit for the sent message. The sender then creates an “Onion” based on the path it is going to take.

**The Onion**

“Onion” is the term used for the message being sent through the network because of the layers of encryption applied to the message. The core of the onion is the actual message the user is trying to send, along with some padding. The message is then encrypted for each hop along the path of nodes. Every time the message is sent along the path to the next hop, a layer of the encryption is peeled off, revealing the next node to send the message. When the last node in the path peels of the last layer of encryption, only the message is left to be sent to the receiver. Since layers of encryption are peeled off at each hop, Tor appends a random bit string to the end of the onion that is the same size as the peeled off layer. This can prevent an attacker from estimating where the onion is along the path (a smaller onion could mean further along the path).

Because the approach of Onion Routing is used, each node only knows the previous node in the path, who sent it the message, and the next node in the path, where they need to send the message. A compromised node can therefore not determine the contents of the message because of the layers of encryption, cannot determine the original sender because the previous node could be any node, and cannot determine the receiver because the next node could also be any node.

This design approach brings a high degree of anonymity in regards to the system itself; however, one of the problems we will discuss later is that the messages sent between the receiver and the Tor network are not encrypted like they are when traversing the network. Next, we will detail the specific mechanisms Tor uses to preserve anonymity over its network.

**Methods of preserving anonymity**

**Keys and their configuration**

Tor uses a variety of nodes with three goals: Encryption, authentication and coordination.

Encryption: All connections in Tor uses TLS link encryption, which stops observes from looking into the message and finding where in the circuit the message is heading. Also the Tor client creates an ephemeral encryption key with each relay, these layers means only the exit node can read the message. The circuit key is then discarded by both sides when the circuit ends, so trying to break into a relay with the same key is ineffective.

Authentication: Every Tor node has a public encryption key called a “onion key”. Keys are rotated every week. When a circuit is established, at each step it asks the tor relay for its onion key. “That way the first node in the path can't just spoof the rest of the path.”[[7]](#footnote-6) Because the Tor client is the one that creates the circuit it can be sure to get the correct onion key from the relay: This way no single relay can know information on the sender.

Coordination: Each node in the aTor network has a long-term public key called the “Id key”. Each directory authority has a “directory signing key” that identifies them. The authorities provide a list of known relays with the signature, specific keys, location exit policies and other information. So unless an adversary can control most of the directories they have no way of knowing all relays or tricking the client to use other relays. The Tor client comes with a list of locations and public key for each authority, the only way to trick the client to use a fake network is to provide them with mod of the client.

**Entry Guards**

Tor uses “Entry Guards.” These are a specific number of relays chosen at random to use as entry points and only for the initial hop. If those relays aren’t observed or under adversity control, then they can’t win. If they are under adversity control they can see a larger fraction of the user traffic but that is all. For example, an attacker controls or can observe C relays. There are then N relays in total. If the user selects an new entry and exit node each time, the attacker will be able to figure out all the traffic sent with a probability of *(c/n)2.* With the use of “Entry Guards” the user has a chance of *(n-c)/n*) to avoid observation.

**The** **Circuit**

Tor clients will use the same random circuit for 10 min as long as the circuit is functioning normally. If for some reason the circuit fails (Message drop, long wait time etc) Tor will immediately change the circuit. Note that a single TCP stream (IRC connection) will stay connected on the same circuit forever. Individual streams are not rotated from one circuit to another. This way an attacker with partial view of the network is given only that one time chance to link the user to the destination, instead of multiple chances over a period of time.

**Limitations**

**Limited Application Security**

When Tor is installed in a web browser it automatically configures certain security settings. Javascript is disabled, plugins will automatically be shut off and when downloading a file the browser will warn the user and will download and open it on another application. Javascript is normally not a security issue, but since there could potentially be a ip address leak when using any of these third party plugins, this prevents the user from using Flash-based sites (youtube etc). This was exploited in the NSA attempt at breaking into the Tor network in the early 2010’s known as “Egotistical giraffe” an exploit in the Mozilla browser. Once a message exits the Tor network all encryption is removed and the message is visible similar to normal internet browsing. Tor does remove header information but if the message has any information that links the message to the user (Ex. username, initials ex) a message can be linked back to the sender completely nullifying Tor networks anonymity effort. However, YouTube is currently doing an [opt-in trial of a video player](https://www.youtube.com/html5) that uses HTML5 instead of Flash, which you can use with the Tor Browser.[[8]](#footnote-7)

**Traffic Confirmation**

Normally when a Tor relay receives a message it removes the layer to find out where it is going and where it came from and sends them out almost immediately. If an attacker has control or is able to observe the relays on both sides of the Tor circuit, by comparing different factors such as volume, traffic timing and other methods to figure out if the relays are on the same circuit. If the attacker concludes that they are, they know the sender's ip address from the first node in the circuit (“entry guard”) and knows the destination from the exit node, combining these two important pieces of information the sender is now deanonymize.[[9]](#footnote-8)

**Tor exit**

An exit relay is the final relay in a Tor circuit before it reaches its destination. Exit relays are known by all users in the network, so that they can be used by any Tor user. Because the message exits Tor, the ip address of the node is seen as the source of the message. If a user on the Tor network uses this exit node for malicious purposes (ex. drug trafficking, etc) the exit node might take the blame. People to run exit nodes should be “...prepared to deal with complaints, copyright takedown notices, and the possibility that their servers may attract the attention of law enforcement agencies.” If a user is taken in by a law enforcement agency because of the relay, they can contact Tor to receive a written confirmation that they are an active Tor exit node or can go to exonerator, a website that can check if an ip address was a node at a given time.

**Tor uses**

**Censorship circumvention**

The Tor network hides a sender's ip address thus making it a powerful tool for users in oppressed or countries with high degrees of censorship (ex China) to use the internet freely. Certain countries try to block the access of known Tor ip addresses. To circumvent that there are Tor relays known as “Bridges”, these specific relays are not publicly listed as part of the Tor network. Since there is no public list of all bridge relays it is difficult for an isp to properly identify and block them.

**Black market and other activities**

Within the Tor network users are completely anonymous to one another as long as they stay inside the network. For this reason Tor is used by numerous websites for illegal activities such gambling, drug sales, arm sales etc. These sales are then usually handled by a third party so that the buyers and sellers anonymity is kept during the sale. Also instead of real money which can be traced from one location to another through serial codes imprinted during make, most of these sites use the online currency “Bitcoins” which is also completely anonymous.

C**onclusion**

One of the main conclusions we wanted to come to was whether it is worth it for normal internet users to use Tor instead of regular browsing. This really is a question of whether anonymity is important to the user. For normal users with nothing to hide, using the Tor network is unnecessary, but can still be effective at reducing/eliminating online tracking from advertisers. But some users actually prefer that their shopping habits be tracked by advertisers so that relevant items can be suggested to them. Either way, users wishing to anonymously browsing the internet can use Tor to do so. The Tor project website gives a few pointers as to how to further achieve anonymity because they recognize that Tor is not a complete solution to our anonymity concerns.[[10]](#footnote-9)

In places where anonymity is required, there is absolutely a need to use Tor. Reporters can communicate with whistleblowers, political dissidents can post ideas anonymously, users in repressed countries can circumvent censorship and users can buy and sell good anonymously using BitCoin. There are many instances where using Tor is unnecessary but there are also many instances where it can be useful or even necessary.

That being said, the reader might wonder why every internet user doesn’t use Tor. If anonymity can be achieved much better than with normal browsing, even if it isn’t necessary, why not use Tor anyways? There are a couple of reasons why using Tor can actually be limiting to the user. Some of the pros of using Tor include increased anonymity and access to hidden services hosted through Tor. But as with most good things, Tor use comes with a tradeoff.

Tor browsers can be limited in functionality because of the connection with certain applications. As discussed earlier, there are limitations with Tor using Flash applications or Java applets. This can be a major inconvenience, given that many normal activities online use or require these plugins/applets. Another drawback is that Tor has a higher latency because of the multitude of relays the message has to go through, meaning it is slower than normal browsing; however, most of the time, the decreased speed is worth the increase in anonymity.

1 . <http://www.onion-router.net/History.html>

2, 5, 10. <https://www.torproject.org/about/overview>

3. <https://metrics.torproject.org/clients-data.html>

4. <http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity>

6. <https://www.torproject.org/getinvolved/volunteer.html.en>

7. "Tor Project: Anonymity Online." 2007. 10 Dec. 2015 <<https://www.torproject.org/>>

8. "What Is Tor - Tom's Guide." 2013. 10 Dec. 2015 <<http://www.tomsguide.com/us/what-is-tor-faq,news-17754.html>>

9. "Tor security advisory: "relay early" traffic confirmation attack ..." 2015. 10 Dec. 2015 <<https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/>>

1. http://www.onion-router.net/History.html [↑](#footnote-ref-0)
2. https://www.torproject.org/about/overview [↑](#footnote-ref-1)
3. https://metrics.torproject.org/clients-data.html [↑](#footnote-ref-2)
4. http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity [↑](#footnote-ref-3)
5. https://www.torproject.org/about/overview [↑](#footnote-ref-4)
6. https://www.torproject.org/getinvolved/volunteer.html.en [↑](#footnote-ref-5)
7. "Tor Project: Anonymity Online." 2007. 10 Dec. 2015 <<https://www.torproject.org/>> [↑](#footnote-ref-6)
8. "What Is Tor - Tom's Guide." 2013. 10 Dec. 2015 <<http://www.tomsguide.com/us/what-is-tor-faq,news-17754.html>> [↑](#footnote-ref-7)
9. "Tor security advisory: "relay early" traffic confirmation attack ..." 2015. 10 Dec. 2015 <<https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/>> [↑](#footnote-ref-8)
10. https://www.torproject.org/about/overview.html.en [↑](#footnote-ref-9)