ONION ROUTING AND TOR

Kyle Swan*

Cite as: 1 GEO. L. TECH. REV. 110 (2016)

https://perma.cc/JV7Y-FNYH

THE ORIGINS OF TOR

Security in online activity, and privacy from those who wish to monitor it, has been a priority for internet users since creation of the web. To achieve this goal, the concept of onion routing was developed by the United States Naval Research Laboratory ("NRL") in the mid-1990s to protect online communications in the U.S. intelligence community.[1] Computer scientists for NRL, working with other government programs on what was then titled The Onion Routing Project, ushered this technology into its next generation, known simply as "Tor."[2] Tor was deployed as open-source software,[3] available to the public for free in 2004,[4] and is now maintained by volunteers and funded by various sources including the U.S. Government, digital rights interest groups, and individual donors.[5]

Tor was created to provide an efficient and secure method for users to protect their identity online. As such, Tor has attracted a large following of users, criminal and legitimate, who could benefit from the cloak of anonymity.

---

* GLTR Staff Member; Georgetown University Law Center, J.D. expected 2018; University of Virginia, B.A. 2014.

[1] Paul Syverson, *Brief Selected History*, ONION ROUTING https://www.onion-router.net/History.html (last visited Nov. 28, 2016).

[2] *Id*.

[3] *Open-source*, MERRIAM-WEBSTER ONLINE DICTIONARY http://www.merriam-webster.com (last visited Oct. 10, 2016) ("pertaining to or denoting software whose source code is available free of charge to the public to use, copy, modify, sublicense, or distribute.").

[4] Syverson, *supra* note 1.

[5] *Tor Sponsors*, THE TOR PROJECT, https://www.torproject.org/about/sponsors.html.en (last visited Nov. 16, 2016).

Journalists, whistleblowers, and political activists can use Tor to circumvent national firewalls and hide their identities, often from authoritarian regimes.[6] The protection offered by Tor also shields illegal activities in a part of the internet dubbed the "Dark Web."[7] Criminals, such as hackers, child pornographers, and black marketers, use Tor to conceal their identities from law enforcement.[8] Tor is not exclusively used for criminal or political activities, however. Individuals concerned with privacy now use Tor simply to browse the internet, with The Tor Project estimating that it has over 1.5 million users.[9]

Tor helps to protect the identities of users through a combination of the structure of the network and a process known as onion routing. The structure of the network prevents an outsider actor from monitoring a user's traffic, or locating a user, while onion routing uses encryption to shield the contents of a user's message. When used in tandem, both aspects prevent websites from tracing data back to a user.

TOR STRUCTURE

Tor, first and foremost, is a network. It is made up of decentralized collective of servers hosted by volunteers all across the globe called "nodes." A node is a connection point in a network with an assigned address; it can be a router, computer terminal, peripheral device, or mobile device.[10] Nodes are the access and transfer points for user data; the bridges for user traffic sent back and forth through the Tor network, connecting users and their destinations. By acting as a middleman between a Tor user and his destination, nodes also protect the user from having his information tracked.

Tor maintains a directory of all nodes on its network, and from its directory, it will designate a path for information through three or more separate nodes. A user's data, after entering the Tor network will pass through an entry

---

[6] *Inception*, THE TOR PROJECT, https://www.torproject.org/about/torusers.html.en (last visited Nov. 16, 2016).

[7] Leslie Caldwell, Assistant Attorney General, U.S. Dep't of Justice, Remarks at "Cybersecurity + Law Enforcement: The Cutting Edge" Symposium (Oct. 16, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law.

[8] Jake Wallis Simons, *Guns, drugs and freedom: the great dark net debate*, THE TEL. (Sept. 17, 2014, 5:00 PM), http://www.telegraph.co.uk/culture/books/11093317/Guns-drugs-and-freedom-the-great-dark-net-debate.html.

[9] *See generally Tor Metrics*, THE TOR PROJECT, https://metrics.torproject.org/ (last visited Nov. 16, 2016).

[10] *See Node*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com (last visited Nov. 16, 2016).

node, also known as a guard node, then at least one middle node, and then an exit node, before reaching its destination. Tor will send the user's data on a random path to its destination through these nodes; each time a user visits another site, it selects a different random path of nodes.[11] The randomization at each node makes data increasingly difficult to track as the variability of potential paths expands. Node diversity allows for greater security because an entity attempting to track a user would have to be able to follow it through each possible pathing, an increasingly difficult task as the number of forks in the road grows.

Tor employs the onion routing encryption process to prevent websites and other services from learning a Tor user's location (through the user's IP address) or intercepting the content of the message sent. Data is encrypted upon entrance into the Tor client for each node. Encryption is a practice that protects data by scrambling it into a message decipherable only by someone with the proper key or algorithm to unscramble and access it. Because Tor goes through several nodes and subsequent scrambles, no single relay can reveal a user's location. In this way, the multi-node setup creates greater security than a proxy using a single node. Unlike other server providers, which will guide traffic through one particular node, Tor, by sending information through multiple nodes, effectively makes those tracking information lose sight of its origin.[12] Tor not only misdirects sites seeking to gather information from users visiting them; it goes one step further, shielding not only the path of the user's requests from node to node, but also the payload data those requests contain and the location of the user.[13]

To illustrate through analogy: imagine you, the user, are a spy attempting to arrive at a villain's lair without being tracked to orally deliver a message to another spy. You must keep your identity (IP address) concealed while evading his pursuing henchmen (outside users attempting analyze web traffic), who might persuade you to reveal the message (intercept message contents of the communications sent). You leave your hideout with various layered disguises (encryption), which will prevent the henchmen from knowing your true identity. To reach the lair, you make your way through several chambers around the lair where the henchmen have lookouts (nodes). At the first lookout, henchmen are expecting an unknown spy to pass at a random spot, but you escape unnoticed because you are in your first disguise, a police

[11] *Tor Overview*, THE TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Nov. 16, 2016).
[12] *Tor FAQ*, THE TOR PROJECT, https://www.torproject.org/docs/faq.html.en#Torisdifferent (last visited Nov. 16, 2016).
[13] *Id.*

uniform. At the second lookout, they are looking for the police officer, but they only see a man dressed as a waiter, your second disguise. When the henchmen are looking for a waiter at their third lookout, all they find is an elderly man, your third disguise. They take no notice as you enter the unsuspecting villain's lair to deliver the message to your waiting ally. The same process occurs on the way back to your hideout with new disguises and different lookout points, and when you make your way back without any henchmen on your tail, your identity is safe. The Tor process combines the encryption (disguises) and random node pathing (choices of lookout points) to keep user identity (which for an IP address, translates easily to user location) private.

HOW DOES ONION ROUTING WORK?

The primary goal of onion routing is to prevent traffic analysis and potential back-tracing. Traffic analysis, often referred to as web analytics in certain contexts, is the process of intercepting and examining messages in order to deduce information about a particular communication. It can be as banal as logging a user's online shopping preferences so that a retailer can advertise to his personal taste, or as significant as an attempt by law enforcement to track down a criminal.[14] Traffic analysis can allow entities to follow the chain of data leading back to an individual user in a process aptly called back-tracing.[15] Tor seeks to subvert this process.[16]

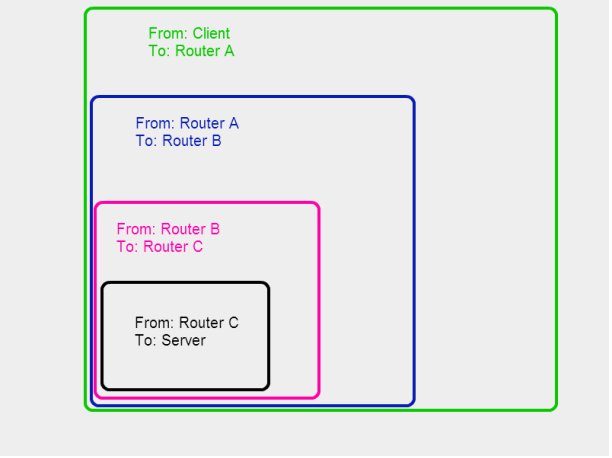
Onion routing protects user data by creating multiple layers of encrypted connections to shield data from potential onlookers.[17] For those of us attempting to understand how onion routing works, an apt metaphor exists in its name. The data sent by a user is the core of the "onion," containing the content of the message. At the onset of the transmittal process by connecting to a Tor client, several layers of encryption surround the core, one atop the other like Russian nesting dolls, so that the core data payload is inaccessible to outside actors.[18] When entering the Tor network, the data is scrambled through encryption; the iterations of the scrambled message are then scrambled again for the number of

---

[14] *See* Chris Hoffman, *The Many Ways Websites Track You Online*, HOW-TO GEEK (June 1, 2012), http://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/; *see also* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End up in Your Computer*, WIRED (Aug. 5, 2014), https://www.wired.com/2014/08/operation_torpedo/.
[15] *See* Yossi Gillad & Amir Herzberg, *Spying in the Dark: TCP and Tor Traffic Analysis*, https://www.freehaven.net/anonbib/cache/tcp-tor-pets12.pdf.
[16] *Id.*
[17] *Overview*, *supra* note 11.
[18] *Id.* ("The client negotiates a separate set of encryption keys for each hop along the circuit").

times it will travel through a node en route to its destination. As the information travels through the Tor network, at each node, a layer of the onion is "peeled" away, exposing the next encrypted message to be decrypted at the next node. No individual node ever knows the complete path of the data packet, so tracking capabilities from a single node are limited.[19] Once the onion is fully peeled and has reached its destination, the core containing the information is the only piece remaining. Once the data is received at the destination server, that information is re-encrypted (imagine the onion re-growing its layers) and "peeled" again on the way back to the user, following the same procedures as before.[20]

The secret to Tor's ability to protect users' identifying information is in the peeling process. The nodes only receive the location of the node sending it information, so the user's location (in the form of an IP address) and the content of the message are never exposed simultaneously. The Tor client encrypts the original data so that only the exit relay can decrypt it. This encrypted data is then encrypted again, so that only the middle relay can decrypt it. Finally, this encrypted data is encrypted once more so that only the entry relay can decrypt it.[21]



http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/

The first node will receive a fully encrypted message with the user's location; the second node will receive a partially encrypted message with only the location of the first node; and the final node will fully decrypt the message

[19] *Id.*
[20] *Id.*
[21] *See* Will Nicol, *A Beginner's Guide to Tor: How to Navigate through the Underground Internet*, DIGITAL TRENDS (Jan. 19, 2016), http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/ (illustrating how encryption is layered for the nodes).

and only have the location of the second node when it transmits its own location and the information to its destination. Each node will see something different from the last, and the onion routing process will separate the user location and the content of the user data so that only the content remains by the time it reaches its destination. Outside users attempting to spy on the contents of the data packet, or ascertain its original location, will be unable to do either. Although the exit node will have access to the user's unencrypted communications, there is no way to track it back to the user's original location because there is no location information attached. This does not prevent users from encrypting their own data for superior security beforehand. To prevent the exit relay from accessing user data, end-to-end encryption such as SSL[22] will deliver a still-encrypted message through Tor.

USING TOR

For an individual seeking to use Tor, public access is available on The Tor Project's website: https://torproject.org. A copycat of Mozilla's Firefox browser, called "Tor Browser," which implements Tor for internet use, is freely offered for download and use on the website. The browser's design is very user-friendly, and various fora and blog posts exist online for potential users who seek to learn more about using Tor, how it works, and issues facing the Tor and Dark Web user community.[23] It is also possible to access the Tor network through other methods, such as specially created software. Plug-ins, mobile apps, and even entire operating systems, are available online and provide the similar protections.[24] The Tor browser is configured to attempt to control extraneous factors (addressed in the section below) which may not be addressed by other software. It is, therefore, also important to ensure that when using Tor, the protections sought by a user are actually put into place. To be sure Tor is working properly, a Tor Check site exists to affirm users that the protections are effective.[25] With these resources at hand, an individual user can effectively navigate the Tor network with relative ease and greater privacy.

---

[22] SSL.COM, http://info.ssl.com/article.aspx?id=10241 (last visited Nov. 16, 2016) ("SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.").

[23] THE TOR PROJECT, https://blog.torproject.org/ (last visited Nov. 16, 2016); DEEP DOT WEB, https://www.deepdotweb.com/ (last visited Nov. 16, 2016).

[24] *See Software and Services*, THE TOR PROJECT, https://www.torproject.org/projects/projects.html.en (last visited Nov. 16, 2016).

[25] CHECK THE TOR PROJECT, https://check.torproject.org/ (last visited Nov. 16, 2016).

Tor also provides protection to the hosts of websites which are created to be reachable only through the Tor network and accessible through a web address ending in ".onion" (rather than ".com"). The configuration of hidden services obscures the source of information by creating an intermediate host for content. Tor users can reach each other at hidden services, using them as rendezvous points for communications where neither can detect the other's identity, never exiting the Tor network[26] The Tor Project estimates that nearly 60,000 unique .onion addresses are up on the network daily on the hidden-service directory.[27] Many of these hidden services are associated with the Dark Web, part of which the FBI and other government enforcement agencies have sought to shut down in the past with some limited success.[28] Many hidden services are used for legitimate purposes, however, and provide an important outlet for content creators to disseminate information while maintaining a high level of protection.[29]

LIMITATIONS OF TOR

Even though Tor provides a high degree of privacy to its users, it is not completely impenetrable; proper usage is important to ensure security. Tor cannot protect users if the applications they use compromise the security Tor provides by making their data accessible in other ways. Tor users who visit sites like Facebook, which require a log in, lose their protections by logging in.[30] A local ISP or network provider may not know the user's physical location or destination site, but because the user logged into the site, they know who the user by virtue of his login credentials.[31] Law enforcement often uses personal identifying information found in transactions, such as those using Bitcoin, or posted in relation to particular online accounts to track down criminals despite

[26] *.Tor: Hidden Service Protocol*, THE TOR PROJECT, https://www.torproject.org/docs/hidden-services.html.en (last visited Nov. 16, 2016).
[27] *Unique .onion addresses*, THE TOR PROJECT, https://metrics.torproject.org/hidserv-dir-onions-seen.html (last visited Nov. 16, 2016).
[28] Press Release, U.S. DEP'T OF JUSTICE, *More Than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network* (November 7, 2014), https://www.justice.gov/opa/pr/more-400-onion-addresses-including-dozens-dark-market-sites-targeted-part-global-enforcement.
[29] JM Porup, *Building a new Tor that can resist next-generation state surveillance*, ARS TECHNICA, (Aug. 31, 2016), http://arstechnica.com/security/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance/.
[30] *Tor FAQ*, *supra* note 12.
[31] *Id.*

their use of Tor.[32] In the takedown of the infamous Dark Web black market known as the Silk Road, FBI agents were able to track its creator, Ross Ulbricht, aka Dread Pirate Roberts, by linking several of his accounts in various online fora to a personal Gmail account, which allowed the FBI to locate him.[33] A user's own activity, as in the case of Dread Pirate Roberts, may be what deprives him of the protections provided by Tor.

Outside of what a user is posting online, actively updating content, such as Javascript, Adobe Flash, and QuickTime, can also access a user's account according to permissions in the user's operating system.[34] These technologies may be able to store data separate from your browser or operating system data stores.[35] This means these applications can access the data that your user account can access, ignoring proxy settings and bypassing Tor to share identifying information directly with other sites. Therefore, these technologies must be disabled in your browser to use Tor to its complete functional capabilities.[36] Although active content has the capability to bridge the gap between the user and his destination site, it can be disabled with relative ease by adjusting online settings.

Some organizations claim that they have compromised the Tor network through particular exploits.[37] Many seek to claim their superiority over Tor's network, from hackers to government agencies, either for bragging rights or to exercise control over the Tor users.[38] Often, however, the compromise of a user's identity is due to exploited human error, such as following a trail of money transfers or identifying information, as seen in like in the FBI investigation of Silk Road and Dread Pirate Roberts. The Tor Project does not seem overly concerned about any purported vulnerabilities to its network

---

[32] Press Release, U.S. DEP'T OF TREAS., *FinCEN Awards Recognize Partnership Between Law Enforcement and Financial Institutions to Fight Financial Crime*, (May 10, 2016), https://www.fincen.gov/sites/default/files/shared/20160510.pdf.

[33] Tim Hume, *How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road*, CNN (Oct. 4, 2013), http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/.

[34] *Tor FAQ*, *supra* note 12.

[35] *Id*.

[36] *Id*.

[37] *See, e.g.*, Andy Greenberg, *Global FBI Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED (Nov. 7, 2014), https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.

[38] *See, e.g.*, JM Porup, *supra* note 29 ("In 2014, the US government paid Carnegie Mellon University to run a series of poisoned Tor relays to de-anonymise Tor users. A 2015 research paper outlined an attack effective, under certain circumstances, at decloaking Tor hidden services (now rebranded as 'onion services'). Most recently, 110 poisoned Tor hidden service directories were discovered probing .onion sites for vulnerabilities").

outside of the realm of human error.[39] Despite any potential vulnerabilities, many recognize the value of having an privacy-protective network configuration such as Tor, and researchers who successfully find potential exploits in the Tor network often help to fix the problems they encounter.[40]

One additional limitation for potential Tor users is the network speed. Because the data needs to travel through several nodes, instead of a direct user-to-destination connection, and because of the limited capabilities of volunteers who run the nodes, the connection speed of the Tor network is slower than a normal internet search. A user considering adopting Tor may have to take the compromised connection speed into account.[41]

A VALUABLE, IF IMPERFECT, PRIVACY TOOL

Many who use Tor, for purposes both legitimate and illegitimate, depend on its protections for their safety. Its utility as a resource for private online communication has led to an expansion of the network and substantial support from all kinds of entities. The technology behind Tor's structure and onion routing system is an area that is constantly developing new methods to solidify its protections, as many groups with varying motivations actively seek to penetrate its network. No security system is perfect— but when used correctly, Tor can be an effective means of communicating, searching, or just browsing the web more securely.

---

[39] Dave Lee, *Dark net raids were 'overblown' by police, says Tor Project*, BBC NEWS (Nov. 10, 2014), http://www.bbc.com/news/technology-29987379.

[40] *See, e.g.*, Eric Bangeman, *Security researcher stumbles across embassy e-mail log-ins*, ARS TECHNICA (August 30, 2007), http://arstechnica.com/security/2007/08/security-researcher-stumbles-across-embassy-e-mail-log-ins/; Larry Hardesty, *Shoring up Tor*, MIT NEWS (July 18, 2015), http://news.mit.edu/2015/tor-vulnerability-0729.

[41] *Tor FAQ*, *supra* note 12.