Jared Smerdell

CS170

Douglas MacGregor

Anonymization

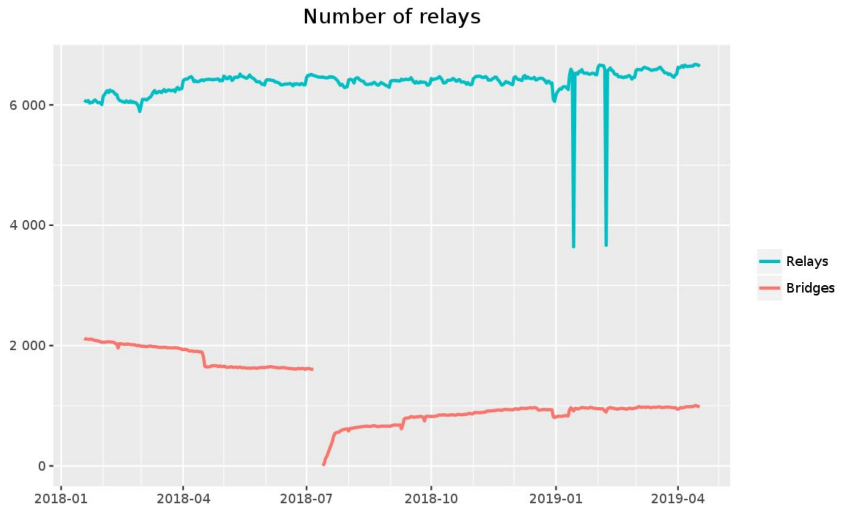
Introduction

The internet is a wild place with surveillance and recording everywhere. It is nearly impossible to stay completely anonymous online but there are definitely steps an individual can take to keep their identity concealed. This paper covers three routes an individual can take to help stay anonymous. The first being Tor, a network aimed at anonymity and privacy. It utilizes many techniques to allow censored citizens, whistle blowers, and any individual to connect to the internet. Another system in place to provide a secure internet connection and location spoofing are VPNs which use encryption to prevent an outsiders for looking in. This system is widely used by business and censored individual to connect to the web. Lastly, there is an operating system called Tails that interfaces with the Tor network to provide massive privacy and identity concealment. This paper will focus on these three topics and how the work, as well as a personal attempt to use them.

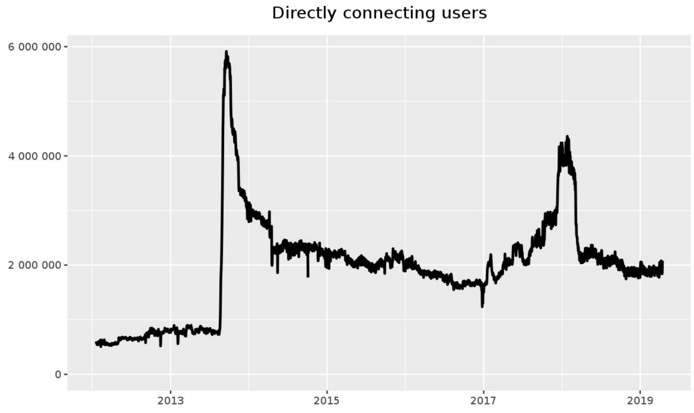
Tor

Overview

Tor or the onion router is a network which aims to conceal an individual's identity through the grapevine. In other words, the network uses relays that jump a users connection around with the idea that it is impossible to trace its origin. One such use of this network is allowing people who live in a country where the internet is heavily censored to access websites and media they would not otherwise have access to. The onion idea is derived from the many encrypted layers the network creates to hide the identity of the user, like the layers of an onion. The Tor network was deployed in October of 2002 under a free and open software license and by the end of 2003 had about a dozen volunteer nodes or relays (The Tor Project | History). Since the project is publicly available, anyone is able to run a relay to support the network. Currently, there are over 6000 relays running worldwide (Servers – Tor Metrics) which is quite impressive considering where the project started. While tor is aimed for legal activities, because of its allegedly untraceable nature, there are many people who use it for evil with the number one use being online markets. On the other hand, tor has allowed suppressed citizens and whistleblowers to communicate with news organizations letting their voices be heard. The community has been growing ever since it’s release, with the direct connecting



The Tor Project - https://metrics.torproject.org/

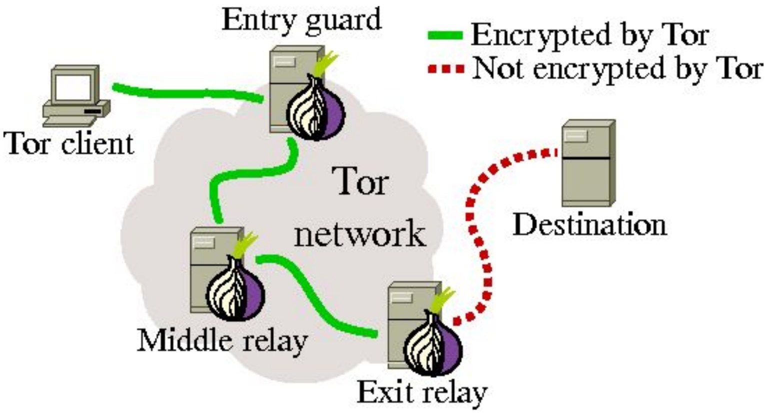


The Tor Project - https://metrics.torproject.org/

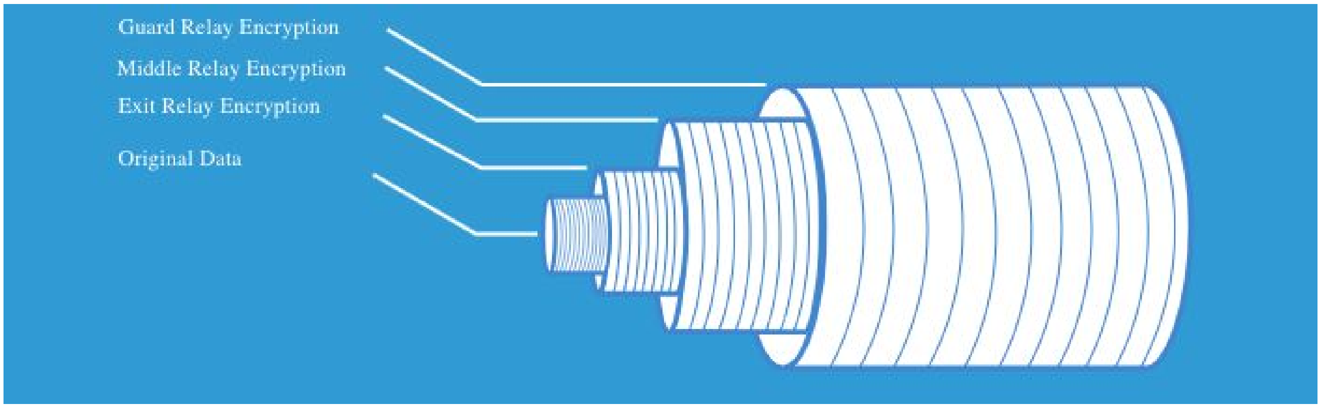
users estimated at around 2,000,000 users. The network has been around for a while and is here to stay to protect individuals and their privacy.

How it Works - Relays

As previously mentioned, the network uses a series of relays to mask the user's identity however, that is the bird's eye view of how the process works. Zooming into the process there are three different types of relays: entry/guard relays, middle relays, and exit relays, all with their respective jobs(TorRelayGuide). Multiple entry guard relays are selected at random by the client for the initial hop through the network. The thinking behind this is that even if an attacker is monitoring all the used entry guard relays, they only see a bit more of the internet traffic which ultimately doesn't help them (Tor Project - What Are Entry Guards). After data goes through the entry guard relays the data is transmitted to the middle relays which are there to prevent the entry and exit relays for knowing each other, which would compromise security. After going through the middle relay the data is passed off to the exit relay which is responsible for sending data to the final destination, however, once out of the exit relay, the data is not encrypted. This system ensures that "No single relay in the path can know about both the client and what the client is doing (Tor Project - Keys)."



It is recommended to not run exit relays out of one's house because of the legal repercussions. As the tor relay guide has stated, “Ideal exit relay operators are affiliated with some institution, like a university, a library, a hackerspace or a privacy-related organization. An institution can not only provide greater bandwidth for the exit but is better positioned to handle abuse complaints or the rare law enforcement inquiry (TorRelayGuide).” These relays are only given minimal information to complete their job and are viewed as untrusted which is a smart safety precaution. The original data is wrapped in layers of TLS encryption(Tor Project - Keys) that can only be decrypted by the respective relay to be passed on to the next. Through this process, the encrypted layers are slowly peeled away until the data passes through the exit relay and is no longer encrypted.



This diagram shows the general idea of how the data is encrypted with layers

How it Works - Bridges

In addition to relays, there is another type of node, which is bridges. The bridges are another layer of protection and are especially helpful in suppressive countries that aim to censor the internet. All the normal relays are published and the public can view them which would allow an isp or country to block all the entry guard relays completely removing access to tor. Luckily there are bridge relays which at their heart are simply unpublished relays. The tor client randomly assigns the user a couple of bridges which allows an alternative access point to the middle relays; since the bridges are not publicly published an isp is not able to block all of them and completely restrict access. The bridge relays simply take the place of the entrance guard relay so there are still three hops the data performs. These bridges are essential for allowing access to the internet in censored countries.

How it Works - Additional Info

While the Tor network is able to circumnavigate most censorship, countries have begun utilizing Deep Packet Inspection or DPI to recognize if network traffic is a tor connection. This is possible because while tor keeps everything encrypted and anonymous, is still is recognizable as a tor connection. This is where Pluggable Transports come in. Pluggable transports disguise the data as innocent looking internet traffic and hide the fact that the Tor network is being used. The pluggable transport's job is to get the data from the client to the bridge. Once the data has made it to the bridge it no longer needs to be disguised(Tor Project: Pluggable Transports).

So how is the network maintained and who gathers the information on all the relay nodes? Every tor client has a list of information for 10 trusted directory authority nodes (DA's) that have the special job of maintaining a document called the consensus. These nodes are scattered throughout the world and are run by trusted individuals who contribute to the project. Out of the 10 nodes, 9 are used to maintain the master list of relays while the other has the very important job of maintaining the list of bridges(Wright). The job of each relay is to compile a list of all known relays and other crucial data by communicating with each other. Afterward, the information is signed by each DA and shared with the others, there should be a majority that agrees on the data resulting in a new consensus that is published by each DA. The tor clients verify the DA's information through their signature and know that the relays are legitimate so that they can access the network.

Vulnerability - Exit Relay Snooping

One of the apparent vulnerability is when data leaves an exit node because it is no longer in the tor network it is not encrypted. Anyone running an exit node can listen in and see the information being transmitted. While this doesn't have a direct link to the client, any personal information can give clues as to where the data came from.

Vulnerabilities - Exploiting P2P Applications (Bad Apple Attack)

Researchers attempting to crack the tor network exploited the popular torrenting application BitTorrent that used the Tor network. By monitoring multiple exit relays, the researchers were able to track the TCP stream to reveal IP addresses of the "anonymous" users. While most attackers have focused on exploiting the browser, these researchers focused on P2P file sharing applications and the vulnerabilities they have. They claim to have revealed 10,000 IP addresses using this method (Le Blond, Stevens., Manils, Pere., Abdelberi, Chaabane., Kaafar, Mohamed Ali., Castelluccia, Claude., Legout, Arnaud., & Dabbous, Walid). The researchers used DHT tracking to trace the IPs. DHT tracking is carried over UDP which tor does not use and when the BitTorrent client fails to connect to the DHT it converts to its public interface revealing the source IP of the stream. This doesn't directly give the origin of the client IP, but by using statistics and the monitored exit node correlations can be made and the IP can be inferred. While this attack is exploiting a P2P file sharing application, this is still a vulnerability in the Tor network.

My Attempt Using Tor

1. I downloaded tor and installed the tor application from https://www.torproject.org/download/ for my mac
2. After launching the browser I was asked if I wanted to "Configure" the network setting if I was in a country that censors tor like Egypt, China or Turkey. I chose to simply connect
3. After the browser configured itself it brought up a private search engine called DuckDuckGo
4. I looked up some websites to visit and decided on the Uncensored Hidden Wiki with the URL: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
5. After perusing the pages it's pretty much the same as any other wiki page
6. Wow! I've accessed the Tor network, I was surprised at how fast it was even with all the hopping and encrypting. Good job Tor team!

Conclusion

Overall the Tor network is an amazing tool for staying anonymous and it uses an array of techniques to keep the client private. The potential this project has is remarkable and as the internet progresses it will be important to be able to surf securely. The applications for this software are numerous and ever growing. While there are still ways an attacker can exploit the network, it's one of the best tools for staying anonymous and protecting essential human rights.

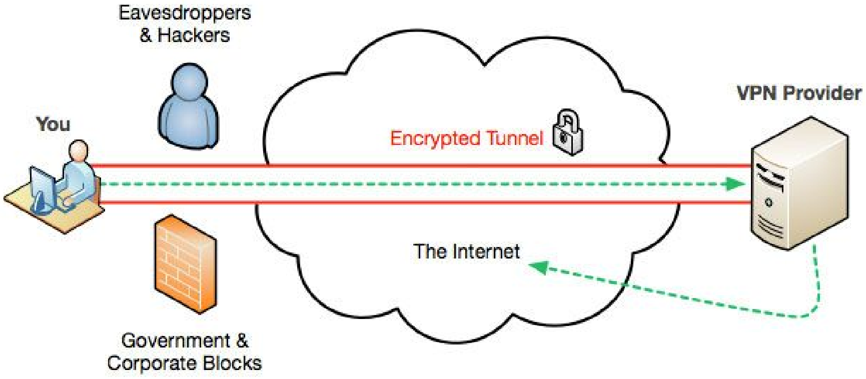
Virtual Private Networks (VPNs)

Overview

Virtual Private Networks or VPNs connect a public network to a private network letting the user send and receive data as if they were actually connected to the private network. This is useful because it is more secure and uses encryption to keep the data secure. In addition, VPNs allow the user to bypass levels of geo-restriction and censorship to access things the otherwise would not have had access to. The act of creating a virtual private network is known as virtual private networking and uses an internetwork infrastructure called tunneling to transfer data between networks. VPNs are especially popular with companies and businesses as they can connect to other companies and offices over a public network while having a secure connection.

How it Works

VPNs work by creating a tunnel between the user and the private network to create a secure encrypted connection. There are various protocols that are utilized with some of the more common ones being layer 2 tunneling protocol (L2TP), IP security (IPSec), Secure Sockets Layer(SSL), Transport Layer Security (TLS), Point to Point Tunneling Protocol (PPTP) and Secure Shell (SSH). Each of these protocols has advantages and disadvantages, some even work in tandem with each other to increase security. IPSec has a tunnel mode which puts a normal IP packet inside of an IPsec packet, the IPSec packet has a new IP header which is used instead with the data being encrypted and harder to decrypt. Layer 2 protocols like PPTP and L2TP have an array of useful feature and when paired with IPSec make a very secure tunnel. Layer 2 protocols take advantage of the older point-to-point protocol or PPP for short. PPP was designed for sending data over a dial-up set up and many of the features of PPP are inherited by the layer 2 protocols (Virtual Private Networking: An Overview). Now for the tunneling itself, after a tunnel has been established the data is prepared for transfer and a data transfer protocol header is added to the payload. This gives the payload the information needed to make it to the target network. However, just like everything else, VPNs have their own vulnerabilities.



Vulnerabilities - Correlation Attack

Now although the data in the VPN tunnel is encrypted, everything on the outside is not. So an attacker with an abundance of resource and time could analyze the internet traffic to make a statistical guess at someone's IP address. If the attacker sees that a client requests something from a VPN and that VPN requests from a website, by looking at the traffic patterns and the VPNs behavior, the attacker can derive the clients IP address(Bettilyon). This approach takes a lot of resources and time so for the most part, it is not something the average Joe needs to worry about.

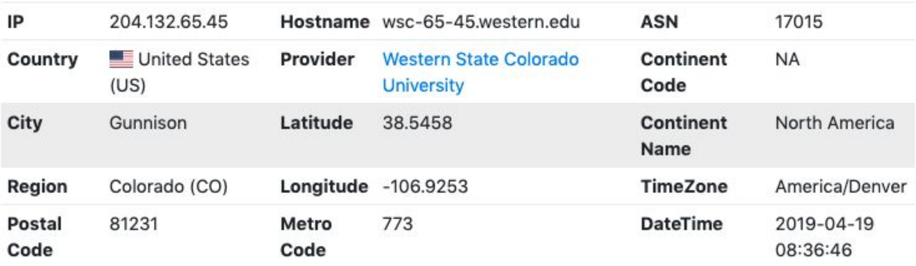
Vulnerabilities - Logging

This isn't so much a direct vulnerability with VPNs but more something at can be taken advantage of by a hacker. Often times VPNs will log everything that a user does which is not a good thing when trying to stay anonymous. If an attacker was able to get that information, a user's anonymity is as good as gone. For this reason, many websites advise against using a VPN that tracks a user's data; for every VPN that logs data, there should be one that can keep a user anonymous.

My Attempt Using a VPN

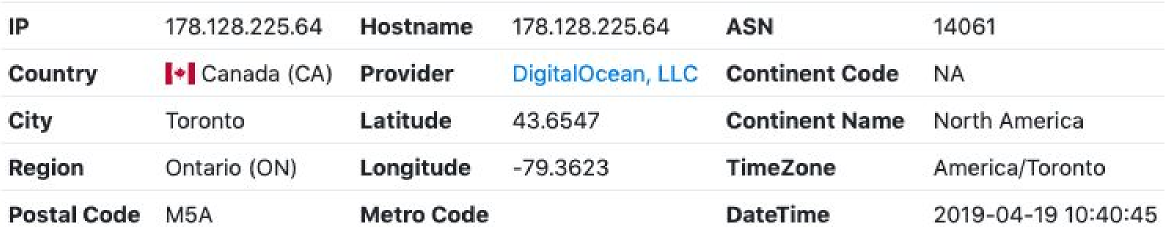
1. After doing some research on free VPNs, I settled on using a free and simple VPN called TunnelBear. While it does have options to pay, it seems like one of the better free VPNs.

2. I downloaded the application and installed the package from https://www.tunnelbear.com/. Afterward, I was prompted to create an account, which I did.
3. To start I looked up my public IP without the VPN and entered it into an IP location finder, the results were rather surprising as they gave away the location of my school which is Western.



IP	204.132.65.45	**Hostname**	wsc-65-45.western.edu	**ASN**	17015
Country	United States (US)	**Provider**	Western State Colorado University	**Continent Code**	NA
City	Gunnison	**Latitude**	38.5458	**Continent Name**	North America
Region	Colorado (CO)	**Longitude**	-106.9253	**TimeZone**	America/Denver
Postal Code	81231	**Metro Code**	773	**DateTime**	2019-04-19 08:36:46

4. After turning on TunnelBear, the application automatically connected me to a location in Canada. My public IP address has completely changed.
5. Now instead of saying that my provider is Western, and I'm in Gunnison Colorado, my IP address says I'm in Toronto Canada and my provider is DigitalOcean, LLC. Very interesting!



IP	178.128.225.64	**Hostname**	178.128.225.64	**ASN**	14061
Country	Canada (CA)	**Provider**	DigitalOcean, LLC	**Continent Code**	NA
City	Toronto	**Latitude**	43.6547	**Continent Name**	North America
Region	Ontario (ON)	**Longitude**	-79.3623	**TimeZone**	America/Toronto
Postal Code	M5A	**Metro Code**		**DateTime**	2019-04-19 10:40:45

Conclusion

VPNs are a great tool if someone needs to keep their information relatively secure or bypass some basic restrains like geo-blocked websites. They take advantage of many different protocols and encryption to create a secure tunnel between a client and the VPN server. One of the key essentials to staying anonymous online is definitely a VPN and when paired with the Tor network can keep an individual mostly safe from attacks and censorship. In addition, VPNs are a great tool for companies and business that need to keep sensitive data secure, it allows for infrastructure that a company's machines can run on, even at home.

Tails

Overview

The Amnesic Incognito Live System or Tails for short is a free open source operating system that runs off of a USB stick or DVD. The purpose of the OS is to keep the user completely anonymous and circumvent censorship. The operating system leaves no trace on the machine it is plugged into and forces all internet connections to go through the Tor network. The operating system is based on Debian GNU/Linux and has multiple built-in applications such as a browser, messaging client, email, and office suite. The Tor project has financially supported the development of the operating system however, it is important to note that they are two different projects run by different people. As previously stated in the Tor section it is possible for an outsider to recognize someone is using Tor, Tails aims to make it "as difficult as possible to distinguish Tails users from other Tor users (Tails - Can I Hide The Fact That I Am Using Tails?)." In addition thails currently only works on x86 and x64 architecture, that it won't run on raspberry pis or phones and tables. Every time the OS is shut down and the USB or CD is removed, all data during that session is destroyed. This means that the OS is essentially factory reset every time it is shut down.

How it Works

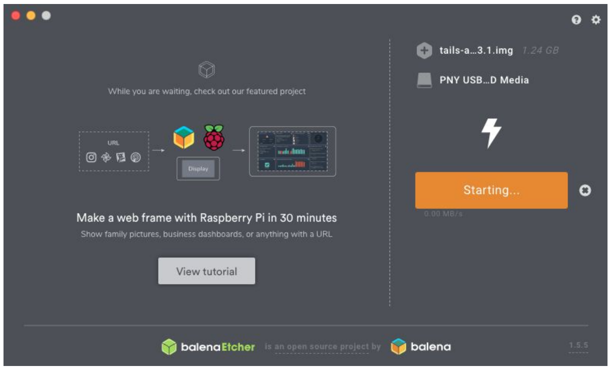
There are many different parts that make Tails operate but the basic idea is that the operating system is built around the Tor network. All internet connections are funneled through the network and any connections that attempt to bypass the tor network are blocked. This is interesting because it allows some things to work while others can not. For example, it is impossible to use the ping command on the tails machine as it “uses the ICMP protocol while Tor can only transport TCP connections (Tails - Frequently Asked Questions).” Although previously mentioned that the OS is wiped every time Tails is shut down, there is an option for a “persistent volume” this allows some files, settings, and encryption keys to be saved even after shut down. The persistent volume is encrypted and protected by a password.

Vulnerability - Cold Boot Attack

So while the OS is reset when tails is shut down, there is still a possibility that information is saved in the computer’s RAM. If someone has physical access to the machine, that information could be extracted from the RAM before the memory is dumped, which takes a couple of minutes after shutdown. Luckily the Tails team has already thought about this and while a user is shutting down tails, the operating systems overwrites the RAM with random data to prevent a cold boot attack (Tails - Protection Against Cold Boot Attacks).

My Attempt Using Tails

1. I downloaded the tails.img from https://tails.boum.org/install/index.en.html and a program called Etcher which is a program used to install Tails on a USB.
2. After selecting the tails.img and the USB drive, the program began loading Tails onto the USB stick.
3. After installing Tails I booted the USB and restarted my computer, launching Tails by selecting it on the boot menu.



While you are waiting, check out our featured project

Make a web frame with Raspberry Pi in 30 minutes

Show family pictures, business dashboards, or anything with a URL

URL
Display
View tutorial
tails-a...3.1.img 1.24 GB
PNY USB...D Media
Starting...
0.00 MB/s
balenaEtcher is an open source project by balena
1.5.5

4. After It started I was prompted for settings like my language and keyboard format which I selected.
5. The operating system started and I was able to connect to the inter. I also tried to use the "ping" command which did not work, interesting!
6. Overall it was extremely straightforward how to install and use tails, which is an important thing for non-tech savvy people. Good job Tails team!

Conclusion

Being 100% anonymous online is a difficult to do thing, however there are most definitely steps one can take to conceal their identity online. In addition the tor network allows suppressed citizens and individual to access the internet when they otherwise could not. VPSs are a great tool for business to keep their network secure as well as let individuals have some degree of privacy. With this come the Tails operating system which can boot from any computer via a USB and let people have a secure operating system that interfaces with the Tor network. In the end staying private and anonymous online can seem daunting but with some simple research anyone can take steps toward being secure.

References

Bettilyon, Tyler. "Do Vpns Actually Protect Your Privacy?". *Medium*, 2018, https://medium.com/tebs-lab/do-vpns-actually-protect-your-privacy-5f98a9cec90a. Accessed 18 Apr 2019.

Le Blond, Stevens., Manils, Pere., Abdelberi, Chaabane., Kaafar, Mohamed Ali., Castelluccia, Claude., Legout, Arnaud., & Dabbous, Walid. “One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users.” *4th USENIX Workshop on Large-Scale Exploits and Emergent Threats*, 2011, https://www.usenix.org/legacy/events/leet11/tech/full_papers/LeBlond.pdf. Accessed 18 Apr 2019.

"Servers – Tor Metrics". *metrics.torproject.org*, https://metrics.torproject.org/networksize.html. Accessed 17 Apr 2019.

"Tails - Can I Hide The Fact That I Am Using Tails?". *Tails.Boum.Org*, https://tails.boum.org/doc/about/fingerprint/index.en.html. Accessed 19 Apr 2019.

"Tails - Frequently Asked Questions". *Tails.Boum.Org*, https://tails.boum.org/support/faq/index.en.html#index26h2. Accessed 19 Apr 2019.

"Tails - Protection Against Cold Boot Attacks". *Tails.Boum.Org*, https://tails.boum.org/doc/advanced_topics/cold_boot_attacks/index.en.html. Accessed 19 Apr 2019.

"The Tor Project | History". *torproject.org*, https://www.torproject.org/about/history/. Accessed 17 Apr 2019.

"Tor Project - Keys". *Torproject.Org*, https://2019.www.torproject.org/docs/faq.html.en#KeyManagement. Accessed 18 Apr 2019.

"Tor Project: Pluggable Transports". *2019.Torproject.Org*, https://2019.www.torproject.org/docs/pluggable-transports.html.en. Accessed 18 Apr 2019.

"Tor Project - What Are Entry Guards?". *Torproject.Org*, https://2019.www.torproject.org/docs/faq.html.en#EntryGuards. Accessed 17 Apr 2019.

"TorRelayGuide". *Trac.Torproject.Org*, https://trac.torproject.org/projects/tor/wiki/TorRelayGuide. Accessed 17 Apr 2019.

"Virtual Private Networking: An Overview". *Docs.Microsoft.Com*, 2009, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10). Accessed 18 Apr 2019.

Wright, Jordan. "How Tor Works: Part One". *Jordan-Wright.Com*, 2015, https://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/. Accessed 17 Apr 2019.

Wright, Jordan. "How Tor Works: Part Three". *Jordan-Wright.Com*, 2015, https://jordan-wright.com/blog/2015/05/14/how-tor-works-part-three-the-consensus/. Accessed 17 Apr 2019.