Tor

Afeefah Manzoor

Deep Dark Web, 001L, Spring 2021

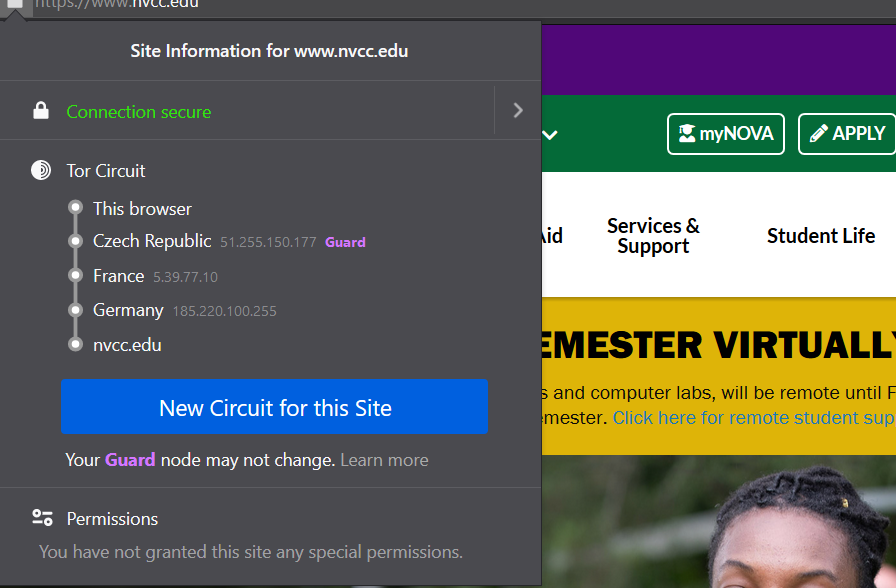
Professor Babur Kohy

Northern Virginia Community College

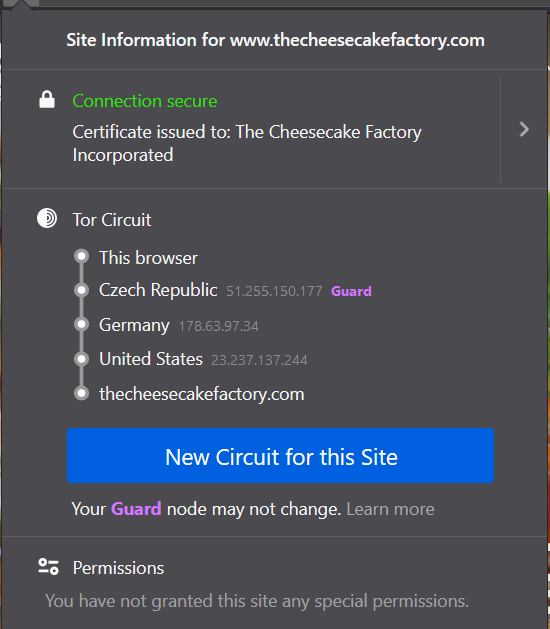
2/1/2021

In this guide I will be explaining what exactly the Tor Bowser is and how this browser works, including how the hops are used to provide near anonymity to the users.

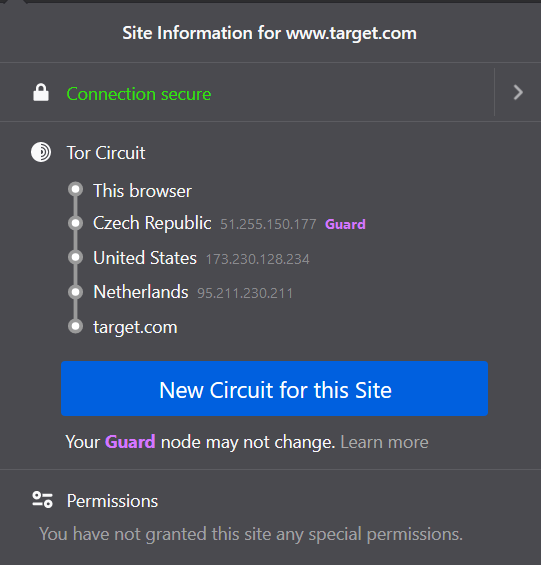
Tor is a web browser that provides near anonymity to all its users if it is used correctly. It provides this anonymity by having all its users having the browser in a pre-defined size and in the middle of their device’s screen as well as creating multiple hops or layers to ensure near anonymity. If the users ever make their browser full screen, the anonymity of the users will be compromised. By maximizing the browser, the user is vulnerable to fingerprinting to be able to be identified by the webserver (SlickStretch, 2016). The Tor Browser is not only for anonymously browsing the web but also can be used by many different applications that want to anonymously route traffic. This is done by using the SOCKS protocol to for the application to route the traffic through Tor (Wordfence, 2018).

Tor also uses several hops to help the users achieve near anonymitty. The first site I went onto was the Northern Virginia Community College’s home page.

(Northern Virginia Community College, n.d.). The Tor Browser in the instance above used five (5) hops. The first in the circuit is the current browser and IP of the device. The second hop is where the user is in which is the Czech Republic with the IP address of 51.255.150.177. The second hop is always considered as the guard. If the user decides to ask for a new circuit of hops, the guard usually stays the same. The next hop was taken in place in France with the IP address of 5.39.77.10, the one after landed in Germany with the IP address of 185.220.100.255. Finally landing at the nvcc.edu webpage. The Northern Virginia Community College will only be able to see the IP address that is in Germany, 185.220.100.255.



(*The Cheesecake Factory*, n.d.). For this page, Tor used the same Guard of 51. 255.150.177 located in Czech Republic. The following IP address after that were in Germany, 178.63.97.34, then hopped to the United States with the IP address 23.237.137.244 before landing onto The Cheesecake Factory webpage. The Cheesecake Factory servers would only recognize the 23.237.137.244 IP address is accessing the webpage.



(Target, n.d.). The hops to reach Target.com had the same guard as the previous two pages, Czech Republic with the IP address of 51.255.150.177. The first hop went to the United States with the IP address 173.230.128.234, then hopped to the Netherland with the IP address of 95.211.230.211 which is recognized by the target.com web servers.

The Tor Browser has many advantages and disadvantages. Some of the advantages include near anonymity to the user, making them much harder to track, provides security since Tor makes it difficult to hide malware in Tor, it is free and accessible, can access the deep web, has privacy-conscious search engine, and helps democracy- for example it was a leading tool in Arab Spring, (Cumins, 2019). These advantages are some of the main features’ users look for in a browser. Many users look specifically for trying to keep their information as private as possible as well as preventing malware to be installed on their machine.

Some of the disadvantages are that the browser can take a minute to load up, can be extremely slow even on a fibre broadband, the data is not encrypted, the data interface resembles the defunct of 1990s NetScape Navigator browser, and may have some security flaws when view webpages that use HTTP rather than HTTPS, (Cumins, 2019). Some of these disadvantages may turn the user completely off from this browser since it is not as fast, streamline, or even appealing to the eye for some users.

Several datatypes that were encountered on this browser include webpages that sell items and forums. Some pages that were found in the demos include webpages that sold guns, illegal drugs as well as pages that you could find and shop on Google Chrome and Firefox like Amazon.com.

Tor is useful for anyone who wants to keep their internet history and browsing history private from advertisements and webservers. It is also useful for any user who wants to find a way around censor or just wanting to hide their IP address. The private sector can use Tor for finding illegal activity and data that they be looking as well as looking through forums to find criminals.

References

Cumins, N. (2019, July 3). *The pros and cons of the Tor browser*. BroadbandDeals.Co.Uk. https://broadbanddeals.co.uk/the-pros-and-cons-of-the-tor-browser/

Northern Virginia Community College. (n.d.). *Error*. Retrieved February 3, 2021, from https://www.nvcc.edu/

SlickStretch. (2016, November 30). *When maximizing \*The Tor Browser\* a warning pops up saying that websites could use my monitor size to track me.* [Reddit]. Reddit. https://www.reddit.com/r/TOR/comments/5fpb5t/when\_maximizing\_the\_tor\_browser\_a\_warning\_pops\_up/

Target. (n.d.). *Target : Expect More. Pay Less.* Retrieved February 3, 2021, from https://www.target.com

*The Cheesecake Factory*. (n.d.). The Cheesecake Factory. Retrieved February 3, 2021, from https://www.thecheesecakefactory.com/

*The Tor Project | Privacy & Freedom Online*. (n.d.). Tor Project. Retrieved February 3, 2021, from https://www.torproject.org/

Wordfence. (2018, June 26). *The Tor Network - FAQ*. https://www.wordfence.com/learn/the-tor-network-faq/