Online Anonymity using the TOR Network through a private Raspberry Pi Wireless Access Point

By: Steven Richmond

The network security problem that my project is addressing is privacy, particularly online anonymity. There seems to be an increasing amount of news concerning internet privacy, which can only evolve as our usage evolves, since most of these adventures transpiring from our technological advances are uncharted territory. To combat the invasion of privacy we are up against, a concept called “Onion Routing” exists. Particularly specialized in the practices of onion routing is a non-profit organization called the Tor Project. TOR stands for ‘The Onion Routing’, so there you have The Onion Routing Project. Their mission statement sums up their purpose quite well: *“To advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.”*

This specific issue is still a problem because there will always be data poachers that want your personal information. Marketing companies tracking your search/browsing history in order to strategically display targeted sponsored advertisements has become borderline creepy. Beyond that, there are many use cases that are made possible (and advocated for) by the Tor Project that I’ll be expanding on as we proceed. This Tor Project maintains the TOR Network. In my research, I came across this pivotal snippet from the Tor Project promotional video:

> "Tor makes all of its users to look the same, which confuses the observer and makes you anonymous. So, the more people use the Tor network, the stronger it gets, as it's easier to hide in a crowd of people who look exactly the same."

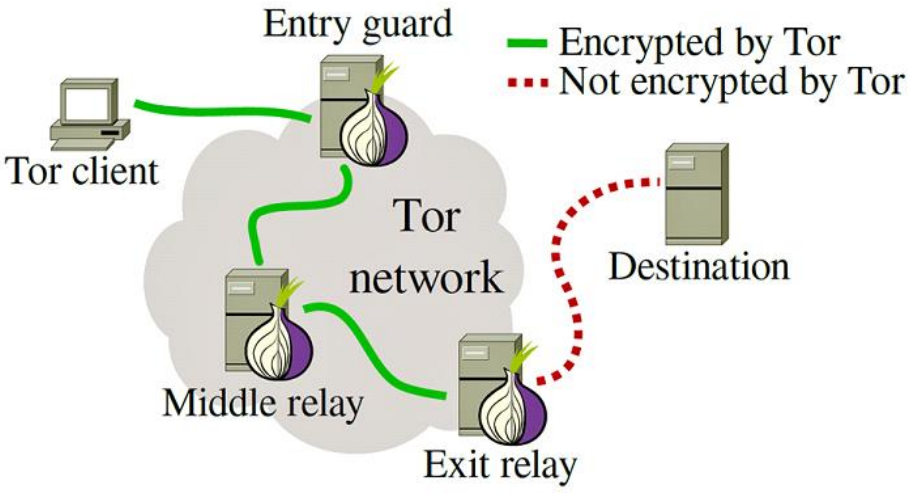
There is a common (yet erroneous) misconception that the TOR network is just a platform for people to do illegal things, such as “dark web” activity. Firstly, the Tor Project merely creates a framework for people to browse anonymously, but this does not make them responsible for how people use it. Don’t blame the gun (“guns don’t kill people; people kill people”). Secondly, the truth is that there are many more appropriate utilizations of TOR for online anonymity, one of the most important and relevant being whistleblowing. Edward Snowden, who in 2013 selflessly revealed to the public some global surveillance programs that the government was running that compromised our individual privacy, said it best:

> “If you look at the way post-2013 whistleblowers have been caught, it is clear the absolute most important thing you can do to maintain your anonymity is reduce the number of places in your operational activity where you can make mistakes. Tor … do[es] precisely that.”
>
> — Edward Snowden, NSA whistleblower

In addition to whistleblowing, there are plenty of other practical uses for people to use the TOR Network to stay anonymous. For instance, journalists and their audiences can use the TOR Network to counteract the suffocating national firewalls if they are in the area of repressive regimes attempting to keep controversial topics contained. Also, bloggers have found comfort in knowing that their blog posts can be truly anonymous, as there are very opinionated and sensitive people out there. Even IT professionals can use the TOR Network to verify their firewall configuration rules and make sure that certain security policies cannot be bypassed.

Furthermore, to avoid the browsing trackers I mentioned earlier from catching and selling your data for targeted ads, average users can use TOR to rest easy knowing that their browsing is private and not being watched.

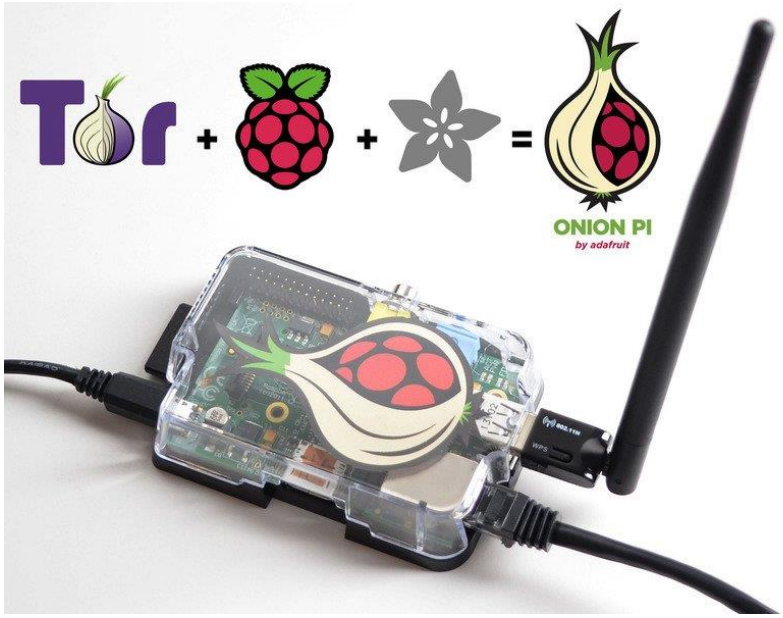
You may be asking what the difference is between the TOR Network and other privacy/security services such as proxies and virtual private networks (VPNs). Since TOR stands for The Onion Routing, let us use their onion analogy to visualize how these constructs theoretically add 'layers' of security to your internet packets. A proxy is simply a hop that will mask your IP by forwarding traffic as to make it look like it is the origin. A VPN is similar to a proxy in the respect of masking the source machine's IP and origin, but also has the added benefit of transporting it through an encrypted tunnel, making it much harder to sniff and trace. These are single layers of protection compared the multi-layering of protection provided by the TOR Network. The TOR Network is an infrastructure of thousands of relay nodes that abstract source data by jumping through multiple random hops, encrypting at each relay. It works its magic by forwarding the internet packets through three separate nodes, each one knowing only where to send it to next, which theoretically makes the source impossible to trace. Here is a visual representation:



There are many amateurs out there that will say, "If you aren't doing anything wrong, what's the point of anonymizing yourself?" To that I say that you do not have to be doing nefarious activities to feel the need to protect your identity when it comes to your online browsing. TOR may be a bit over the top for most internet users, and I'll admit that it takes a particular kind of introverted geek to care enough about masking their online presence that they spend hours researching different VPN services and their no-log policies, but I believe it is time well spent. Our digital privacy should be considered a right covered by the 14th amendment which grants us liberty, defined as freedom from arbitrary control or rule.

With that, my final project demonstrates the utilization of the TOR Network beyond simple theory. I have taken upon the task of purposing a Raspberry Pi 3 B+ to act as a private wireless access point that is then hardened by passing all traffic through the TOR Network. This is achieved by any device connecting wirelessly to the access point via the Raspberry Pi's wireless interface card, and then it does it's TOR magic to the internet packets before being forwarded out via the Ethernet interface that is connected to an outward-facing modem/router by an ethernet cable.

The successes of my solution allow a privacy-minded and anonymity-conscious user to proactively take their online browsing security to the next level. The Tor Project offers their own anonymous browser, called the Tor Browser, that serves as a locked-down browser and operates on the application level of a user's environment. This may work well for simple website browsing, but the solution I am demonstrating for my final project encapsulates ALL traffic from ALL devices connected to the access point at the network level. No need for devices to download any special software or worry about a link opening in Chrome instead of their special Tor Browser. A recorded demonstration will soon follow in order to properly portray how the Raspberry Pi is programmed to achieve these tasks.



References:

Tor Project. https://www.torproject.org/

Who Uses Tor? https://2019.www.torproject.org/about/torusers.html.en

Everything about Tor: What is Tor? How Tor Works. https://fossbytes.com/everything-tor-tor-tor-works/

Onion Pi: Make a Raspberry Pi into an Anonymizing Tor Proxy. https://learn.adafruit.com/onion-pi/overview