Research Project

(Tor Security Concerns and Considerations)

Bryan McKinney

Liberty University

Dr. Jennifer Lee

CSCI 620 - Issues in Security, Privacy and Anonymity

June 23, 2019

Introduction

Tor came on the internet scene during the mid 1990's. Tor (an acronym for "The Onion Network") was developed by the United States Naval Research Laboratory employees Paul Syverson, Michael Reed, and David Goldschlag. The main purpose behind creating the browser and network was to protect the communications of the United States intelligence division. Tor can be broken down into 2 different applications. First the Tor network or Tor routing "runs through the computer servers of thousands of volunteers (over 4,500 at time of publishing) spread throughout the world. Your data is bundled into an encrypted packet when it enters the Tor network. Then, unlike the case with normal Internet connections, Tor strips away part of the packet's header, which is a part of the addressing information that could be used to learn things about the sender such as the operating system from which the message was sent. Finally, Tor encrypts the rest of the addressing information, called the packet wrapper. Regular Internet connections don't do this. The modified and encrypted data packet is then routed through many of these servers, called relays, on the way to its final destination.The roundabout way packets travel through the Tor network is akin to a person taking a roundabout path through a city to shake a pursuer" (Scharr, 2013). After the initial work was complete Tor was later developed further by DARPA. Tor came on the public scene around 2004 to provide a new method of being able to browse the internet in a way that had yet been seen by the public. A way to be private without having to hide one's identity via a VPN or third party proxy service. The second part of the Tor family is the Tor browser. The Tor browser is a modified version of Mozilla firefox ESR (Extended Support Release). One of the biggest differences between Tor and other browsers is the inherent ability to route all of it's traffic

though the tor network. While the Tor browser is not specifically needed to achieve this, they do make it a lot easier for the basic user to just install the browser and have minor configuration changes to make to stay anonymous. This paper will look further at the security concerns of the tor network and different attacks that an attacker could use to still gain access/information from their victims. From a biblical perspective I believe the theme of doing the right thing. While many people use Tor because they value their online anonymity there are quite a few people who use Tor as a means of doing evil or misleading activities. From scripture we can see that “For those who are evil will be destroyed, but those who hope in the LORD will inherit the land” (Psalm 37:9, NIV). The bible is very clear that we should turn away from evil desires and deceitful actions. There is a growing number of people who use Tor as a means for destruction, perversion, and deceit. We as believers are to act against those notions and flee from those desires. While Tor has its positives and if used correctly can be a great asset to the security professional, it also has a dark side that we must actively try to avoid.

Review

In the introduction section we briefly described the history of Tor and the 2 major component of the Tor package; The Tor network and the Tor browser. Now we will take a closer look at the Tor network and how it works at a deeper level. Tor network’s architecture can be broken down into an added level of TCP security called the three-hop path, or as they call it a circuit. Escentally what the three-hop pad does is it adds a level of VPN access where all the traffic that is being routed through the path is encrypted for each other. The path is unique in that while VPN’s have been around for ages, the use of

three different nodes that only know certain aspects of the routing path is quite unheard of. But before you can have a good understanding of how the Onion network works you must first know how Regular TCP/IP routing works. Regular TCP/IP routing works by a three way handshake commonly called SYN, SYN-ACK, ACK. The whole process can be broken down into a few steps:

1. SYN (SYNchronize); SYN works by Host A sends a TCP SYN packet to Host B.
2. Host B receives A's SYN packet
3. Host B Sends its own SYN - ACK (ACKnowledgement) packet back to Host A
4. Host A Receives B's Packet (SYN-ACK)
5. Host A then sends their own ACK packet to Host B
6. Host B receives ACK
7. At this point the Socket is established.

So how is the traditional TCP/IP routing different from Tor's onion routing? Tor's onion routing works as follows:

1. Host A encrypts a message using 3 different keys (Key 1, Key 2, Key 3)
2. Host A sends the message to the first Node (node 1). Node 1 evaluates the message with Key 1 and realizes it cannot decrypt the rest of the message, so it sends the part it has decrypted and the remaining information to Node 2. Node 1 also only has the address of Node 2, it does not know the rest of the data stream.

3. Node 2 has key 2 and node 2 has the input and exit nodes. Node 2 decrypts the next level of encryption...understands there is more encryption that it does not have access too and then sends the message to the exit node.
4. Node 3 (or the exit node) uses its key (Key 3) and sees the GET request for a website and then passes the original message onto that server that is being requested.
5. The destination server processes the request and makes a response packet.
6. Finally the process is reversed and the original Host A gets its response and can decrypt all the messages since it they have access to all the keys.

Tor's onion routing is usually broken down into three different nodes. Those nodes include: Node 1 or the entrance tor router, Node 2 or the middle tor router, and finally Node 3 or the exit Tor router. From a biblical perspective we can see the words of Jesus in Matthew 6:1. Jesus says "Be careful not to practice your righteousness in front of others to be seen by them. If you do, you will have no reward from your Father in heaven." (Matthew 6:1, NIV). The verse here is specifically talking about giving to the needy and poor in his community. But I think there can be comparisons made between making a spectacle of oneself so everyone can see what your doing and the latter of doing things in private so that only you and God knows what's going on. With that stated using Tor to do illegal or immoral actions should not use as the bible does not support those actions. With Tor's complicated method of keeping a message encrypted and untouched from other nodes while simultaneously using those nodes as jumping off points to other nodes for further decryption can the network be trusted and is it secure? In the final section we

will look at the security concerns that can arise from this type of routing. For example do different protocols present a vulnerability that could leave the network compromised. For instance POP, IMAP, Telnet, and FTP traffic all over the tor network.

Bibliography

Dingledine, Roger; Mathewson, Nick; Syverson, Paul (2019).Tor: The Second-Generation Onion Router Retrieved from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

McCoy, Damon; Bauer, Kvin; Grunwalk, Dirk; Hohno, Tadayoshi; Sicker, Douglas. (2019). Shining Light in Dark Places:Understanding the Tor Network Retrieved from https://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf

Scharr, Jill (2013, October 13) What Is Tor? Answers to Frequently Asked Questions Retrieved From https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

O'Neill, Patrick. (2013, October 2). The real problem with Tor's security Retrieved From https://kernelmag.dailydot.com/issue-sections/features-issue-sections/13606/tor-arrest-history/

Hoffman, Chris (2017, July 12).Is Tor Really Anonymous and Secure Retrieved From https://www.howtogeek.com/142380/htg-explains-is-tor-really-anonymous-and-secure/

Tor (n.d). In Wikipedia. Retrieved June, 08 2019, From https://en.wikipedia.org/wiki/Tor_(anonymity_network)