Tor Networking Vulnerabilities and Breaches

Niketan Patel

December 14th, 2016

1. Abstract

Tor networking provides an approachable solution for users of The Internet to perceivably remain anonymous. This is done by using the onion routing protocol, a method of encryption that completes a request by encrypting the destination IP address in multiple layers, like an onion, and sending it along to a random series of Tor relays. Tor relays are voluntarily ran by anyone in the world which provides bandwidth to this anonymous network by decrypting a layer of encryption and sending it to the next relay, until the actual IP address is decrypted. The Tor Browser, developed by The Tor Project, is a browser readily configured to access certain onion networks. Therefore, this technology permits people who are doing illicit activity on the internet to have anonymous connections to the network. However, the communications across relay nodes cannot be guaranteed to be anonymous. Furthermore, an onion network is vulnerable at the exit nodes, which is where the final layer of encryption of the payload is decrypted. This paper investigates and analyzes the vulnerabilities of the Tor network, as well as discusses events in the recent past exposing breaches in the security of onion routing.

2. Introduction

With the advances of government regulations and web applications of The Internet come the ability to identify users from every trace of their activity. Government bodies have been mandating that ISPs monitor and analyze data of their internet subscribers in real time so that in the case of criminal investigations, subscribers can be questioned [1]. Furthermore, usage of internet protocols other than HTTP in applications such as email dispatches or IRC channels is polluted with anonymity breaches by nature of hosting systems.

This raises the need for users to be able to communicate among others and visit content on the internet without leaving behind information about themselves, such as geographical locations and IP addresses. In order to achieve such a level of perceived anonymity, users have found the Tor network an approachable solution to conceal their identity as they pursue either licit or illicit activities on The Internet.

However, in spite of the improved anonymity provided by an onion network, multiple hidden services that have been hosted on the Tor network have been busted in the recent years. Hidden services are initiated on the Tor network by configuring servers to only open up connections through onion routing. These services are accessed by its onion address, an address that is not an actual DNS name but one that can be accessed by looking up its respective public keys in a distributed hash table within an onion network [2]. A plethora of hidden services can be found on sites like Reddit, Pastebin, 4chan, etc., and some have been targeted by international law enforcements and taken down by methods that have not been publicized but only speculated upon.

3. To The Community

Throughout the past decade, Tor networking has been utilized and perceived as a simple solution to allow users to connect with other computers while keeping their identity concealed. The Tor Browser has been the go-to tool in order to utilize onion networks. The Tor network can be helpful for users to protect data from unprincipled vendors and to circumvent censorship in over-authoritative countries. Furthermore, the Tor network has established its position in the Dark Web in order to help preserve the anonymity of users that use hidden services hosted on the network. However, despite the level of trust placed on onion networks, traffic can still be analyzed to pinpoint the exact computer connected to a service. Understanding how the Tor network functions is an absolute prerequisite to actually using the Tor network in practice. For the community, this paper outlines how the Tor network functions from a client's standpoint and its respective vulnerabilities, as well as previous breaches of hidden services to convey that Tor does not keep a user invisible on The Internet.

4. The Tor Network

The Tor network is an arrangement of servers that are voluntarily operated in order to direct internet traffic through a random sequence of nodes to help conceal it users communication with other services on The Internet. The name “Tor” is an acronym standing for “The Onion Router”, which is the protocol used to bounce a user’s encrypted request across multiple servers in the onion network. The underlying attribution of anonymity is that upon a user initiating a request via an onion network, the user’s request is bounced around a random sequence of machines interpreting the onion routing protocol. This procedure ends when the request arrives at the exit node, at which point the request is entirely decrypted and sent to the destination [3].

4.1 Tor Relays

Tor relays function as the nodes in the onion network which provide pathways for requests to be relayed among random nodes in the network until it reaches its destination. Tor relays are voluntarily operated [3], and thus the onion network is powered by machines that act as interpreters for the onion routing protocol. When a user initiates a request via the Tor network, the request is encrypted from the user’s machine and sent to an entrance node, which is a Tor relay, in the network [4].

Before it is sent to the entrance node, the request is encrypted in multiple layers of encryption, where each node in the network decrypts a single layer, revealing another encrypted layer which contains information on the next destination of the request. Thus, each relay only has two pieces of information; which node the request came from, and which node it needs to be

passed to next [5]. The important part to note here is that a relay does not have any information about the full path of the request. As noted before, Tor relays are voluntary operated, and thus it is possible for anyone to be in control of a Tor relay. Thus, it's possible that law enforcement agencies host their own Tor relays along with additional traffic analysis technologies. More on this later.

4.2 Onion Routing Protocol

Tor relays pass messages among other relays in an onion network by use of the onion routing protocol, which utilizes asymmetric key cryptography to conceal sender identities. The sender of the message randomly selects a random subsequence of a large set of Tor relays and assembles them into a circuit, which defines the number and order of nodes the message will pass through [5]. The large set of Tor relays is maintained by a select small group of well-trusted onion routers, where each server maintains lists of Tor relay IP addresses and public encryption keys. Server admins of these well-trusted onion routers must approve new Tor relay nodes in order for the relays to join the onion network [6].

Along with assembling the circuit, the sender maintains a set of public keys to pass through the circuit to each node as the connections of the circuit grow incrementally to the next node. This allows for the sender's identity to remain concealed for all nodes in the circuit except for the entrance node. Once the circuit is established by incrementally expanding by one node and by receiving an additional public key from the sender, the response is sent in this same circuit backwards, starting from the exit node since the nodes within the circuit maintain their respective connections [5].

4.3 The Tor Browser

The Tor Browser is a self-contained, portable internet browser developed by The Tor Project that allows users to easily get started with using onion routing among onion networks without needing to install any additional software. The Tor Browser jumpstarts a user's access to onion networks by helping protect both computer and user data when sending information through onion routing. It comes preconfigured with settings that essentially abstract the process of gaining access to directories of Tor relays. It's important to note that the Tor Browser does not protect all Internet traffic of the computer; only traffic that is sent to onion networks via the browser [7].

5. Vulnerabilities in Tor networking

To reiterate, the Tor network does not perfectly keep the user anonymized. It's also very possible for users of Tor networking to misuse the tools to access the onion network and to give away their identity.

5.1 Exit Nodes of an Onion Route

The sender system encrypts message in multiple layers of encryption to send to a random sequence of nodes in a circuit. Each node in the circuit is responsible to peel off a layer (i.e. decrypting a single layer). The last node in the circuit, the exit node, decrypts the final layer and reveals the message essentially in plaintext. At this point, it is dependent on the receiver of the message to require certain encryption formats of messages in order to keep the payload information secure (e.g. TLS or SSL) [8]. This opens up two options for breaches.

The first is if the exit node is a compromised Tor relay, for example if a government agency was successful in listing its voluntary relay in the directory of trusted nodes, then they have access to the entire decrypted message. Note that this message will not contain the original sender's IP address, however it will contain the payload sent along with it. This payload may contain information such as usernames, passwords, bank account information, etc [8]. Thus, getting hands on this payload can eventually identify the user with further exploitation of the exit node.

The second is largely dependent on the receiver of the message. As noted before, the receiver may require payloads to be sent in certain encrypted methods, which will make things

difficult. However, a lot of sketchy services do not require encryption, and thus packets sent from the exit node to the receiver can be intercepted and sniffed.

5.2 DDoS Attacks on Tor Relays

Distributed Denial of Service (DDoS) attacks on trusted Tor Relays would cause traffic within an onion network to be routed to those relays that are not under heavy load. Briefly, DDoS attacks are a type of Denial of Service attack where multiple computers target a single system in order to overload it with requests. Thus, by obtaining a Tor relay list via a simple HTTP GET request to Tor directory nodes, an attacker can target each individual IP within an onion network [9].

Since these would essentially take down these nodes within the network, this would force traffic to be redirected to other nodes that are available in the network. The vulnerability comes into play when these other nodes are setup and operated by government agencies. Therefore, requests that are sent via onion routing are going to be bounced across a combination of multiple infected nodes and other Tor relay nodes. But the high concentration of infected nodes allows requests to be traced [9].

5.3 Timing Analysis of Onion Routed Messages

In order to sent a request through an onion network, a message is wrapped in multiple layers of encryption that is sent across a circuit of nodes, where each node decrypts a layer and only knows where the message came from and where to send it to. Since the reversed path is taken in order to deliver the response of the message, it's possible that analyzing the timing of

the traffic among nodes across multiple ISPs can reveal the original sender coupled with the sender's desired destination [10].

Note that even though the information of the user (IP address, information contained in payload) is encrypted throughout transmission of the onion network, ISPs passively log connections established between servers and computers, specifically the timing, respective IP addresses, and the size of data transferred. Because of the nature of onion routing, there is a sizeable amount of latency from when a request is made to when the response is received. Thus, with some timing analysis on the size of data transferring between multiple computers and the amount of time it takes for that particular size to reach its respective destinations can be used to get a rough path of where the data was passed around [10].

5.4 Misuse of The Tor Browser

A very important detail that is often overlooked by naive Tor Browser users is that the browser itself only protects users from revealing information about themselves within the onion network, not across all Internet traffic on the machine. Thus, there are multiple exploits for this common misunderstanding. One of which is opening or executing downloaded data from the Tor network. For example, word documents or PDFs can contain macros that, upon opening of the document, are executed and make network calls. These network calls will be done outside of the Tor Browser, and ultimately expose the user's IP address and computer information [11].

The selling point for The Tor Browser is that it is a browser that ships with preconfigured settings to jumpstart a user with using the onion network. One of these preconfigured settings is a list of trusted Tor entry nodes, as well as trusted Tor directory nodes to retrieve information about trusted Tor relays in order to send messages across a randomly generated circuit [7]. Thus,

it’s possible for users with unupdated copies of the Tor Browser to contain Tor relays within their preconfigured list that are compromised, since this list is only updated by initially connecting to the onion network.

6. Breaches of Hidden Services on Onion Networks

Throughout the past decade, Tor networking has been utilized to host illicit hidden services throughout corners of the Dark Web. The idea behind hidden services is that the servers that provide these services are configured to only establish connections with other computers within the onion network. Furthermore, these hidden services have an onion specific domain name, which is not one that is registered on the Web's DNS but rather one that is translated via distributed hash tables across multiple nodes of an onion network. There are tons of hidden services that are active today and lists of them can be found on sites like Reddit and Pastebin and sometimes people tweet about some of their findings.

6.1 FBI taking down Playpen

Playpen was a website registered in August 2014 that advertised itself as an image sharing website but was actually a site that distributed child pornography. This site was hosted on the Dark Web within an onion network and had over 200k members. In February 2015, the FBI seized the computer hosting the website (which was in North Carolina), and took control of it for 2 weeks so that they can inject malware into each of the members' responses [12]. This malware came in multiple forms, one of which was sending over video files and upon the video files being opened by the member, a connection would be established to the FBI's computers so they can get their IP.

6.2 Carnegie Mellon University and FBI take down Silk Road 2.0

Silk Road 2.0 is a successor to the original Silk Road, both of which were online black market places hosted on the Dark Web. The original silk road was launched in February 2011 and shutdown in October 2013 by the FBI; Silk Road 2.0 was launched in November 2013 and shutdown in November 2014. The FBI partnered with Carnegie Mellon University's Software Engineering Institute in order to crack down the IP address of the main host service. It is known that CMU operated Tor Relays that tampered with onion messages as the relays received them. It is not publicized exactly what CMU did in order to pinpoint the Silk Road's host service IP address, however it is speculated that since onion network traffic was bounced on CMU operated relays, the relays themselves were able to trace sender and receiver IP addresses by exploiting Tor [13]. As a fun fact, there's currently a Silk Road 3.0 running as another successor.

7. Conclusion

Rapid advancements in technology and its expansive capabilities to fix our daily issues tends to tone down its users priority for privacy. The government and large corporations have started a trend to be able to record tons of information about users of The Internet. However, advocates of Tor networking have been working towards improving the ability of Tor to conceal the identities of its users. Yet, as Tor networking grows stronger, bodies like research institutes and the FBI improve their skills to exploit nodes of onion networks in order to fool users to capture their information. From the breaches discussed, it's evident that Tor networking users can take extra precautions in order to improve their anonymity on the Dark Web. Ultimately, it's at the discretion of Tor networking users in order to control the amount of information they give away about themselves.

8. References

1. "Mandatory Data Retention in United States." Electronic Frontier Foundation. N.p., 2012. Web. 14 Dec. 2016.
2. "Hidden Service Protocol." The Tor Project. N.p., n.d. Web. 14 Dec. 2016.
3. "Overview of Tor." The Tor Project. N.p., n.d. Web. 14 Dec. 2016.
4. "What Is Tor?" Tor Challenge. N.p., n.d. Web. 14 Dec. 2016.
5. R. Dingledine, N. Mathewson, and P. Syverson. TOR: The second generation onion router. In Proceedings of the Usenix Security Symposium, 2004.
6. "Directory Authorities: Possible Upcoming Attempts to Disable the Tor Network." The Tor Project. N.p., 19 Dec. 2014. Web. 14 Dec. 2016.
7. "What Is Tor Browser?" The Tor Project. N.p., n.d. Web. 14 Dec. 2016.
8. Jai, Vijayan. "Researcher Shows Why Tor Anonymity Is No Guarantee Of Security." Dark Reading. N.p., 27 Oct. 2014. Web. 14 Dec. 2016.
9. Gallagher, Sean. "Silk Road, Other Tor “darknet” Sites May Have Been “decloaked” through DDoS." Ars Technica. N.p., 09 Nov. 2014. Web. 14 Dec. 2016.
10. Shmatikov V., Wang MH. (2006) Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses. In: Gollmann D., Meier J., Sabelfeld A. (eds) Computer Security – ESORICS 2006. ESORICS 2006. Lecture Notes in Computer Science, vol 4189. Springer, Berlin, Heidelberg
11. Hutzler, Derek. "Malware Spread Via Tor Exit Node." OPSWAT. N.p., 30 Dec. 2014. Web. 14 Dec. 2016.
12. Russon, Mary. "FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web." International Business Times UK. N.p., 6 Jan. 2016. Web. 14 Dec. 2016.
13. "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds." Motherboard. N.p., 24 Feb. 2016. Web. 14 Dec. 2016.