The Effectiveness of the Tor Anonymity Network

David Gingerich

68-590-K

11/30/2014

Abstract

Recent reports of government agencies monitoring their own citizens' internet activity has led to an increasing demand for anonymity on internet. The purpose of this project is to present the research and findings that relate to the reliability of the web anonymity network Tor. Tor works by relaying public internet traffic to a predetermined set of nodes that hide the original sender and receiver's information from an individual's internet traffic as it travels over the internet. Each Tor node only knows which node the packet came from and where the packet is going. The project explains the core technologies that make Tor work as well as the various attacks that Tor is designed to circumvent. Tor's roots as an anonymity project designed by the US Naval Laboratory intended to protect the identities of government employees working out of hostile territories, to its current status as a non-profit organization is detailed. The reader will be guided through an explanation of how Tor works, as well as how Tor's hidden services allow for a website's physical location to be hidden. The reader is also guided through various examples of when the Tor network's integrity was faulted, as Tor is a common target of various US government agencies such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). Over the last several years many Tor users' identities have been exposed due to various factors that were of their own makings. Many Tor users have been exposed, but the overall integrity of the technology itself has remained intact. While the encryption that Tor uses is a solid technology, it is still an individual's responsibility to be mindful of how they use this technology in order to remain anonymous.

Table of Contents

Chapter 1: Introduction 5

History of the Tor Project 6

Roots as a US Naval Research Project 7

The Beginnings of the Tor Project 8

The Tor Project Today 9

Chapter 2: Core Technologies and Concepts 12

The Internet 12

TCP/IP 13

Transport Layer Security (TLS) 14

Onion routing 15

SOCKS 15

Diffie-Hellman Handshake 15

Chapter 3: How Tor works 17

The Inner Workings of Tor 17

Rendezvous points and hidden services 20

Tor Browser Bundle 21

Chapter 4: Attacks on the Tor Network 23

Attacks that Tor is designed to thwart 23

Man in the middle 23

Eavesdropping attacks 24

Traffic analysis 25

Attacks that Tor is susceptible to: 26

Cryptanalysis 26

Denial-of-Service Attack 26

Real-world Examples of attacks on the Tor Network 27

The NSA and the Edward Snowden Documents 27

FBI's Use of Drive by Downloads to Expose Tor Users 29

FBI Raid of Freedom Hosting 31

Silk Road 32
The Heartbleed Bug 35
Bitcoin Proof of Concept Exploit 36
China and Tor 38
Summary of Tor's Vulnerabilities 39
Chapter 5: Conclusion 40
Bibliography 43

Chapter 1: Introduction

Online privacy advocates appreciate Tor, law enforcement agencies have a tenuous relationship with it. Many US government agencies use it to hide their identities in hostile foreign countries while the Russian government has an $111,000 bounty open for anyone who can crack Tor. Regardless of what side someone is on, it is clear that the web anonymity network Tor has been making headlines over the past year or two. Tor works as a relay network that operates on top of the public internet and is based on a technology called onion routing. Tor is used for averting eavesdropping attacks and traffic analysis. It does this in real-time through bidirectional connections that keep the sender and receiver anonymous over a public network and are transparent to the applications that Tor is being used for [1].

Tor is run as a client on an end-user's workstation, and connects to the Tor network using a supplied list of Directory servers that determines its network path across different Tor relays. The Tor Proxy on the user's machine connects to an entry node and negotiates an encryption key, and the entry node negotiates a key with the next tor relay, and so on until the last key is negotiated with the exit node which sends the payload to the user's destination. These keys are sent back to the user's Tor proxy which layers the different keys and hides the sources and destination of each hop from the public network – the destination never knows where the packet really came from and assumes it originated from the exit node. The layers in question are like that of an onion – hence the name onion routing [2].

Tor is often used by privacy advocates, individuals in countries that monitor internet traffic, as well as criminals. The result of criminals using Tor has resulted in Tor being a prime target for law enforcement agencies all over the world. Russia's official stance for offering the $111,000 reward to anyone who can crack Tor's encryption is that Tor violates national security.

The NSA is also doing extensive research in regards to exposing Tor users [3]. Tor makes it possible for users to host hidden services such as web sites. These are sites that end with the .onion domain, and their physical addresses are untraceable. While many human rights activists use these to hide their identities, they are also used for drug trafficking, and child exploitation – these sites are grouped in a category called the *Dark Net* [4].

The purpose of this capstone project is to introduce the reader to the background and history of the Tor project and details its inner workings to provide an understanding of why this approach to web anonymity may or may not work. The reader will then be presented with a series of real-world examples of when the Tor network's integrity was at stake. Being a target of US government agencies such as the NSA and FBI, many Tor users have been apprehended for performing illegal activities while using the network. Many of their identities were exposed as a result of social engineering and not any inherent flaw in the technology itself [5]. The benefits and downfalls of Tor are presented together to show a complete picture of the true effectiveness of Tor.

History of the Tor Project

The roots of Tor began as a project developed by the US Naval Laboratory; the Tor project has come a long way since them. What was once closed to all but a select group of government sponsored researchers is now an open sourced project with volunteers all over the world. Even though the project is open sourced it is still heavily funded by the US Government. The following section introduces key individuals behind the project's development, the motivations behind the project, and how an obscure government sponsored project became an open source collaboration that trumps others like it.

Roots as a US Naval Research Project

Tor was preceded by research in Onion Routing by a group of military mathematicians and computer system researchers that began in 1995 by the Office of Naval Research in an effort to solve the problem with traffic analysis to allow military and intelligence personnel to perform their duties in hostile countries without the possibility of being discovered. The research was led by Paul Syverson, Michael Reed, and David Goldschlag. A number of different ideas were considered, with many being rejected and an even smaller number being rejected but considered in the development of the Tor project. In 1996, the first publicly accessible onion routing network was put into place and was hosted on a series of naval systems as a demonstration of the concept. In 1997 the project received additional funding by the Defense Advanced Research Projects Agency (DARPA) [6].

During testing, a problem arose with only US intelligence using the network, since it allowed for a third party monitoring traffic to easily deduce that all traffic going through any Onion Routing node belonged to US intelligence. To counter this, it was decided to diversify the traffic by opening up the Onion Routing network to the public. This allowed for any US intelligence traffic to simply blend in with privacy advocates, criminals, and among all groups using the network. The consequence of the decision to open the network up was that they now had to move the nodes away from naval intelligence networks and design them in a way to allow anyone to host a node even from a home PC. In 2002 the project shifted towards a different direction and was crowd sourced with volunteers from all over the world. MIT grads Roger Dingledine and Nick Mathewson joined the project as contractors for DARPA and the U.S. Naval Research Laboratory's Center for High Assurance Computer Systems. They began

researching the changes on the Navy's Onion Routing research program for what later became Tor. The overall goal of the project was to bring the concept of Onion Routing to the general public [7].

The Beginnings of the Tor Project

Dingledine and Mathewson started adding in changes to the original design in order to improve several aspects of the project. These changes included implementing perfect forward secrecy**.** The original design used a single multiplied encrypted data circuit to lay each circuit, which allowed for a single hostile node to record traffic, forcing the successive nodes to decrypt the traffic. The updated design uses an incremental path building design where each node negotiates session keys with the next hop in the circuit. Congestion control was another improvement implemented. The result utilized a decentralized system that detects congestion and flooding while maintaining anonymity for the users. Tor also made use of directory servers. The original design flooded the network with information regarding the locations of available nodes. Now, Tor uses signed trusted directory servers to provide Tor clients with the addresses of directories with known routers along with their current state. End-to-end integrity checking was implemented in the updated design as well. Originally there was no integrity checking, which allowed for an attacker to modify connection requests to connect to different servers and flag encrypted traffic. The design change also ensures that Tor verifies all data before it leaves the Tor network. Configurable exit policies were added that allowed for Tor exit node volunteers to have their options in regards to what type of traffic their nodes will route. For instance, if a volunteer is uncomfortable with SMTP traffic because of the possibility of their Exit node being used for e-mailing unwanted spam messages, they have the option to reject that traffic. And

rendezvous points allow for hidden web services. The allowance for the so-called *Deep Web*, or *Dark Net* sites to be hosted. These are sites whose web server connects to a series of rendezvous points connected through a Tor connection, which hides their physical location.

In 2004, when Tor was ready for deployment, the US Navy cut most of the funding. The Navy released the source code under an open sourced license and handed control to the Electronic Frontier Foundation (EFF), a nonprofit organization formed in 1990 that defends civil liberties in regards to technical practices. The Tor Project transitioned into a non-profit organization with 501(c)(3) status. When the EFF announced its support, it failed to mention Tor's military roots and only focused on Tor's ability to protect free speech. The EFF later mentioned the military roots but downplayed them in brief mentions while maintaining a stance that the US government no longer has any involvement in the project. Despite their lack of involvement, per tax documents, the federal government provided a large portion of the Tor Project's funding through various grants. For instance, more than half of the project's revenue in 2012 came from over one million dollars in US government grants [7].

The Tor Project Today

Today the Tor project is headquartered out of a one-room office of a YWCA, a transition house for victims of domestic abuse, in Cambridge, Massachusetts. The project has 33 core employees with nine being full time employees. The majority of team members work remotely with only a few that work out of the office in Cambridge. The Tor Project's current Executive Director is Andrew Lewman, who manages the day to day business operations. He began participation as a volunteer in 2003 as a code developer for the project. At the time he was working for a company based out of China who was looking for affordable methods for averting

China's increasingly evasive censorship tools. In 2009, he took on the position as Executive Director of the Tor Project. Lewman's interest in Tor and web anonymity peaked in the early 2000's when he was working for an internet marketing firm that sent mass marketing e-mails. One of the recipients of these e-mails grew irritated by them and found Lewman's name on the company's web site. He proceeded to track Lewman down and threatened to harm him and his family before he showed up at Lewman's office where police needed to be called. Lewman also works with the transition house the Tor Project shares office space with and instructs victims of domestic violence how to hide their identities online.

The project also is composed of hundreds of volunteers from all over the world who work on solving problems such as circumventing China's censorship systems. The current Tor network is composed of over 5000 computers serving as Tor relay points and over four million people have used it, with an average of 300,000 people who use it daily. Tor is used by a wide variety of people that range from Iranian activists eluding government censors to share images and information about the 2009 protests of that year's presidential election all the way to Chinese citizens who use it to get around the country's firewall that blocks everything including social networking sites including Facebook as well as international news organizations such as the *New York Times*. Tor is also used by individuals who use it to share child pornography, coordinate terrorism, and sell and trade drugs. Tor project supporters feel that the press tends to only point out the negative uses of Tor, such as when someone gets away with downloading child pornography, rather than the more positive uses such as protecting the identity of a victim of domestic abuse using the service to anonymously report their abuser.

Going forward, the project aims to gain more funding as well as increase their number of volunteers. The project is also working towards improving Tor's public image by shying it away

from being a tool to avoid government surveillance and using it to perform illegal activities, to a tool that protects one's physical well-being and civil liberties. Currently, the project is working towards increasing bandwidth on the Tor network by working with universities to serve as nodes. Their goal is to use the increased bandwidth of public universities to improve the performance of the Tor network. The Tor development team is also currently working out additional flaws and concerns with a goal of having businesses host Tor nodes as well. Currently very few large companies are hosting Tor nodes as many are concerned that Tor is not a finished product [8].

Chapter 2: Core Technologies and Concepts

Tor, like any networked application, does not work by itself but rather with many different technologies. For instance, an understanding of how the Internet works is a key concept of why Tor exists in the first place. Working together with these many different technologies also are the source of Tor's problems. The result of these many different points of failure presents many different points of exploitation.

The Internet

The internet's purpose is to connect devices of all sorts from across the globe. These devices use an internet service provider (ISP) to transmit their data in pieces called packets through a series of communication links and packet switches. The data is reassembled at its final destination. Due to the costs, ISPs are unable to connect directly to every other ISP as it requires a connection to every service provider on the Internet. Instead, ISPs charge fees to other service providers to connect to ISPs they do have direct connections to. These charges are based on the amount of traffic the destination service provider receives. Internet service providers are categorized as Access ISPs, Regional ISPs, and Tier-1 ISPs. Access ISPs provide access on the consumer level. Regional ISPs connect small Access ISPs together to connect to Tier-1 ISPs. Tier-1 ISPs provide the backbone of the internet and work on a global level and connects these Regional ISPs to the wider Internet.

In between ISPs are a number of connection points that include Points of Presence (PoPs), peers, multi-homing, and Internet Exchange Points (IXPs). PoPs are groups of routers that connect Access ISPs to Regional ISPs. Multi-homing points connect multiple ISPs to each

other. Then there are peers, which are two ISPs with connected networks for the purpose of traffic control. Finally, there are IXPs where multiple ISPs can peer in a group. See Figure 1 for a diagram of these connecting points. With all of these points of communication it is understandable that Internet traffic does not simply travel from point A to B, but rather to and from a number of points where it is questionable who has access to what traffic [9].

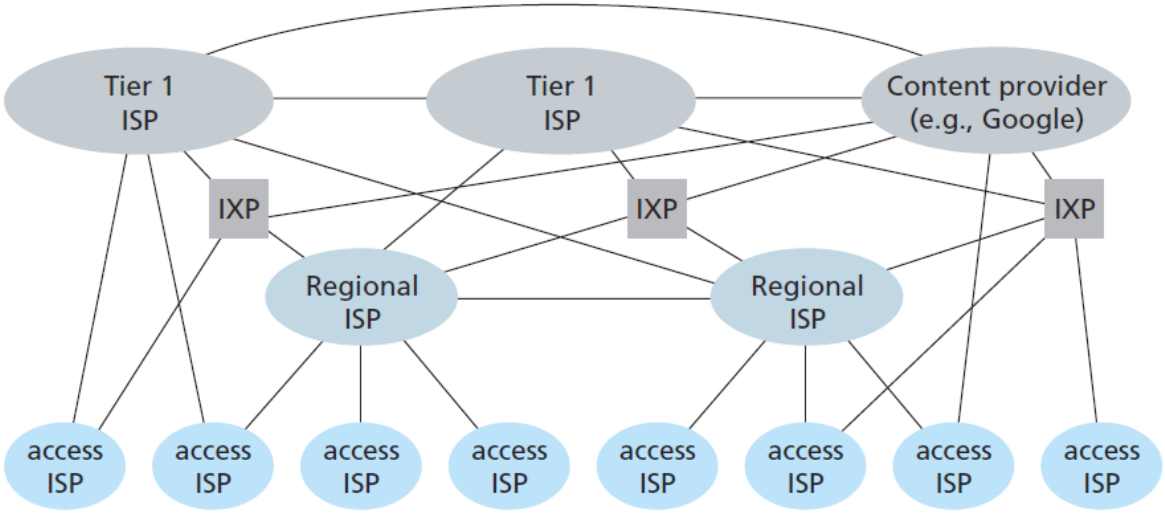

Figure 1. Interconnection of ISPs

TCP/IP

TCP/IP started out as a Department of Defense sponsored research project to connect a network of networks, which later became the Internet. TCP/IP is the series of protocols that control how sending and receiving packets of information over the Internet work. Traffic is broken down into packets to give it a higher chance of reaching its destination. Routing is designed so if one network link goes down or is congested then the preceding router will calculate a new routing path.

TCP is responsible for ensuring packet delivery, and IP is responsible for sending packets to various nodes before they arrive to their destinations. The data can be carried over a number of mediums such as Ethernet, fiber, coaxial, or wireless. To differentiate between devices and locations, each device (whether is a PC, tablet, mobile device, or router) is designated a unique four byte number called an IP address. These addresses can either be assigned internally for devices within a network, or externally for devices that can be reached from the Internet, such as a router or network firewall [10].

Transport Layer Security (TLS)

Transport Layer Security (TLS) is used for securing online communications that involve sensitive data. It provides confidentiality through the use of symmetric encryption, and message integrity through the use of message authentication codes (MAC). Developed by the Internet Engineering Task Force (IETF), an open international community of technical experts that develop standards used on the Internet, in an effort to standardize the similar protocol, Secure Sockets Layer (SSL). TLS includes mechanisms that enable two end points using TCP to determine the encryption algorithms and services that will be used beforehand by using the TLS Record and TLS Handshake protocols.

The client machine initiates contact with the server, requesting several pieces of key information such as what encryption protocol will be used, and the server responds with that information. Then the server exchanges the session key that is used to encrypt the data sent from both the client and server. The server and client then verify that all information in regards to the choice of encryption has been exchanged. When the secure communication is finished, the client

and server send messages verifying that the connection is over [11].

Onion routing

Onion routing provides real time anonymous connections from a sender and receiver over a public network like the Internet. Onion routing is designed to avert network eavesdropping and traffic analysis. It works under the application layer, making the connection transparent to the program itself. The name is in reference to the traffic being wrapped under several layers and being unwrapped as they travel along the circuit. It is the technology that the Tor project is based off [2].

SOCKS

Developed by David Koblas, SOCKS is a proxy interface that allows most TCP-based applications to route their traffic through Tor without modification. SOCKS basic design makes it efficient when developing network applications that may need to connect through a proxy. The proxy library provides a mechanism to hide internal systems through a transparent proxy that operates at the TCP level through the SOCKS library [12].

Diffie-Hellman Handshake

The Diffie-Hellman Handshake is a protocol that allows two parties to set up a shared key over an insecure communication channel, such as the Internet, so they can exchange messages that can be viewed by a third party. Tor uses the handshake to initiate TLS connections. The shared keys are exchanged by the sender requesting the public key of the receiver, which is retrieved in clear text. The sender encrypts a message with the sender's public

key and sends it to the receiver. When the message arrives the receiver decrypts it with the private key [1].

Chapter 3: How Tor works

Now that the reader is familiar with the concepts that make Tor possible, it is now essential to explain the inner workings of Tor. A number of steps have to be performed in order for a Tor user to maintain their anonymity, which includes multiple handshakes and three layers of encryption to name a few. The designers of Tor decided to make the process both simplistic and transparent. They believed that this allowed for increased usability, and the more users on the Tor network the more secure it is. The following section covers the inner workings of Tor, hidden services, and the Tor Browser Bundle.

The Inner Workings of Tor

Tor works as an overlay network, a network that is built above another network. It is a series of Tor nodes that are also referred to as relays or Onion Routers (ORs), which are used to route traffic between each other over the public internet. Onion Routers maintain TLS connections with other ORs, and with user's Onion Proxies (OPs). An OP is run from the user's local computer and maintains connections and updates with directory servers, establishes the circuits across the network, and handles the connections to the user's applications. TLS is used to encrypt the data on the connection and provides perfect forward secrecy to prevent attackers from tampering with data or spoofing an OR. Each OR has a long term-identity key used to sign TLS certificates, router descriptors, and directory updates. ORs also have short term onion keys for decrypting user requests when configuring circuits and negotiating ephemeral keys, keys that are established for each new connection. These short term keys are rotated periodically to prevent key compromise.

Tor traffic is passed along the public internet in cells set to a fixed size of 512 bytes. Each cell consists of a header and payload. The header contains a circuit identifier (circID) and a command used for instructing the Tor node what to do with the cell's payload data. The circID specifies the circuit that the cell relates to as many different circuits can be on the TLS connection on an OR. The command in the cell's payload dictates if the cell is a control or relay cell. A control cell is information that relates to the configuration of a circuit path between the user's OP and each Tor relay, the exit node, and the cell's final destination. A relay cell is information regarding the cell's payload information after the circuit has been created, such as when the relay begins and ends.

Tor circuits are shared by multiple TCP streams. Each circuit is constructed beforehand by the user's Tor client. Circuits are rebuilt once per minute and expire after they have been used or are no longer holding any open streams. The user's OP constructs circuits incrementally, and negotiates symmetric keys with each relay, one hop at a time. A new circuit starts with the OP requesting a create cell with the first node in the path and they negotiate a new circID that is not in use. The cell's payload contains the first half of the Diffie-Hellman handshake encrypted to the Tor relay's onion key. The relay replies with a cell confirming the creation of the circuit with a hash of the negotiated key. When the circuit is established, the OP and relay can send cells to each other using the negotiated key.

The OP then extends the circuit by sending a relay extend request to the first relay with the IP address of the next relay and another negotiated key. The first relay creates a new circID for use between itself and the second relay. The OP never needs to know this key. The first relay associates this connection only between the OP and the second relay. The second relay responds to the first relay with a confirmation that the circuit has been created. The first relay wraps this

payload with its own key and sends it back to the user's OP. The OP then extends the circuit between itself and a third relay and so on telling each successive node to extend one hop further. Normally there are only three hops created in the circuit, two relays and one exit node.
After the OP has established a circuit and their keys have been shared with each OR, they can begin to send relay cells.

When a Tor node receives a relay cell it looks up in the corresponding circID. It then decrypts the relay header and payload with the session key it established with that specific circuit. When a cell is going outbound it is first checked for integrity. If it passes, it is then processed accordingly by unwrapping header and payload with the session keys. The OR looks up circID and sends to next OR. The circID field is updated with the circID of the next destination. In the event the relay at the end of the circuit receives an unrecognized cell, it tears down the circuit using the destroy signal. Tearing down circuits is similar to the process of creating them as it's done incrementally.

Tor will start a connection with an application, such as a web browser, mail client, or SSH client, that is configured or preconfigured to use Tor through the SOCKS proxy library. It requests a new connection by the Tor client choosing the last circuit that it established and chooses an OR whose rules allow it to become an appropriate exit node, as exit nodes can be configured to block certain traffic.

The OP ends a stream by sending a relay message to exit node. When the message is received from the exit node, the Tor client notifies the application that the connection was established and it will now route the data from the application and repackage it as relay cells to send it along the circuit. A stream can be closed two ways, by either a two-step handshake for a normal stream, or with the relay end command. This also allows for Tor to use applications that

require half-closed connections. Tor can close connections with a one-step handshake when there are errors with the relay teardown command [2].

Rendezvous points and hidden services

Rendezvous points allow users to host location hidden services such as web servers. The advantage rendezvous points provide is they do not reveal the real IP address of the server, allowing the server to hide its physical location. They are often used to host web sites that host illegal content such as drug trading or child exploitation. Legitimate uses include protecting sites from DoS attacks or hosting blogs that expose human rights violations. Web pages that host illegal content are referred to as Dark Net sites.

A hidden service is hosted on a web server that is configured with an OP. The web server is unmodified and unaware that it is hidden behind a Tor network. Only the OP knows the hidden server's real IP address and location. The hidden service generates a long term public key used to identify its service in the form of longtermkey.onion. The hidden service advertises its location to several ORs, referred to an introduction points. The hidden service's OP anonymously advertises these introduction points by signing the advertisement with its public key. Furthermore, the hidden service uses this same public key to add more introduction points for its server and periodically refreshes its entry in the lookup service. The hidden service then configures a three hop circuit to each of the introduction points and tells them to be on standby for any requests to access the hidden service. A Tor user who wants to connect to a hidden service obtains the long term key address to connect to the lookup service. The user then connects to the Tor network with their Tor client, which then connects to their rendezvous point (RP). The user builds a circuit to the RP which randomly connects the user's Tor client to one of

the hidden services' introduction points using a rendezvous cookie to recognize the hidden circuit.

Once the user opens the circuit to one of the hidden services' introduction points, the Tor client sends a cell to the hidden service encrypted with the hidden service's public key which contains information about the user, such as the RP and rendezvous cookie they were issued. The user and hidden service then complete the Diffie-Hellman handshake and share a hash of the session key. The RP then connects the user's circuit to the hidden services circuit. The RP is never aware of the sender or destination and is unable to see the data being transmitted. The user's Tor client then sends a relay begin cell to the hidden services OP which completes the connection to the physical server hosting the hidden service [2].

Tor Browser Bundle

The Tor Browser Bundle (TBB) is a software suite that provides a user friendly method for running Tor from a desktop operating system such as Windows, OSX, and Linux. The bundle contains a modified version of Firefox, Torbutton, Tor Launcher, and the Firefox add ons NoScript and HTTP-Everywhere. Previously the software also contained Vidalia, a control panel for Tor, but it has since been removed in newer versions, although it is currently available separately. The version of Firefox that is packaged in the bundle is called Firefox Extended Support Release (ESR), which is a version that only receives security and stability updates. This version is packaged as it is considered more stable than the normal Firefox releases due to its lack of extra features. The Firefox add on NoScript is a browser plugin that prevents running scripts and programs from untrusted web sites as there have been attacks revealing the identities of Tor users using JavaScript. The other browser add on, HTTPS-Everywhere, is used as added

security that enables secure connections to websites that normally have secure connections available but not enabled by default [13].

Chapter 4: Attacks on the Tor Network

Tor is used by criminals and political activists alike. Because of that, this makes Tor a target for governments and law enforcement agencies all over the world. While Tor is designed to prevent network eavesdropping, many government agencies will spend much of their resources to expose Tor users using a variety methods both of the technical nature as well as those that involve social engineering. This section will outline the types of network attacks that Tor is designed to thwart, followed by real world examples of when the Tor network's integrity was at risk.

Attacks that Tor is designed to thwart

Man in the middle

A man-in-the-middle attack is when an attacker forges a response from a legitimate communication and replaces it with theirs. They are performed by giving the appearance on a network that two machines are communicating when in reality one or both are communicating with the attacker. The TLS encryption protocol that Tor uses is designed to thwart these attacks. It is possible for the attack to occur between the exit node and the destination where the traffic is sent in plaintext. A man-in-the-middle attack is outlined in Figure 2 below [1].

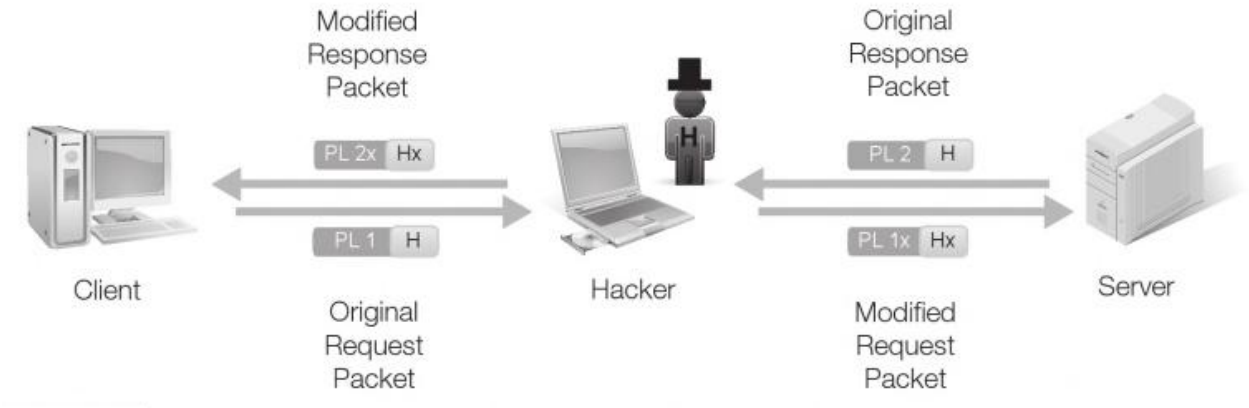

Figure 2. Man-in-the-middle attack coercing a client into initiating a session with a hacker instead of the destination.

Eavesdropping attacks

A network eavesdropping attack is when an attacker listens in on a communication over a network. This is commonly performed by using network packet sniffing devices or software. Packet captures are viewed in software such as Wireshark that allows for reassembly of packets. If the traffic was in plaintext it can be viewed with ease. If the traffic was encrypted it can be decrypted with much time and effort, but the sender and receiver portion of the packet are visible. Tor circumvents even dropping attacks by encrypting all traffic between the user and the first Tor node. The only part of a Tor transaction that would be in plaintext and visible to a network eavesdropper would be the traffic between the exit node and destination. An eavesdropping attack is outlined in Figure 3 below [14].

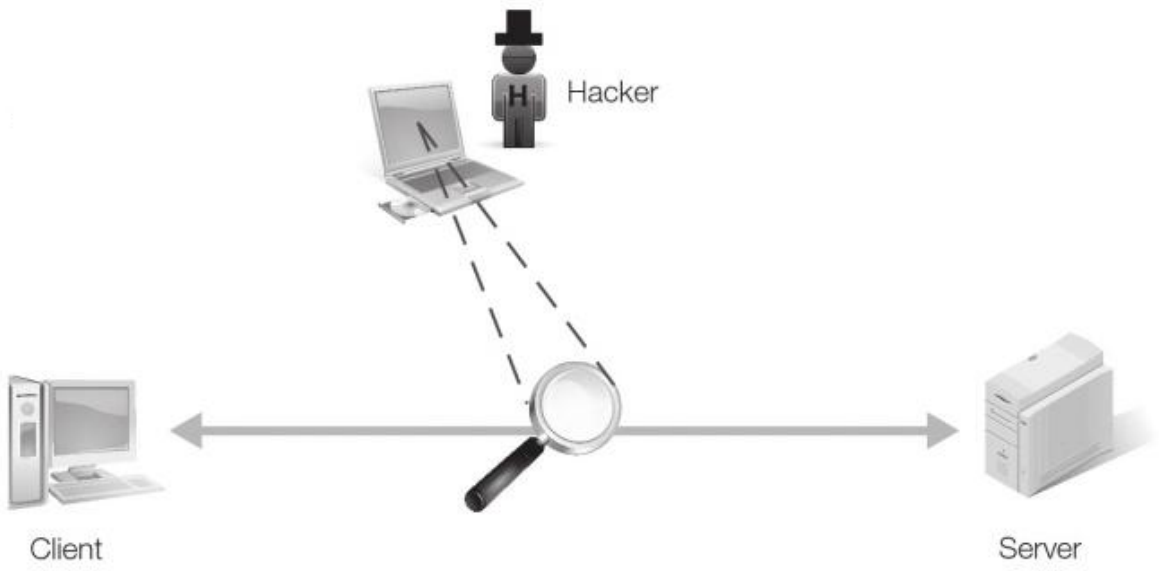

Figure 3. Eavesdropping attack on an existing session between a client and server.

Traffic analysis

Traffic analysis is the process of deducing where network traffic is originating from and going to. The origin and destination are figured out even if the traffic is encrypted. Traffic analysis is often performed by law enforcement agencies, and is what Tor is designed to circumvent. By Tor hiding the sender and receiver information between Tor nodes, this prevents a third party from performing traffic analysis from viewing the true sender and receiver IP addresses in Tor traffic [15].

Attacks that Tor is susceptible to:

Cryptanalysis

A cryptanalysis attack is when an attacker (or cryptanalyst) works to understand the nature of an encryption algorithm in an effort to figure out the plaintext or key for an encrypted message. If the attack is successful then all messages using that key can be compromised [16]. Tor is a target of cryptanalysis attack because it heavily relies on various encryption algorithms such as the Diffie-Hellman handshake. Security Researcher Rob Graham has speculated that the NSA has the capabilities of breaking Diffie-Hellman keys that are as long as 1024-bits, which is a common key length of a Tor transaction. In the event that a Tor circuit's encryption key is broken the Tor user can be de-anonymized and the traffic could be read in clear text [17].

Denial-of-Service Attack

Denial-of-service attacks (DoS) deprive users or organizations of services or resources that are available under normal circumstances. The attack can be performed with a variety of methods such as flooding a resource with data or sending malformed packets that are known to crash a server [1]. Users of Tor's hidden services often times use them in an effort to hide their server's real locations in an effort to avoid DoS attacks [18]. It's also been assumed that denial-of-service attacks were used to reveal the locations of the hidden servers in the FBI's November of 2014 raid [19].

Real-world Examples of attacks on the Tor Network

The NSA and the Edward Snowden Documents

Tor came to public prominence in 2013 with the Edward Snowden leaks. Snowden, a former NSA employee, disclosed a number of top-secret NSA documents including several revealing the agencies attempts at de-anonymizing the identities of Tor users. Ironically, the Tor Project receives the majority of its funding from the Department of Defense which houses the NSA. Regardless of these contributions, the NSA still devotes a great deal of resources to attempts at attacking the Tor network's integrity due to its use by terrorists, drug dealers, and pedophiles. One document, a PowerPoint presentation titled "Tor Stinks" details how the fundamental security of the Tor network is reliable and how the NSA is unable to decrypt traffic at every turn unless they were to control all three of a Tor sessions' relay points which is beyond the scope of what the NSA is capable of doing. The agency can uncover a small fraction of users through other means. For instance, the agency exploited a vulnerability in Firefox, which is prepackaged with the Tor Browser Bundle, which allowed the agency to install software running without the user's knowledge or consent. This software gave them access to the target's file system, monitored keystrokes, and analyzed web browsing habits [20].

NSA spokesperson Vanee Vines, counters that the NSA is not doing its job if they were not trying to decrypt Tor traffic and de-anonymize its users. In addition, the agency has tried to reconstruct encrypted packets to trace reveal Tor users by monitoring relays. The approach was not worth considering because all three Tor nodes in the circuit would have to be a part of a set of nodes that the NSA would have access to monitor. The agency has access to so few it is believed that there is a low probability that this approach will work [8].

The NSA's attacks on the Tor network's integrity have made privacy and human rights groups concerned. While the NSA has admitted in the leaked documents that it has yet to compromise the network or has had any success in de-anonymizing a particular Tor user on a specific request, these documents do reveal they have experimented with several proof of concept attacks. These proof of concepts include the agency taking over a large number of Tor exit nodes and monitoring traffic for patterns going in and out of the network. This proves difficult as the NSA has access to very small percentage of exit nodes and there are no indications that they have ever exposed identities of Tor users doing so. Another presentation from the Snowden leaks titled "Tor: Overview of Existing Techniques", suggests the NSA shaping and influencing the development process of the Tor Project, measuring the timing of messages going in and out of the Tor network in an effort to identify users, and efforts to disrupt the Tor network in hopes of users abandon using Tor all together. One of the more successful efforts the NSA used to expose Tor users involved exploiting a vulnerability in Firefox, the browser of the Tor bundle. The NSA detailed this attack in presentation called "Peeling back the layers of Tor with Egotisticalgiraffe". The exploit took advantage of a vulnerability in older version of Firefox. The Tor Browser Bundle had no mechanism to automatically update, and this left many Tor users vulnerable. The exploit later was used by the FBI in exposing users visiting child exploitation websites.

There have been many legal questions in regards to the NSA's actions. These include the question of if the NSA is purposely acting against Tor users based out of the United States as Tor is designed to hide the originating country of the user. Also, attacks involving infecting malicious code on the computers of Tor users may impact innocent people such as journalists or researchers. While the NSA does acknowledge Tor's uses for general privacy and use in

countries where the internet is censored, they still show no signs of relaxing their efforts in exposing the law breaking side of the service [20].

FBI's Use of Drive by Downloads to Expose Tor Users

The FBI has used rogue tactics to expose the identities of Tor users. The FBI has implemented drive-by downloads, this is when the agency takes control of a high trafficked website and modifies its code to allow the installation of malware on its visitor's workstations [21]. The FBI calls their drive-by download malware campaigns NITs, which stands for network investigative technique, and they have been in use since at least 2002. The FBI uses drive-by downloads in cases where users conceal their real locations using services such as Tor. Drive-by malware can be heavy in terms of code where it can do as much as grant law enforcement access to a user's files, location, web cam, and web history and continue to monitor the target for months, but they can also be small applications that run once and delete themselves after they've sent a law enforcement agency a target's computer name and actual IP address.

Drive-by downloads were originally performed by hackers for the purpose of stealing personal information such as credit card numbers and passwords, but are now being deployed by government agencies for the purpose of gaining the identities of Tor users. The use of drive by malware exploits has resulted in dozens of Tor users being arrested for possession of child pornography, drug dealing, and extortion. The Department of Justice has downplayed the steps it has taken to arrest the individuals by using the same techniques as criminals through the use of drive by malware attacks.

The FBI's solutions to cracking down on online child exploitation led to the development of Operation Torpedo (a portmanteau of Tor and pedophile). The investigation began with the

Netherlands national police writing a web crawler that indexed sites on the Dark Net to find as many .onion sites as possible. They visited each site and noted those that were hosting child pornography. The Netherlands' national police obtained search warrants and began the process of finding the actual physical locations of these hidden servers. While they considered the task laborious they did a find a site in which the owner left the administrator account password blank.

They were able to log in and find the servers real IP, which lead them to Bellevue, Nebraska. The Netherlands national police then forwarded this information to the FBI who found the identity of the owner of this site, Aaron McGrath, revealing that he actually hosted three child pornography sites, two from his server farm at his place of business and one from his home. The FBI spent the next year on full time surveillance activities on McGrath as they began to organize their course of legal action they would take before raiding his server farm and his home.

Three different search warrants were signed for each of McGrath's servers which would authorize authorities to modify McGrath's sites to add code that delivered malware to the sites' visitors. The warrants also authorized the FBI to delay any notification to the targets for 30 days after the malware was deployed. The FBI later used this 30 day grace period as justification for using the malware in order to identify their targets. In November of 2012 federal authorities raided McGrath and took custody of his servers. The malware was written to only identify the user and within two weeks the FBI had collected a number of IP and MAC addresses from visitors of the sites. With the IP addresses in hand the FBI was able to identify a number of users and coordinated raids to their homes in April of 2013. A defense lawyer for one of the suspects argued that by not informing the suspects for more than a year that they were under surveillance, their Fourth Amendment rights were violated.

The US Magistrate Judge Thomas Thalken rejected the idea of the government acting in bad faith by pointing out that the warrant were prepared with the assistance of legal counsel from various levels of the Department of Justice and not a rogue FBI agent out to target any particular individual. Christopher Soghoian, a representative of the ACLU, has pointed out that it is difficult for a suspect to justify visiting a child pornography web site for any reason and that the drive-by malware is the FBI's best use of catching suspects who conceal their identities with tools such as Tor. There is still debate on whether or not government agencies use drive-by downloads to apprehend innocent people visiting sites that are not illegal, such as jihadi forums. Soghoian also points out that in many cases judges who sign search warrants that involve the use of drive-by malware are unaware of that fact that these applications breach an individual's security defenses on their personal computers through the use of software exploits, as these warrants lack the proper language that states so [22].

FBI Raid of Freedom Hosting

Freedom Hosting was a Dark Net hosting service known for its reputation of tolerating sites that hosted child pornography. In July of 2013 Freedom Hosting operator Eric Marques was arrested in Ireland and now faces child pornography charges from the US government. After Marques' arrest, the FBI took control of his servers by cloning and relocating them at the FBI headquarters in Maryland. They proceeded to modify the website's code so that it executed instructions to install malware on the visitor's PC. In August of 2013, users began to notice a hidden iFrame, a web site within a website, embedded in several web pages hosted by Freedom Hosting. The iFrame loaded a small piece of Javascript code that exploited a memory

management vulnerability in Firefox. Upon further investigation it appeared that the code was targeted towards users browsing using the Tor Browser Bundle.

The malware was a variant of a small Windows based exploit called Magneto which gathered the target's MAC address and Windows name. It then sent the information back to the FBI using their real IP address. What also served as a concern, were the reports of the malware on non-criminal websites. This includes Tormail, which provides a service for protecting the identities of users in countries that censor the internet. The Tor Browser Bundle at the time had no mechanism to automatically update the browser for the user and this allowed for the FBI to take advantage of a long since patched security vulnerability in the Firefox web browser. Because of the Freedom Hosting attack the Tor Project has since begun development of solutions to silently update the Tor Browser Bundle [4].

Silk Road

In October of 2013, two months after the Freedom Hosting raid, the FBI orchestrated a takedown of the online drug market Silk Road. The FBI had difficulties as it took years to track down the physical server due to it running as a Tor hidden service. Silk Road's administrator, Ross Ulbricht, a graduate researcher in material sciences at Pennsylvania State University, was arrested on charges of money laundering and narcotics trafficking. The department also seized over three million dollars in bitcoins, a cryptographic currency that was used to buy items on Silk Road. It is estimated that Silk Road was making between $30 and $45 million in revenue per year but it turned out that it was more in the range of $1.2 billion which was determined after the raid and was based on seized documents. After the raid, an unnamed spokesperson for the FBI declared that nobody is beyond their reach and they will find them.

Ulbricht did not create the site, but rather inherited it from another individual for an undisclosed sum. Ulbricht touched base with the original owner after pointing out several of the sites security flaws. Before his arrest, Ulbricht touted in an interview with Forbes that the use of Bitcoins combined with Tor has allowed them to circumvent the war on drugs. Ulbricht also began to make efforts to bring Silk Road into the mainstream by hosting a version of the site that allowed visitors to view the site's content without the use of Tor. Ulbricht's attitude at that point was that there was so much awareness of the site that hiding in plain sight was no longer necessary.

While the FBI did not reveal how they exposed Ulbricht's identity, they did hint they found him through a" simple mistake" that he made, despite his careful and persistent use of services like Tor and VPNs. It is believed that they found him through the interception of a package that contained fake identities that was addressed to a location in San Francisco that he was associated with. Investigators matched his face with the photographs on one of the many fake IDs. Ulbricht also made the mistake of making public the IP address of one of the VPN services he used in the Silk Road website code, as well as positing on a web forum that revealed his time zone. It is also speculated that the FBI may have hacked into Silk Road by sending unexpected commands to the server to force it to give up its physical location. Many of the sites frequent visitors lamented the closing of site, with several blaming Ulbricht for calling too much attention to the site by doing mainstream interviews such as the piece he did with Forbes [23].

In addition to Ulbricht's arrest, several Silk Road administrators were arrested, as they were required to give proof of identity to Ulbricht, information that was obtained by the FBI during the raid on Ulbricht's home. Vendors using Silk Road have also been targets of law enforcement since the sites inception. In January of 2012, a heroin dealer using the site was

arrested after a number of shipments were intercepted over a six month period. Many of his shipments were considered poorly packaged and were brought to the attention of law enforcement by both post office employees and drug sniffing dogs. Another major drug vendor was caught by making enough visits to the post office to purchase stamp purchases in bulk, which alerted law enforcement and made it easy for them to have post office employees identify the vendor and their handwriting on their packages containing heroin [5].

On November 4th, 2014 the FBI raided the successor of Silk Road called Silk Road 2.0, in addition to 27 other Dark Net drug market sites in a raid called Operation Onymous. As of this writing not many details have been released but many are suspecting that there may have been a breach in the Tor network. It was pointed out that in July of 2014 two researchers from Carnegie Mellon were preparing a presentation that was pulled at the last minute for a Black Hat conference. The presenters were going to demonstrate a method to "break Tor". A conference spokesperson later explained that the presentation was canceled as the researchers had yet to clear their work through their organization - The Software Engineering Institute which is funded by the US Defense Department. Still many are speculating that it was this research that exposed the Tor hidden services being raided. The FBI has stated that they used an undercover investigator to join the site as a moderator that led them to the site's owner and physical location [24].

By the end of the week, another successor, Silk Road 3.0, had already opened. While many of the site operators are in police custody one operator remains at large. The owner of a Dark Net site called Doxbin, which posts information for the purpose of identity theft, remains at large. The unnamed owner posted site logs that demonstrated a denial-of-service attack. This

DoS attack would send millions of malformed packets to the Dark Net sites in an effort to redirect replies from the Dark Net sites' originating IP address to an FBI operated server [19].

The Heartbleed Bug

In April of 2014, over 20% of Tor exit nodes were in danger of being revoked because of the Heartbleed Bug in OpenSSL, which allowed an attacker to send 64kb of memory from a server to any client pinging that server. The exploit had the potential of sending unencrypted information about Tor users over the public internet. The information sent in clear text included hostnames, and credentials as it passed through Tor exit nodes, which use TLS encryption as part of the OpenSSL library. As a failsafe for the integrity of the Tor network, the Tor Project began flagging relay and exit nodes that were still susceptible to the Heartbleed bug. When a node was flagged it no longer was allowed to pass traffic through the Tor network [25].

Roger Dingledine explained in a blog post on the Tor Project's webpage, after the bug was made public that all Tor clients were safe and that only relays, bridges, hidden services, and directory servers were vulnerable. Tor relays and bridges were vulnerable as they could be forced into revealing their onion and identity keys. If an attacker obtains a relay's identity key they can announce that the relay is in a new location and can snoop in on traffic flows by impersonating that relay. This attack may not be useful due to Tor's multi-hop design as impersonating one relay in no way is able to reveal the identity of a Tor user. Still, the Tor project advised relay operators to update their keys. Hidden services were vulnerable as there was a possibility that they were able to leak their long-term identity keys to their relay points - the relays between the hidden service and the rendezvous points. With the hidden service's long-term identity key an attacker can impersonate that hidden service. Dingledine advised all hidden

service hosts to change their .onion addresses. Directory servers were at risk as there was a possibility of them leaking their directory list signing keys and they were advised to generate new keys [26].

Two months later in June of 2014 it was announced that there were several additional OpenSSL vulnerabilities that affected Tor users. Some viewed it as an extension of the Heartbleed bug but wouldn't receive the same media attention due to its less than scary name - EarlyCSS. These vulnerabilities still undermine Tor's functions to anonymize users by allowing an attacker to execute a man-in-the-middle attack, thus allowing a Tor relay to negotiate a TLS connection without any actual encryption or authentication mechanisms put into place, making traffic analysis possible. Despite the attack not being as serious as the Heartbleed bug, all Tor node operators were still advised to update OpenSSL and their Tor software [27].

Bitcoin Proof of Concept Exploit

Bitcoin is an online payment system that combines cryptography and peer-to-peer networking to keep track of online transactions. Bitcoin is the payment method of many Dark Net sites due to the level of anonymity it provides to the buyer and seller. Bitcoin uses a peer-to-peer system where each peer keeps a copy of everyone's balances. When one peer pays another peer in Bitcoin that transaction is broadcasted to the entire Bitcoin network. This prevents individuals from double spending. Bitcoin currently consists of cryptographic puzzles called blocks that are generated by Bitcoin miners who volunteer their hardware to generate these cryptographic hashes. While it is not required to use Tor when making a Bitcoin transaction, many users still choose it to maintain a level of anonymity.

In October of 2014, a proof of concept exploit was detailed that can trick Bitcoins' anti-Denial-of-Service Attack protection system into forcing Bitcoin servers to ban specific Tor exit nodes, forcing a Tor user to only connect through the attacker's exit nodes or Bitcoin peers, which requires the attacker to add a large number of Bitcoin peers to the Bitcoin peer-to-peer network, and to run a number of Tor exit nodes. The attacker then spoofs the IP address of a legitimate Tor exit node and sends a malformed packet to a Bitcoin client. The Bitcoin client will analyze the malformed packet, determine that it is an attempt at a DoS attack, and ban the Tor exit node's IP for 24 hours. If another Tor user tries to make a Bitcoin transaction through this exit node then they are unable to connect to the Bitcoin network.

Now that the target using Tor can only connect to the attacker's exit node or Bitcoin peer network - they are effectively isolated from the rest of the Bitcoin network. This means that the attacker then controls the target's network of transactions meaning if the target makes a transaction while connecting to the attacker's network it will not be replicated across the real Bitcoin network. Furthermore, the attack reduces the target's level of anonymity on the Tor network as the attacker has manipulated the user into routing traffic through their exit node and that traffic may reveal personal data about the target, as Bitcoin traffic is not encrypted. While the attack is possible to perform due to the ease of banning Bitcoin peers, it still requires the attacker to have a large block of IP addresses in their possession. Suggested countermeasures to prevent this attack from occurring includes relaxing Bitcoins' DoS protection system, to encrypt Bitcoin traffic, make Bitcoin peers aware of Tor nodes to allow them to adjust their banning measures as Tor exit nodes are shared amongst many users, and for Bitcoin developers to maintain a list of stable Tor nodes [28].

China and Tor

China has a long history of censoring their citizen's internet access and the methods that are used to evade that censorship, such as using tools like Tor. The Great Firewall of China (GFC) blocks Tor's website and connections to Tor relays. The Chinese government can easily block Tor relays as they are publicly listed on Tor directory servers. China's blocking of Tor was originally maintained by straightforward IP address blocking and HTTP header filtering. In 2009 the Tor Project introduced bridges that are privately listed entry nodes. Due to the fact they are privately listed, they are difficult for the Chinese government to detect and block. In 2011 reports of Tor users in China were being blocked even if using these Tor bridges. It turned out that the Chinese government had introduced a more sophisticated method for blocking Tor traffic using deep packet inspection which enabled them to block Tor bridges in real time.

When a Tor connection is detected by its TLS hello message, an active scanner attempts to make connection with the Tor node, if the connection detects that it is a Tor node, it proceeds to block the bridge. When a TLS hello message is sent to a Tor node it responds with a unique cipher list that only a Tor node will respond with. The Tor Project has responded to this additional blocking mechanism by developing a tool called obfsproxy. The application must be installed on both the bridge and the client. It obfuscates the traffic so China's deep packet inspection protocols are unable to receive the response to the TLS hello message. This can allow the Tor bridge to appear as a combination of 13 different types of servers such as telnet or SSH. Another method used to avoid China's censorship system is utilizing packet fragmentation. Packet fragmentation takes advantage of how many network scanners are unable to reassemble network packets [29].

Summary of Tor's Vulnerabilities

While it appears that Tor as a technology is secure from its foundation, it is often times the user who is the biggest vulnerability. To de- anonymize a Tor user requires resources beyond what the typical hacker or script kiddie has to offer. Law enforcement agencies have proven themselves progressive with today's criminals and their use of technology. Attacks on the Tor network have been complicated and at high enough scale to have successful results, and even then there is still only a slim chance of a target's identity being revealed. It should also be noted that with Tor being an application that requires the coordination of many other services and protocols, it is often an error on the third party application's end – such as in the case of the SSL Heartbleed Bug. No matter what the source of the Tor vulnerability is, one must keep in mind basic security principals when using Tor to maintain anonymity. This can include keeping their software up to date, and hardening their systems if they are hosting a hidden service.

Chapter 5: Conclusion

There are many conflicting interests in Tor. Whether it is evading law enforcement or evading censorship. Finding the balance of the true purpose of the project is always going to be a controversial topic. While the core components of the technology itself are solid, there is still one main component that always leads to the downfall of the criminals that use the network - user error. In all examples of Tor users being exposed, it was attributed to either a misconfigured web page or not doing something basic such as updating software. The idea of wrapping three levels of encryption is something not even the US government has figured out how to counter, even given their immense amount of resources.

To crack Tor will require cracking modern encryption algorithms which is not feasible given today's technology. While this idea does not seem farfetched as technology advances, this is still something that is not quite there yet. Following basic hardening principles such as changing default passwords and checking to make sure that software is up to date, Tor users can consider themselves safe from eavesdropping, but there are always going to be zero day exploits that are not yet publicized or too current for a software vendor to patch that can be exploited. It is also apparent that the Tor Project has many dedicated individuals who donate their time and talents to what they consider a good cause. The Tor Network volunteers keep constant communication amongst each other and keep track of various ways the network can be exploited and have been quick to ban any Tor nodes they believe are monitoring traffic in bad faith.

It is worth noting that an individual's real life activities often reflect their online personas. The longer that one involves themselves with hosting a website that provides illegal content, the higher the probability that they will be negligent in their activities and give themselves away. Agencies such as the FBI have both the time and the resources to find these individual’s

identities and it is apparent that they will do whatever it takes to expose their identities and take action. In the end, we should question these individuals' choices to involve themselves with this type of activity in the first place.

We also cannot forget about those who use the service to hide their identities from people with ill intent while reporting information about human rights violations or government misconduct. These individuals use Tor services to protect their identities and wellbeing for causes that are important to many. When law enforcement agencies try to undermine the integrity of the Tor network it also puts these individuals at risk. This raises the question that with all the grey areas in the law that allows for the use of various hacking tools that exploits an individual's right to privacy if they should apply to those individuals using the service for legal purposes as well.

Despite the two ends of the spectrum that the project is currently being used for, it can be said that as long as one is careful and mindful of their activities, the Tor network is currently the best option one has for maintaining their anonymity. One also needs to ensure that they use the service in a lawful and responsible manner, as the network is currently a prime target of law enforcement that does pay attention to rising technologies and tries to adapt to them as best they can. It is worth noting that the Tor network's intentions are to protect one's right to privacy for the greater good and not evading the law. It is also worth mentioning that Tor is a technology that works with many different technologies and requires the human element - both of which can be exploited and undermined.

The key question is this: is Tor the best solution for maintaining web anonymity? How are all of these hidden services being raided? We need to consider the difference between an individual browsing the internet using Tor and someone hosting a web server as a hidden service

through Tor. The typical user is not going to generate a large amount of bandwidth on a given day. A popular web site can generate gigabytes in hours. As Tor nodes are publicly listed it is easy to differentiate and filter between Tor and non-Tor IP addresses on the Tor network. With enough time and resources one can control a large number of Tor Exit Nodes and monitor traffic covertly. Over time a large enough sample can be analyzed and by filtering only the non-Tor node traffic and deduce which non-Tor IPs are generating a large amount of traffic. From there a law enforcement agency can begin looking further and gather enough evidence to issue a subpoena to an ISP. Most ISPs are not going to court to fight a subpoena for one of their customers and will readily give a customer's information to a law enforcement agency with a valid reason. From there an investigation can begin to unravel and a site can be taken down with ease. Solutions to this scenario are to either have Tor designed to prevent repeat use of Exit nodes, which may be difficult for user experience purposes, of for one hosting a hidden service to cycle through public IP addresses on a frequent basis.

While there are many productive uses of the service, there are always going to be those using it for purposes that many believe degrade the integrity of our society, and it is those individuals that make the service a target of law enforcement. Tor is a good solution for those using it in moderation, and probably not a good solution for those using it to host services that evade abiding the law. An individual communicating with a member of the press is not going to generate enough traffic to call attention on to themselves in comparison to a hidden web site facilitating the online drug trade. Using the service in a responsible manner is always the best options for anyone using Tor if they want to stay off the radar.

Bibliography

[1] John Vacca, *Computer and Information Security Handbook*. Burlington, MA, USA: Morgan Kaufmann Publishers, 2009.

[2] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," 2004.

[3] Pierluigi Paganini. (2014, August) InfoSec Institute. [Online]. http://resources.infosecinstitute.com/hacking-tor-online-anonymity/

[4] Kevin Poulsen. (2014, August) Visit the Wrong Website, and the FBI Could End Up in Your Computer. [Online]. http://www.wired.com/2014/08/operation_torpedo/

[5] Patrick Howell O'Neill. (2014, October) The real chink in Tor's armor. [Online]. http://www.dailydot.com/crime/silk-road-tor-arrests/

[6] Paul Syverson. (2005) Brief Selected History. [Online]. http://www.onion-router.net/History.html

[7] Yasha Levine. (2014, July) Almost everyone involved in developing Tor was (or is) funded by the US government. [Online]. http://pando.com/2014/07/16/tor-spooks/

[8] Dune Lawrence. (2014, January) The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built. [Online]. http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency

[9] Jim Kurose and Keith Ross, *Computer Networking: A Top-Down Approach*, 6th ed., Marcia Horton, Ed. Boston, United States of America: Pearson, 2012.

[10] Howard Gilbert. (1995, February) Introduction to TCP/IP. [Online]. http://www.yale.edu/pclt/COMM/TCPIP.HTM

[11] Holly Lynne McKinley. (2003) SSL and TLS: A Beginners Guide. [Online]. http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029

[12] David Koblas and Michelle R. Koblas. SOCKS. [Online]. https://www.usenix.org/legacy/events/sec92/full_papers/koblas.pdf

[13] Peter Loshin, *Practical Anonymity: Hiding in Plain Sight Online*, 1st ed., Benjamin Rearick, Ed. Waltham, United States of America: Syngress, 2013.

[14] J. Michael Stewart, *Network Security, Firewalls and VPNs*, 2nd ed., Ty Field, Ed. Burlington, United States of America: Jones & Bartlett Learning, 2014.

[15] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Hiding Routing Information. [Online]. http://www.onion-router.net/Publications/IH-1996.pdf

[16] William Stallings, *Cryptography and Network Security*, 5th ed., Marcia Horton, Ed. Boston, Unitied States of America: Prentice Hall, 2011.

[17] Dan Goodin. (2013, September) Majority of Tor crypto keys could be broken by NSA, researcher says. [Online]. http://arstechnica.com/security/2013/09/majority-of-tor-crypto-keys-could-be-broken-by-nsa-researcher-says/

[18] Steve Gibson and Laporte Leo. (2013, March) Tor 2.0 with Hidden Services. [Online]. https://www.grc.com/sn/sn-394.htm

[19] Sean Gallagher. (2014, November) Silk Road, other Tor "darknet" sites may have been "decloaked" through DDoS. [Online]. http://arstechnica.com/security/2014/11/silk-road-other-tor-darknet-sites-may-have-been-decloaked-through-ddos/

[20] James Ball, Bruce Schneier, and Glenn Greenwald. (2013, October) NSA and GCHQ target Tor network that protects anonymity of web users. [Online]. http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

[21] Kevin Poulsen. (2013, August) Feds Are Suspects in New Malware That Attacks Tor Anonymity. [Online]. http://www.wired.com/2013/08/freedom-hosting/

[22] Kevin Poulsen. (2013, September) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack. [Online]. http://www.wired.com/2013/09/freedom-hosting-fbi/

[23] Andy Greenberg. (2013, October) End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market. [Online]. http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

[24] Kashmir Hill. (2014, November) How Did The FBI Break Tor?. [Online]. http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/

[25] Michael Mimoso. (2014, April) Tor Begins Blacklisting Exit Nodes Vulnerable to Heartbleed. [Online]. http://threatpost.com/tor-begins-blacklisting-exit-nodes-vulnerable-to-heartbleed

[26] Roger Dingledine. (2014, April) OpenSSL bug CVE-2014-0160. [Online]. https://blog.torproject.org/blog/openssl-bug-cve-2014-0160

[27] James Lyne. (2014, June) New OpenSSL Defects - Another Heartbleed? Tor Stripped?. [Online]. http://www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed/

[28] Alex Biryukov and Ivan Pustogarov. (2014, October) Bitcoin over Tor isn't a good idea. [Online]. http://arxiv.org/pdf/1410.6079v1.pdf

[29] Philipp Winter and Stefan Lindskog. (2012, August) How the Great Firewall of China is Blocking Tor. [Online]. https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf