Anonymity Through The Silk Road

In the pursuit of gaining anonymity online, there is a continuous ebb and flow that involves one party attempting to gain permanent and lasting anonymity while a second party attempts to compromise that anonymity. In this paper, I will be using The Silk Road as a means to explore this notion and as a real life example of this constant back and forth of maintaining anonymity.

1. Abstract

The Silk Road is an online marketplace that allows users to anonymously buy and sell just about any good, whether it be legal or illegal. Because the goal of The Silk Road is to maintain the anonymity of users, the Tor browser is what users use to connect to the website and Bitcoins are used for transactions. Both Tor and Bitcoin, while solid ways to remain anonymous, do have some flaws and vulnerabilities that can potentially remove the necessary anonymity that a user requires in order to safely use the site.

2. Silk Road Overview

2.1 What is the Silk Road?

The Silk Road is an anonymous online marketplace that was created in order to allow for the online sales of all items, legal and illegal. The entire concept is fascinating because it allows for people from around the entire world to both buy and sell any and all goods to each other without ever having their identity compromised and without having to worry about any buying or selling restrictions that may be in effect due to geographical location (country, state, province, etc.).

There are many factors required for anonymity on The Silk Road that must be maintained in order for anonymity to be fully encompassing and complete. Any breach or failure in any one aspect of The Silk Road could lead to a compromise of all anonymity. When thinking about the creation of an online anonymous marketplace, there are several requirements that must be achievable without the compromise of identity in order for this marketplace to be successful. A user of the site must be able to access the website, register him/herself to the website, sellers must be able to post and advertise all items that they would

like to sell, buyers must be able to peruse all available items for purchase, transactions involving the trading of currency for a product must be possible, and there must be a mechanism to send the physical item from the seller to the buyer. Once again, all of these requirements must be done while maintaining the anonymity of the user.

Generally speaking, The Silk Road has an anonymous solution for each of the requirements stated previously. In order to access The Silk Road anonymously, there needs to be a way for a user to hide his or her IP Address. This can be easily accomplished by installing a Tor client onto his or her machine. The Tor Browser allows for the anonymous browsing of the internet by skipping the use of an IP Address and DNS lookup and instead uses .onion domain [1]. I will go into more detail on Tor a little bit later. Users must register for a very basic account that simply has a username and a password. By having an account, the user has essentially created an anonymous online persona that can be used to manage who posts items for sale and who would like to purchase items. The account creates a pseudonym of sorts for each user that gives them a presence on the site without revealing any personal information. Once a user finds an item that he or she wishes to purchase, the currency used to protect anonymity is Bitcoin. While Bitcoin is not 100% anonymous on its own, The Silk Road acts as a sort of middle man to transfer Bitcoins to and from users to unlink the individual buyers and sellers. This process of having a third party to temporarily hold money during a transaction is called an escrow and is perfect for the situation of The Silk Road. When a buyer decides that they would like to purchase an item, he or she will alert the seller and then pay the owed money to The Silk Road. The seller will then be alerted that The Silk Road has received the payment and send the item to the buyer. Once the buyer has received the item, he or she will then alert The Silk Road that the item was received and The Silk Road will transfer the payment to the seller, completing the transaction [1]. That all sounds very simple, but the last major issue to deal with is the actual physical address to give to the seller so that the item can be shipped. That one piece of information is both completely necessary, because without it the entire system wouldn't work, and also a dangerous piece of information. It is literally a geographical location that the buyer has to visit at least one time in order to receive the item. If this piece of information is compromised, anonymity is compromised. It would allow an attacker to know the location that

the buyer lives or at least will visit at least a one time. Because of this, The Silk Road recommends that a user not give their own address but perhaps a P.O. Box or some alternative address [1].

3. Tor

Tor is a form of Onion Routing used by The Silk Road that allows for users to access the website, browse, and communicate on it with anonymity. Tor was developed by The Tor Project, Inc. in September of 2002.

3.1 How Tor provides Anonymity

When a user downloads the Tor browser, essentially what they are downloading is a means of sending their network data through a series of nodes that are all supplied on a volunteer basis and only know the node that they received the data from and the next node to send the data to. By only knowing the previous node and the next node, a chain of nodes can be created in order to send the data to a destination (a server) and having the chain reversed to send the reply. If one node is somehow compromised, the only information that the attacker would be able to obtain would be the previous node and the next node. From this broad overview, it is pretty clear that Tor is excellent at maintaining anonymity.

To go into a little bit more detail, the Tor software installs an Onion Proxy onto the user's computer. What the Onion Proxy does is create a virtual circuit that defines the path through the Tor nodes that leads to the user's end destination. How the Onion Proxy does this is it starts out by downloading a list of all of the potential Tor nodes in the network. Once the Onion Proxy has a list of all of the nodes, it can use that list to create a circuit. A circuit is essentially a path of nodes that the Onion Proxy will use to send its data and requests to its desired end server. A circuit for Tor always consists of three nodes: The Entry node, the Intermediate node, and the Exit node.

The first thing that the Onion Proxy does is establish an Entry node. To do so, it finds the first node in the Tor nodes list that it wants to send data to and it creates a TLS connection with that node. A TLS connection is a Transport Layer Security protocol that "allows

client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery" [3]. Once the TLS connection is established between the Onion Proxy and the Entry node, there is a unique key established between the two. At this point, the Onion Proxy needs to create a circuit, as the Entry node will be the first node along the path it creates to the end server. When editing the circuit, the Onion Proxy essentially has three commands that it can give to the nodes along its path: create, extend, and delete. Because the Onion Proxy does not have a circuit yet, after the TLS connection is established between it and the entry node, the Onion Proxy can then send a create message to the Entry node. The Entry node will use the unique key to decrypt the message, and respond with a created message [2]. This will create the circuit and at this point it will only consist of one node.

While a circuit with one node in it is nice and may help with anonymity, the Onion Proxy will want to add more nodes to the circuit. In order to do that, the Onion Proxy can once again look at the list of all of the Tor nodes in the network. The Onion Proxy will select a node to be an Intermediate node and will send an extend message to the Entry node. The Entry node will use the unique key between it and the Onion Proxy to decrypt the message. When it sees the extend command, it will send a create command to the Intermediate node selected by the Onion Proxy. When the Intermediate node responds to the Entry node with a created message, a unique key between it and the Onion Proxy is created so that it and the Onion Proxy can send each other encrypted messages through the circuit. This key, as well as the created message will be sent to the Entry node which will then encrypt it using the unique key used by it and the Onion Proxy. Once the Onion Proxy receives the message, it can decrypt it using the key from the Entry node and it then knows that it has two nodes in the circuit and it has two unique keys to encrypt messages to and from each node.

At this point, two out of three nodes in the circuit have been created and established and it leaves only one final node to create. Once again, the Onion Proxy chooses a node from the list of Tor nodes that it would like to be the Exit node and repeats the same process used to create the first two nodes except this time, the message is forwarded through two nodes. What the Onion Proxy does is first create an extend message and encrypt it with the Intermediate node's key and the Exit node that it wants. Then it creates another extend message, includes

the Intermediate node's encrypted extend message, and encrypts it with the Entry nodes key and sends the message to the Entry node. Each node, in turn, decrypts the message and then follows its instructions. What is returned in the end is a created message from the Exit node with the key used to encrypt/decrypt the messages sent to and from the Exit node. At this point, the circuit is complete and messages can be anonymously sent from the user to their desired web server using the Onion Proxy.

Now that you know what Tor is and how Tor works, you're probably wondering, how does Tor play a part in Anonymity on The Silk Road? That's an excellent question! When users of the Silk Road connect to the website, to protect their anonymity, they obviously don't want observers or attackers to be able to see where they are sending their traffic. As well, when a response is sent from The Silk Road, these same users don't want an attacker to see that they are the final destination. By using Tor to connect to The Silk Road and receive responses, users remain anonymous and are able to create anonymous accounts (assuming they don't use any personal information), post items that they would like to sell, and request to purchase items. Basically, by using Tor, all actions taken while browsing and using The Silk Road would be anonymous.

4. Bitcoin

Bitcoin is a peer-to-peer electronic cash system. The goal of Bitcoin is to move away from the traditional form of cash exchange that involves a trusted third-party (a bank) that can mediate the transaction. By having a trusted third party, if two people would like to make some sort of transaction, the buyer would inform the bank the amount of money that should be transferred to the seller and then the bank would transfer that amount of money from the buyer's account to the seller's account. With a trusted third-party cash system, there come disadvantages which include a third party having access to a user's money, a third party knowing about all transactions that a user makes (which is horrible for people who want anonymity), and transactions can be disputed and reversed.

Bitcoin was created as a way to remove the trusted third-party from the equation so that a user could have access to all of his or her money (Bitcoins) and spend them without

depending on any third-party and without the transaction being reversible [4]. To facilitate the removal of a trusted third-party, rather than having the third-party mediate all transactions, each transaction is broadcast out to every other node in the Bitcoin network.

The Bitcoins can be characterized as a “chain of digital signatures” [4]. Each user in the Bitcoin network has a wallet that holds all of their Bitcoins and is what is referenced when a transaction occurs. So, what is to stop someone from just using someone else’s wallet? Excellent question! Each owner of Bitcoins has a public key and a private key that are used to only allow for the transfer of Bitcoins from the real owner’s wallet. “Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin”[4]. The digital signature is what is used to validate the ownership of the Bitcoins.

Bitcoin provides for anonymity in the sense that it removes a trusted third party from the transaction equation entirely. While every transaction is broadcast out to every node on the Bitcoin network, users’ names are not used to identify them. Instead, a digital signature is used and that certainly adds some degree of anonymity. In regards to The Silk Road, it would not be a wise decision to allow a third party to mediate transactions for your purchases. Seeing as The Silk Road is meant to allow for online anonymous purchasing, using Bitcoin completely decouples the good or service from the transaction with the actual money that exchanges hands. While in a normal online transaction, a buyer would enter their banking information and need to inform their bank who they need to send money to and, generally, what the money is for. Using Bitcoins on The Silk Road, a user will decide that they want to purchase an item. At that point, they transfer the Bitcoins into a Silk Road escrow and the seller is alerted to send the agreed upon item. Once the item is received, the Silk Road escrow is notified and transfers the Bitcoins in the account to the seller. From an outside perspective, all that anyone not involved in the transaction would see is that Bitcoins from one digital signature were transferred to a different digital signature. The reason for the transfer remains unknown and it protects both the buyer and the seller.

5. Failures in Anonymity on The Silk Road

While The Silk Road does have a great deal of measures in place to preserve the anonymity of its users, it is not perfect. There are many moving parts in this online marketplace and if even one of them is compromised, all anonymity is compromised. Just as users have a need to buy goods and services online while maintaining their anonymity, there are attackers out there who want to prevent anonymity and use the information for their own purposes. Because there are attackers out there, there is a constant need to improve all facets of The Silk Road that provide anonymity. By first identifying faults in the system, the system itself can be improved.

The first aspect of The Silk Road that I believe could lead to compromise is the fact that Tor, by itself, does not encrypt the data that is sent out of the Exit node or returned to the Exit node. If an attacker is able to monitor the exit node in the circuit or any node following the exit node, that data can be intercepted and potentially used to compromise anonymity if there is any information that can be used to link the sender to the receiver [2]. On top of that, a passive attacker who watches both the sender of the message and the receiver of the message would be able to link the two with a high probability. Especially if several messages can be observed [2]. Tor relies solely on the fact that it uses a TLS connection between the Onion Proxy and each of the three nodes it uses. If an attacker can compromise a key for the Onion Proxy or any of the nodes along the circuit, then information can be gained about the path and the traffic to and from revealed nodes can be scrutinized, reducing anonymity. If the TLS key for the Onion Proxy is compromised by an attacker, the attacker can impersonate the Onion Proxy until the TLS key's lifetime ends. While the attacker still won't have the keys for previously established circuits, it can still create new circuits and help use that information to weaken the anonymity [2].

Another point of failure that could compromise anonymity on The Silk Road is the use of Bitcoins. While Bitcoins do provide some level of anonymity, they have an anti-Denial of Service protection that can be used to create a man-in-the-middle attack if used with Tor. What the anti-DoS protection does is essentially gives each IP Address a penalty score. If a node in the Bitcoin network sends an incorrect message, it will have its penalty score decreased and it will be banned for 24 hours [5]. If Bitcoin is used with Tor, an attacker can essentially force the user

of interest to only connect to evil Bitcoin nodes or the Exit node of the attacker which could greatly reduce the anonymity of the user and even cause a compromise [5].

6. Conclusion

While The Silk Road does provide the service of being a marketplace for users to anonymously buy and sell goods, it certainly has some flaws. The site has been shut down multiple times and the facilitators have been arrested since its original creation. What really fascinates me, though is that each time the site gets shut down, someone has a cloned copy of it and gets it up and running again within a matter of months. This really speaks to me because it shows just how important it is to people to have anonymity. People are willing to risk their futures and their freedom in order to provide this anonymous service. Of course, money is made in the process, but the risks really show just how important maintaining anonymity is for the users and the owners of the site.

Each time the website is taken down, the next person who starts it up again has to ensure that the security and anonymity flaws are fixed and improved upon or suffer the same fate. The constant back and forth between attackers and users of The Silk Road is just an example of the many games of cat and mouse that occur between people who would like to maintain anonymity and people who want that anonymity compromised.

7. References

[1] Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." (2012): n. pag. Carnegie Mellon, 30 July 2012. Web. 12 Oct. 2015. <https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf>.

[2] Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router." (n.d.): n. pag. Web. 5 Oct. 2015. < https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>.

[3] Dierks, T. & C. Allen. “The TLS Protocol Version 1.0.” January 1999. (6 November 2015)

[4] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." (n.d.): n. pag. Web. 5 Oct. 2015. <https://bitcoin.org/bitcoin.pdf>.

[5] Biryukov, Alex, and Ivan Pustogarov. "Bitcoin over Tor Isn't a Good Idea." *2015 IEEE Symposium on Security and Privacy* (2015): n. pag. 8 Jan. 2015. Web.