Gardner Fiveash
12/7/15

Takedown of the Silk Road

For my final project, I performed a case study on the Silk Road and how the FBI was able to take it down. This topic sparked my curiosity when we briefly discussed it in class, and one of my goals was to learn how the Silk Road was implemented. In this paper, I look at the Silk Road through the eyes of different "stakeholders": users such as college students (but not me!), the creator- Dread Pirate Roberts, and law enforcers such as the DEA and FBI. Specifically, I look through the lens of technologies like Tor and Bitcoin, and analyze the role they had in the Silk Road's security (or lack there of). For the section on the takedown, I use court documents from the case to explain the arguments from both sides. Finally, I conclude by applying my analysis to comment on current replacements to the Silk Road and if they will meet a similar fate.

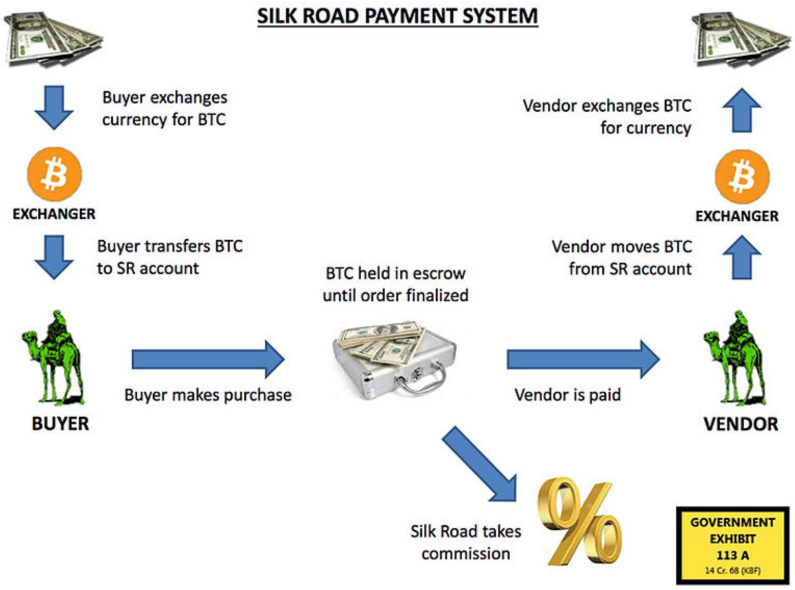
First, I walk through the steps of how a user could buy items of the Silk Road. Throughout the paper, I will refer to the mock scenario of Cole the cop trying to catch Hannah the heroin user buying from Danny dealer. As a disclaimer, I never bought anything from the site and do not have first hand experience on the matter. This walk-through comes from my research on how the Silk Road and its current replacements were implemented. In short, a user needed Tor to access the Silk Road and Bitcoin to purchase an item. A VPN (virtual private network) was not necessary but highly recommended to maximize security. A new user e.g. Hannah could log into a VPN, and then open up a Tor browser. Logging into the VPN first ensures is no record of Hannah accessing Tor. Although Tor is not illegal, it raises suspicion in certain cases. Once browsing with Tor, she could get to the Silk Road with the URL silkroad6ownowfk.onion. Registering as a new user simply required a username, password, and country of origin. Remarkably, these few steps allowed access to an online bazaar full of illicit items.

From a user's perspective, Tor is the key to maintaining anonymity online. As we learned in class, Tor prevents the release of a traceable IP address. By traceable, I mean provided by an ISP that link a device and its Internet activity to a geo-location. Web traffic from a Tor browser passes through a different network of nodes than the visible Internet, and the server only sees the IP of the relay exit node. As a result, law enforcement cannot observe a computer with IP address 12.34.56.78 bought heroin and is located at 123 XYZ Street. However, a user still must provide a shipping address to the vendor, which seems risky. The only alternative would be to have a third party handle the shipping, but the whole point of systems like these is to avoid centralized power of 3rd parties. Even if Cole the cop poses as a vendor and then shows up at Hannah's door, he has no way to prove it was her who made the purchase. Hannah still runs the risk of the package being intercepted by officials, in which case if her purchased item has personal information she could be in trouble. This actually happened to Silk Road founder

Ross Ulbricht. He ordered fake documents that from Canada that were caught at customs and ended up contributing to his arrest.

From the point of view of Dread Pirate Roberts (aka Ross Ulbricht), Tor also plays the role of a hosting service. Hidden services are servers that can be configured to only accept requests from onion addresses. A hidden service uses random nodes in the Tor network as introduction points, and builds circuits connecting them. There hidden service then creates a hash table with the public key of all its introduction points, signed by the server's private key. The descriptor can be found from a Tor browser with a specific onion URL. A client can then reach the hidden service by downloading the descriptor and getting the set of introduction points. The client then instantiates in own circuit with a rendezvous point to the hidden service and an encrypted introduction message. Now the client and server can use their circuits to communicate through the same rendezvous point. While this is a brief summary of a complex technical protocol, the main takeaway is that hidden services provide a way to host a website anonymously. They can only be reached through the Tor browser. This is why the Silk Road was able to stay live for nearly 3 years. Law enforcement knew it was there and could even buy products from it, but had no way of locating the server hosting the site. Finding this server was a key point of controversy in the court case and will be further discussed later in this paper.

The second key technology to the implementation of the Silk Road is Bitcoin. As we have studied extensively in class, Bitcoin makes it very hard to link transactions to identities. From both a user and vendor perspective, this anonymity factor makes it the ideal currency for an illegal online marketplace. The payment system for Silk Rod is shown the below diagram. A specific point of interest is that the bitcoins were held in escrow accounts until the sales were finalized. Since Bitcoin anonymizes payments, the escrow accounts were necessary to protect against scammers.


SILK ROAD PAYMENT SYSTEM
Buyer exchanges currency for BTC
EXCHANGER
Buyer transfers BTC to SR account
BUYER
Buyer makes purchase
BTC held in escrow until order finalized
Vendor is paid
Silk Road takes commission
Vendor exchanges BTC for currency
EXCHANGER
Vendor moves BTC from SR account
VENDOR
GOVERNMENT EXHIBIT 113 A 14 Cr. 68 (KBF)

DPR's vision for the Silk Road was rooted in libertarian philosophy. He believed that as long as there were consenting adults to buy and sell the item, no one should interfere with them trading. The escrow accounts were meant as a "center of trust" that essentially replaced a 3rd party intermediary like a bank or government. On a related note, what happens when a darknet site tries to operate without Bitcoin? A similar site called Farmer's Market was hosted on Tor but allowed for payment via Paypal and Western Union. The payments on the site were traceable to personal identities and it was quickly shut down.

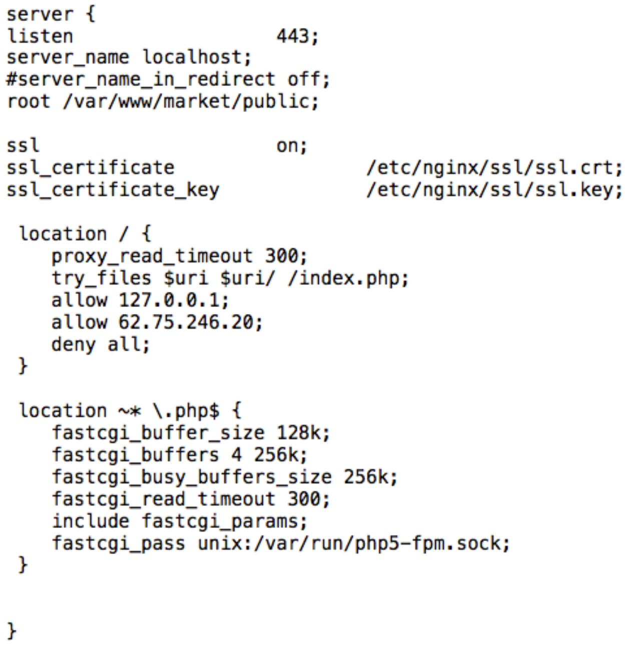
I will now look at some of the investigative methods Cole the cop can use to catch Hannah the heroin user and Danny the dealer. In the first example, the marketplace is Amazon and the method of payment is credit card. How does Cole catch the buyer? There are many ways to do this, starting with the names on the credit card and Amazon account personal details. Law enforcement could subpoena Amazon to get the transaction record, or subpoena the credit card company for records. How does Cole catch the vendor? Similarly, he could get the selling records from Amazon linking Danny's name to his illicit activity. What if we alter the example so that the payment method is Bitcoin instead of credit card? Amazon currently doesn't allow the direct purchase of goods with Bitcoin, but alternatives like TigerDirect do. However, a user still needs to sign up with a name and home address. Even if the payment itself was anonymized, a record will exist linking personal details to an illicit purchase. So, this isn't much better. Also, Hannah isn't using a Tor browser. Law enforcement could subpoena her Internet service provider and learn the location of the device that made the purchase, which could lead to Hannah.

Now let's say the marketplace is Silk Road and the payment is Bitcoin. Theoretically, there is no longer an obvious way to tie the illicit activity to an identity or a location. One investigative method would be for Cole the cop could pretend to be a buyer or seller. In the actual Silk Road case, the FBI made over one hundred undercover purchases as part of their investigation. When Hannah solicits Cole for heroin, Cole sends Hannah a package and then confronts her upon delivery. However how does he know that she was the one who made the purchase? He doesn't. The DEA used this tactic to arrest one of DPR's employees, Curtis Green, however it's unclear if they were acting within their legal bounds.

The short answer there is not a known efficient investigative method for cracking a darknet site that doesn't involve human error. In the Silk Road case, FBI agent Tarbell exploited an operational coding mistake from DPR to find the real server. He repeatedly tried logging into the Silk Road with both valid and invalid accounts. Upon examination of the data packets coming back indirectly from the server, he noticed that some of the headers had a non Tor IP address: 193.107.86.49. Tarbell claimed in his court documents that when he entered that IP into a regular browser, a portion of the Silk Road login page was returned. He deduced this IP address must be the real location of the server, located in Iceland.

Icelandic authorities cooperated and let him to copy the server, which then allowed Tarbell to re-create the Silk Road back in New York.

The discovery of the server was a huge turning point in the case, but was loaded with controversy. The defense lawyer Joshua Horowitz argued that Tarbell's claim was technically impossible. A few months before the arrest of Ulbricht, the Silk Road site was split into a back-end server to host all the data and a front-end server to access the back-end. The front-end server had IP address 62.75.246.20 and was located in Germany, while the backend server had IP address 193.107.86.49 (the one found in Iceland). The server configuration files for the backend server specify that it only accepts requests from the localhost and the front-end server. This can be seen in the below code snippet in the lines directly above "deny all".



```
server {
listen                  443;
server_name localhost;
#server_name_in_redirect off;
root /var/www/market/public;

ssl                     on;
ssl_certificate                 /etc/nginx/ssl/ssl.crt;
ssl_certificate_key             /etc/nginx/ssl/ssl.key;

 location / {
    proxy_read_timeout 300;
    try_files $uri $uri/ /index.php;
    allow 127.0.0.1;
    allow 62.75.246.20;
    deny all;
 }

 location ~* \.php$ {
    fastcgi_buffer_size 128k;
    fastcgi_buffers 4 256k;
    fastcgi_busy_buffers_size 256k;
    fastcgi_read_timeout 300;
    include fastcgi_params;
    fastcgi_pass unix:/var/run/php5-fpm.sock;
 }


}
```

Horowitz argues that the login page Tarbell claims to have seen was hosted on the back-end server with the rest of the data. The contradiction arises because Tarbell entered the 193.107.86.49 IP, which should have been denied since it was neither the local host nor the front-end server. Although this contradiction wasn't enough to save Ross Ulbricht from a life-time sentence, it does make for a good conspiracy theory.

In my personal opinion, even if Tarbell didn't actually reach a login page with that IP like he said, the fact that he got back a non-Tor IP merits enough suspicion to investigate the Iceland server. The general trend I noticed during my research was Tor is a very effective anonymity service when used correctly, however it is very prone to user error. Following the takedown, a post on the Tor Project explained how there was no evidence that Tor itself was broken as a service. Therefore, it's not surprising that currently there are live Silk Road replacements on the darknet. As long as they remain hosted as hidden services and use Bitcoin as a payment system, I have every reason to believe darknet markets are here to stay.

Sources:

How to Access the Silk Road:
http://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/

Context of Court Case:
http://www.wired.com/2015/04/silk-road-1/
http://www.wired.com/2015/05/silk-road-2/
Deep Web Documentary

Hidden Services:
https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf
https://www.torproject.org/docs/hidden-services.html.en

Tor's Reaction to Silk Road Takedown:
https://blog.torproject.org/blog/tor-and-silk-road-takedown

Court Documents:

Prosecution-

1. https://www.documentcloud.org/documents/1284178-238796613-silk-road-prosecution-4th-amendment.html
2. https://upload.wikimedia.org/wikipedia/commons/e/e4/Tarbell_declaration.pdf

Defense-

1. http://cdn.arstechnica.net/wp-content/uploads/2014/10/horowitzdec.pdf