Isaiah Fischer-Brown
Comp 116
Final Project
December 13th, 2017

Unmasking 101: How [not] to use Anonymous Browsing

Mentor: Ming Chow

Table of Contents

1. Abstract

The Onion Router, commonly known as Tor, has been the gold standard for free internet anonymity. Tor was originally developed for the U.S. Navy, with the purpose of keeping government communications secret and protecting the identity of government internet sources. In current society, Tor is used by all types of users, such as people aiming to avoid censorship on the internet, those trying to protect their children from targeted ads, or for perhaps more nefarious purposes. Given that virtual private networks (VPNs) are being banned in countries like Russia and China, and new surveillance laws are being pushed through internationally to combat terrorism, Tor will likely grow in popularity. The following research will examine Tor as a tool, explain proper usage, and present documented situations where users have been caught using Tor in illegal ways to demonstrate weaknesses in the system and how users can protect against them.

2. To the Community

Our activity on the Internet is constantly monitored. The purpose in writing this is to demistify anonymous browsing so that a person with very little knowledge of cyber security can understand how anonymous broswing is currently constructed. More importantly however, this paper exposes some weaknesses in the privacy of this type of internet usage and demonstrates ways in which identities can be revealed while using Tor.

“Without Tor, the streets of the Internet become like the streets of a very heavily surveilled city”

- Edward Snowden, December 30th, 2015 [15]

3. Introduction

The Tor Project states that Tor allows users to cirmcumvent surveillance by routing through a network of servers rather than connecting directly to a destination.[18] In short, using Tor provides users anonymity of origin, masking a user’s initial IP, but not completely cloaking their activity. Once on the Tor Browser, a user can visit any site indexed by a typical search engine like Google but also can also see sites that are hosted outside of the Domain Name System, called onion services. The original purpose of Tor was so that the military could carry out anonymous, encrypted digital communication, and this is still one of the primary purposes of Tor today.

3.1 How Tor Works

Tor utilizes a process known as Onion Routing to cloak the user’s starting IP and location. It is similar to a proxy, but as we will see in later examples, proxies are vulnerable to government warrants and often track users. Onion routing uses a series of servers, in Tor’s case, powered by volunteers, to encrypt data and allow the user to reach a destination server while using the IP of one of the Tor servers. From a user’s home computer, the Tor Browser selects a random path through the list of Tor Servers, and allows the final server to connect to the selected destination. This final connection is the only one that is unencrypted.

3.2 Hidden Services and Tor Browsing

When on Tor, users can browse the internet as they normally would, and expect typical sites to behave similarly to any other browser, just a little bit slower given the added layers of encryption. Alternatively, users can also visit .onion sites, hidden services that are not a part of the Domain Name System. These hidden services are not registered, but instead are a hash of a public key, where the first half is the “base32 encoded SHA-1 hash of a public key, from a 1024-bit RSA key pair” with the .onion suffix. [7]

Example:

http://3g2upl4pq6kufc4m.onion/

Above is the URL for the hidden service DuckDuckGo, a search engine that doesn’t track user behavior or leverage searching patterns for targeted advertisements, like Google does. To search for these hidden services, users often use Ahmia.fi, a tool for looking up hidden services by name instead of by hash.

3.3 Tor Funding and Regular Usage

Though government agencies constantly try to break the anonymity of the network, the irony of Tor is that is continues to exist on funding from these same state actors. Indeed, the project is funded by the US government, the National Science Foundation, Google, Mozilla, the German government, and even the National Christian Foundation. [18]

According to their own metrics, about 3 million people use Tor every month and this number is steadily growing. This statistic excludes bridges and any non-direct connection.[18] Research done at the Oxford Internet Institute demonstrates that the network is used by over "750,000 Internet users each day" and in Europe, "the service is used by an average of 80 per 100,000 European Internet users".[10] It is unsurpising that Tor usage in Europe is growing, given laws passed in the EU recently to legalize increased government surveillance of the internet. Between the Investigatory Powers Act in Britain, the Communications Intelligence Gathering Act in Germany, and the International Electronic Communications Law in France, the past few years are filled with legislation giving government intelligence agencies access to citizen browsing and communication patterns in the name of public safety.[11]

4. How Users Should Not Use Tor

At this point in time, most have heard about the Silk Road, the hidden service marketplace for anything illegal, from cocaine to child pornography to lab supplies. To this day, the downfall of its original creator has been arguably the most high profile unmasking of an anonymous internet user. Well, how exactly did this all go down? According to security expert Adrian Crenshaw (also known as Iron Geek), using publicly searchable forum posts from the early days of the hidden service, the FBI was able to track down a potential mastermind behind the operation.[6] A handle by the name of altoid posted on forums such as BitCoinTalk and Shroomery advertising the Silk Road. In one of these posts, altoid gave the email "rossulbricht at gmail dot com" as a contact and resource for interested parties, linking the previously anonymous handle to a real email account (the forum post is shown below).[2, 1] In a subsequent stackoverflow post from 2013, a user with a similar name to the email (which was later changed to the generic username frosty) asked about how to connect to a hidden service using cURL in php.[8] Among other things, this was enough for the FBI to get a warrant and eventually track down the owner of that email, Ross Ulbricht, and sentence him to life in prison without parole. There is much to learn from this case about anonymity, how to unmask users, and how users can protect their identities from such de-anonymization and the follwing section will expand on each of these topics through the detailing of technical and non-technical attacks and a series of high-profile cases.

Author | Topic: IT pro needed for venture backed bitcoin startup (Read 37809 times)

altoid
Jr. Member
Activity: 48

IT pro needed for venture backed bitcoin startup
October 11, 2011, 08:06:22 PM #1

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

If interested, please send your answers to the following questions to rossulbricht at gmail dot com

1) What are your qualifications for this position?
2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.

4.1 End-to-End Confirmation Attacks (and some basic defense techniques)

The most used attack on anonymity is a type of Correlation attack known as an end-to-end confirmation attack. In basic terms, this type of attack is implemented by controlling two nodes, specifically the entry and exit nodes on the network. If the attacker modifies these two nodes to record and analyze traffic on them, the attacker can then match traffic to deanonymize the user. Researchers at the U.S. Research Laboratory and Georgetown University utilized this type of traffic correlation analysis and concluded that “80% of all types of users may be de-anonymized by a relatively moderate Tor-relay adversary within six months”.[12]

Most high profile attacks use this method, and to defend against such snooping, there are two main strategies: packet delay and dummy traffic, outlined by Konstantin Müller in his Master’s thesis. Packet delay is a technique where incoming packets are delayed before being forwarded to the receiving node. This in turn makes the timing of incoming and outgoing packets independent from each other and thus seemingly unrelated. The second evasion is dummy traffic, where the user sends packets without actual data. These empty packets make “different connections indestinguishable”.[16]

4.2 High Profile Case Studies + Defenses Against Them

By examining the technical causes of de-anonymization, readers can learn strategies to protect themselves against such identification and more importantly, develop a healthy skepticism of anything deemed anonymous on the Internet. First, a university run attack on Tor will be discussed, followed by the takeaways of a talk given at DefCon, where Adrian Crenshaw discussed a few well known deanonymizations, carried out by both state actors and accidentally by users themselves.

4.2.1 Carnegie Mellon Research using Correlation attacks

A blog post on Tor recently documented this attack, where allegations first arose that researchers at Carnegia Mellon University had infiltrated the Tor network and using a correlation attack, were able to monitor traffic in two ways. First, the team set up and controlled many nodes in the network at once, known as a Sybil attack. Combined with the Sybil attack, the

researchers used traffic confirmation and their array of entry nodes to inject into the passing traffic a signal containing each hidden service visited on one of their nodes. Thus, the originating IP address could be associated with the ultimate destination, by tracking the path of the injected signal from source to hidden service.[3] This research was linked to recent FBI busts and rumours circulated that the university was paid off to unmask certain users, associated with the Silk Road 2.0 and child pornography.[5] This type of attack is hard to mitigate as an individual, and thus should be acknowledged as a real threat to anonymity.

4.2.2 Harvard Bomb Threat

A somewhat less technical approach was used in response to an email sent anonymously to the entirety of a small, lesser-known college in New England (Harvard University), stating that there were bombs placed in a few of the buildings. The perpetrator sent this message via Guerrilla Mail, a service that normally includes an originating IP address in the email header. Harvard could see that the IP given was that of a Tor exit node, because those are publicly listed on the internet. After sniffing traffic on the university network at the time of the attack, the IT department quickly traced Tor usage to one particular student. If the student hadn't used Harvard's monitored campus internet or if he had used a bridge with Tor he may have avoided being caught. A bridge, according to the Tor Project documentation, is a node that is not publicly listed, meaning that whoever is monitoring a user's local internet cannot identify that a user is going to Tor.[18] While such impulsive behavior should not be condoned, this case study exemplifies how easily one's identity can be revealed, even when using Tor. An awareness of one's internet connection coupled with proper implementation of a bridge could have protected this student's identity.

4.2.3 LulzSec

In a similar case, Sabu, the leader of LulzSec, a hacking group responsible for high profile cases such as the huge Sony leak in 2011, was apprehended by the FBI through deanonymizing Tor activity.[14] While on Tor, Sabu had been using the Internet relay chat (IRC) to talk to his fellow group members and coordinate efforts in future attacks. Unfortunately for him, he accessed the IRC once without going through Tor, exposing his IP address and allowing the FBI, who had been surveilling for any connection to him, to link Sabu with all his other previously anonymous activity. Once caught, Sabu then became an FBI informant, and in exchange for his eventual freedom, helped catch other members of his group. These members were caught when they mistakenly exposed specific personal details about themselves while on IRC, such as involvement in other known criminal activity and high profile hacks. In retrospect, it is obvious that a user should not expose personal data while on Tor, because it can be used to deanonymize someone without any sort of technical attack. To protect anonymity, users should never disclose identifying information on Tor and should consistently withhold personal information on every Tor site where identity needs to be protected.

4.2.4 Freedom Hosting

The case of Freedom Hosting exposes us to one flawed belief while using Tor: while Tor provides anonymity of origin to the user, it does not guarentee that the accessed hidden service is in itself secure. Freedom Hosting was a service that allowed users to host hidden services on Tor anonymously. While it may have been used normally, many users visited Freedom Hosting sites seeking child porn and the like. Because of the nefariousness of Freedom Hosting, the FBI was able to exploit a vulnerability (CVE-2013-1690) in Mozilla Firefox within the Tor browser bundle to reveal the IP addresses of users accessing these sites and eventually track down and arrest the host of Freedom Hosting.[4, 17] The moral of this case is 1) a user should not blindly trust a hidden service, and 2) update Tor browser bundle when vulnerabilities are publicly announced. Just this past month, Tor realeased a crucial update that patched a bug where users would inadvertadly leak their IP addresses due to a Firefox bug.[9]

4.2.5 VPN Usage

The argument has been made that using a VPN can help further mask the user's identity. However, this is only true if a user can place trust in the VPN to not collect data on user traffic and monitor the network. As in the case of other LulzSec members who were using the VPN HideMyAss at the time to conduct activity, the government was able to issue a court order to collect user information from HideMyAss. The VPN was then forced to hand over sensitive data to the government, which featured incriminating evidence of SQLi from members of LulzSec.[13]

5 Conclusion

Given the problems with Tor, which is considered the standard for anonymous usage, is it possible that users can achieve actual anonymity?

While Tor is not the end-to-end encryption tool we hope and wish it was, Tor is constantly being improved by the Tor Project team. We as internet users can help it succeed by volunteering our computers to be part of the relay network; more independently operated nodes make the network more secure and harder to spy on.

A glaring vulnerability in Tor is not one that can be exposed through complex penetration techniques artfully enacted by the most elite of hackers, but a problem that exists in the set up of the network itself. The security of the project relies in the trust a user can place in their exit node. As security researcher Dan Egerstad exposed in 2007, by investing in running exit nodes, any private group can spy on the traffic that runs through their nodes.[19]

Based on Egerstad's research, it seems possible that any well-funded agency could indeed support high-powered exit nodes equipped with surveillance technology. It is therefore highly plausible that the FBI and NSA maintain a portion of the Tor network. It is crucial that anyone considering using Tor to mask their origin understands that the US government (and foreign ones as well) maintains Tor through various grants and funding while simultaneously investing in attacks and the running of nodes to continue their relentless assault on user privacy.

To conclude, the information presented in this paper is not to aid those seeking child porn, guns or drugs in actualizing those goals without being caught, but rather to advise potential users about the dangers of Tor and the potential for being monitored on a network known chiefly for its anonymity. Understanding why this network exists, who uses Tor, who funds Tor, and what has been done through the network in the past is a necessity for anyone considering using Tor to mask their identity.

6. References

1. altoid. *A Heroine Store*, Bitcointalk, 29 Jan. 2011, bitcointalk.org/index.php?topic=175.msg42479.

2. altoid. *IT pro Needed for Venture Backed Bitcoin Startup*, Bitcointalk, 11 Oct. 2011, bitcointalk.org/index.php?topic=47811.msg568744.

3. arma. "Tor Security Advisory: 'Relay Early' Traffic Confirmation Attack." *Tor Blog*, Tor Project, 30 July 2014, blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.

4. "Common Vulnerabilities and Exposures." *CVE - CVE-2013-1690*, MITRE, cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2013-1690.

5. Cox, Joseph. "Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects." *Motherboard*, Vice, 11 Nov. 2015, motherboard.vice.com/en_us/article/gv5x4q/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects.

6. "DEF CON 22 - Adrian Crenshaw- Dropping Docs on Darknets: How People Got Caught." DEFCON, 29 Dec. 2014, www.youtube.com/watch?v=eQ2OZKitRwc.

7. "ExpressVPN | How to Generate a .Onion Address on Tor." *Home of Internet Privacy*, 5 July 2017, www.expressvpn.com/blog/how-to-create-a-onion-address/.

8. frosty. *How can I connect to a Tor hidden service using cURL in PHP?*, stackoverflow, 16 Mar. 2013, stackoverflow.com/questions/15445285/how-can-i-connect-to-a-tor-hidden-service-using-curl-in-php.

9. gk. "Tor Browser 7.0.9 is released." Tor Project, 3 Nov. 2017 www.torproject.org/tor-browser-709-released.

10. *Information Geographies*, geography.oii.ox.ac.uk/?page=tor.

11. International, Privacy. "A New Era of Mass Surveillance Is Emerging Across Europe."*Medium*, Privacy International, 17 Jan. 2017, medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d.

12. Johnson, Aaron, et al. "Users get routed: Traffic correlation on Tor by realistic adversaries." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.

13. Leyden, John. "HideMyAss Defends Role in LulzSec Hack Arrest." *The Register*, www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/.

14. Martin, Adam. "LulzSec's Sony Hack Really Was as Simple as It Claimed." *The Atlantic*, Atlantic Media Company, 22 Sept. 2011, www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/.

15. mikeperry. “This Is What a Tor Supporter Looks Like: Edward Snowden.” *Tor Blog*, Tor Project, 30 Dec. 2015, blog.torproject.org/what-tor-supporter-looks-edward-snowden.

16. Müller, Konstantin. “Defending End-to-End Confirmation Attacks against the Tor Network.” *Defending End-to-End Confirmation Attacks against the Tor Network*, 2015.

17. Poulsen, Kevin. “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack.” *Wired*, Conde Nast, 3 June 2017, www.wired.com/2013/09/freedom-hosting-fbi/.

18. *Tor Project | Privacy Online*, www.torproject.org/.

19. Zetter, Kim. “Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise.” *Wired*, Conde Nast, 4 June 2017, www.wired.com/2007/09/rogue-nodes-turn-tor-anonymizer-into-eavesdroppers-paradise/?currentPage=all.