Exploring the Threats Posed by Botnets on Onion-Routing

Internet Anonymity Systems as a Product of Government Imaginaries

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Justin Fabrizio

November 1, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Sean Ferguson, Department of Engineering and Society

Daniel Graham, Department of Computer Science

Introduction

Over the past two decades, the use of both computers and the internet has skyrocketed. In 2018, the U.S. Census Bureau found that 92% of American households owned a computer and 85% had broadband internet access(United State Census Bureau, 2018). With the prevalence of computer usage come concerns about what data is being collected by both state and non-state actors. While data collection can be seen as financially beneficial for many private companies and can improve user experience, data breaches have become an increasingly common occurrence in the United States and expose users to identity theft and other forms of fraud. Additionally, data breaches can also be financially destructive to the companies storing data; in 2015 it was estimated that data breaches cost a total of $10 billion annually in the U.S.(Romanosky, 2016). Internet data mining has also produced fears about government surveillance; federal wiretapping laws were once thought to protect citizens from online government surveillance, but evidence exists that federal entities including the NSA have in the past partnered with major tech companies to obtain data on their users. In recent years, these and many other concerns have put a spotlight on internet anonymity systems as a way to limit the amount of data given to websites and internet service providers. An internet anonymity system is any piece of infrastructure that provides internet communication without leaking enough information to identify the communicating parties(Oujani, 2011). The science, technology, and society portion of this paper will explore how the creators of internet anonymity systems have created a public imaginary around digital living that values anonymity and data privacy. The technical topic portion of this paper will discuss how the prevalence of botnets pose unique threats to modern internet anonymity systems that rely on onion routing.

Technical Topic

The most popular internet anonymity system is widely regarded to be Tor Browser, which is regularly estimated to have between 2 and 2.5 million distinct users annually (Tor Project, 2021). The security of Tor Browser lies in the layered encryption it provides by routing a client's traffic through a network of designated Tor nodes. Tor Browser uses AES encryption at the application layer in addition to TLS/SSLv3 encryption at the transport layer. When a client attempts to connect to a server through the Tor Browser, the first step in the connection is to establish a path through the network of Tor nodes. It is important to note that Tor nodes can be hosted by any volunteer, and as such, Tor Browser's path construction protocol abides by several rules to reduce the risk of profiling attacks. These include: never selecting the same node twice in any given path, never selecting multiple

nodes from the same family (groups of related nodes) for a given path, never selecting multiple nodes from the same subnet for a given path, and never selecting non-running or non-valid nodes.

For the majority of the past decade, between 6 and 8 thousand Tor Browser nodes have been active in the network (Tor Project, 2021). This number is dwarfed when compared to the size of many active botnets; groups of "zombie" computers that can be controlled by a single entity. For example, the Mirai botnet, which was discovered in 2016, was estimated to be composed of over 587,000 machines (Antonakakis, 2017). With botnets of this size and larger currently in operation, many more attacks against Tor Browser could be realized with the use of botnets. The Mirai botnet was primarily used to conduct distributed denial of service (DDoS) attacks, and, at face value, something as simple as a DDoS attack from the Mirai botnet could potentially be used to disrupt Tor traffic by flooding nodes with requests. However, when considering that Tor nodes can be hosted by nearly any willing machine, botnets could present a unique problem to the Tor network if many zombie machines in a botnet were configured to run Tor nodes. The current Tor path construction protocol detailed above would have no way of preventing Tor nodes running on zombie machines from being placed in the same path, which would allow for traffic correlation analysis to deanonymize Tor users when both the traffic of the entry and exit nodes are accessible to a malicious party. The continued security of anonymity systems in the face of such threats is of great importance as these systems have frequently been used to circumvent censorship and other forms of government overreach; one example of such uses was in 2011 when Egyptian activists expressed dissent online via Tor Browser after the Egyptian government cutoff internet connections during widespread protests (Cochrane, 2011).

The objective of this technical research paper will be to synthesize internet privacy topics with network security topics by exploring in more depth the problems botnets present to internet anonymity systems that use onion-routing, such as Tor Browser. Additionally, this paper will hope to provide solutions to these problems, or reasoning behind the lack thereof. Since this paper will be written outside of any larger team, the responsibilities of the author include the entirety of the research and writing required to fully explore this topic.

STS Topic

This section will explore how the creators of anonymity systems have produced a public imaginary in the United States that values both data privacy and anonymity systems. Considering that the U.S. government has remained a primary stakeholder in the development, regulation, and use of anonymity systems throughout their existence, a good

starting point for this research is to examine how government-held imaginaries have changed over the history of modern internet anonymity systems and how they have led to the public status quo of these systems.

A key piece of evidence that stands out when determining what the government's expectations were for the future of data privacy (in the early 2000's) can be found in the history of onion routing. The U.S. Naval Research Laboratory in Washington D.C. began researching secure encryption and routing methods in the early 1990's and had revealed a publicly accessible onion routing system in 1996. Furthermore, one of the computer scientists at that lab, Paul Syverson, would go on to co-found the Tor Project, a non-profit group that developed the open-source Tor browser that is the most popular implementation of onion routing today(Tor Project, 2021). This information can be interpreted in many ways with respect to the sociotechnical imaginaries prevalent in the government at the time. At a minimum, it shows that many people within the federal government expected a data-rich future as they were already funding research into secure internet communications over two decades ago. It is also important to note that providing this technology to the public for free appeared to be contradictory to the actions described in several government data surveillance leaks that would reach the public in the 2010s. The most prominent leak regarding government data surveillance occurred in 2013 and indicated that the National Security Agency (NSA) had been conducting data surveillance in partnership with major tech companies under a program codenamed "PRISM"(FTC, 2013). The disparity of these two government actions could be evidence of either a shift of imaginaries over time or simply the conflict between two different imaginaries, both remaining prevalent. Either of these explanations could help account for the large increase in use of online anonymity systems in recent years.

Additionally, it could be that many anonymity imaginaries exist within the federal government, but one is given preference over the others by American policy-makers. There is a multitude of evidence that supports this explanation as many incidents regarding anonymity systems have gained national attention only to highlight the detrimental effects of the technology while failing to show the benefits. This could result in a more negative opinion of anonymity systems in the eyes of American policy-makers, especially those who do not have a complete understanding of the technology. One such current event that drew negative attention to anonymity systems was the arrest of Ross Ulbricht in 2013 for his involvement in the operation of the "Silk Road", a Tor hidden service(U.S. District Court Southern District of New York, 2013). Tor hidden services are servers that are only accessible through the Tor network; Ulbricht's "Silk Road" service acted as an online black market in which it is estimated over 70% of the products offered were illegal drugs (Zajacz, 2016). Ulbricht's arrest led to increased attention on Tor and internet anonymity systems

from both the public and politicians alike. More importantly, this particular incident showed the American people the criminal uses of anonymity systems, in particular, how they could be used to channel illicit goods and services throughout the nation. Furthermore, the investigation and arrests were conducted by an entity of the federal government, the FBI, likely showing policy makers that pursuing criminals behind anonymity systems was not futile. When examining the incident from this angle, it can be concluded that it likely contributed to the popularity of a less data-private imaginary held by both the federal government and the public, as it showed how anonymity systems can greatly propagate illicit activity.

When considering the government's imaginaries regarding anonymity systems, it can also be valuable to examine their expectations of data privacy as a whole. Closely regulated wiretapping at the federal level has been permitted for criminal investigations since 1968 (Hibbard, 2012); however, much broader internet surveillance was authorized with the passage of the USA PATRIOT Act in October of 2001 which allowed Internet Service Providers to disclose customer information and traffic content to law enforcement agencies simply if the provider believed that death or serious injury would result without law enforcement intervention (Birnhack & Elkin-Koren, 2003). The passage of this law was preceded by the September 11th terrorist attacks by only a month; it can be presumed that the heightened fears of terrorist activity led to a less-private imaginary surrounding internet data to be preferred by federal entities during this time. The notion of government partnership with private entities for the purpose of data collection would be further reinforced by the NSA leak in 2013 which was mentioned earlier. Even within the past decade many incidents that fall under the broader category of "cyber attacks" have drawn concern from politicians at the federal level. One such example is the alleged presidential election interference in 2016, in which claims were made that Russian entities were responsible for information leaks involving employees of major U.S. political campaigns (United State Senate, 2019). While this particular piece of evidence may not directly involve systems like onion routing, they show how increased internet data surveillance is of use to federal entities and can be valuable to politicians. This, in turn, affects the sociotechnical imaginaries surrounding anonymity systems as a whole. Despite the apparent increase in internet data surveillance by the U.S. government from 2001 onwards, it is important to note that federal funding of anonymity systems had not ceased; the Tor Project itself received over $1.8 million in grant funding from the federal government in 2013 alone(Tor Project, 2013).

Considering this evidence, it is apparent that government research and funding has been at the cornerstone of internet anonymity systems throughout their existence. From the varied actions of the U.S. government regarding both anonymity systems and data

privacy, it can be inferred that many competing imaginaries surrounding anonymity systems coexist within the government. This is to be expected due to the democratic nature of the U.S. government and the large number of separate agencies that operate under it. These competing imaginaries have all contributed to the popularity of anonymity systems within the American population as pro-privacy imaginaries led to the very creation of these systems and, on the other hand, the emergence of data-surveillant imaginaries emphasized their beneficial uses to the public.

Next Steps

For the technical research topic described above, the next steps in this project include providing more in-depth and detailed research into the threats that botnets pose to anonymity systems that use onion-routing. In particular, this research will hope to explore more real-world evidence of the current capabilities of botnets and what internet anonymity systems have implemented to prevent such attacks. The overall feasibility and efficacy of such attacks will also be analyzed. Additionally, I hope to put forth solutions to problems that my research may uncover, and, if not, describe the technical reasoning behind why solutions could not be proposed. A timeline of future work for this project consists of concluding background research by mid-February with a complete draft being completed by the end of March 2022. This schedule will provide ample time for both research into existing problems concerning onion routing as well as possible solutions for such problems.

For the STS topic in this paper, continued research into government actions that are indicative of imaginaries surrounding anonymity systems will be necessary to reach a more well-rounded conclusion. It may also be helpful to broaden the amount of stakeholders being examined to include any non-state actors that have played a role in the creation of anonymity systems. Additionally, more evidence must be gathered on the status quo of internet anonymity systems from a public standpoint. This information will be valuable when examining how sociotechnical imaginaries within the government have affected the public status quo of these systems. The timeline for this work is to finish gathering evidence by March 2022 and have reached a conclusion and produced a complete draft by the beginning of April.

References

Bureau, U. S. C. (2021, April 19). Computer and internet use in the United States: 2018. The United States Census Bureau. Retrieved October 4, 2021, from https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html.

Romanosky, S. (n.d.). Examining the costs and causes of cyber incidents. Federal Trade Commission. Retrieved October 17, 2021, from https://academic.oup.com/cybersecurity/article/2/2/121/2525524.

Government surveillance and the internet. (n.d.). Retrieved October 4, 2021, from https://www.ftc.gov/system/files/documents/public_comments/2015/10/00023-97629.pdf.

The Tor Project: Privacy & Freedom Online. Tor Project. (n.d.). Retrieved October 4, 2021, from https://www.torproject.org/about/history/.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017, January 1). Understanding the Mirai botnet. Google Research. Retrieved October 17, 2021, from https://research.google/pubs/pub46301/.

Birnhack, M., & Elkin-Koren, N. (2003, April 10). The invisible handshake: The reemergence of the state in the digital environment. SSRN. Retrieved October 17, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=381020.

Hibbard, C. M. (n.d.). Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance. Retrieved October 17, 2021, from https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1617&context=fclj.

Oujani, A. (n.d.). Tools and protocols for anonymity on the internet. Retrieved October 17, 2021, from https://www.cse.wustl.edu/~jain/cse571-11/ftp/anonym/index.html#Anonymity.

Second Post-Complaint Protective Order - Silk Road. (n.d.). Retrieved October 17, 2021, from

https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Second%20Post-Complaint%20Protective%20Order%20-%20Silk%20Road.pdf.

Servers. Tor Metrics. (n.d.). Retrieved October 17, 2021, from https://metrics.torproject.org/networksize.html.

The Tor Project, inc.. and affiliate consolidated financial ... (2013, December 31). Retrieved October 17, 2021, from https://www.torproject.org/static/findoc/2013-TorProject-FinancialStatements.pdf.

United States Senate Select Committee on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. (n.d.). Retrieved October 17, 2021, from https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

Zajacz, R. (2016, April 17). Silk road: The market beyond the reach of the State. Retrieved November 1, 2021, from https://clas.uiowa.edu/commstudies/sites/clas.uiowa.edu.commstudies/files/Zajacz_SR16_proofs.pdf.

Cochrane, N. (2011, February 2). Egyptians turn to Tor to organise dissent online. SC Magazine. Retrieved November 1, 2021, from https://web.archive.org/web/20111213154629/http://www.scmagazine.com.au/News/246707,egyptians-turn-to-tor-to-organise-dissent-online.aspx.