INFRASTRUCTURE CONCERNS IN DESIGNING A CLOUD-BASED ONION ROUTING NETWORK

POLICY CONSIDERATIONS FOR IMPROVING THE NET IMPACT OF ONION ROUTING TECHNOLOGY

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
VINEET KALPATHI

November 2, 2020

Technical Project Team Members
Jack Good and Brandie Young

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.

Signed Vineet Kalpathi Date: November 2, 2020

Approved: Date:
Ashish Venkat, Department of Computer Science

Digitally signed by Ashish Venkat
Date: 2020.11.02 15:52:45 -05'00'

Approved: Date:
Catherine D. Baritaud, Department of Engineering and Society

The world's unfaltering use and extensive dependance on the internet has resulted in a wide variety of mechanisms used to target and surveil users, websites, or entire organizations online. This heightened tracking of internet activity stems from a plethora of motives, whether it be for marketing schemes, government surveillance, or malicious cyberattacks on a specific entity. The increased vulnerability of user privacy on the internet is largely attributable to the well-known protocols that our internet has been running on since its inception. For example, a compromised encryption key could allow a malicious user to intercept messages en route from sender to receiver and easily decode an encrypted message, subsequently identifying both parties involved and the data sent between them. Given the importance of many present-day processes that rely on the internet, attacks on privacy could potentially have grave consequences depending on the nature of the communication. This identifies a need for a routing protocol that could prevent such large-scale monitoring of internet activity.

The Onion Router (TOR), also known as anonymity network or the dark web, is a system of both software and hardware dedicated to providing users with a completely anonymous way to browse the internet. Backed by a network of volunteered servers (also known as relays or nodes), TOR provides anonymity to users by implementing an internet routing protocol called 'onion routing.' Unlike ordinary protocols, onion routing intentionally obfuscates transmitted messages through layered, asymmetric encryption, thus preventing any outsider from discerning a message's source, destination, or content.

When a client wants to communicate with a server on TOR, the protocol first establishes a connection between the two parties by defining an *onion*, or a random path of relays and each relay's relevant cryptographic information. Using the public keys of every node along the circuit, the sender encrypts the message multiple times in layers, such that each node along the

message's path can only decrypt a single layer of the message—much like the peeling of an onion. Each decryption during the message's journey only reveals the identity of the next node along the path, ensuring that only the destination relay can decode the true message, and that each intermediate relay only knows its immediate neighbors along the route; therefore, the identities of the true source and destination of every message on the TOR network are hidden (Goldschlag, Reed, & Syverson, 1999, p. 2).

By establishing these secure connections that prevent both packet sniffing and traffic analysis, onion routing grants anonymity to both clients and servers on the TOR network, allowing for the existence of hidden services accessible only through TOR. These anonymity-granting systems enable the proliferation of cybercrime such as illegal markets and pedophilia rings; however, in an age of increased internet censorship, data mining, and surveillance, these systems also grant users with increased security, privacy, and freedom while surfing the web.

I, along with fellow fourth-year computer science students Jack Good and Brandie Young, plan to explore the design details of a cloud-based onion routing system for the purpose of improving the overall security and performance of TOR over the course of the Fall 2020 semester. We plan to finish our technical research and report by the week of November 9. My tightly-coupled sociotechnical topic deals with analyzing the wide-ranging interpretive flexibility of TOR and discussing the potential of online policing and other policy to mitigate cybercrime while promoting global internet freedom. The majority of my STS research will be completed in the Spring 2020 semester, resulting in a complete report by the middle of March.

INFRASTRUCTURE CONCERNS IN DESIGNING A CLOUD-BASED ONION ROUTING NETWORK

Although the dark web's volunteer-based infrastructure model preserves anonymity through its decentralized nature, it also poses adverse effects on the network's overall performance and security. There are a limited number of volunteer-run relays located worldwide, subject to highly variable network performance depending on the host's location and Internet Service Provider plan. Relays with limited access to network bandwidth create bottlenecks within onion-routed circuits, negatively affecting the latency of TOR connections (Jones, Arye, Cesareo, & Freedman, 2011, p. 1). Additionally, the dark web relies on a few well-known entry nodes for onboarding users to the network, which allows for network administrators to easily censor content or block all anonymous traffic by blacklisting all known TOR addresses (Laurikainen, 2010, p. 3). This is also how authoritarian governments can censor the spread of information amongst and beyond its populations, stifle criticism, and ultimately oppress its citizens.

Several studies suggest the potential for cloud infrastructure to greatly mitigate these performance and security issues caused by TOR's current infrastructure model, presenting an incredibly efficient and secure method of browsing the internet freely. Thus, the objective of our project is to explore the fairly novel design space of applying cloud computing to TOR, otherwise known as cloud-based onion routing (COR).

THE APPLICATION OF CLOUD TECHNOLOGY TO TOR

The sheer scalability and elasticity of services presented by major cloud hosting providers (CHPs), such as Amazon Web Services, Microsoft Azure, or Google Cloud, could tremendously enhance TOR's user experience. An experimental implementation and analysis of COR yielded results that exhibit client download times 7.6× faster than TOR (Jones et al, 2011, p. 5). Another

small-scale implementation that utilized dynamically-addressed virtual machine (VM) relays proved to be highly tolerant against denial-of-service attacks, given that CHPs can simply spin up new VM relay instances to handle overwhelming amounts of traffic (Nedeltcheva, Vila, & Marinova, 2019, p. 395). These initial results are extraordinarily promising; however, these experiments fail to encompass the added complexity of involving CHPs in the anonymity network's infrastructure at a large scale.

The preservation of anonymity provided by TOR lies within the trust of users and the volunteers running and maintaining the network's relays. A cloud-based model adds several relationships to the picture, including the relationship between CHPs and end users. Given that direct payment systems between CHPs and users could completely deanonymize all network activity and render all onion routing useless, a large concern for implementing COR is deciding who is responsible for the cost of running relays provided by CHPs. Jones et al (2011) suggest the need for an additional entity, called an "anonymity service provider" (ASP), to purchase relays and provide a secure, anonymous transaction for users to pay for access to these nodes (p. 2). Additionally, a fully anonymized implementation of COR requires the existence of *multiple* ASPs to ensure that no single entity has the ability to oversee and discern which relays are carrying a given user's traffic. The distinction between users, destination servers, CHPs, and ASPs is illustrated in Figure 1. The figure shows the role of ASPs

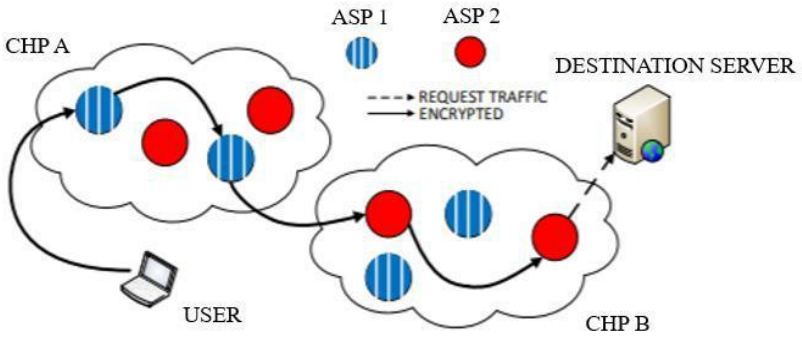

Figure 1: Typical Cloud-based Onion-Routed Circuit. A depiction of a COR circuit, illustrating the relationships between user clients, destination servers, cloud hosting providers, and anonymity service providers (Adapted by Kalpathi, 2020 from Jones, 2011, p. 2).

in purchasing relay access from CHPs, and granting access to users who want to communicate with servers anonymously. The illustration also depicts a user's traffic routed through multiple CHP data centers and relays owned by multiple ASPs in order to preserve the connection's anonymity. The issue of designing an anonymous payment framework for COR is an untapped area of research that our team is looking to dive into.

THE HOLE IN CURRENT RESEARCH AROUND COR

Our technical research will utilize existing literature and data to analyze the tradeoffs of different types of cloud compute resources and network configurations and their effect on the key metrics of secure communications within a cloud-based onion routing network. The target metrics will likely include latency, throughput, monetary cost per user, usability, and of course the preservation of security from local and global network adversaries. Our current plan of attack is to divide the various cloud computational resources amongst ourselves and each to conduct a deep dive into assigned our subject areas. Our group also hopes to conduct small experiments with small-scale COR circuits to exhibit the benefits of certain AWS resources over others.

With the oversight of professor Ashish Venkat and graduate student Felix Lin from the Department of Computer Science, we aim to conduct a comprehensive investigation which will result in reasonable suggestions towards what kind of computational resources and configurations will yield the highest performance, multi-user capacity, preservation of security, and usability at the lowest cost to the ASP and end users. Our work will result in a scholarly article that could act as a reference for anybody looking to start an ASP-like entity. We sincerely hope that our work will add value to the fairly novel design space of COR, and that once implemented, COR will better defend the Internet freedom and privacy of users over the existing TOR.

IMPROVING THE NET IMPACT OF ONION ROUTING TECHNOLOGY

The empowering character of anonymity-granting systems makes technologies like TOR inherently political. Media coverage often focuses on the gruesome cybercrime that occurs on the dark web, such as law enforcement's crackdown on child pornography site Freedom Hosting and the largest online anonymous drug market, the Silk Road—two of the dark web's most prominent hidden services (Weimann, 2016). This naturally creates antipathy towards TOR, regardless of the freedom that the it grants repressed individuals. The dark web is not typically associated with the ability of journalists to communicate with sources and political activists in more authoritarian regimes. Nor is there significant media coverage of TOR's ability to aid the oppressed, notably in helping Syrian families communicate and survive in war-torn areas like Homs. (Borland, 2013). Needless to say, TOR's diverse usage is largely dependent on the regimes that users reside within.

Jardine (2018) exhibits a consistent, U-shaped association between political structure and TOR usage, suggesting that "repression [drives] usage of Tor the most in … highly liberal and highly repressive contexts and the least in partly free countries" (p. 445). The opportunity, or lack thereof, that individuals are granted by political regimes directly affects how TOR is used, observing the highest rates of cybercrime in democratic countries and the highest rates of political activism in more restrictive countries (Jardine, 2015, p. 4). Using the Technology and Social Relationships model (Carlson, 2007, p. 3), Figure 2 maps the prominent relationships between TOR-using citizens and regimes of both authoritarian and democratic nature.

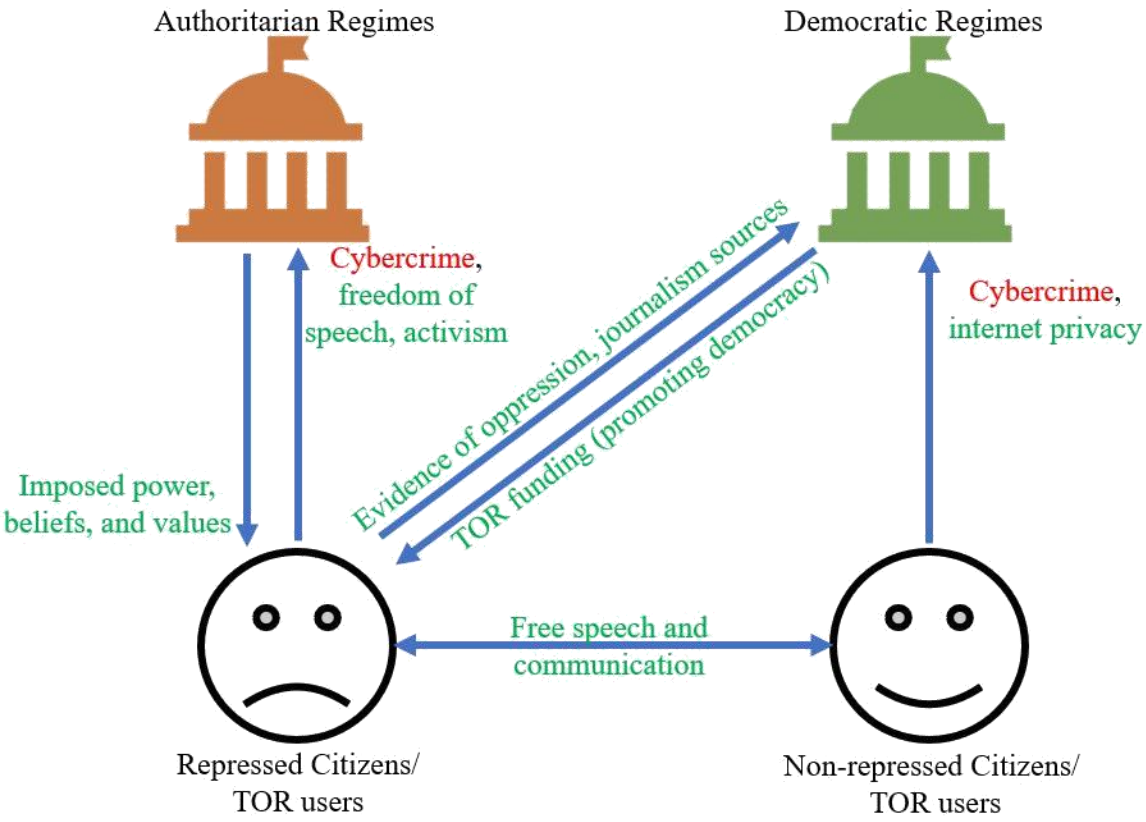

Figure 2: A Sociotechnical View of Relationships between TOR Users and National Regimes. A depiction of the relevant interactions between regimes and TOR-using citizens (Kalpathi, 2020).

It can be observed that much of TOR's utilization is beneficial, given its widespread promotion of democracy. But the overwhelming presence of cybercrime on the network continues to outshine the advantages, giving rise to conversations about putting an end to anonymity-granting networks. How can TOR shake its evil reputation and begin to be known for its tremendous avails?

MITIGATING THE NEGATIVE IMPACTS OF TOR

Given the prevalence of cybercrime on the anonymous network, it is reasonable to expect that TOR's net effect could be improved by attacking the ability of users to conduct illegal activity through the dark web. But unfortunately, onion routing technology is only in charge of

regulating how data is transmitted on the internet to provide anonymity for the user, and largely unconcerned with how users leverage this technology. If developers were to modify TOR with the intention of identifying cybercriminals, they would simultaneously be working to aid oppressive regimes in identifying which citizens are acting out of line. Given that repressed citizens and cybercriminals both benefit from the anonymity of TOR, any development to onion routing technology will have a negligible effect on its ultimate impact.

As shown in Figure 3, Pacey's Triangle of Technology Practice (Pacey, 1983, p. 6) identifies two more potential realms of modification: cultural and organizational. The figure demonstrates the larger network that onion routing technology is embedded within. Pursuing a change in culture to mitigate the malice of TOR would suggest changing the very nature of authoritarianism and democracy, or alternatively, the mindset and motives of cybercriminals; the world would be a much more benevolent place if humans had this power. Any modification to aid in improving the dark web's net impact should therefore be an organizational concern, primarily a change in institutions and policy.

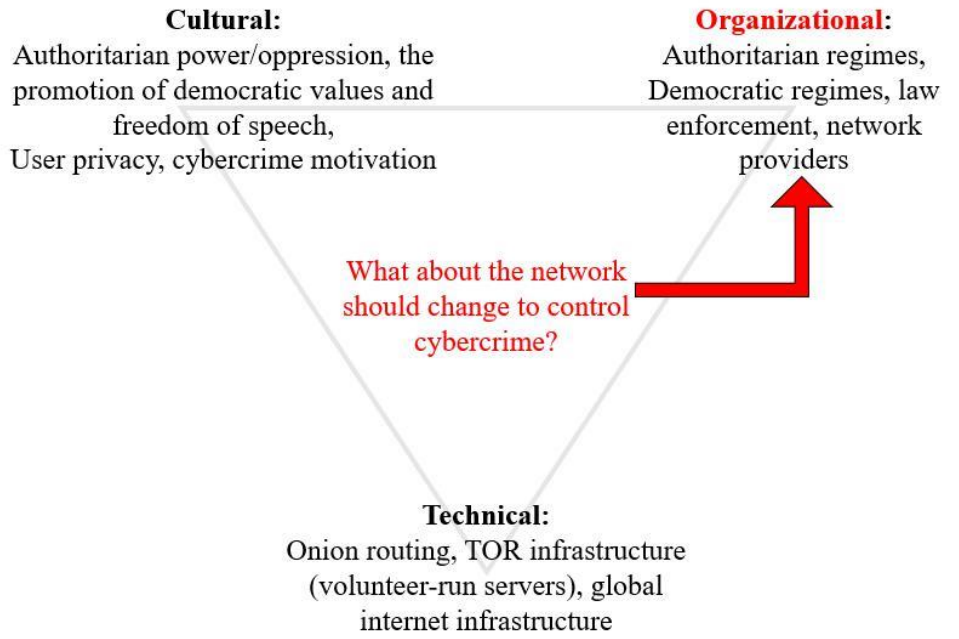

Figure 3: The Onion Router in the Context of Pacey's Triangle. This illustration highlights the cultural, organizational, and technical aspects of the network surrounding TOR and its users (Kalpathi, 2020).

As suggested by the figure above, the most feasible approach to prevent the proliferation of illegal activity on TOR would be to propose a change to institutional aspects of the larger social network in which the anonymity network resides.

A reasonable solution to control cybercrime while allowing repressed citizens to practice internet freedom would be to actively police the TOR network, but the application of new institutions and policy requires several considerations to ensure that existing organizational, cultural, and technological systems are not broken. Jardine (2015) acknowledges the required growth of law enforcement to support online policing, including global jurisdiction complications, national and local cooperation, and required cybercrime training for officials. He also touches on the ambiguity around enforcement regulations, encouraging the warrant-based monitoring of hidden illegal websites *on top* of existing internet infrastructure to avoid illegal breaches of privacy and the destruction of internet technology (p. 9-10). These concerns elucidate the complexity of implementing such a modern institution, and the lack of practical examples available in the realm of internet governance.

My STS research will focus on exploring the potential of online policing and other policy to mitigate the ills of onion routing technology while simultaneously allowing TOR to continue to promote democracy. I plan to investigate TOR's interpretive flexibility within an Actor Network Theory (ANT) framework, inspecting the interactions between repressive regimes and their citizens, democratic regimes and their citizens, law enforcement agencies, and network providers to provide logical propositions for policy while taking conflicting interests within the overall network into account. Under the guidance of professor Catherine Baritaud, from the Department of Engineering and Society, I hope to compose a comprehensive research paper highlighting the major considerations in enacting policy to promote policing, or otherwise controlling cybercrime on the TOR network.

The Onion Router is not without its drawbacks; TOR's network can exhibit poor performance, reliability, and has the potential to be blocked. The advent of cloud computing, which has the ability to solve TOR's shortcomings, allows for on-demand provisioning of massive computing performance and connectivity. Additionally, the dark web's anonymity empowers a variety of users, ranging from cybercriminals to helpless citizens under authoritative rule. Mitigating the cybercrime that circulates the TOR network would allocate more bandwidth for positive, democracy-promoting uses of the anonymity network. Through our project we hope to answer the sociotechnical question: *How can the security and integrity of the TOR ("The Onion Router") anonymity network be strengthened to better protect Internet users' privacy and Internet freedom?*

REFERENCES

Borland, J. (2013, December 28) For tor, publicity a mixed blessing. *Wired*. Retrieved from http://www.wired.com/2013/12/tor-publicity-mixed-blessing/

Carlson, W. (2007) STS frameworks [Online handout]. Retrieved from UVA Collab: https://collab.its.virginia.edu/access/content/

Gehl, R. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219-1235.

Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion routing for anonymous and private internet connections. *Communications of the ACM*, *42*(2), 39-41.

Jardine, E. (2015). The dark web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series*, 21, Retrieved from https://papers.ssrn.com/sol3/

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New media & society*, *20*(2), 435-452.

Jones, N., Arye, M., Cesareo, J., & Freedman, M. (2011). Hiding amongst the clouds: A proposal for cloud-based onion routing. *FOCI*. Retrieved from https://www.usenix.org/legacy/

Kalpathi, V. (2020). *A sociotechnical view of relationships between TOR users and national regimes*. [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Kalpathi, V. (2020). *The onion router in the context of Pacey's Triangle.* [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Khan, S. M., & Hamlen, K. W. (2012, June). AnonymousCloud: A data ownership privacy provider framework in cloud computing. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 170-176). IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/

Laurikainen, R. (2010). Secure and anonymous communication in the cloud. *Aalto University School of Science and Technology—Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10*, 1-5.

Mortier, R., Madhavapeddy, A., Hong, T., Murray, D., & Schwarzkopf, M. (2010). Using dust clouds to enhance anonymous communication. *Cambridge International Workshop on Security Protocols* (pp. 54-59). Springer, Berlin, Heidelberg.

Nastuła, A. (2020). Dilemmas related to the functioning and growth of Darknet and the Onion Router network. *Journal of Scientific Papers—Social development and Security*, *10*(2), 3-10.

Nedeltcheva, G. N., Vila, E., & Marinova, M. (2019). The onion router: Is the onion network suitable for cloud technologies. *Smart Technologies and Innovation for a Sustainable Future* (pp. 389-398). Springer, Cham.

Pacey, A. (1983). *The culture of technology*. MIT press.

Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015). SoK: secure messaging. *2015 IEEE Symposium on Security and Privacy* (pp. 232-249). IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, *39*(3), 195-206.