IMPROVING THE PERFORMANCE, SECURITY, AND NET IMPACT OF ONION ROUTING TECHNOLOGY

An STS Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

By
VINEET KALPATHI

Spring 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

Signature VINEET KALPATHI Date __________
Vineet Kalpathi

Approved ____ Date __________
Richard Jacques, Department of Engineering and Society

SOCIOTECHNICAL SYNTHESIS

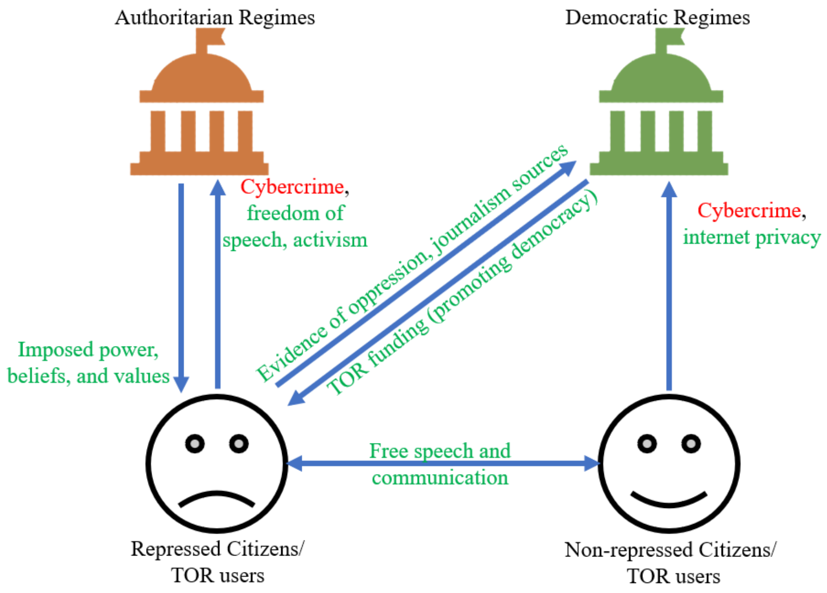
(Executive Summary)

Society's widespread use and extensive dependence on the internet has resulted in a large variety of mechanisms used to target and surveil users online. This 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. The Onion Router (TOR), also known as anonymity network or the dark web, is a system of both software and hardware dedicated to providing anonymity to users by implementing an internet routing protocol called onion routing. This scheme intentionally obfuscates transmitted messages through layered, asymmetric encryption, thereby preventing any outsider from discerning a message's source, destination, or content.

Although the technology has a tremendous potential to preserve our online privacy, the Onion Router is not without its drawbacks; TOR's current infrastructure often exhibits poor performance and permits authoritative adversaries to block the network entirely. In addition, much of the anonymous network's bandwidth is leveraged for cybercrime such as illegal markets and pedophilia rings. My research attempts to improve upon TOR's shortcomings to allow for a more extensive adoption of onion routing technology within the multitudinous procedures that depend on secure internet connections to preserve user privacy. Through my research, I aim to diminish the power of unauthorized entities to surveil users and boost the public's confidence in their capacity to surf the internet freely. My technical work focuses on leveraging the scalability and elasticity of cloud computing to overcome TOR's performance and security issues, and my STS research deals with institutional changes to mitigate the unlawful exploitation of the dark web.

While existing literature proves the feasibility of a cloud-based onion routing system, the technical portion of my thesis explores specific configuration tradeoffs in implementing a large-scale anonymous network in the cloud. Our group evaluates specific Amazon Web Services (AWS) configurations—notably Elastic Compute Cloud (EC2) purchasing options and instance types, bandwidth requirements, Amazon Regions and Availability Zones, and network topologies—under the metrics of latency, throughput, monetary cost per user, usability, and the preservation of security from local and global network adversaries. The results of our research prescribe appropriate AWS services and configurations for future research aiming to implement a cloud-based onion routing network.

In my STS research, I describe the dual nature of the dark web. While TOR's anonymity allows citizens of repressive regimes to circumvent censorship, voice minority opinions, communicate with journalists in more liberal countries, and otherwise browse the internet freely, the same cloak of anonymity enables criminals to conduct illegal transactions online. I use Actor Network Theory to identify the different groups concerned with TOR's usage, notably authoritarian and liberal regimes and their citizens. The following figure depicts these actors and their relationships in the context of the dark web.



After outlining the conflicts of interest involved in the usage of the anonymous network, I consider potential solutions to mitigate the evils of TOR while bolstering its boons. Through my analysis, I propose that establishing an online policing institution is perhaps the most effective method to achieve this goal; however, the required growth of law enforcement agencies, complexity of determining whose jurisdiction a given cybercrime falls under, and difficulty of conducting a legally-sound online investigation are all complications that must be overcome in order to ensure the efficacy of such an institution. Considering these factors, I suggest the establishment of a multi-national agency that has its own technical cybercrime training institution and spans multiple jurisdictions, with an established, warrant-based method to monitor hidden illegal activity on top of existing internet infrastructure. Although this solution requires significant attention from powerful world organizations, it is an important first step in adopting onion routing technology to enhance the overall security of the internet.

Through my attempt to strengthen the performance, security, and integrity of the dark web, I have come to recognize the importance of respecting the ramifications of my work on the stakeholders of the technology. I cannot merely heed only the technical aspects of my work—the cultural and organizational aspects are equally as important. As our lives become increasingly reliant on cyberspace, I aim to ensure that the internet promotes values of privacy and equality for all. The enhancement of internet privacy is a vital step in ensuring that the internet is a reliable place for the future of our global society.