Thesis Project Portfolio

Round Trip Time and Hop Count for Geolocation in Request Tracing and Classification

(Technical Report)

Social Media Manipulation and the Impact on Digital Security

(STS Research Paper)

An Undergraduate Thesis

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

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

Connor Robert Wilson
Spring, 2024
Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Round Trip Time and Hop Count for Geolocation in Request Tracing and Classification

Social Media Manipulation and the Impact on Digital Security

Thesis Prospectus

Sociotechnical Synthesis

The underlying theme shared by my technical proposal and STS research paper is the concern for digital security in a world that becomes increasingly digitized every day. While this digitization comes with countless benefits and those should not be discounted, it is also important to address the threats that accompany building our world upon a complex combination of fiber optic cables and vast computer networks. As society continues to become more and more reliant on computers to communicate and do business, the attack surface, or opportunity for exploitation of those systems, increases. While digital security is a multifaceted topic with many subtopics deserving of discussion, this capstone focuses on two specifically: packet filtering and classification in computer networks for my technical proposal and the impact of social media manipulation on digital security for my STS research paper.

The internet, to put it simply, is composed of a large number of interconnected networks, which themselves are composed of smaller networks and end points (devices). One of the challenges currently faced by network and security administrators is that of classifying and filtering traffic coming into one's network to ensure the safety of the network as a whole. Such traffic comes in packets and each packet has a variety of fields that can be used to classify where it comes from, where it wants to go, and other associated information. Despite having that information, the more the administrator(s) of the network in question know about the traffic flowing in and out, the better. One such piece of information is the location of origination. At first, this seems a simple problem; one can determine the approximate and sometimes precise geographic location of origination by looking up the sender's IP address. However, with the introduction of IP spoofing and other related techniques to obscure the identity of the packet's sender, this information is significantly harder to come by.

My technical report outlines a proposal for methodology that uses a combination of round trip time, hop count, and known dominant pathways for packet travel to approximate location of origination. This solution is novel in that while related work is largely centered around detecting IP spoofing and related IP obfuscation techniques, this methodology aims to provide information on where the traffic came from. The proposed method is most applicable in a network security context, with a high potential for application in a defense context or any other context in which a large portion of incoming malicious traffic originates from the same region(s). Future work should aim to employ and optimize this methodology as it currently would involve significant computation resources to run iteratively.

My STS research paper aims to bring attention to manipulation in social media and the impact that it can have on a user's or organization's digital security. Over the past few decades, the introduction and proliferation of social media has changed the way that society interacts and consumes information drastically. More and more, the newer generation is consuming its news and communicating via platforms like Facebook, X (formerly Twitter), Instagram, and TikTok. With this pattern, it becomes increasingly important to ask oneself not only about not only the validity of the information one consumes on social media but also the intent of the content creator.

The STS analysis focuses primarily on two cases to support the claim that social media can be used as a medium to influence the actions of large groups of users: that of Twitter in the 2016 and 2020 U.S. presidential elections and that of TikTok. Discussion of supplementary literature is also used to highlight the connection between the power that social media has to influence large user groups and the risk to holistic digital security of that population. Specifically, the STS framework of Conversation Analysis (stemming from the Theory of

Technological Mediation) is used to highlight patterns observed in the general conversation about those cases and raise questions about the motive behind creating and posting content, how users react, and what it means for digital security. Key in combating the threat posed to digital security will be the education of users not only on best-practices in digital security but also on informed decision making.

Ultimately, this thesis portfolio serves not only to propose and inspire a new method to improve general organizational ability to secure networks, but to inform users on a topic that will only become more prevalent as we continuously rely on social media over the next decade and more.