Round Trip Time and Hop Count for Geolocation in Request Tracing and Classification (Technical Topic)

Social Media Manipulation and the Impact on Digital Security (STS Topic)

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 of the Degree
Bachelor of Science in Computer Science

By
Connor Wilson

December 8, 2023

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

ADVISORS:

William Davis, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

Table of Contents:

Introduction:

In a time where digital technology permeates almost every aspect of modern life, the security of the various computing systems we use every day has become paramount to our ability to function in society. According to an independent study done by the Ponemon Institute in 2012, the average cost for each minute of downtime following a Distributed Denial of Service (DDoS) attack [on an organization] is $22,000 (Ponemon Institute, 2012). For an individual user, a data breach of a company that you trust could mean your identity is stolen or even make you the target of an individual attack depending on the information stolen. Such things happen more often than you might think – credit card reporting company Experian reports that your social security number will sell for as little as $1 on the dark web, while other logins and medical records can start at as little as $1 or sell for much more depending on the nature of the document or login information in question (Experian, 2017). Other types of attacks on individuals can also result in loss of important information like school or work documents due to ransomware or sabotage, not to mention the personal financial loss that often accompanies such attacks. In the midst of this constantly evolving threat landscape, users are faced with the decisions of whether or not to trust a service or application enough to use it.

Digital security, within the context of this analysis, pertains to the protection of networks, computer hardware, computer software, or data from unauthorized or malicious access, modification, destruction, or theft. Computer Security is a broad, constantly evolving field that consists of a variety of technologies and practices designed to ensure the confidentiality, availability, and integrity of the computing systems on which modern society so heavily depends on (Lin, 2023).

Technical Topic:

The rise of cyber security as a field has been an exciting one. Notable in that realm is the more specific field of network security, which is focused on fortifying the vast computer networks that modern society operates on and around. Key in network security is protecting one's network from outside threats, often accomplished by classifying and filtering potentially malicious traffic as it attempts to enter a network. One example would be that of a Security Operations Center (SOC) analyst creating rules classifying what behavior should or should not be flagged as suspicious. This often took the form of a hard-coded rule in which activity or traffic that contained certain indicators or came from/went to certain sources was always flagged. Similarly, an SOC will often utilize a database of known malware and attack patterns and compare traffic coming into the system they are responsible for to that database. This technique is known as signature-based detection and provides a fantastic first line of defense against *known* exploits and attack patterns.

However, it is the nature of the computer and network security field that the threat landscape is constantly changing and evolving. New attack vectors are constantly being developed by all sorts of actors both malicious and benign. These never-seen-before exploits, known as "Zero Days" are incredibly valuable and have created their own market in the global economy (Egelman et al., 2013, p. 1). On the other hand, malicious cyber actors are constantly finding new ways to change the signature of their malware and avoid signature detection. The existence of such exploits means that signature matching will never be a perfect or even effective solution, especially in the modern threat landscape (Scott, 2017, p. 8). Defense against such exploits requires a diligent and well educated user to stop or mitigate the effects of the exploit in question.

The seemingly obvious answer to this problem is to make the security posture of the network or system very rigid. Permissiveness is an important concept in security as it determines how likely a network or system is to allow things in. The two most basic postures are to always allow traffic and always deny traffic. Always allowing traffic means that a system will implicitly trust things unless told otherwise by a user. To always deny traffic means the opposite. A very rigid, non-permissive system will typically have a policy that will deny most or all traffic and allow only traffic that the user specifies. While they are more secure, systems with this posture can be difficult for users because whenever a user has to do something that has not been explicitly allowed they must go through the trouble of allowing it (sometimes a complicated/tedious process). On the other hand, a less secure but more permissive system allows the user much more flexibility while requiring more diligence as far as security is concerned (Malik, 2003).

In an effort to combat these difficulties in classifying incoming threats and developing an effective security posture, the technical portion of this thesis portfolio proposes a method for determining the geographic location of origination for incoming packets in an effort to give analysts and administrators the information needed to make better decisions concerning the security of their network. While such information may not seem significant initially in a security context, it is actually incredibly applicable. For many large networks but especially in defense contexts, it is not uncommon for a majority of traffic originating from certain geographic regions to be malicious. Knowledge of the true geographic location of the sender could prove an invaluable piece of data for analysts as they attempt to identify patterns and flag suspicious traffic.

STS Topic:

Now focusing on the STS aspect of this analysis, the problem in question is that of how social media can affect a user's digital security. A study conducted by the Pew Research center in 2022 found that around half of US adults use social media as a news source at least some of the time, while almost a third of surveyed adults responded that they regularly use Facebook (Meta) as a news source. Platforms like Twitter, now rebranded X, (14%) and TikTok (10%) also saw a significant percentage of survey respondents regularly using their platforms to consume news. For Platforms like Snapchat, Reddit, and TikTok, 50% or more of users that regularly consumed news on those platforms were under the age of 30 (Pew Research Center, 2022).

These findings show a trend – social media is becoming more and more relevant as a news platform rather than just an avenue to share life with friends and family. This is evidenced not only by the presence of large scale media outlets such as Fox, CNN, and others on social media platforms but also by the prolific use of social media in political maneuvering and elections. There have been numerous studies done on social media's effects in various elections, some notably indicating that platforms like X (formerly Twitter) lowered the Republican vote share in both the 2016 and 2020 United States Presidential elections (Fujiwara et al., 2023).

These platforms and their services are valued enough by such a large majority of users that it has created pressure on individuals to participate in these forms of social media (Qin et al., 2011). This popularization and pressure to participate in social media has made social media platforms especially important in shaping public opinion in today's American society. Social media is therefore not only an avenue through which user perception can be directly affected though explicitly addressing a topic like digital security, but also provides an avenue to indirectly influence a user's perception. The latter is perhaps more concerning as a user's perspective and

consequential actions could affect a user's security without said user ever realizing it. As an example, one particularly alarming study was done in which a vast majority of users signed agreements hidden in the terms of service and privacy policy of a fictitious social networking service without reading them. In doing so, those users unknowingly agreed to sharing data with the NSA and providing a first born child as payment for access to said service (Obar & Oeldorf-Hirsch, 2020). In this way, using social media as an avenue through which to promote the use of such services or the capabilities those services provide could indirectly cause a user to compromise their security.

Related closely to this idea of the way social media interacts with its human users is Peter-Paul Verbeek's theory of technological mediation. Technological mediation theory approaches technologies, social media in this case, and seeks to analyze them as mediators of the relationships humans have with the world around them (Verbeek, 2015, p. 190). This theory can easily be applied to social media as it affects human interactions with digital security, with further potential for digital security technologies to be analyzed through a lens of technological mediation in turn. Conversation analysis (CA), as Verbeek describes it, seems particularly promising as a framework through which to analyze this interaction, providing a way to think about how people make claims or take actions that will affect digital security based on what they see on social media (Verbeek, 2015, p. 192, 195).

Using Verbeek's theory of technological mediation and specifically CA as a framework through which to explore the interactions between not only social media and humans but also digital security technologies and humans, this analysis will aim to shed light on the way users interact with social media and how those interactions may be negatively impacting the digital security of those users.

Conclusion:

With the widespread implementation of identity obfuscation techniques like IP spoofing in computer networking, it is becoming harder than ever to accurately determine the source of the millions of packets that constantly flow into large networks. Location of origination is a piece of data that, if successfully determined, could help network administrators everywhere classify and filter incoming traffic to prevent traffic that is likely malicious from entering the network. If the method of determining that location as proposed in the technical report was to be successfully implemented, it would allow administrators to see location based attack trends and better protect their clients/employers from cyber threats across the board.

Considering the STS portion, social media has become a powerful tool for influencing modern day society and as a result can influence users as individuals or groups of individuals in various ways with a myriad of downstream effects. Users who make decisions based on information or pressure from social media may be influenced intentionally or unintentionally to make decisions that may have serious consequences concerning their digital security. These interactions between humans and social media can be evaluated using the theory of technological mediation as a lens through which the factors that drive such decisions can be identified and subsequently a solution may be proposed.

References:

Egelman, S., Herley, C., & van Oorschot, P. C. (2013). Markets for zero-day exploits: Ethics and implications. *Proceedings of the 2013 New Security Paradigms Workshop*, 41–46. https://doi.org/10.1145/2535813.2535818

Experian. (2017, December 6). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

Fujiwara, T., Müller, K., & Schwarz, C. (2023). The Effect of Social Media on Elections: Evidence from the United States. *Journal of the European Economic Association*, jvad058. https://doi.org/10.1093/jeea/jvad058

Lin, Y. (2023). Construction of Computer Network Security System in the Era of Big Data. *Advances in Computer and Communication*, *4*(3), 181–185. https://doi.org/10.26855/acc.2023.06.015

Malik, S. (2003). *Network Security Principles and Practices*. Cisco Press.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Pew Research Center. (2022, September 22). Social Media and News Fact Sheet. *Pew Research Center's Journalism Project*. https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/

Ponemon Institute, LLC. (2012, November). *Cyber Security on the Offense: A Study of IT Security Experts - PDF Free Download*. https://docplayer.net/2657531-Cyber-security-on-the-offense-a-study-of-it-security-experts.html

Scott, J. (2017). Signature based malware detection is dead. *Institute for Critical Infrastructure Technology*.

Verbeek, P. P. (2015). Toward a theory of technological mediation. *Technoscience and postphenomenology: The Manhattan papers*, *189*.