Thesis Project Portfolio

Exploring the Threats Posed by Botnets on Onion-Routing

(Technical Report)

Internet Anonymity Systems: A Tool for Negotiating Privacy in the United States

(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

Justin Fabrizio
Spring, 2022
Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Technical Report Title

STS Research Paper Title

Prospectus

Sociotechnical Synthesis

Internet usage has skyrocketed over the past two decades, and so has internet data collection. Internet anonymity systems like Tor Browser provide a means for people of all walks of life to maintain a level of data privacy while using the internet. As such, these systems have become a focal point for many aspects of the internet, from legislation to innovation. The following theses will touch on both the societal effects of the presence of internet anonymity systems as well as the technical strengths and weaknesses of modern internet anonymity systems.

The STS thesis explored internet anonymity systems through the lens of sociotechnical imaginaries, dividing the imaginaries surrounding these systems into two groups: those of their implementers and those of their users. The increasing popularity and steady government funding of Tor Browser suggests the prevalence of pro-data privacy values in both imaginaries; however, government surveillance programs, among other evidence, indicates conflict between these two imaginaries. In this way, internet anonymity systems have become a tool for negotiating privacy and power between these two groups.

The technical thesis proposes a deanonymizing attack on Tor Browser through the use of botnets. The proposed attack involves hosting Tor relays on large botnets as a means of conducting a traffic correlation analysis attack. Since hosting a Tor relay is a voluntary process with little regulation, a botnet could feasibly account for a very large portion of the Tor network by hosting relays on every member machine. This would give a single entity access to the majority of traffic in the Tor network. Using these traffic logs, one could potentially deanonymize Tor users by correlating the inbound traffic with the outbound traffic, effectively bypassing the layered encryption by linking the identities of senders with their corresponding unencrypted traffic. A proposed solution to this would be to modify Tor’s path construction protocol to incorporate each relay’s “published” field, which records the date and time of activation, and only construct paths through the network that have a high time difference between the start and end relays.

Internet anonymity systems proved to be a difficult topic to research from a sociotechnical standpoint as their decentralized nature made it difficult to identify key stakeholders; however, the research ended up providing valuable results for both theses. The STS research clarified Tor Browser’s position as a pivotal technology between two competing imaginaries while the technical research gave an in-depth assessment of a current weakness of Tor Browser and proposed a possible solution. On the STS side, future research should expand in scope to include internet anonymity systems that are not open-source, as the implementers’ imaginaries of for-profit systems will likely contain different values than those of Tor Browser, while still interacting with the same users’ imaginary. In terms of technical research, validation of the proposed designs via testing would be valuable in supporting the technical thesis. The open-source nature of Tor Browser would make testing the modifications described in the thesis a relatively straightforward process on a closed network.