Fingerprintability of Tor Hidden Service Traffic Proxied Through Obfs4

(Technical Report)

Behind the Great Firewall: How China's Government, Businesses, and Populace Compete to Shape the Chinese Internet

(STS Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

by

James Houghton

May 5, 2020

List of Contents

Preface

Online anonymity systems such as Tor offer users internet privacy and freedom even under oppressive regimes, but they also shield cybercriminals. How, then, may online anonymity and internet freedom be maintained without compromising public safety?

In a Website Fingerprinting (WFP) attack, information leaked by packet sequence information is used to detect the page a target is visiting. WFP defenses are difficult for Tor users to deploy. In states with oppressive governments where bridges and pluggable transports may already be used, WFP defenses may become necessary. The research team evaluates the existing packet size and timing obfuscation (IAT) modes in the *obfs4* pluggable transport against some WFP attacks, and implements and evaluates a new IAT mode. We found that the existing obfuscation modes may not be adequate WFP defenses for small populations of monitored hidden services, but new IAT modes can be implemented to reduce information leakage.

China has become the world's leader in internet censorship, but not without resistance from Chinese people. How do China's government, businesses, and populace compete to shape the Chinese internet? The Communist Party of China (CPC) controls internet media by law and through ideology, censoring many Western news organizations and politically sensitive academic works. Some organizations are exempt from strict internet censorship, but most Chinese web users remain complacent, using domestic internet services that are easily manipulated by the CPC, leaving them susceptible to CPC surveillance and propaganda.

The Chinese government and the Tor Project have been engaged in a censorship arms race. Innovations in Tor, such as anonymous relays (bridges) and traffic obfuscation (pluggable transports), were developed for use in China to evade censorship and to conceal Tor usage. In

response, CPC may introduce techniques such as website fingerprinting to de-anonymize its web users. Tor researchers and developers must be resourceful to keep pace in this arms race.