Undergraduate Thesis Prospectus

Thwarting Tor Hidden Service Fingerprinting Attacks Using Pluggable Transports

(technical research project in Computer Science)

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

(STS research project)

by

James Houghton

December 8, 2019

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.

signed: _____ date: _____

approved: _____ date: _____
Peter Norton, Department of Engineering and Society

approved: _____ date: _____
David Evans, Department of Computer Science

General Research Problem

How can online anonymity be maintained without compromising public safety?

In China, internet access is restricted. Websites such as Facebook, Reddit, and Wikipedia, as well as most Google services, are blocked. To access the entire internet is to use anonymity systems, such as Tor. Virtual Private Network (VPN) services can serve a similar purpose, but government authorities can shut them down or force them to de-anonymize their users, and they do not provide comparable protection guarantees (Traudt, 2019).

Tor lets users bypass censorship, but also opens the floodgates to cybercrime worldwide. Many new computer viruses connect to Tor-anonymized internet services ("hidden services") to receive commands from an attack orchestrator. The infamous WannaCry ransomware, which caused approximately $4 billion in damage in 2017, is one such example (Symantec, 2017; Berr, 2017). Citizens of oppressive regimes need anonymity systems to speak freely, yet such systems empower cybercriminals.

Thwarting Tor Hidden Service Fingerprinting Attacks Using Pluggable Transports

How can Tor bridges be used to defend against website fingerprinting attacks on Tor hidden services?

Tor is a volunteer-run overlay network that attempts to anonymize both internet users and internet service hosts. All web services, including Tor hidden services, have identifiable traffic patterns that make usage of certain services theoretically detectable. This type of analysis, called traffic fingerprinting (WF), is available to any internet service provider and therefore any government. Today, this analysis cannot be done effectively at internet scale, but because there are not many hidden services (approximately several thousand), it is possible to determine which are being used or operated by a particular Tor user (Panchenko et al., 2017).

Usually Tor is accessed by first generating a three-relay circuit, and connecting to the first relay, known as the guard relay. Relays used for circuit generation can be enumerated completely, so it is easy for an ISP to block connections to the Tor network when connecting like this.

To combat this, non-publically-enumerable relays, "bridge relays," were added to Tor. They are optional for users. Bridge relays proxy traffic between a user and their guard relay and may manipulate the traffic in various ways. The traffic manipulation modules are called pluggable transports (PTs). Bridges were created after China blocked traffic to the publically enumerable Tor guard relays, and several PTs were developed once the Chinese and Iranian governments' censorship techniques improved (Dingledine, 2012).

Current methods can hinder website fingerprintability, but most of them require running a custom version of Tor and aren't used by the general public. One of the most successful

algorithms in terms of effectiveness and bandwidth overhead is DynaFlow (Lu, D., et al., 2018), and a custom version of Tor has been built with it.

My goal in this project is to determine if current traffic obfuscation techniques can be implemented in a pluggable transport, requiring no changes to the core Tor code itself, while remaining a reasonable defense against WF attacks with low bandwidth and latency overhead. I will likely port the DynaFlow algorithm to a PT. To test the WF protections the PT provides, I will conduct WF fingerprinting attacks similar to those used to test DynaFlow's effectiveness**,** collecting packet data for various hidden services for use as training data in a machine learning model. I have not decided which attributes of the packets I will use. This is an independent project; I am working with David Evans and Yixin Sun in the Department of Computer Science. If I succeed, Tor users will have an easy-to-use method of protecting themselves against current WF attacks. The developed PT may be considered for inclusion into the Tor Browser Bundle.

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

How are Chinese authorities and web users competing to apply the Internet to their advantage?

Chinese citizens are subject to some of the strictest censorship in the world. With censorship circumvention systems such as Tor, people living in authoritarian regimes can access the internet freely. To guide the development of anonymity systems, developers must understand the Chinese internet landscape and threat models. Although Tor is more heavily used in Russia and Iran (Tor Project, 2019), China's censorship techniques are the most advanced in the world (Yuan, 2019) and are therefore the focus of this research.

China's success in censoring its internet has sparked a lot of research interest. Research has measured Chinese online political engagement despite the CPC's efforts (Chen, 2016; Lu and Zhao, 2018) and used formal theories such as the Theory of Reasoned Action to explain the Chinese government's success in building public support for censorship (Guo and Feng, 2012). Chin (2018) studied the origins and development of media censorship in China since the 1950s. Nisbet, Kamenchuk, and Dal (2017) studied public support for online censorship in Russia, finding that Russian national news media can convince their viewers that the uncensored internet is a risk.

The Communist Party of China (CPC) launched the Cyberspace Administration of China (CAC) in 2014 to implement new censorship policies (Creemers, 2015). The CPC had previously been quiet about its censorship activities, often denying censorship allegations, but with the creation of the CAC they accepted their status as the world's most powerful internet censor (Chin, 2015). CAC declares its sole purpose to "protect the lawful rights and interests of citizens, legal persons, and other organizations" and to "preserve national security and public well-being" (CAC, 2017). President Xi Jinping himself asserts China's heavily censored internet model protects its citizens and can serve as a global standard (Mai, 2017).

Although the CPC claims to promote public safety, dissidents have been threatened or detained for acts like posting to Twitter (Shih, 2019). To comply with Chinese law, tech companies delete politically charged posts en masse (Bamman et al., 2012).

Large Chinese technology companies have had to tread a fine line between censorship and user engagement. In 2017, following the introduction of a new cybersecurity law, Tencent, Weibo, and WeChat were all fined the maximum legal amount for allowing certain kinds of information on their platforms that the CPC deemed damaging (Cadell and Li, 2017).Yet the

business of internet censorship among private companies has been growing quickly. Many censors feel they are doing a public service by hiding the vast amounts of "evil and pollution" that can be spread on the internet, but Chinese internet users who face censorship generally perceive the government as too restrictive of political discourse (Cadell and Li, 2017).

Constant censorship and threats from the Chinese government have hindered political expression online (Lu and Zhao, 2018). Residents have relied on VPNs and Tor to side-step censorship, but VPN providers acknowledge that their Chinese users may be prosecuted by the CPC (Markuson, 2019). VPN services aim to provide uncensored and unmonitored Internet access for all their users, protecting activism, Internet freedom, and human rights (Andrea, 2019).

Despite China's efforts, Tor and several VPN services remain fully operational in China; however, only an estimated 1% of Chinese citizens use them. Most of the approximately 800 million Chinese internet users are apparently content with convenient, highly integrated online services such as WeChat that the government can easily monitor and control (MacKinnon, 2012; McCarthy, 2018). The few who strive to access the uncensored internet must cope with the performance penalties that come with circumvention services and the language barriers of non-Chinese websites. Such disadvantages can deter efforts to evade internet censorship. The performance penalties can impair productivity for some Chinese technology companies, increase costs, and stifle innovation (Bao, 2013).

Beyond simple content censorship, the CPC has deterred organizing and protests. In Hong Kong, protestors have used their uncensored internet access to organize, leading Hong Kong authorities to consider internet censorship as a means to control the on-going violence (Agence France Presse, 2019). Since the Fugitive Offenders bill was proposed, protestors in

Hong Kong have fought for the region's civil liberties, including uncensored internet access, especially for journalists and activists (Hu, 2019). To interfere with the protests, the CPC has used malicious software to disable some services protestors use to organize (O'Brien, 2019).

References

Agence France Presse. (2019, Oct 7). Hong Kong Cabinet member floats Internet censorship to contain unrest. https://www.channelnewsasia.com/news/asia/hong-kong-protests-internet-censorship-idea-unrest-11978312

Andrea, Sybil. (2019, Jun 7). How NordVPN is protecting activism, internet freedom, and human rights. https://nordvpn.com/blog/social-responsibility/

Bamman, D., O'Connor B., Smith, N. A. (2012, Mar 5) Censorship and deletion practices in Chinese social media. *First Monday.* https://journals.uic.edu/ojs/index.php/fm/article/view/3943/3169

Bao, B. (2013, Apr 22). How Internet Censorship Is Curbing Innovation in China. *The Atlantic.* https://www.theatlantic.com/china/archive/2013/04/how-internet-censorship-is-curbing-innovation-in-china/275188/

Berr, J. (2017, May 16). "WannaCry" ransomware attack losses could reach $4 billion. *CBS News.* https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

CAC. (2017, May 2). Cyberspace Administration of China. **互**联网**信息内容管理行政**执法程序规定 [Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management]. http://www.cac.gov.cn/2017-05/02/c_1120902931.htm

Cadell, C., Li, P. (2017, Sept 29). Tea and Tiananmen: Inside China's new censorship machine. *Reuters.* https://www.reuters.com/article/china-congress-censorship/tea-and-tiananmen-inside-chinas-new-censorship-machine-idUSL4N1LW25C

Chen, Yashu. (2016). WeChat use among Chinese college students: Exploring gratifications and political engagement in China. *Journal of International and Intercultural Communication*. 1-19. 10.1080/17513057.2016.1235222.

Chin, J. (2015, April 28). China Internet Regulators Announce More Explicit Rules on Web Censorship. *The Wall Street Journal*. https://www.wsj.com/articles/chinas-internet-regulators-put-explicit-new-censorship-rules-in-place-1430233546

Chin, S. J. (2018). Institutional Origins of the Media Censorship in China: The Making of the Socialist Media Censorship System in 1950s Shanghai. *Journal of Contemporary China*, 27(114), 956–972. https://doi.org/10.1080/10670564.2018.1488108

Creemers, R. (2015, Dec 1). The Pivot of Chinese Cybergovernance: Integrating Internal Control in Xi Jinping's China. *China Perspectives.* https://journals.openedition.org/chinaperspectives/pdf/6835

Dingledine, R. (2012, Feb 16). Obfsproxy: the next step in the censorship arms race. [Blog post]. https://blog.torproject.org/obfsproxy-next-step-censorship-arms-race

Hu, C. (2019, Sept 12). What Hong Kong's masked protesters fear. *CNN.* https://www.cnn.com/2019/09/09/asia/smart-lamp-hong-kong-hnk-intl/index.html

Guo, S., & Feng, G. (2012). Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action. *Journal of Chinese Political Science,* 17(1), 33–52. https://doi.org/10.1007/s11366-011-9177-8

Lu, D., et al. (2018, Oct 15). DynaFlow: An Efficient Website Fingerprinting Defense Based on Dynamically-Adjusting Flows. *Proceedings of the 2018 on Workshop on Privacy in the Electronic Society,* 109-113. http://people.csail.mit.edu/devadas/pubs/wpes18.pdf

Lu, J., Zhao, Y. (2018, Jan). Implicit and Explicit Control: Modeling the Effect of Internet Censorship on Political Protest in China. *International Journal of Communication.* https://ijoc.org/index.php/ijoc/article/view/8532/2427

MacKinnon, R. (2012, Jan 29). Inside China's censorship machine. *National Post.* https://nationalpost.com/opinion/rebecca-mackinnon-inside-chinas-censorship-machine

Mai, J. (2017, Dec 3). Xi Jinping renews 'cyber sovereignty' call at China's top meeting of internet minds. *South China Morning Post*. https://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top

Markuson, D. (2019, Aug 25). *What is the best VPN for China?* https://nordvpn.com/blog/vpn-for-china/

McCarthy, N. (2018, Aug 23). China Now Boasts More Than 800 Million Internet Users And 98% of Them Are Mobile. *Forbes.* https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/#63c0b8607092

O'Brien, D. (2019, Oct 10). China's Global Reach: Surveillance and Censorship Beyond the Great Firewall. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall

Panchenko et al. (2017, Oct 30). Analysis of Fingerprinting Techniques for Tor Hidden Services. *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society,* 165-175. https://www.freehaven.net/anonbib/cache/fingerprinting-wpes17.pdf

Shih, J. (2019, Jan 4). Chinese censors go old school to clamp down on Twitter: A knock on the door. *The Washington Post.* https://www.washingtonpost.com

Symantec. (2019, May 24). Ransom.Wannacry. https://www.symantec.com/security-center/writeup/2017-051310-3522-99

The Tor Project. (2019). Top-10 countries by bridge users between August 2, 2019 and October 31, 2019. https://metrics.torproject.org/userstats-bridge-table.html

Traudt, M. (2019, Oct 28). You want Tor Browser… not a VPN. [Blog post]. https://matt.traudt.xyz/p/24tFBCJV.html

Yuan, L. (2019, Jan 2). Learning China's Forbidden History, So They Can Censor It. *The New York Times.* https://www.nytimes.com/2019/01/02/business/china-internet-censor.html