Poster: Introducing MassBrowser: A Censorship Circumvention System Run by the Masses

Milad Nasr*, Anonymous*, and Amir Houmansadr
University of Massachusetts Amherst
{*milad,amir*}@*cs.umass.edu*
*Equal contribution

***Abstract*—We will present a new censorship circumvention system, currently being developed in our group. The new system is called MassBrowser, and combines several techniques from state-of-the-art censorship studies to design a hard-to-block, practical censorship circumvention system. MassBrowser is a one-hop proxy system where the proxies are volunteer Internet users in the free world. The power of MassBrowser comes from the large number of volunteer proxies who frequently change their IP addresses as the volunteer users move to different networks. To get a large number of volunteer proxies, we provide the volunteers the control over how their computers are used by the censored users. Particularly, the volunteer users can decide what websites they will proxy for censored users, and how much bandwidth they will allocate.**

MassBrowser is currently in the beta release mode with software available for various operating systems (https://massbrowser.cs.umass.edu/). We hope to get feedback from the audience at Oakland by presenting MassBrowser and showing a demo of how it works.

1. Introduction

Repressive regimes, totalitarian governments, and corrupt corporations regulate, monitor, and restrict the access to the Internet, which is broadly known as Internet *censorship*. The techniques commonly used to enforce censorship include IP address blocking, DNS hijacking, and TCP content filtering [2], [9] to block access to certain destinations or to prevent certain forms of content from being transmitted. To ensure compliance and to detect undercover political/social activists, repressive regimes additionally utilize advanced networking tools, including deep packet inspection (DPI), to prevent the use of the censorship circumvention technologies by their citizens.

To restore the openness of the Internet, researchers have designed and deployed an arsenal of tools that help users bypass censorship. Such tools, known as *circumvention systems*, deploy a variety of techniques ranging from IP indirection to onion routing to traffic obfuscation [8], [13].

Key shortcomings of existing systems. Unfortunately, existing circumvention systems suffer from one or all of the following weaknesses: *(1) Easily blocked:* A majority of circumvention systems work by setting up *proxy* servers outside the censorship regions, which relay the Internet traffic of the censored users. This includes systems like Tor, VPNs, Psiphon, etc. Unfortunately, such circumvention systems are easily blocked by the censors by enumerating their limited set of proxy server IP addresses [14]. *(2) Costly to operate:* To resist proxy blocking by the censors, recent circumvention systems have started to deploy the proxies on shared-IP platforms such as CDNs, App Engines, and Cloud Storage, a technique broadly referred to as *domain fronting* [3]. This mechanism, however, is prohibitively expensive [11] to operate for large scales of users. *(3) Poor QoS:* Proxy-based circumvention systems like Tor and it's variants suffer from low quality of service (e.g., high latencies and low bandwidths). This is due to various factors such as the small number of proxies to clients, and the large volume of client traffic used to access voluminous content (like pirated movies). *(4) Hard to deploy:* Several circumvention systems proposed in the literature are impractical to be used at large scale due to various reasons. For instance, decoy routing systemsrequire wide adoption by Internet ISPs, and tunneling systems [6], [7] can be disabled by third-party service providers they use for tunneling.

Our approach. The goal of this paper is to design a new circumvention system that offers practical circumvention by tackling the aforementioned shortcomings of circumvention systems. We base our design on a *new design principle* not considered by prior circumvention designs. Our principle, which we call the *separation of properties* principle, states that *the key property expected from an effective circumvention system is blocking resistance, and it does not need to provide other properties such as browsing privacy or anonymity.* Our real-world observation [1], [4] suggests that the majority of censored users are solely interested in blocking resistance, but not other properties like anonymity. For instance, typical censored users trust any open proxy or VPN provider just to get access to censored websites despite the trivial absence of anonymity and browsing privacy [4]. Therefore, we argue that a circumvention system needs to be designed in a way to optimize blocking resistance; bundling additional properties like anonymity is the main reason for the majority of weaknesses mentioned above. For censored users who need additional properties like anonymity, they can achieve those by cascading the circumvention system

with other privacy-enhancing technologies like anonymity systems (and, consequently trading off QoS and cost to get those additional properties). In this paper, we demonstrate that designing a circumvention system based on this principle enables us to offer strong blocking resistance in addition to practical QoS and low cost of operation. For instance, the separation of properties principle allows us to run single-proxy circumvention connections, improving the QoS-cost tradeoff. It also enables us to limit the use of our circumvention system only for accessing circumvention content. This not only reduces congestion on the proxies (therefore improving the QoS-cost tradeoff), but also increases the potential number of volunteer proxies by minimizing the legal risks of running circumvention proxies.

Contributions. We design a new circumvention system, called MassBrowser, that aims at addressing the weaknesses of prior designs, as discussed above. That is, MassBrowser aims at offering reliable blocking resistance while providing practical QoS and low operational costs. The *core idea* of MassBrowser is to use normal Internet users with access to the free Internet, which we call *Buddies*, as relays to proxy censored web traffic for censored users, which we call *Clients*. This will address the challenges of circumvention systems discussed above in different ways. First, the diversity, abundance, and dynamicity of the IPs used by the Buddies will make any attempt of IP enumeration by the censors prone to significant collateral damage (i.e., due to falsely blocking significant non-circumvention traffic). Particularly, normal Internet users connect from behind NATs, therefore blocking NATed Buddies has similar collateral damage impact on the censors as in the (impractically expensive) domain fronting systems [3] (i.e., to block a NATed Buddy, the censors will need to block the Buddy's subnet). Second, MassBrowser combines various state-of-the-art circumvention techniques including CacheBrowsing [5] and Domain Fronting [3] to optimize the QoS of circumvention connections while minimizing the operational costs of circumvention. We estimate the total cost of deploying MassBrowser to be no more than *$0.001 per active client per month*.

We have built a fully operational implementation of MassBrowser, with end-user graphical user interfaces for MassBrowser Client and Buddy users with minimal technical background. We have been testing MassBrowser's software for several months using volunteer clients from inside censored countries. MassBrowser will make a real-world impact only with wide adoption by volunteers who run MassBrowser Buddies. Therefore, a major challenge to MassBrowser's success is to facilitate and encourage wide-scale adoption by volunteer relays. Towards this, we perform *the first* user study on the willingness of Internet users in voluntarily helping circumvention technologies. The results of our user study suggest that *a significant fraction of Internet users are willing to run software that helps censored users—if they get guarantees on their safety and security*. Advised by this, we build MassBrowser to provide high levels of safety and security to the volunteer Buddies. Particularly, we design a user-friendly GUI software for Buddies that provides them with *transparency* and *full control* on how their computers are used to help censored users. For instance, our Buddy software enables a proxy operator to control the websites she feels comfortable proxying traffic to, as well as the volume of traffic she is willing to proxy for censored users.

Note that our implementation of MassBrowser supports *connecting through Tor* for users who need anonymity in addition to blocking resistance (at the expense of a lowered QoS comparable to Tor's QoS). More specifically, our Buddy software enables a volunteer to optionally become a Tor bridge as well. Therefore, existing Tor bridges can adopt MassBrowser as a pluggable transport [12]. We evaluate MassBrowser's cost of operation when used as a Tor pluggable transport, showing that it is drastically cheaper than meek [10], while they both offer similar blocking resistance properties (both meek and MassBrowser aim at increasing the censors' collateral damage by making use of shared IP addresses).

References

[1] Penalties For Using VPN In Various Countries. https://www.vpnunlimitedapp.com/blog/penalties-for-using-vpn/.

[2] Defeat Internet Censorship: Overview of Advanced Technologies and Products. http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf, 2007.

[3] FIFIELD, D., LAN, C., HYNES, R., WEGMANN, P., AND PAXSON, V. Blocking-resistant Communication through Domain Fronting. In *PETS* (2015).

[4] Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide. http://www.nartv.org/mirror/circ_guide.pdf.

[5] HOLOWCZAK, J., AND HOUMANSADR, A. CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content. In *The 22nd ACM Conference on Computer and Communications Security (CCS)* (2015).

[6] HOUMANSADR, A., RIEDL, T., BORISOV, N., AND SINGER, A. I Want My Voice to Be Heard: IP over Voice-over-IP for Unobservable Censorship Circumvention. In *NDSS* (2013).

[7] HOUMANSADR, A., ZHOU, W., CAESAR, M., AND BORISOV, N. SWEET: Serving the Web by Exploiting Email Tunnels. In *PETS* (2013).

[8] KHATTAK, S., ELAHI, T., SIMON, L., SWANSON, C. M., MURDOCH, S. J., AND GOLDBERG, I. SoK: Making sense of censorship resistance systems. *Proceedings on Privacy Enhancing Technologies 2016*, 4 (2016), 37–61.

[9] LEBERKNIGHT, C., CHIANG, M., POOR, H., AND WONG, F. A Taxonomy of Internet Censorship and Anti-censorship. http://www.princeton.edu/~chiangm/anticensorship.pdf, 2010.

[10] meek Pluggable Transport. https://trac.torproject.org/projects/tor/wiki/doc/meek.

[11] [tor-project] summary of meek's costs, march 2017. https://lists.torproject.org/pipermail/tor-project/2017-April/001097.html.

[12] Tor: Pluggable Transports. https://www.torproject.org/docs/pluggable-transports.html.en.

[13] TSCHANTZ, M. C., AFROZ, S., PAXSON, V., ET AL. SoK: Towards Grounding Censorship Circumvention in Empiricism. In *Security and Privacy (SP), 2016 IEEE Symposium on* (2016), IEEE, pp. 914–933.

[14] WINTER, P., AND LINDSKOG, S. How the Great Firewall of China Is Blocking Tor. In *FOCI* (2012).