MassBrowser: Fighting Internet Censorship in a Mass!

Milad Nasr, Hadi Zolfaghari, Amir Houmansadr

College of Information and Computer Sciences, University of Massachusetts Amherst

Introduction and Motivation

- Internet censorship is a global threat to Internet freedom.
- Existing censorship circumvention systems suffer from the following weaknesses:
  - **Easily Blocked**: The majority of circumvention systems are proxy-based. The proxies are easily blacklisted by the censors.
  - **High Cost of Operation**: To evade IP blacklisting, some circumvention systems host their proxies on "domain fronted" services (like CDNs). This is however prohibitively expensive at scale.
  - **Poor QoS**: Some academic circumvention systems offer impractically poor QoS.
  - **Hard to Deploy**: Several suggestion circumvention systems are hard to deploy as they require cooperation from oblivious technology third-parties like ISPs and content publishers.

  The Table below demonstrates such weaknesses for major classes of circumvention systems.

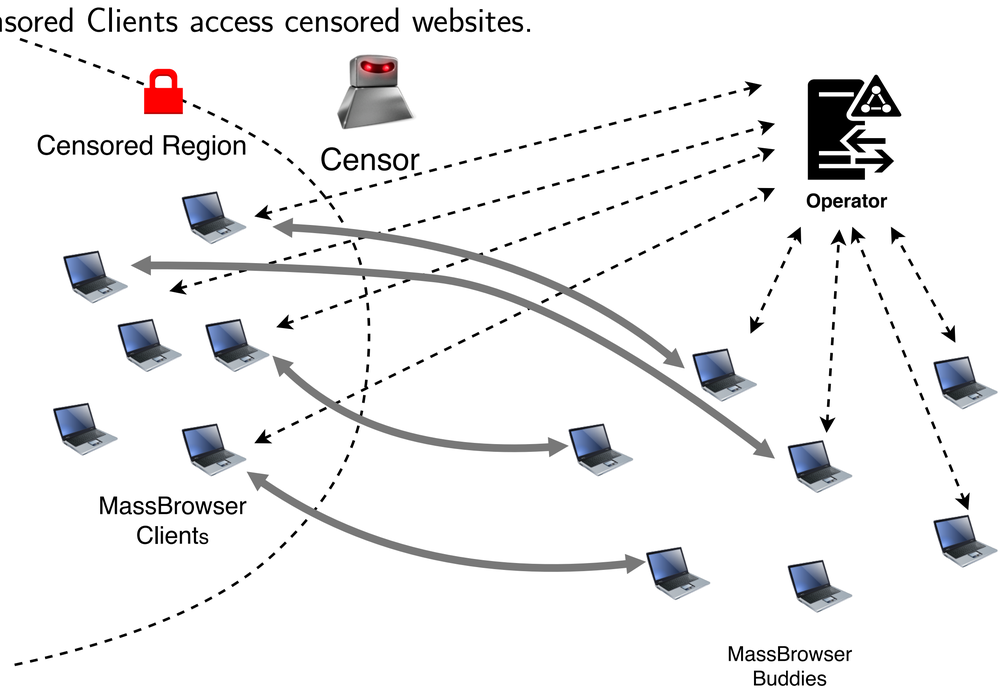
Table: Weaknesses of major types of circumvention systems

Category	Easily blocked	Costly	Poor QoS	Deployability
Proxy-Based	●	◐	●	○
Domain Fronting	○	●	○	○
CacheBrowsing	○	○	●	○
Tunneling	○	◐	●	◐
Decoy Routing	○	◐	○	●

- Our Goal: Design and deploy a censorship circumvention system that provides strong blocking resilience while offering a practical balance between QoS and cost of operation.

Design Principles

- MassBrowser's design is based on the following principle:
  - The **Separation of Properties (SoP) Principle**: the key feature targeted by an effective circumvention system should be blocking resistance, and other features such as anonymity and browsing privacy should be left as optional to the users.
- The SoP principle allows us to optimize MassBrowser's performance around blocking resilience than additional privacy properties like anonymity.
  - In-the-wild observations show that the majority of ordinary censored users do not care about such additional features.
  - Users who care about such additional features can obtain them by cascading MassBrowser with a system like Tor.
- **Key Architecture:** MassBrowser is a volunteer-run proxy-based circumvention system. As shown in the figure below, volunteer proxies, called Buddies, help censored Clients access censored websites.



- We deploy various mechanisms to encourage wide adoption by volunteers. Importantly, Buddies have full control and transparency over what they proxy.

Acknowledgements

This work is supported in part by the NSF CAREER grant CNS-1553301.

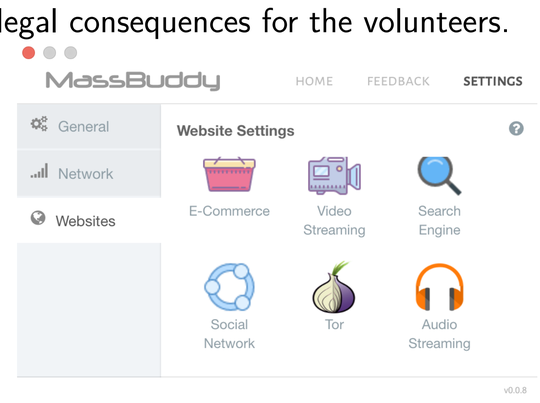
The Key Techniques Used

MassBrowser uses the following techniques to achieve core circumvention requirements.

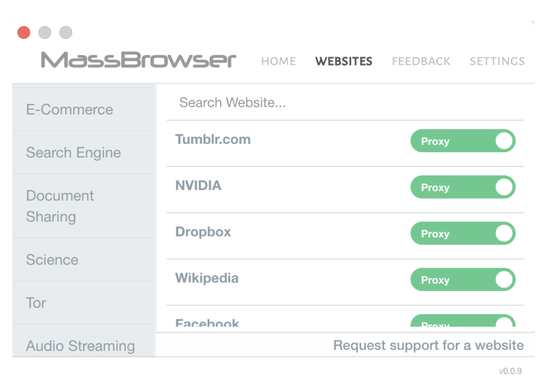
- **Blocking Resistance**:
  - **Shared and dynamic IPs**: MassBrowser proxies are run by normal Internet users who connect from shared and dynamic IP addresses (i.e., NATed IPs). Therefore, blocking them is costly and prone to collateral damage.
  - **Traffic obfuscation and encryption**: MassBrowser communications are encrypted to prevent deep-packet inspection. Also, MassBrowser uses traffic obfuscation to prevent fingerprinting.
  - **Domain fronting**: The central component of MassBrowser (called the operator) is hosted as a domain fronted service to resist blocking.
- **Optimizing Cost and QoS**:
  - **Censored-content only proxying**: Tunneling non-censored content puts additional burden on the proxies.
  - **CacheBrowsing**: MassBrowser clients directly fetch censored CDN browseable contents, not through proxies.
  - **Strategic proxy assignment**: To prevent Sybil attack and load balancing, MassBrowser's operator uses a strategic proxy assignment algorithm.
  - **Buddy software operates transparently**: The MassBuddy software does not interfere with the volunteers' normal activities.
  - **MassBuddies can set bandwidth limits**: Volunteers can specify the bandwidth the devote to MassBrowser.
  - **MassBuddies can whitelist destinations**: Volunteers can specify what type of destinations they are willing to proxy traffic to.
- **Deployment**:MassBrowser has recently been released in beta version to limited number of users. We have built user-friendly GUI software for both MassClients and MassBuddies for the major operating systems.

MassBrowser's GUI Software

- We have build user-friendly GUI software for clients and volunteers.
  - As shown below, a volunteer has full control and transparency over what she proxies for censored clients. This is to encourage wide voluntary participation by minimizing the legal consequences for the volunteers.



  - As shown below, a client can decide what websites and services are proxied through MassBrowser. For instance, a client can tunnel Tor traffic through MassBrowser.



We need your help!

- Help us fight censorship by becoming a Buddy!
- Contribute to our open source **code** https://github.com/SPIN-UMass/MassBrowser
- **Website**: `http://massbrowser.cs.umass.edu/`
- Email your **feedback** to `massbrowser@cs.umass.edu`

MassBrowser is not a trademark of UMass, nor affiliated with it!