Tor's Usability for Censorship Circumvention

David Fifield[1] and Linda N. Lee[1], Serge Egelman[1,2], David Wagner[1]
[1]University of California, Berkeley, {fifield,lnl,egelman,daw}@cs.berkeley.edu,
[2]International Computer Science Institute, egelman@icsi.berkeley.edu

ABSTRACT

Tor has grown beyond its original purpose as and has since become an important Internet circumvention tool. We specifically examine it usability as a censorship circumvention tool, an essential facet for adoption and use. We focus our analysis on the connection configuration dialog of Tor browser, as censorship circumvention requires correct transport configurations. Our talk will describe a future study aimed at evaluating if and how easily users can circumvent censorship using Tor Browser, isolating specific browser features to study in the process. To this end, we will conduct a large-scale user study examining hundreds of users on how they navigate Tor's configuration wizard to complete seven browsing tasks in three different adversarial settings. We solicit feedback to improve our study's design.

Keywords

Censorship, Security, User Studies, Anonymity, Tor

1. TOR'S USABILITY

Tor is the most widely used anonymity tool today. However, there are complaints that Tor is not usable. Norcie [1] did an experiment which identified stopping points in Tor browser, finding out when people would get frustrated with Tor so much they would stop using it. But what about the people who are using Tor? What usability issues would there be if people were not stopped? To our knowledge, that has been the only user study of Tor. Since then, Tor has had a lot of updates. Additionally, there were a lot of features that were untested. There have been been no major usability evaluations of Tor Browser since the introduction of the 4.0 series, which introduced radical UI changes.

We briefly describe the results of a completed study that examined the download and installation processes, as well as basic browsing behaviors. This study uncovered a number of bugs and stopping points which has already effected concrete change in the browser.

We ran a small pilot study of five journalists which involved a cognitive walk through in which participants explained the motivation for their actions and any confusion that they had during the process. We did this to find new stopping points, and sources of confusion. But in the process, we were also able to observe how users would download Tor, if they could understand the address bar/menu, how well they were able to complete basic tasks (searching, setting new circuits, etc.), and generally if they had any usability complaints about the browser.

We recruited five journalists from Berkeley by reaching out to journalist contacts. During the study, we made a video recording of each participant's computer screen and simultaneously projected it into another room with Tor developers. We recorded what they were saying out loud in their cognitive walk through, and later added these words to the screen videos as subtitles. The participants also took an exit survey which estimated their familiarity with technology and security. On average, participants took 26 minutes to complete the study (σ = 7 min). The result was that people did have difficulty with installing Tor Browser (principally because of the Gatekeeper code-signing feature on OS X), did not understand what many of the many options meant, and were confused about why certain things were happening. Our talk will feature brief highlights of the screen videos and a summary of interface changes.

After our first usability evaluation of Tor, it was clear to us that so many of the features had been left unevaluated—such as advanced web browsing tasks, the configuration menu, automatic updates, and identity and cookie management. We found that the most effective way to resolve the problems encountered was more user guidance and interface remodeling rather than continued user observations. Rather than selecting the features to study in isolation, we decided to focus on an important use case of Tor browser, censorship circumvention. To our knowledge, this is the first user study investigating the usability of Tor as a censorship circumvention tool, rather than an anonymity tool.

2. DESIGN

Overview For users to circumvent censorship in their resident countries, they will need to configure Tor to set up a proxy, bridge, or both. There is a configuration wizard to help guide users through setting up their connection, but our hypothesis is that the average user will not easily be able to configure Tor correctly in these adverse settings, as they require the user to provide IP addresses of proxies or bridges to use. The goal of our experiment is to see how successful users are at carrying out common browsing tasks in an adversarial setting using Tor.

We start off the experiment by telling them that they are in an adversarial setting, and that some websites are blocked and some websites are not. We will instruct them to visit notblocked.com and also blocked.com to illustrate the situation that they are in. We will also explain what Tor is, and how they can use it if necessary, and ask them to complete the set of tasks. To complete all the tasks, the participants will ultimately need to get the correct configuration settings

for the country they are simulated to be in. We will end the experiment with a survey which asks them things like their security background, tech exposure, what was unexpected, what was hard, etc. We plan to analyze: which configuration tasks are hard (bridges versus proxies, etc.), how many were successful, how long it took users to configure, if they understood the process, if they were confident that it was working as expected, etc.

Censorship Environment Simulation We plan to simulate three censorship environments. They are informed by our experience with pluggable transports and knowledge of commonly seen censorship techniques. They are not meant perfectly to replicate the network environment in any particular country; rather, they are abstract simulations that are nevertheless inspired by reality.

- Corporate network. A simulation of an enterprise or educational firewall. Blocks all services but HTTP, HTTPS, and DNS. Certain non-work-related domains, like youtube.com and torproject.org, are blocked by DNS and HTTP inspection. Blocked requests are redirected to a block page.
- DNS-only censor. This censor injects false replies to DNS queries for forbidden domain names (DNS poisoning), but does not do deep packet inspection on TCP streams. Unlike the corporate censor, this censor allows protocols outside a small whitelisted set.
- Comprehensive censor. Employs a variety of techniques, depending on the target. May do DNS poisoning, IP blocking, and inspection of TCP streams (examining the URL of HTTP requests, for example). Some domains may be blocked by DNS and deep packet inspection; others may additionally be blocked by IP address. Tor relays are blocked by IP address. Some domains, like wikipedia.org, may allow HTTP but not HTTPS. Blocked requests fail silently (no block page).

List of Tasks The tasks below were originally inspired by the top Alexa sites, an indication of representative and relevant browsing behavior. We then selected sites which were commonly censored and refined the tasks to remove ethical concerns, such as tasks which would require a participant to reveal private information (such as login information). We hope the resulting tasks convey an idea of sites which are censored today, while remaining representative of how a user might browse the Internet.

All participants will be given the same set of tasks, regardless of the censorship environment. Although every participant will attempt the same set of tasks, the difficulty of completing these tasks will vary based on their chosen censorship environment. The tasks are not all intended to be challenging to complete. Some may not even require the use or Tor Browser, depending on the environment.

- Do a Google web search.
- Watch a YouTube video.
- Find the Amazon best-selling books.
- Find Yahoo's exchange rate between dollars and euros.
- Read the Wikipedia featured article.
- Find the Twitter trending topics.
- Find directions on Bing Maps.

Experiment Execution Details We plan to recruit up to 200 users for the purpose of this study, making it largest user study to date examining Tor (check this). This study will be conducted at the Experimental Social Science Laboratory (Xlab) at the University of California, Berkeley, which consists of 36 laptops with cubicle walls separating each laptop. We will use individual host firewalls to simulate the censorship environments and will write a browser extension to log when user activity, such as what websites they were successfully able to visit. The total length of the experiment, including briefing, completing the censorship circumvention tasks, exit survey, and debriefing, will take less than an hour. Participants will be compensated $30 for their time, which is more to cover minimum wage and transportation costs.

3. WHAT WE WANT FEEDBACK ON

During the question-and-answer session, we will be especially interested in soliciting feedback on these topics:

- **Targeting specific pluggable transports** Some of Tor's pluggable transports work in censorship environments where others do not. Additionally, some of them require additional information (like bridge addresses) before they work. Is there a way to target testing of specific transports? Is there anything to infer from participants' selection of transports, or do we assume they are trying transports at random?
- **Censorship environments** Our proposed censorship simulation is informed by real-world censors. What other representative environments should be tested?
- **Browsing tasks** Circumvention is broader than the stereotypical "dissident blogger" use case. We have invented some tasks that use some of the most popular web sites. What other browsing tasks make sense to test?
- **Experimental design** Our initial study was aimed at a specific subset of users (journalists). We plan to remove this restriction in order to have a larger participant population. We aim to make our results reproducible by publishing our software and firewall configurations.

4. RESOURCES

Our online artifacts of our completed pilot study, such as the summary, results, and resulting browser changes are below:

- `https://trac.torproject.org/projects/tor/wiki/org/meetings/2015UXsprint`
- `https://blog.torproject.org/blog/ux-sprint-2015-wrapup`

Subtitled screen videos:

- `https://people.torproject.org/~dcf/uxsprint2015/`

5. REFERENCES

[1] G. Norcie, K. Caine, and L. J. Camp. Eliminating stop-points in the installation and use of anonymity systems: A usability evaluation of the Tor Browser Bundle. In *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)*. Citeseer, 2012.