Tor's Usability for Censorship Circumvention

Linda N. Lee, David Fifield, Nathan Malkin
University of California, Berkeley
{lnl,fifield,nmalkin}@cs.berkeley.edu

ABSTRACT

Tor has grown beyond its original purpose as an anonymity tool and has since become an important censorship circumvention tool. cite something here.. We specifically examine its usability as a censorship circumvention tool, an essential facet for adoption and use. We focus our analysis on the connection configuration interface of Tor browser, as censorship circumvention requires correct transport configurations. We will conduct a large-scale user study examining 60-100 of users on how they navigate Tor's configuration wizard to complete seven browsing tasks in three different adversarial settings. Our study combines quantitative measurements (interface paths taken to success, time to success, and which configuration was chosen) and qualitative measurements (if users were comfortable with use, what was most confusing, and if they would use the browser again). The first phase of the study will evaluate if and how easily users can circumvent censorship using Tor Browser, isolating specific browser features to study in the process. The second phase of the study will test improvements to the interface and an alternate interface. Our goal is to integrate positive usability changes into the Tor Browser. Since the configuration interface is modular and does not require changes to the Tor Browser functionality, these changes will be easy to deploy.

Keywords

Censorship, Security, User Studies, Anonymity, Tor

1. TOR'S USABILITY

Tor is primarily known as an anonymity tool. In fact, it is the most widely used anonymity tool today. However, there are complaints that Tor is not usable. Norcie [2] 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. 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 ran a small pilot study of five journalists. This study uncovered a number of bugs and stopping points which has already effected concrete change in the browser.

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 does not have knowledge knowledge on how certain pluggable transports work, or to provide non-publicly listed IP addresses bridges. Certain real-world censorship settings require the user to provide this information during configuration, which will affect how successful users are at circumventing censorship using Tor. There are blogs in countries which have extensive censorship on how to configure Tor correctly cite something, and participants may receive additional informatio through word of mouth. Our study will measure if the configuration interface successfully guides users to correctly configuring their browser, not accounting for any additional information that a real user may have.

Experiment Logistics The IRB protocol to run this user study has been approved (2014-12-6995). We plan to recruit from 100-200 users for the purpose of this study, making it the largest user study of Tor to date. This study will be conducted at the Experimental Social Science Laboratory (Xlab) at the University of California, Berkeley, which consists of 36 laptops, separated by cubicle walls. We will use individual host firewalls to simulate censorship environments and will record computer screens to capture user activity. The total length of the experiment, including briefing, completing the censorship circumvention tasks, exit survey, and debriefing, will be about an hour. Participants will be compensated $30 for their time, which covers minimum wage for an hour and any transportation costs to the lab.

Experiment Flow We will run three sets of the experiment, the first set to test the current configuration interface, a second set to test the improved interface, and a third set to test the alternate configuration interface. The experiment flow will be the same across all sets of experiments, with the

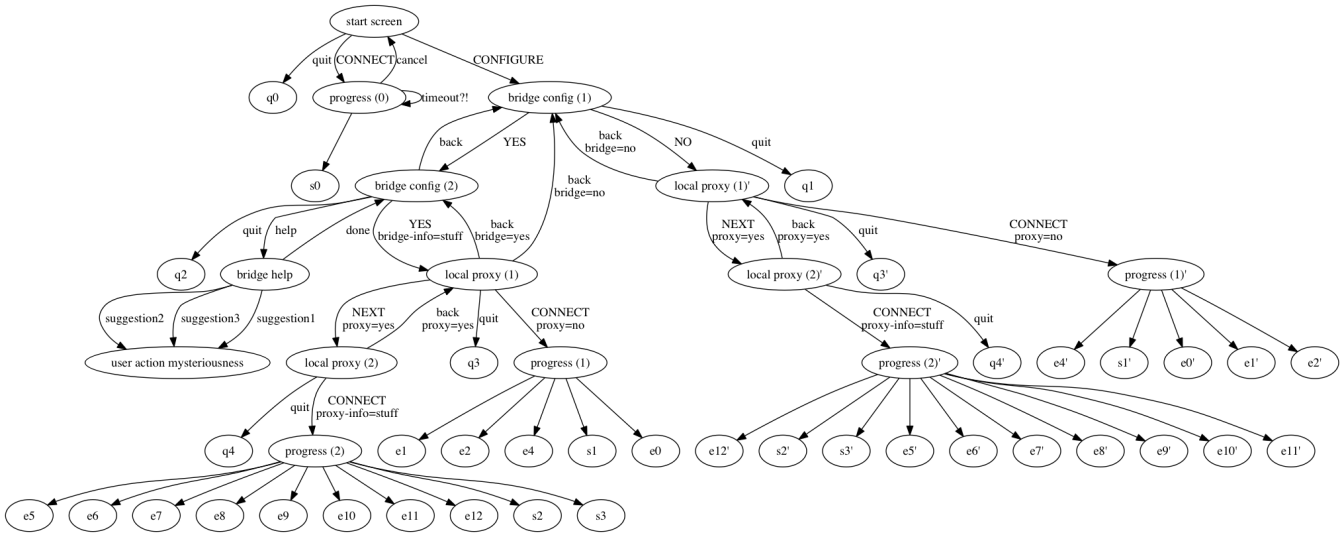

Figure 1: This flow chart shows all of the possible paths taken through the Tor configuration interface. A state represents a window in the interface, with the exception of the leaves, which indicate the final action taken by the interface ("q" for quit, "s" for success, and "e" for error). The transitions between the states indicate which user action causes that transition. The cause for error is can be found here.

fact that the configuration interface will be altered across sets.

The experiment begins with the participants being informed that they are in a simulated censorship environment, where some — but not all — websites are blocked. We will instruct them to visit a non-blocked website and a blocked website on a "standard" browser (one that is not used for censorship circumvention, such as Chrome, Safari, or Firefox) to illustrate the situation. Then, the participants will find out the role they they will be playing in the study. This role is that of a regular citizen, who is trying to visit blocked websites for non-critical leisurely purposes, and that there is a minimal chance of risk. This information is given to achieve consistency across participants: their behavior might be different if they were visiting websites to accomplish a critical task, or if they knew that there were great risks.

After explaining the situation and their role, we will explain what Tor is, and how they can use it if necessary, and instruct them to complete a set of tasks which will require visiting blocked websites. Ultimately, the participants will need to configure their Tor Browser to circumvent the simulated censorship environment. These tasks have a threefold purpose of providing participants with feedback (if they did not correctly configure their browser, they cannot reach the website), motivating the participants to configure the browser correctly, and providing the researchers with an indicator of successful censorship circumvention. Participants' screens will be recorded to capture how they configure their browser, and to provide additional evidence that they have completed the tasks.

After users complete the browsing tasks, we will administer a survey that 1) measures demographics, technical fluency, and familiarity with Tor and 2) collects qualitative feedback from participants about their browsing experience as a whole and the configuration interface specifically. A rough draft of the survey can be found here.

The experiment will conclude with a debriefing, which will inform that the participants of their screen capture and obtaining re-consent for the information.

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. Although inspired by reality, these abstract simulations are intended to require distinct configurations of the Tor Browser from our participants.

- **Mild censorship** (Reflective of countries such as ?? and ??.) Certain domain names are blocked. Reaching these domains requires any use of a censorship circumvention tool. The default option to "connect" to the Tor network directly will circumvent this censor. Additional correct bridge or proxy configuration are optional.
- **Intermediate censorship** (Reflective of countries such as ?? and ??.) Certain domain names are blocked. Censorship circumvention tools are blocked. Since Tor is blocked by blocking all public Tor relay nodes, the default option to "connect" to the Tor network directly will fail. A choice of a hard-coded bridge (see Figure 2) or a valid non-public bridge is required to circumvent this censor. Additional correct proxy configuration is optional.
- **Comprehensive censorship** (Reflective of countries such as China and Syria.) Certain domain names are blocked. Censorship circumvention tools are thoroughly blocked. Tor is blocked by blocking all public Tor relay nodes, and the censor has examined source code to block all hard-coded bridge relays in the configuration interface. The default option to "connect" to the Tor network directly will fail. Choosing any other bridges than "meek-amazon," "meek-azure," and"meek-

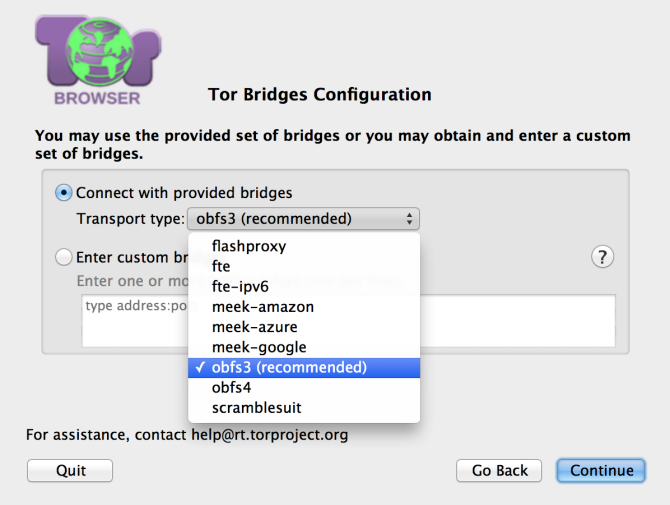

Figure 2: The Tor Bridges Configuration window of the Tor configuration interface. Tor users in censored environments and some of our participants will be required to select the correct bridge for circumventing censorship. Note that the interface prompts users to choose a transport type, which can be the source of confusion. Bridges are non-listed guard relays to the Tor network, and some of them can have transport types which obfuscate traffic in different ways.

google," will fail. This is because domain-fronting requires censors to block entire CDNs to also block this transport (which will cause huge collateral blocking damage), making it resistant to agressive censorship environments. Additional details, see [1].

List of Tasks In our experimental setup, successful completion of these given tasks requires of correct configuration. The difficulty of circumventing censorship to visit the websites required for the tasks will vary on the simulated censorship environment. Since all participants will be given the same set of tasks, regardless of the censorship environment, the difficulty of completing the tasks remains constant assuming correct configuration. The tasks themselves are not intended to be challenging.

The tasks were initially inspired by the top Alexa sites, an indication of representative and relevant browsing behavior. From these, we selected sites which were commonly censored, but filtered tasks that would require a participant to reveal private information (such as login information) for ethical considerations. These tasks were further refined after performing a pilot study of the experiment. We hope the tasks convey an example of how of a user might browse the Internet in a censored environment.

- Google search for the population of Zimbabwe.
- On Youtube, find a video playing Bach's "Ode to Joy."
- Find the Amazon best-sellers in "Movies & TV."
- On Yahoo, find the exchange rate of dollars to euros.
- Find the Wikipedia "History" portal's featured article.
- On Twitter, find the currently trending topics.
- On Bing Maps, find directions from Time Square to Carnegie Hall.

3. WHAT WE HOPE TO ACCOMPLISH

We plan to finish the user study by the end of the semester. From this experiment, we hope to accomplish the following:

- **Test the Tor configuration interface** We will perform the largest-scale user study of Tor to date, measuring how users configure Tor in three different adversarial settings.
- **Test an improved configuration interface** With the measurements collected from testing the interface as-is, Nathan will be designing ways to improve the interface to minimize time taken, paths taken, and error states reached.
- **Test an alternative configuration interface** A Tor developer has offered to design a mock-up interface for an alternative configuration interface which will greatly automate the process. There are tradeoffs between ease of use and transparency of the system's, and ethical considerations with loggable errors resulting from automated configuration.
- **Push changes** We have the support of Tor developers to improve this interface. Additionally, since the configuration interface does not require any changes to the Tor Browser functionality, improvements to the interface will be easy to deploy.

4. RESOURCES

Our online artifacts of the work done during this class, Fall 2015, are below:

- github repo with experiment plans, code, and paper
- pilot video 1 pilot video 2
- experimental setup code: firewall and screen capture
- experimental takedown code: saving files and cleanup

Our online artifacts of study of Tor as an anonymity tool, such as the summary, results, and resulting browser changes are below:

- blog post summary
- changes made to Tor
- subtitled screen videos

5. REFERENCES

[1] D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson. Blocking-resistant communication through domain fronting. *Proceedings on Privacy Enhancing Technologies*, 2015(2):1–19, 2015.

[2] 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.