Designing for Multiple Use and At-Risk Users: Tor Configuration Launcher

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

ABSTRACT

stuff here

Keywords

User Studies, Tor, Security, Censorship, Anonymity

1. INTRODUCTION

Introduce what Tor is, and what the configuration interface does in the Tor Browser Bundle. Explain the story of how it began as an anonymity tool, but it has since changed to become a censorship circumvention tool. Give statistics of how many people use it (although we can't say how many for what reason exactly), and interesting trends, such as a spike in use around election times or some big political event.

This study aims to understand of what is confusing about the configuration process and what find changes make the process easier. Our study consists of three stages. User interactions with the current interface in various censorship environments generated the problems we address in the study. User feedback and observations of users steered the design process for an improved configuration interface. User metrics, such as success rate and time to completion, measured how well the interfaces served their purpose.

Explain the state of censorship circumvention today, and what governments do to Tor (block it, etc.). Mention the current consequences of people if they try to connect to Tor. Then drive home why it is important for the interface to be usable. And that there have been previous work on Tor Browser, but not any previous work done for its usability as a censorship circumvention tool.

Currently, x% of users fail and with the current interface for reasons a, b, and c. Of those that do succeed, the average time to completion is y. This can lead to a bad user experience, users quitting Tor, or causing high-risk users to make mistakes. With the new design, only x'% of users fail to configure successfully and the average time to completion is y'. Tor has already implemented some of these changes.

2. BACKGROUND

2.1 The Interface

storyboard of the old interface

1. No bridge, no proxy
2. with bridge, no proxy
3. No bridge, with proxy
4. With bridge, with proxy

2.2 Kinds of Users

2.3 Network Components

2.4 Censorship Environments

3. GOALS/EVALUATION CRITERIA

1. **Task Completion** Almost all can successfully connect to Tor
2. **Time to Completion** Time to completion.
3. **Safe for High-Risk Users** It should be possible to configure Tor with the interface that it doesn't leak that they are using Tor.

4. QUALITATIVE ANALYSIS OF THE EXISTING INTERFACE (STUDY 1)

4.1 Motivation

4.2 Methodology

4.2.1 Simulated censorship environments

We simulated three censorship environments for our experiment. These reproducible, stable environments are informed by our experience with pluggable transports and knowledge of commonly seen censorship techniques. Their goal in our user study is not to replicate the network environment in any particular country, but to require our participants to configure Tor Browser in distinct configurations.

- **Mild censorship** (Representative of countries such as France and Australia.) Certain domains are blocked. Reaching these domains requires a censorship circumvention tool. The default option to "connect" to the Tor network directly will circumvent this censor. Additional correct bridge or proxy configurations are optional.
- **Intermediate censorship** (Representative of countries such as Tunisia.) Certain domains are blocked. Censorship circumvention tools such as Tor are blocked. Since all public Tor relay nodes are blocked, the default option to "connect" to the Tor network directly will fail. Any choice of a hard-coded bridge or a valid non-public bridge will circumvent this censor. Additional correct proxy configuration is optional.

- **Comprehensive censorship** (Representative of countries such as China and Syria.) Certain domains 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. Most bridges will fail, but "meek-amazon," "meek-azure," and "meek-google" still work. 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 aggressive censorship environments. (See [**?**] for additional details.)

4.2.2 *Procedure*

We conducted a qualitative evaluation of the interface by creating an environment for users to interact with the configuration interface in a censored environment, observing their interactions in real time without interacting with the participants, and following up with interviews about their experiences. Using established best practices from the field of user experience research ([**?**]), we recruited five users for each censorship environment. We pre-screened our participants to have a good mix of gender, age, technical background, and familiarity with Tor in each environment.

The 1-hour, single-participant procedure begins when a participant enters a small room with a single computer, which is equipped with Chrome, Firefox, Internet Explorer, Chrome, and VLC (for screen recording). A participant is firstly informed of the risks of the study and consenting to data collection. If they consent, the experiment begins. The participant is informed that they are in a simulated censorship environment, where some websites are blocked. We instruct them to visit a sample blocked website and a sample non-blocked website on a non-Tor browser of their choice to illustrate the situation.

After illustrating the censorship environment, participants are asked to complete a worksheet that asks to visit one blocked website and one non-blocked website. We chose Wikipedia's featured article of the day as the blocked website and the CNN homepage as our non-blocked website because the familiarity that most users have with these websites makes the browsing task relatively easy, which focuses participants' attention to configuring Tor Browser.

After instructions, researchers stepped out of the room so that there was no interaction between the participant and researcher for the rest of the session. Participants' screens were recorded and streamed to another room, where the researchers were able to observe how a participant configured their browser. Participants had an average of 45 minutes to complete their worksheet. At this point, the participants do not know the details of their censorship environment, only that they are actively being censored. We believe that this is representative of the mental model of users in censored countries, and therefore chose to simulate this for the experiment. Ultimately, participants needed to configure Tor Browser to circumvent the simulated censorship.

After users completed the browsing tasks or have spent the rest of the time trying to configure Tor Browser, we interviewed participants about their experience. We asked three standard questions asking about their general experience, confusing interface features, and soliciting feedback for improvements. We followed up with specific questions we had for a particular participant from observing their screen. This was to verify any hypothesis we had about the participant (i.e. "they didn't know what to do on window 3").

4.2.3 *Results*

We noticed four common challenges:

- **Challenge 1:** Users don't know how to choose between connecting directly to the Tor network or manually configuring their connection (Figure **??**). The text was unread or not understood by most users. When the user read the text, they found no instructions, but were given information to make a decision for themselves, which they did not feel equipped to do.
- **Challenge 2:** People feel compelled to set up a bridge, even if they don't need one. We believe this is due to the text on the first screen, which refers to a "censored internee connection" (Figure **??**). Bridges are only necessary when the government actively censored Tor relays, but participants are not able to determine the difference between a censor that blocks websites and a censor that blocks websites and the Tor network.
- **Challenge 3:** When their first attempt to connect fails, the interface directs people to the last window they saw before the connection failure. The problem is not necessarily where the interface directs users, misguiding them. It was common for the interface to redirect users to the proxy window in Figure **??**, even when they needed to pick another bridge.
- **Challenge 4:** Users did not know what to do after a failure. Error messages (see Figure **??**) did not guide users into taking specific actions (such as trying a different bridge, trying the same configuration again, try connecting directly, etc.).

5. REDESIGNING THE CONFIGURATION INTERFACE

Only use the following if it helps explain some things. Make sure the tone of things are positive, and explain that making a good interface is harder than it seems.

What it's trying to do

1. separate people who use Tor for anonymity and for censorship
2. if anonymity, to connect people directly
3. if censorship, guide users to make the correct configuration
4. minimize network traces to protect high-risk users

Why certain decisions were made

1. **Asking the User** asking users about their situation rather than hardcoding or probing
2. **No Explicit Advice** no suggestion of what to try and in what order
3. **No Automation** manual configuration of bridges and proxies required
4. **Optimizing for the Average Case** connect, bridges before proxy

What to talk about in this section:

- Talk about the process of translating observations and feedback into feature changes.
- Polishing the interface by working with a designer, using heuristics, and using technical information.
- Iterative design and feedback cycle.
- How we made a functional, instrumented prototype (forking from the interface repo on github and hacking on it) and instrumented the old prototype.

Talk about how the design as a conservative design. And why the conservative choices were made. For at-risk users, maintainability, etc.

6. QUANTITATIVE ANALYSIS OF THE INTERFACES (STUDY 2)

6.1 Motivation

6.2 Methodology

What to talk about in this section:

- experiment design
- how we chose our metrics
- how we collected our metrics

6.3 Results

7. FUTURE WORK

Changing the Current Interface merge, push.
Finishing Touches

- **Detecting the need for proxies.** We hacked this together for now.
- **Handling rare error cases.** Mention clock drift and proxy connection cases.
- **Additional user feedback.** Animation in the progress window.
- **Stylization.** Comply with design style guides, if any.

Measuring Impact Tor metrics to see if this is helping at the large scale, and for future user study work in general.

8. DISCUSSION

If we had more concrete information on the number of high-risk users or users who need to configure a proxy, we would have made additional changes in the prototype. Since we lacked this information, the following changes did not make it into our prototype, but are worth discussing. Depending on the number of high-risk users or proxy-configuring users, these additional changes may be helpful:

- **Tell people to click connect.** On the first screen, the user needs to decide to connect or configure. Although there is a description of what each option entails and when one may consider using that option, there are no instructions for the user on what to do. Ideally, we would people to click connect, and then try the manual configuration if a direct connection fails. We currently do not communicate this because may put some users at risk. However, it is believed that a majority of the users will succeed if they click connect on the first screen, and giving them instructions on what to do can lessen their cognitive load during the configuration process.
- **Hide the proxy screen.** Don't give users the option to configure a proxy unless it has been detected that it would be necessary. The amount of people who use proxies is low, but then ... this would not give users control in the beginning of the configuration process.
- **Help the at-risk users.** There are people who would benefit from, on the first attempt, connecting with a meek bridge or custom bridge, without trying a vanilla tor connection or the recommended bridge in the dialog. Currently, we guide these people to the correct decision, but after trying the default bridge first. Helping these users to make a connection safely without ever being logged as connecting to Tor would be a benefit, but might be a case of overfitting to these types of users. A majority of users should not use a meek bridge or custom bridge, so it would be unideal to lead all users to this decision.

We took an approach that optimized for the average case user yet was conservative in automation to allow at-risk users to possibly connect without leaking that they use Tor. We believe that this is a sound approach to interacting with the user and the one we would recommend personally. However, there are alternative approaches to interacting with the user that may be of interest:

- **Automate the entire configuration process.** This sounds like a radical idea, but it really isn't. Today, this wouldn't harm most of our users. Our study finds that most users do not configure better than we do and would leak that they are using Tor anyway.
- **Auto-configure after connect.** After a person has already clicked connect and the connection was unsuccessful, they have already been logged. I am assuming that the significant difference is between being logged trying to connect to Tor or not at all, rather than the number of connection attempts made. This would greatly save our users a lot of headache.
- **Ask about the risk.** Rather than having the configuration dialog be manual by default, just ask if the users are at risk if the process was automated. If they are not at risk, we can do it automatically, and the at-risk users can configure manually. The issue with this is that people may not answer this question honestly, or they might not know the correct answer to this question.
- **Ask if they are qualified to make decisions.** Asking users if they know which bridge to choose, and choosing for them if they say they don't know. We probably know better than they do. But there are ethical implications of choosing bridges for them rather them making the mistakes themselves. The issue with this is that people may not answer honestly.

9. RELATED WORK

10. ACKNOWLEDGMENTS

11. CONCLUSION

APPENDIX

A. TODO

Include:

- participant worksheet
- participant survey
- participant recruitment prompt
- any instructions we gave participants