

Assessing Usability of Tor Browser

David Fifield¹ and Linda N. Lee¹, Serge Egelman^{1,2}, David Wagner¹

¹University of California, Berkeley, {fifield,lnl,egelman,daw}@cs.berkeley.edu,

²International Computer Science Institute, egelman@icsi.berkeley.edu

TODO: write the paper for PETS currently, it is the same as the class paper..

ABSTRACT

Abstract here.

Keywords

Privacy, Security, User Studies, Anonymity, Tor

1. INTRODUCTION

Text here.

2. RELATED WORK

In this section, we outline previous research regarding how users understand and act on the Internet, communicating relevant risks to users, and usability of Tor Browser

2.1 User Perceptions and Behaviors

It is not surprising to note that the general public is very willing to trade their personal information for little rewards [?]. A part of this phenomenon is due to the fact that the Internet provides instant gratification for this exchange [?]. Indeed, there is a discrepancy between users' reported privacy preferences and their browsing habits [?].

The behavior profiles, as well as the demographics of Tor Browser, are kept anonymous for obvious reasons. No one knows exactly what the average Tor user is like. Some information can be inferred from the bug reports filed by users, but this is a self-selecting subset of the users who are arguably much more motivated and technically savvy than the average user. Anecdotes are another source to gain an understanding of the average user, although these may not be ground truth. A surprising resource is research investigating attacks on Tor users. Le Blond *et al.* trace back and profile a subset of users in the process, and talk about the results [?]. However, this is also a small subset of the user space.

2.2 Risk Communication

Effectively communicating the current risks to a user can have a significant impact on user behavior. A field study of browser warnings show that browser warnings do have the potential to greatly affect user behavior, and work somewhat well in practice [?]. However, many browsers and their

warnings have a history of failing to inform users, who become habituated to warnings; active warnings which interrupt the user process can be a more effective warning mechanism [?]. Warnings are critical in informing users for Tor Browser, since consequences of becoming deanonymized can mean drastic consequences, especially users who live in countries which have outlawed encryption or employ nation-state level censorship [?, ?].

2.3 Tor Browser and Usability

Tor, the clear frontrunner today in anonymous browsing, was specifically designed with usability, or the ease of use, in mind [?, ?]. Although usability is generally critical to the security of any system, this human factors field has traditionally played a limited role in research [?]. However, anonymous systems especially benefit from usability. Usability means more users—and more users mean more security and privacy in such systems [?]. Currently, a wide range of people use Tor Browser, including normal people, militaries, journalists, law enforcements, activists, businessmen, bloggers, and IT professionals [?].

As a whole, Tor is very usable. This is evidenced by the popularity of the system. Clark's usability study of Tor Browser and related software find that in general, Tor Browser is very usable, and suggest that changes made should be in communicating to users, rather than altering the current system. However, the average novice user would most likely have problems installing, configuring, and using Tor Browser [?]. Other usability concerns include the increased latency in using Tor. Even though Tor is a low-latency anonymizing system, there is a noticeable difference in user experience [?]. With usability as intricately linked to the anonymity of its users as it is, additional research to further improve usability is a worthwhile endeavor. Work by Norcie investigates "stop points," or point where a user would give up in frustration, in installation and use of Tor Browser [?]. We contribute in the same spirit, also identifying stop points in the system, but also gauging users' understanding of features, and investigating ways to improve the user experience.

3. EXPERIMENT

Recruited through journalist contacts.

Ran five experiments.

One-on-one with researcher. Researcher limited interaction. Demo cognitive walkthrough. Cognitive walkthrough under-

standing task (Zimbabwe).

List of tasks. Removed "Configure" from list of tasks after p2 because of confusion.

Live viewing by Tor Project developers.

Transcribed audio and made captioned screen recording videos.

4. RESULTS

Common errors and confusion.

Apple Gatekeeper problems, difficulty of fixing (concerns with the App Store).

Selected interesting quotes.

As a result of our study, our partners at the Tor Project created 16 new tickets in their bug tracker [?]. Seven of those tickets were fixed as of this writing, with others in progress.

5. CONCLUSION

Text here.