

Foxtor: Anonymous Web Browsing

Sasha Romanosky
Carnegie Mellon University
sromanos@cmu.edu

Cynthia Kuo
Carnegie Mellon University
cykuo@cmu.edu

ABSTRACT

Tor¹ is an internet anonymity tool that uses the Onion Routing protocol to provide users with a free and secure way of communicating anonymously while online. However, for many users it's usefulness is overshadowed by the difficulty of configuration and operation. We present Foxtor, a packaged installer and Firefox extension that we believe improves upon the usability of Tor.

1. INTRODUCTION

As computer users become more and more connected they are able to access more information online. By doing this, they often leave digital trails and expose themselves to unknown privacy risks.

Enter anonymity software. Tor is a proven anonymity tool with little to no existing user-interface. We wanted to make anonymity software available to everyone by creating an interface that was easy to install and easy to use.

2. FOXTOR

The motivation for this work began with the Tor GUI design contest and came from a realization that anonymity software can be useful to anyone who does not want to be identified while browsing online. The design competition was composed of two parts. First, participants were requested to design an improved Tor user interface. Then, participants were challenged to implement that design in code. This paper focuses on the second part.

2.1 Initial Design

Our initial design tried to identify common types of users and determine their needs. We therefore created an interface that addressed those needs. We decided to target a broad audience of users with moderate to low privacy needs. These users would have learned of Tor from newspapers, online articles, or friends but would have little experience with anonymity software. We anticipated that those users would have very little patience for a difficult setup and might give up easily if the task proved too challenging. In the original Tor installation, the user downloaded and manually configured multiple pieces of software. We felt this was unacceptably complex and instead proposed an all-in-one installation program.

Additionally, these users would likely only use Tor for web browsing and so we chose to design a Firefox extension. We also imagined that users could be confused by the slower download speeds Tor causes or the fact that some websites will not work if the user is connecting through the Tor network. This insight led us to incorporate an on/off feature to allow users to enable or disable Tor. We also included a status bar that displayed the exit node Tor was using.

2.2 The Windows Installer

A Windows installer was created using the NSIS development platform.² The first page of the installer is shown in Figure 1.



Figure 1: Installation, Page 1

The installer combines the Tor and Privoxy³ NSIS scripts as well as installs the Firefox extension and installs these components into a single directory on the user's system.

The user is never prompted to select installation of individual components. This was done in an attempt to remove complexity from the installation process. Once installed, the user is directed to the Foxtor web page⁴.

2.3 The Firefox Extension

The extension resides in the left-hand side of the Firefox status bar. It consists of an icon and text that represent whether the browser is configured to communicate through Privoxy and Tor, or not.

The extension uses the "Masked" and "Unmasked" metaphor, as shown in Figure 2. The "Masked" state represents anonymous

¹ <http://tor.eff.org>

² <http://nsis.sourceforge.net>

³ <http://www.privoxy.org>

⁴ <http://cups.cs.cmu.edu/foxtor>

browsing, while the “Unmasked” state represents the user’s default browser settings.

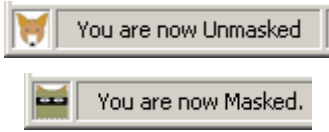


Figure 2: States of FoxTor

The user can change states from Unmasked to Masked either by left-clicking the icon, or right-clicking the text. Because it takes a few seconds to validate the Tor connection, “Putting on your mask...” is displayed until either an error occurs, or a connection is established, as shown in Figure 3.

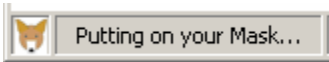


Figure 3: Setting up the Tor connection

2.4 User Feedback

When the user is Masked, the IP address of the exiting Tor node is displayed in the status bar as shown in Figure 4.⁵



Figure 4: Feedback to the user while Masked

Right-clicking the text displays the menu as shown in Figure 5.

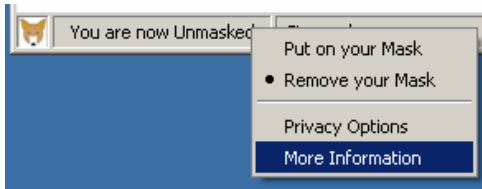
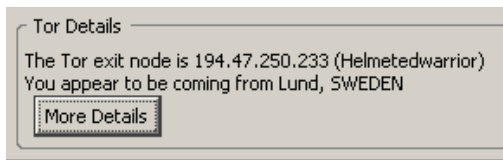


Figure 5: FoxTor Menu Options

Selecting “Privacy Options” opens the standard Firefox Tools:Options menu, allowing the user to modify their privacy settings as necessary in either “Masked” or “Unmasked” states. Selecting “More Information” opens a new window that provides the user with basic instructions on the operation of the extension. Effort was made to provide only the necessary amount of detail especially in regard to the underlying components (Tor and Privoxy). Pressing the “More Details” button queries a website⁶ to retrieve geographical information and the Tor exit node and IP address as shown in Figure 6.



⁵ We appreciate that not all users will recognize the significance of this new IP address because they may not even know their own IP address. However, there is great opportunity to improve this feedback mechanism to provide the right balance of useful but uncluttered information in the status bar.

⁶ <http://api.hostip.info>

Figure 6: Geographical details while Masked

2.5 Firefox Preferences

Part of the benefit of browsing anonymously is achieved by not having the browser set cookies, automatically fill in form data, or store a file cache. The extension satisfies this by altering Firefox privacy preferences when a user becomes Masked. These preferences are shown below in Table 1.

| Parameter | Setting |
|------------------------------------|------------------------------------|
| History | Zero days |
| Save Form Information | No |
| Save Passwords | No |
| Download Manager History | Delete upon successful download |
| Cookies | No cookies are set |
| Cache | 0 bytes |
| Block Popup Windows | Yes |
| Allow websites to install software | No |
| Load Images | From the originating web site only |
| Enable Java | No |
| Enable Javascript | No |
| Software updates | Disabled |
| Proxy Settings | Configured to use Privoxy |

Table 1: Firefox “Masked” preferences

When the user toggles between Unmasked and Masked, the extension saves the user’s preferences. It then restores these preferences when the user reverts to the Unmasked state. This enables the user to alter the default Masked or Unmasked preferences to suit their needs.

2.6 Future Work

While it was beyond the scope of this project to bundle Tor, TorCP and Privoxy into a single application (with a single system tray icon), we believe having a single application would greatly improve the overall usability of Tor. We observed that a number of users were misled into thinking that Privoxy provided the anonymous connection when, in fact, it is just one component.

We would like to perform a comprehensive user study of Foxtor to understand the following:

- Does the extension perform as expected?
- Are the metaphor and functionality intuitive?
- Does the extension provide sufficient feedback?
- Does the extension lack any necessary feature?

3. ACKNOWLEDGMENTS

The FoxTor extension was developed by Sasha Romanosky. The installer was originally developed by Kami Vaniea and modified by Sasha Romanosky. The FoxTor concept was designed and developed by members of the Carnegie Mellon Usable Privacy and Security Laboratory (CUPS). The FoxTor home page is <http://cups.cs.cmu.edu/foxtor/>.