# FoxTor: Anonymous Web Browsing

Sasha Romanosky
sromanos@cmu.edu
Carnegie Mellon University
Usable Privacy and Security Laboratory

May 31, 2006

## 1. Overview

FoxTor is as application that bundles Tor/TorCP[1], Privoxy[2] and a Firefox[3] extension (of the same name). FoxTor helps protect one's identity while browsing online by masking identifiable information of a Firefox web user. It was designed to be as usable as possible for a non-technical audience.

## 1.1 Features

The FoxTor application offers the following features:

- Provides one-click method to toggle between anonymous and normal browsing by clicking an icon (or text) in the Firefox status bar

- Employs an intuitive metaphor of "Masked" and "Unmasked" to represent anonymous and identifiable browsing, respectively

- Synchronizes state between multiple Firefox windows or tabs

- Enhances anonymity by temporarily disabling particular Firefox preferences such as browser history, disk cache, saved form data, passwords and cookies.

## 2. Limitations

Currently, the extension suffers from the following limitations:

- While the extension disables cookies from being *set*, it does not prevent them from being *sent*. A solution is currently being investigated.

- A more comprehensive user study should be performed to test the usability of FoxTor. Specifically,

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

- Currently, a remote website[4] is used to validate the Tor connection. This creates an uncomfortable dependency on the website; the site may be down, or they may not recognize a particular Tor node as being legitimate. Either case may produce a false positive

- Currently the Windows installer assumes Firefox has been installed in the default directory (C:\Program Files\Mozilla Firefox).

- Compatible with Firefox v1.5.0 and greater, only

- Better error trapping, reporting and problem *fixing* could be implemented

## 3. Introduction

The Firefox FoxTor extension allows a user to browse anonymously using Privoxy and Tor without requiring any knowledge of Privoxy, Tor or Onion Routing.[5]

## 4. The Windows Installer

A Windows installer was created using the NSIS development platform.[6] The first page of the installer is shown in Figure 1.



**Figure 1: Installation, Page 1**

---

[1] http://www.tor.eff.org

[2] http://www.privoxy.org

[3] http://www.mozilla.com

[4] Harvard's Tor test page at http://serifos.eecs.harvard.edu/cgi-bin/ipaddr.pl?tor=1

[5] http://www.onion-router.net

[6] http://nsis.sourceforge.net

The installer combines the Tor and Privoxy 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 prompted to launch Firefox which loads the FoxTor web page[7]. This page provides the user with basic information on the functionality of FoxTor.

An unfortunate consequence of launching Privoxy is the window that appears. We have found this window to be distracting. Unfortunately, there does not seem to be a way to launch Privoxy in a *minimized* mode. [8]

## 4.1 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 browsing, while the "Unmasked" state represents the user's default browser settings.
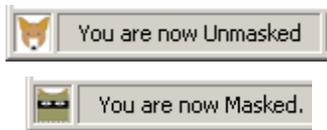
**Figure 2: States of FoxTor**

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.
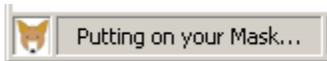
**Figure 3: Setting up the Tor connection**

## 4.2 User Feedback

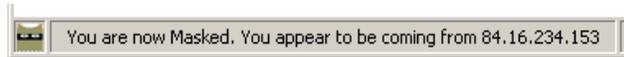When the user is Masked, the IP address of the exiting Tor node is displayed in the status bar as shown in Figure 4.[9]

**Figure 4: Feedback to the user while Masked**

---

[7] http://cups.cs.cmu.edu/foxtor/

[8] The author would be grateful for any suggestions to overcome this distraction.

[9] 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.

If an error occurs while establishing an anonymous connection through Privoxy and Tor, an error message and icon are displayed to the user as shown in Figure 5.

**Figure 5: Error Condition**

Right-clicking the text displays the menu as shown in Figure 6.

**Figure 6: 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 as shown in Figure 7.
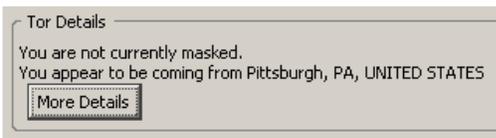
**Figure 7: More Information**

This window 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). The user is also invited to click the text in blue to launch Harvard's test Tor web page to test the connection themselves.

Pressing the "More Details" button queries a website[10] to retrieve geographical information and displays it to the user as shown in Figure 8.



**Figure 8: Geographical details while Unmasked**

Pressing the same button while Masked displays more information, including the Tor exit node IP and name as shown in Figure 9.



**Figure 9: Geographical details while Masked**

## 4.3 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.

## 5. Acknowledgements

---

[10] http://api.hostip.info

[11] Mel Reyes, "Hacking Firefox" Wiley Publishing Inc., 2005.