FoxTor

A Tor Design Proposal

CMU
Usable
Privacy and
Security
Laboratory

November 30, 2005

This document has been submitted to the Tor GUI competition by members of Carnegie Mellon University's Usable Privacy and Security (CUPS) Laboratory: Lorrie Faith Cranor, Serge Egelman, Jason Hong, Ponnurangam Kumaraguru, Cynthia Kuo, Sasha Romanosky, Janice Tsai, and Kami Vaniea.

1.0 Design Overview

1.1 Goals and Priorities

Based on the information provided on the Tor GUI Contest website, observations made during a small user study (described in the Appendix), and discussions about potential Tor users, we developed the following goals for this submission:

1) To provide an intuitive method for installing Tor suitable to each user's needs, and without requiring them to understand the underlying technology
2) To provide clear indication as to whether an application is using Tor or not
3) To provide the ability to easily enable or disable Tor for any given application

The first goal was motivated by the observation that Tor is currently difficult to install and that users are generally unfamiliar with onion routing, proxy servers, and other components required for anonymous browsing. We recognize users have differing needs and we want to allow them to configure Tor by specifying their needs rather than forcing them to understand a multitude of configuration options.

The second goal was motivated by the information on the contest website as well as our own observations that users are often confused about whether or not their traffic is passing through Tor.

The third goal was motivated by our observation that some users would not use Tor if it sacrificed network performance or prevented them from visiting web sites or using certain applications. We speculate that once Tor is turned off, they may forget (or not take the effort) to turn it back on. We therefore wanted to make it easy for users to bypass Tor when necessary without disabling it completely.

1.2 Design Principles

We designed our GUI with the following principles in mind:

- Increase the usability of Tor:
  - Minimize the number of steps required to perform an action -- reducing the number of steps to one whenever possible; and
  - Allow users to easily discern the status of Tor and to turn Tor on or off as needed;
- Simplify the configuration of Tor:
  - Allow users to select a configuration based on their *needs*, rather than forcing them to specify particular settings;
  - Specify default settings applicable to the majority of users so that users are not required to make configuration decisions that they are not qualified to make; and
  - Design the advanced configuration options in a manner that makes them clear and easy to access.

1.3 Design Approach

While there are many applications that might benefit from having their traffic passed through Tor, we believe that anonymous web browsing is likely to be the most common use of Tor. We therefore propose a version of the Firefox web browser named “FoxTor” which will be distributed as a package that includes Firefox (with a set of extensions that implements our Tor user interface), Tor, Privoxy, and a Tor system tray application.[1] To users, FoxTor would appear as a single anonymous web browsing application that is also capable of anonymizing traffic associated with any other networked application.

During the installation of FoxTor, users will have the ability to configure all or only particular applications to use Tor. In order to have all applications use Tor, a network interface component must intercept and pass all traffic through Tor. For applications other than FoxTor, additional software would be needed to provide Tor-related controls (that could be developed and distributed with the FoxTor package).

Within FoxTor, users can enable and disable anonymous browsing both within tabbed panels and standalone windows. We use the metaphor of "Masked" and "Unmasked" personas to indicate whether a browser window or application is invoking Tor. We believe this is to be a metaphor that users will relate to easily and understand quickly from appropriate visual indicators.[2] Users can also adjust Tor behavior according to their privacy vs. performance needs without disabling Tor completely.

Note that only the design concept (and not the code) for FoxTor has been included in this proposal. We recommend performing a paper prototype evaluation of our design as a next step.

1.4 Assumptions

We make the following assumptions:

- Users have some awareness of the level of privacy they want (or need) to maintain
- None of the modification to FoxTor will alter a user's existing Firefox installation when the user is browsing the web Unmasked (i.e. cookies, favorites, etc. will not be changed)
- Changing between Masked and Unmasked (or disabling Tor) within a Tab will affect the behavior of that Tab only
- No assumptions are made about the network performance or stability of the destination website, the Tor servers, the user's computer or the Internet
- The user has a basic fluency with their computer, the Web, and a web browser; however, we assume that most potential Tor users are not computer experts, nor should they be. On the other hand, we believe that they have a heightened concern for their online privacy and recognize that they can be identified unless they use tools such as Tor.

[1] Currently envisioned for the Windows platform

[2] User studies should be performed to confirm that this metaphor makes sense and to refine the visual indicators.

2.0 Target Users

When designing a software application it is important to have a good understanding of the likely users of that application. Early in our design process we discussed who our target users were and what they had in common with each other. Our brainstorming led us to develop profiles for three categories of users, which appear to encompass most of the target users we have considered. The remainder of our design process focused on the needs of these three categories of users.

2.1 Users with critical privacy needs

This category includes people for whom online anonymity is extremely important. They are willing to sacrifice performance and forgo access to some web sites because they are not willing to risk being identified. They require all their Internet interactions to be protected with Tor. Examples include:

- People who live in countries where it can be dangerous to speak out against the government or express one's religious or political beliefs
- Individuals working for certain government agencies
- Soldiers deployed in combat zones

2.2 Users with selective privacy needs

This category includes people who want to be anonymous when visiting certain web sites or when engaging in particular online activities, but otherwise do not mind being identified. When not engaging in anonymous activities, these users will use Tor only if they can do so easily and without significant performance degradation. Examples include:

- Newspaper reporters / journalists researching a particular story
- Corporate whistle blowers
- Crime solvers - anonymous tips from witnesses
- Consumers who don't want to be tracked by businesses
- People looking for sensitive healthcare information
- Political activists

2.3 Users with basic privacy needs

This category includes people who rarely, if ever, have a specific reason to be anonymous; however they generally prefer not to have their online activity tracked. This category also includes people who believe that anonymity systems should be available for those who need them and would like to contribute *cover traffic.*[3] People in this category typically have a low tolerance for degraded performance due to the Tor network. They would like to be able to turn Tor off easily when performance degrades or when it is preventing them from visiting a particular web site.

[3] Cover traffic refers to the concept of providing "normal" traffic in which confidential traffic can be hidden. Without cover traffic there may be insufficient traffic to provide high levels of anonymity. Individuals who use the Tor network may therefore be seen as people with something to hide.

3.0 Tor User Interface Design

Our user interface design includes an installation wizard that installs and configures necessary FoxTor components. As well, it includes interfaces for changing the FoxTor configuration for a particular web browser window or for all browser windows, and a traffic monitor that allows users to monitor the status of Tor traffic coming from their computers.

3.1 Installation Wizard

Application setup has been one of the biggest barriers to large-scale Tor adoption. We propose bundling Tor, Privoxy, and FoxTor into one installation package. Users would download one file, and the installation wizard will pick the correct configuration options automatically based on the user's privacy needs. The wizard asks questions only when absolutely necessary.

The installation begins as presented below in Figure 3-1 and, Figure 3-2.

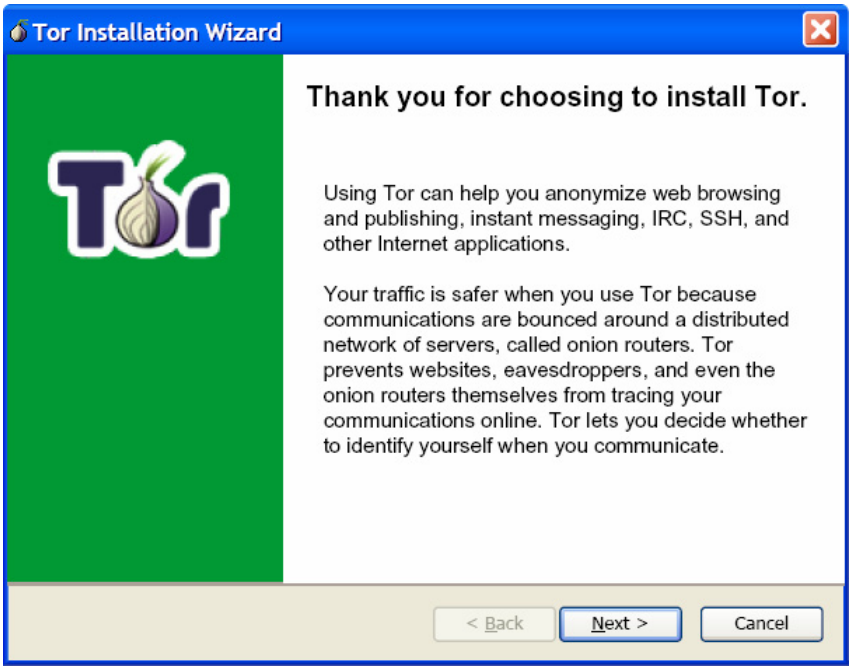

Figure 3-1: Wizard Welcome Screen

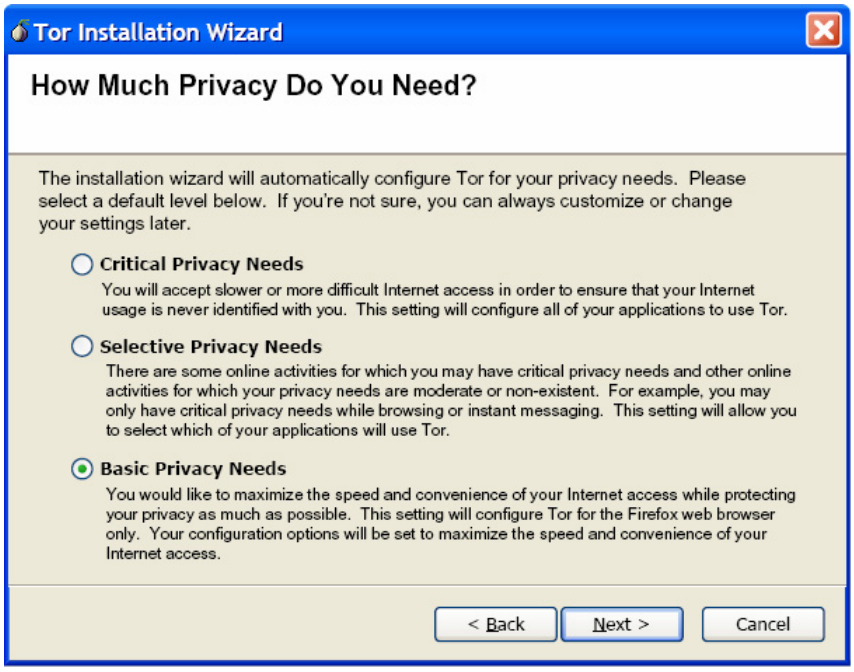

Figure 3-2: Installation Wizard Screen 1

If users choose "Selective Privacy Needs," they will be prompted to select the applications that should be routed through Tor,[4] as shown in Figure 3-3.

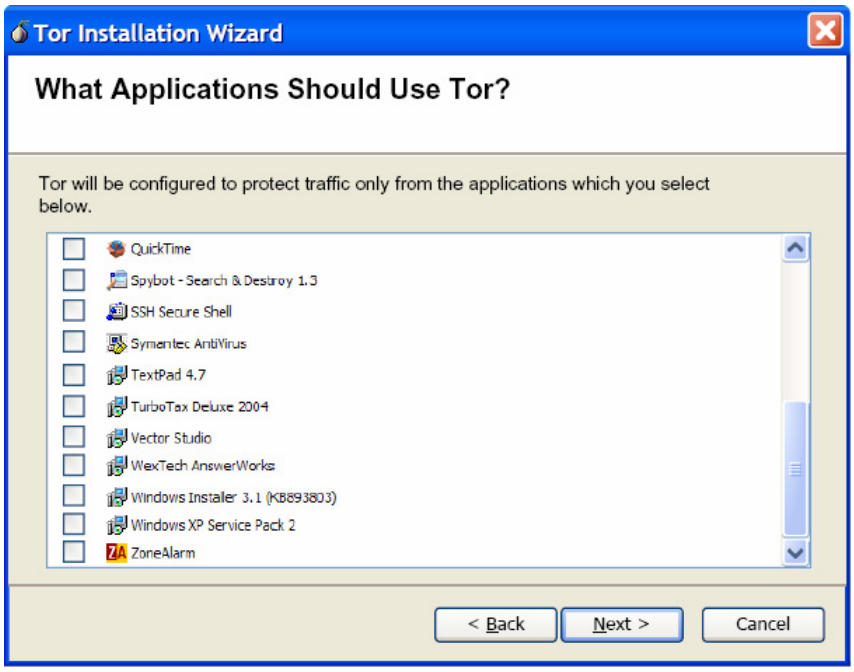

Figure 3-3: Wizard Screen 1a: Selective Privacy Needs Only

[4] Understandably, this list may be very long. Ideally, there should be a way to identify only the programs that require network access. We will continue to investigate the feasibility of this idea.

The installation continues as shown in Figure 3-4 and Figure 3-5.

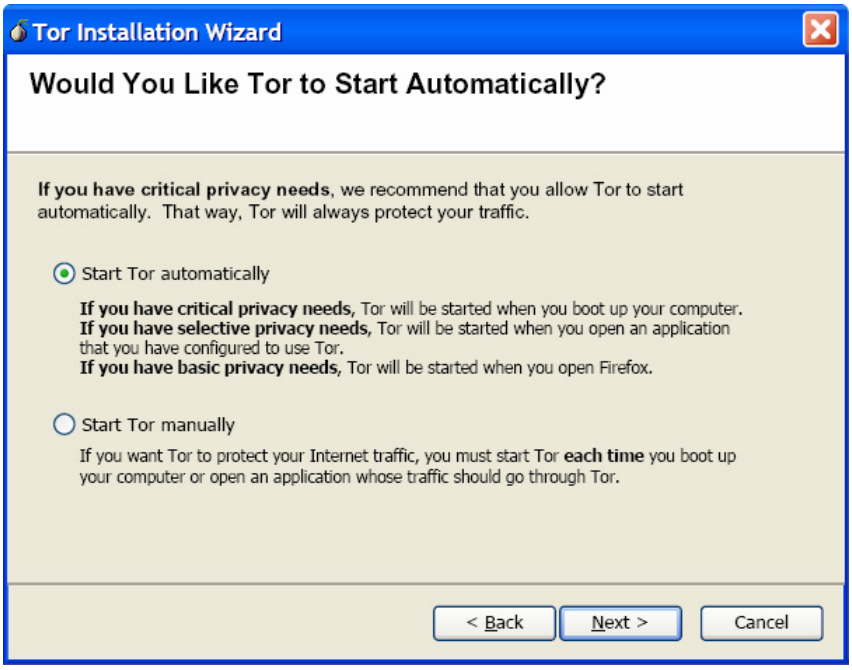

Figure 3-4: Wizard Screen 2

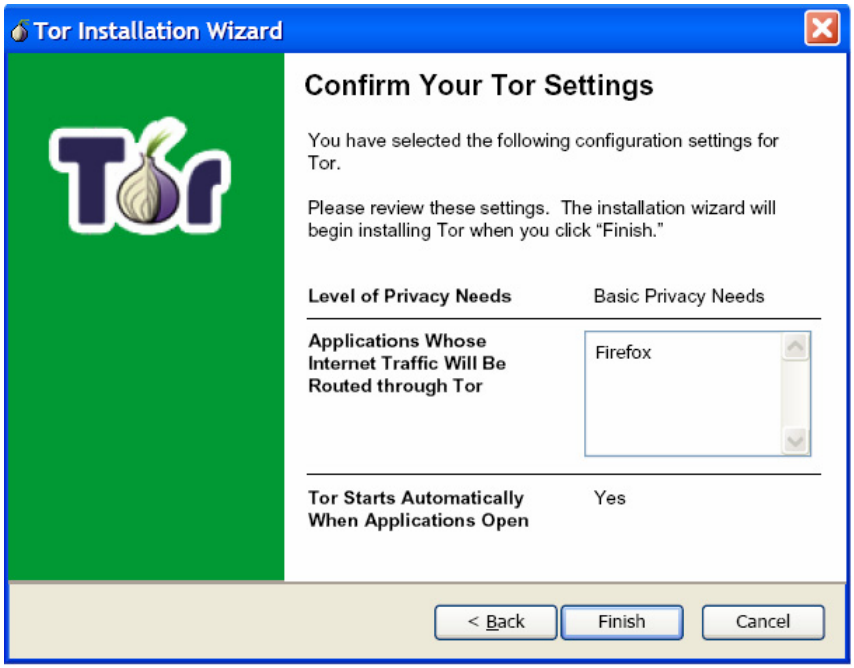

Figure 3-5: Final Wizard Screen: Final Wizard screen

If Tor is configured to start automatically, users will see the alert shown in Figure 3-6 after Tor is successfully installed.

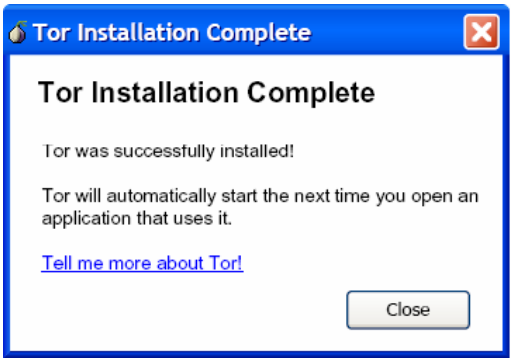

Figure 3-6: Completed installation Alert: Automatic start

If Tor is configured to start manually, users will see the alert shown in Figure 3-7 after Tor is successfully installed.

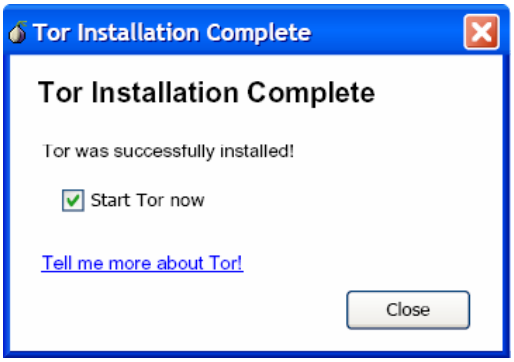

Figure 3-7: Completed installation alert: Manual start

A version of FoxTor might be released for users who already have installed the latest version of Firefox. The installer for this version would verify that Firefox was properly installed before proceeding. We also anticipate that as new versions of Firefox, Tor, Privoxy, or other FoxTor components become available, an upgrader would be made available that would detect which of the user's FoxTor components needed to be upgraded and download only the necessary components.

3.2 FoxTor Configuration

3.2.1 Mask Manager

This section describes the user interface to allow users to enable/disable the Tor service within FoxTor. As well, it illustrates how users are able to quickly and easily identify whether Tor is active or not. By default, FoxTor is pre-configured with two personas: Masked and Unmasked as shown in Figure 3-8. The Masked persona uses Tor while the Unmasked persona does not.

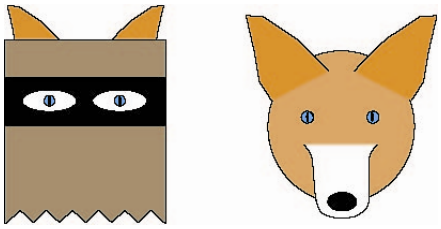

Figure 3-8: Tor Personas

3.2.1.1 FoxTor Persona Plug-in

The FoxTor Persona plug-in appears on the bottom of the browser window as shown in Figure 3-9. We chose the bottom of the browser window because we believe that users generally associate the bottom of the browser window with security and status icons (e.g. SSL lock, connection status).

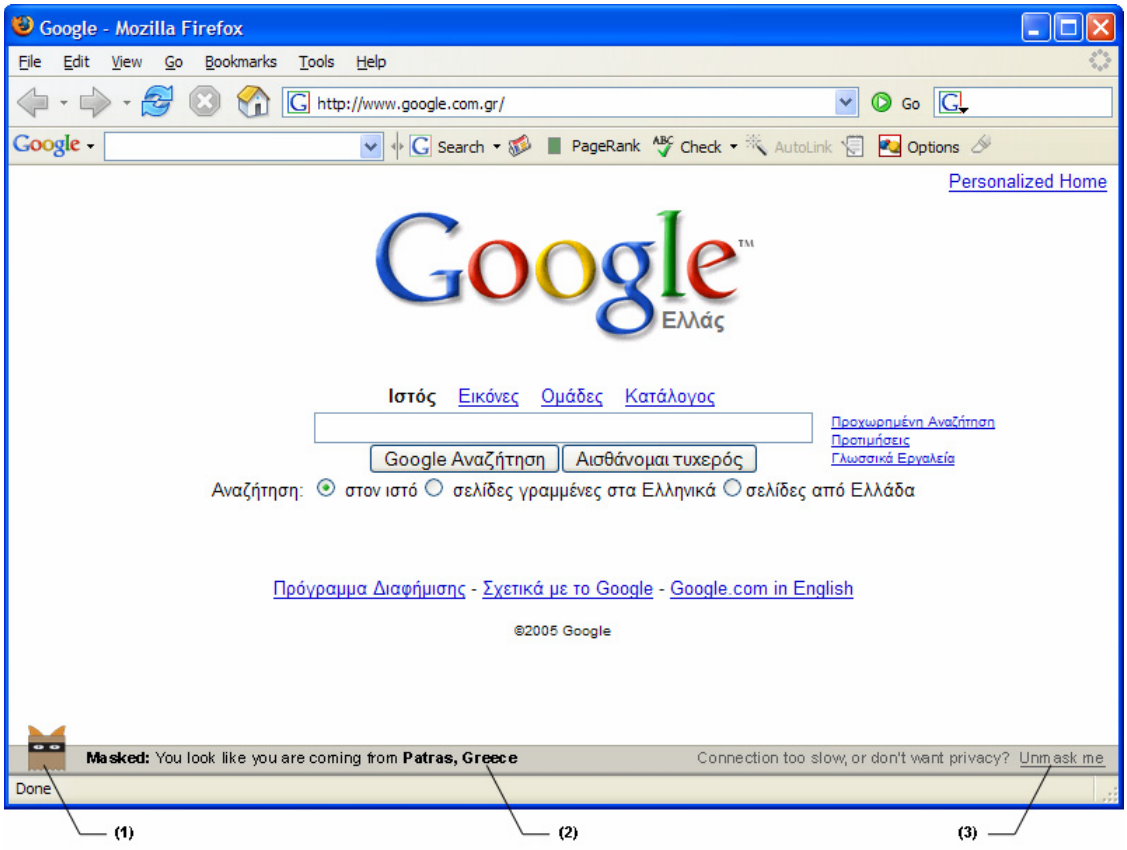

Figure 3-9: FoxTor Browser Plug-in: Masked

Note the following items of interest from Figure 3-9:

(1) This displays the current persona
(2) This status information shows the location of the Tor exit node and demonstrates that Tor is functioning properly. In addition, it may help explain unusual behavior; for example, if a page is displayed in a different language.
(3) Clicking on the "Unmask me" link switches to the Unmasked persona and reloads the page with Tor turned off.

Item (4) on Figure 3-10 illustrates how users can switch to the Masked persona by clicking on the "Put on my mask" link.

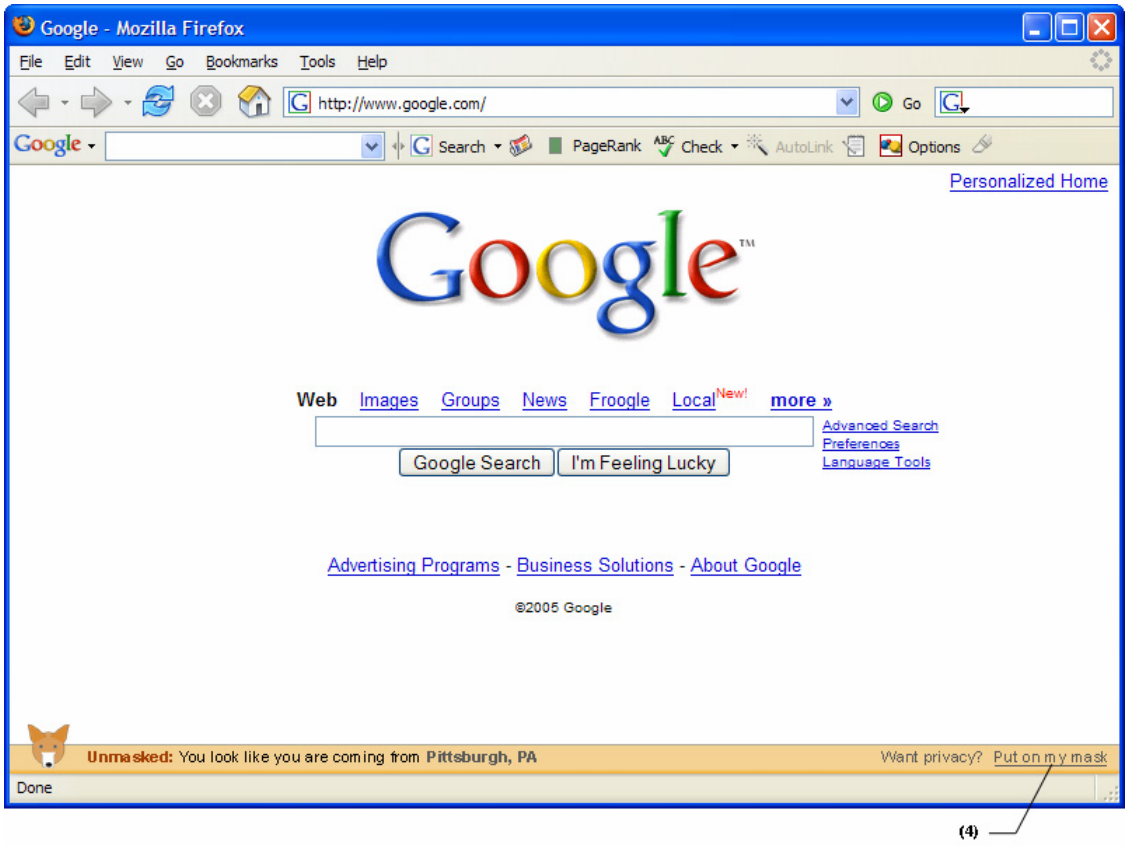

Figure 3-10: FoxTor Browser Plug-in: Rollover and Right-click

The FoxTor bar changes colors with different personas. For masked mode, the bar is gray to suggest blandness and anonymity. For the Unmasked persona, the bar is more colorful to suggest having more personality – and less anonymity. Generally, it is more dangerous for users to accidentally browse unmasked when they think they are masked than to accidentally browse masked when they think they are unmasked. We believe that the colorful unmasked icon will be more noticeable to users than the bland unmasked icon, reducing the chances that users will make a dangerous error.[5]

[5] This should be tested in a user study.

When the mouse hovers over the status bar, a rollover message appears. The message shows the IP address that the visited site will see, as shown in Figure 3-11.

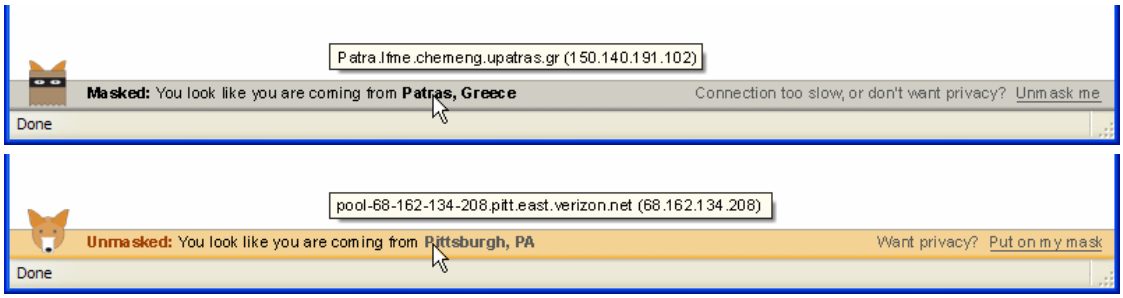

Figure 3-11: FoxTor Browser Plug-in: Rollover Message

3.2.1.2 Right-Click Privacy Menu

When the user right-clicks on the status bar, a menu appears as shown below in Figure 3-12.

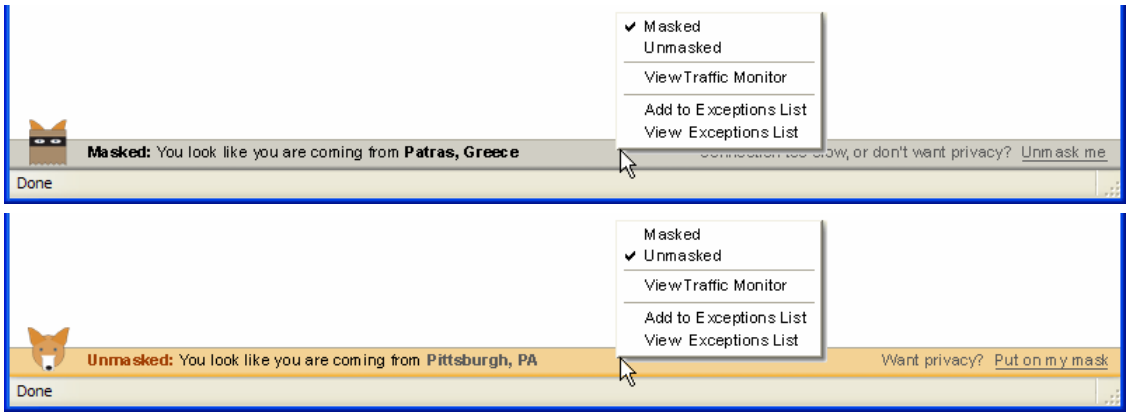

Figure 3-12: Right-Click Privacy Menu

The menu displays the appropriate persona (Masked or Unmasked) allowing the following functions:

- Changing personas from Masked to Unmasked and vice versa
- Viewing the Traffic Monitor (see Section 3.3)
- Add current site to Exceptions List (see Section 3.2.1.3)
- View Exceptions List

3.2.1.3 Exceptions List Options

Users may flag sites that are difficult or impossible to use with Tor. For example, sites on a university or corporate intranet may be inaccessible to people coming from an IP address external to that university or company. Rather than having to remember to unmask whenever they visit these sites, we provide users with the ability to specify sites where they should always be unmasked. Likewise, some users may prefer to browse unmasked, but may have certain sites for which it is critical that they be masked. Here, they can specify that they be masked whenever they visit these sites.

When users select the “Add current site to Exceptions List” option, they are prompted to choose whether they would like to access this site as a Masked or Unmasked site as shown in Figure 3-13. We propose adding sites to the exceptions list on a per-host basis. However, more exploration should be done to determine whether more granularity (full URL) or less granularity (domain) would be more useful.

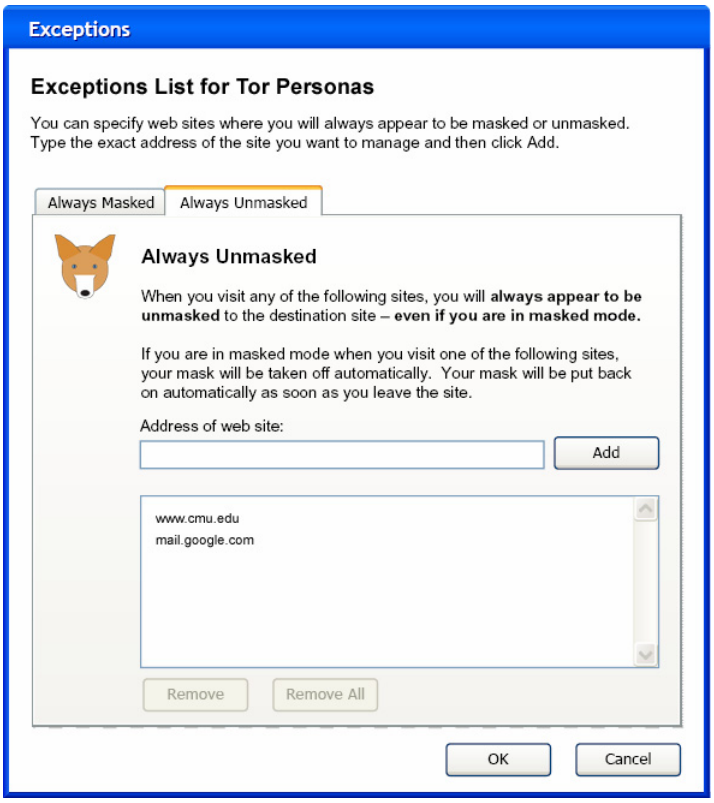

Figure 3-13: Manage Exception List

3.2.2 FoxTor Privacy Configuration

This section describes the privacy configurations within the FoxTor browser.

The options dialog is opened using the main Firefox menu bar (Tools -> Options). As shown in Figure 3-14 below, the two personas are presented on the left frame -- Masked and Unmasked. Each persona is associated with its own History, Saved Passwords, Download History, Cookies, and Cache. As a result, the “Privacy” settings in Firefox are duplicated for each Tor persona.

If a user installing FoxTor does not already have Firefox installed, the default Firefox settings are used for the Unmasked persona. If a user already has Firefox installed, the user’s settings are imported into FoxTor and used for the Unmasked persona and for any configuration setting not impacted by Tor.

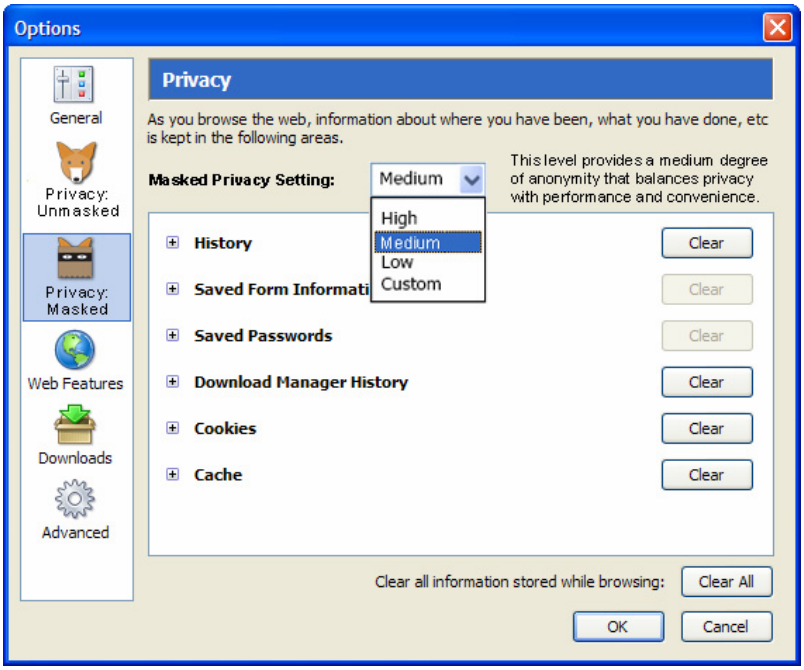

Figure 3-14: FoxTor Privacy Main Options Menu

After selecting the "Privacy: Masked" icon on the left navigation bar, the user may select from four privacy levels: "High," "Medium," "Low," and "Custom." A comparison of the configurations for the High, Medium, and Low privacy settings is shown below in Table 3-1.

Parameter	High	Medium	Low
History	No history is recorded at all (a greater degree of protection than even zero days)	Zero days	Default (9 days)
Save Form Information	No	No	Yes
Save Passwords	No	No	Yes
Download Manager History	Delete upon successful download	Delete upon successful download	Delete upon successful download
Cookies	No cookies are set	Cookies may be set from the originating server only and will be kept "until I close FoxTor"	Cookies may be set from the originating server only and will be kept "until they expire"
Cache	0 bytes	0 bytes	0 bytes
Block Popup Windows	Yes	Yes	Yes
Allow websites to install software	No	No	No
Load Images	From the originating web site only	From the originating web site only	Load all images
Enable Java	No	No	Yes
Enable Javascript	No	No	Yes
Software updates	Prompt user before updating	Allow	Allow
Proxy Settings	Automatically configured to use Privoxy	Automatically configured to use Privoxy	Automatically configured to use Privoxy
Privoxy: Options ->Enable (logging)	No logging	No logging	No logging

Table 3-1: FoxTor Privacy Settings

Table 3-2 shows the text descriptions that are displayed when each of the privacy levels are selected.

Privacy Setting	Description
High	This level provides the greatest degree of anonymity, possibly at the cost of convenience and performance.
Medium	This level provides a medium degree of anonymity that balances privacy with performance and convenience.
Low	This level provides a basic degree of anonymity that maximizes convenience and performance.
Custom	This level offers the ability to customize any of the privacy settings. This should only be used by advanced users.

Table 3-2: FoxTor Privacy Settings

Note that when a user modifies any of the settings from "High," "Medium," or "Low" the "Custom" setting is automatically selected and duplicates the configurations of the user's previous privacy level.

3.2.3 Cookie Manager

This section describes cookie management within FoxTor.

Each persona has its own "cookie jar." That is, cookies that are set using the Masked persona are added to the Masked cookie jar and segregated from the those of the Unmasked persona. FoxTor will notify the user when it blocks a cookie and provide the user with the option to allow it.

We envision using a similar interface to that which Firefox currently uses for blocking popup windows as shown in Figure 3-15. We believe users are comfortable seeing notifications at the top of the Firefox window informing them when items are blocked.

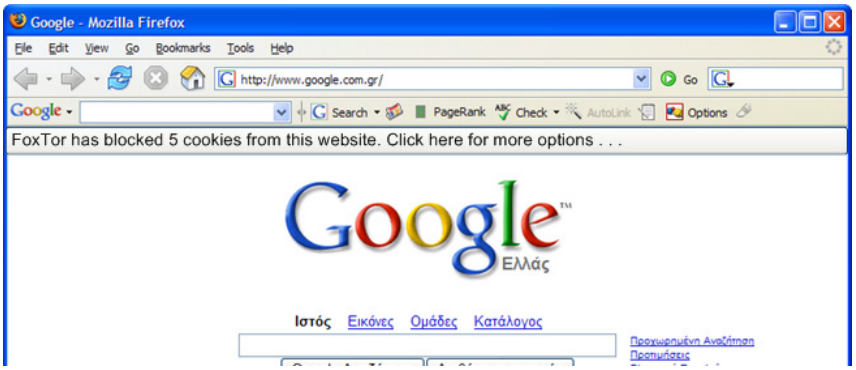

Figure 3-15: FoxTor Cookie Blocking

Clicking on the menu bar would reveal the following list of options as shown in Figure 3-16.

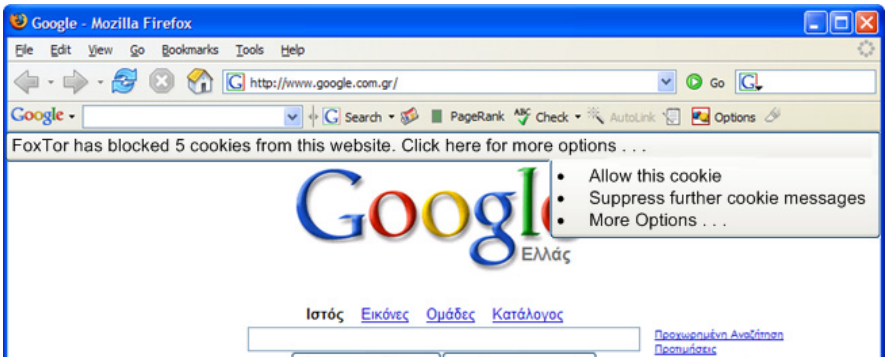

Figure 3-16: FoxTor Cookie Blocking Options

- Allow this cookie: Adds the cookie to the cookie jar
- Suppress further messages: Prevents further messages from being displayed[7].
- More Options: Brings up the cookie jar manager (see Figure 3-17 below)

Users who right-click on the FoxTor browser bar and select "More Options" will be brought to the configuration screen shown in Figure 3-17.

Figure 3-17: FoxTor Cookie Manager

This provides the standard cookie management options but includes useful description of the purpose (benefits and risks) of cookies.

[7] A user study will be required to determine whether this should suppress all further messages or simply messages for the current site only.

3.3 System Tray Application

The system tray will contain a Tor icon (see Figure 3-18). Clicking on the Tor icon will allow the user to configure Tor's global settings.

Figure 3-18: Task Tray Icon

Traffic Monitor

The Tor Traffic Monitor (Figure 3-19) is a stand-alone application that lets users see the traffic they are sending over the Internet. By using the Traffic Monitor, users can detect when traffic is traveling directly to the Internet or is encrypted through Tor. Recall that users can invoke the traffic monitor from within FoxTor through the right-click privacy menu as well as through the icon in the system tray.

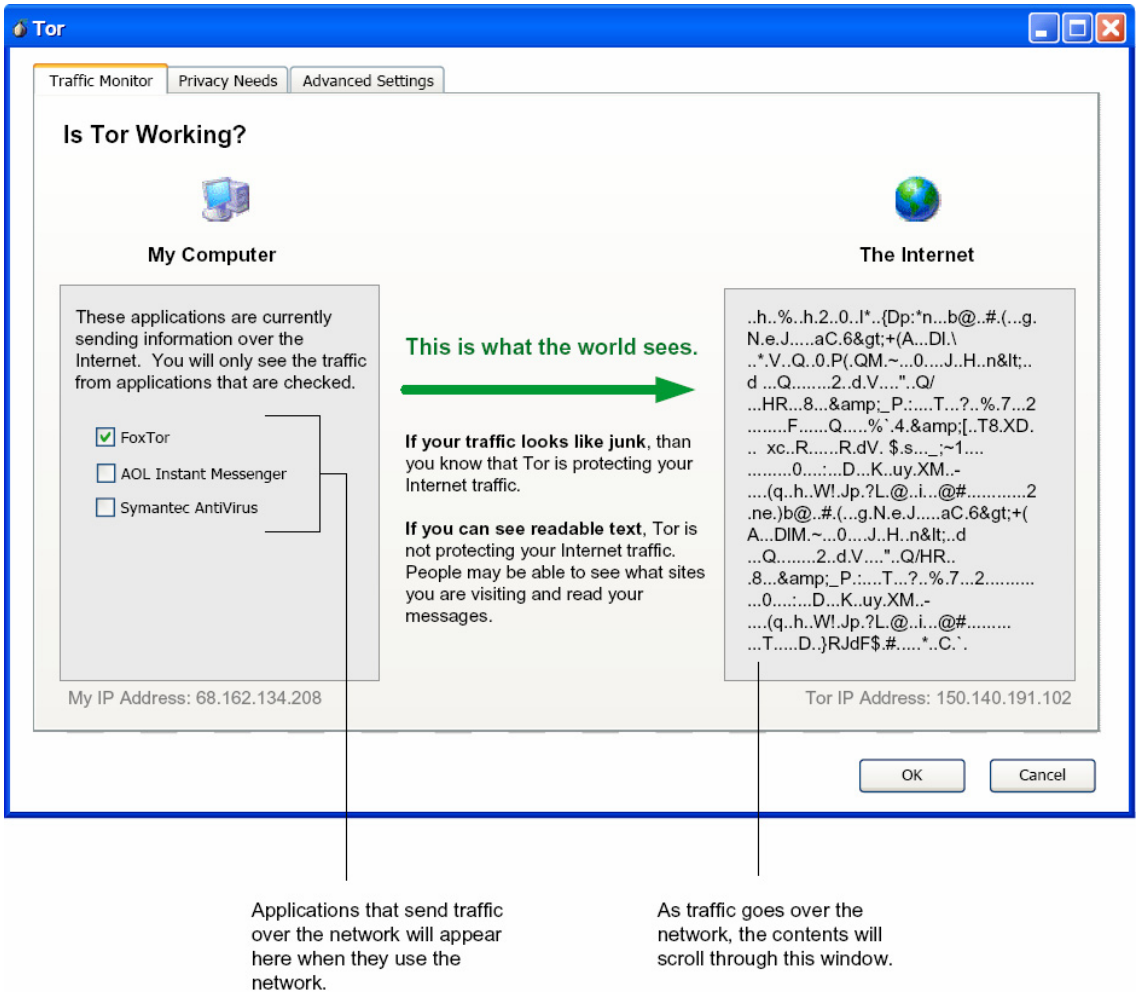

Figure 3-19: Tor Traffic Monitor

3.3.2 Privacy Needs

Clicking the Privacy Needs tab in the system tray application allows the user to configure Tor's global settings. Here the user can change the profile that was selected during installation, select new applications to use with Tor, disable applications from being used with Tor, as well as choose more advanced options. The application selection dialog is the same as the one presented during installation. This dialog can be seen in Figure 3-20.

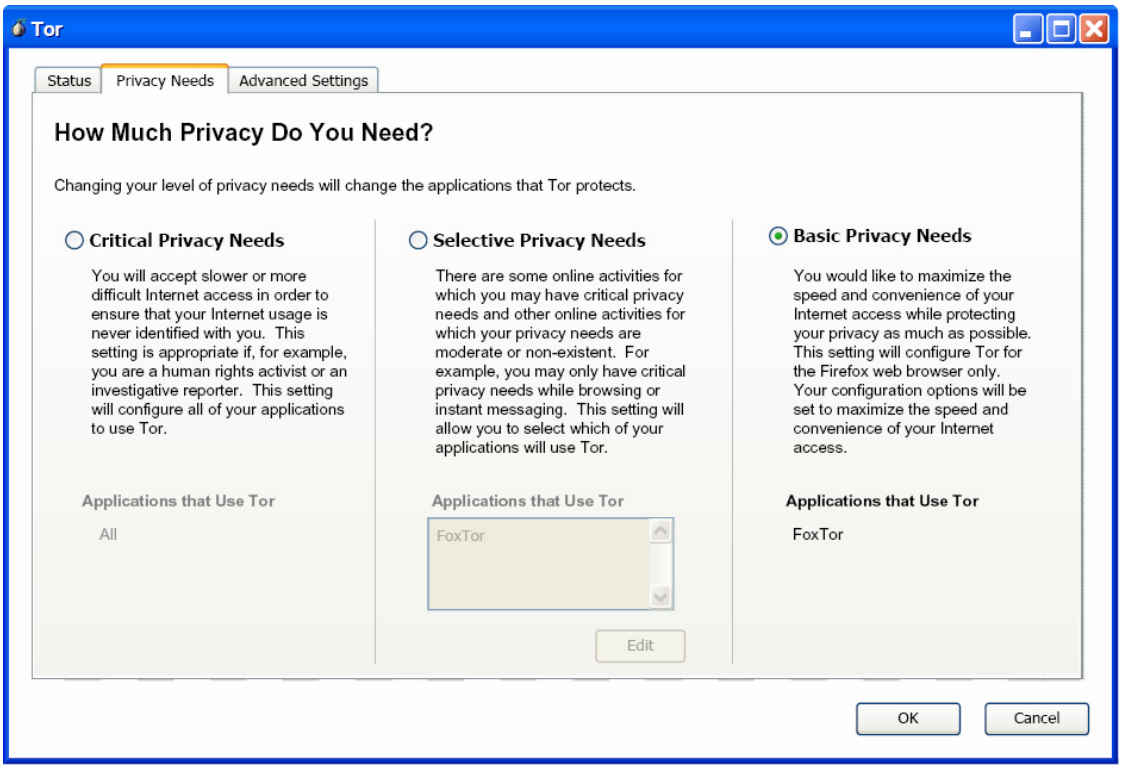

Figure 3-20: Privacy Needs Configuration in Tor

Tor has a number of settings that can be adjusted to gain more privacy at the expense of network performance (or to gain better performance at the expense of privacy). These settings include the number of hops in a route, the number of countries included among these hops, the set of nodes to consider when selecting a route, and the frequency with which a route is recalculated.

For users with critical privacy needs, it is important to maximize privacy by selecting relatively long routes, choosing among all active Tor nodes, and frequently selecting new routes. However, users with basic privacy needs might prefer to increase their network performance by selecting relatively short routes, excluding low bandwidth nodes, and rarely selecting new routes. Furthermore, any user may monitor the performance of the current route and select a new route whenever performance drops below a certain threshold.

The settings on the Advanced tab allow knowledgeable users to determine the most appropriate privacy/speed tradeoff. They can recalculate a route when they believe the current route is too slow and limit the number of hops to pass through on any given route. Additionally, users can also force Tor to choose a route that goes through a certain number of countries as well as limit Tor to choosing a route through the top *X* % of fastest nodes. The fastest nodes are calculated when Tor starts and are based on the total amount of bandwidth that they report, as well as the latency to each node. This dialog can be seen in Figure 3-21.

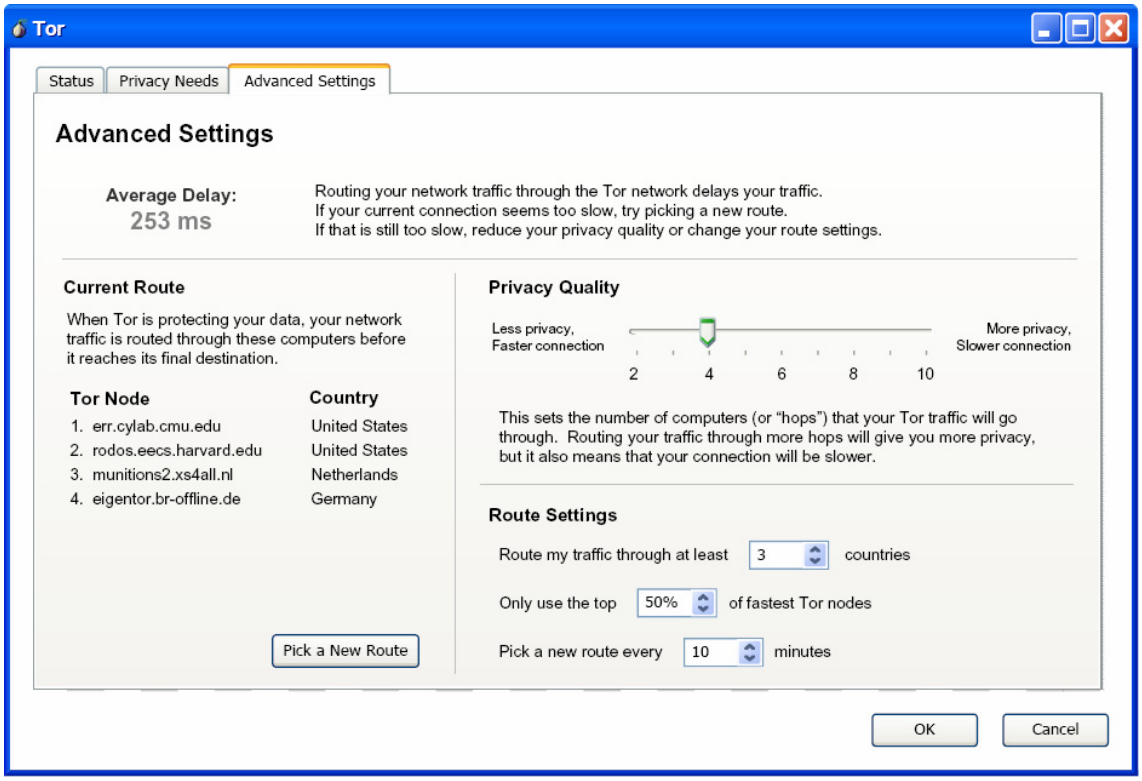

Figure 3-21: Tor Advanced Settings

4.0 Appendix: User Study

4.1 Setup

Our design team observed students in a university class installing and using Tor as part of an in-class exercise. These students followed the instructions on the Tor website to install Tor on their own laptops, which included Windows, Linux PCs and Macs. Most of these students had some technical background, but still found the installation process cumbersome.

4.2 Observations

Many users found Tor's feedback unsatisfactory for determining whether or not it was really running. Users were also frustrated by the network performance degradation they experienced when running Tor.

We observed students trying a variety of strategies when they encountered web sites they were not able to access with Tor. Some users turned Tor off while others opened a non-Tor browser to access the site. That seemed to work relatively well and suggests the idea that we build a UI that makes it easy to have a Tor and non-Tor window so that users can switch between windows rather than turning Tor on and off.

Some users noted that if they visited sites where they had previously set cookies they were still identified even when using Tor.

4.3 Student Feedback

Users stated that they would prefer to download and install a single application that included a wizard to guide them through essential configuration options. The current system where Windows users are required to download multiple components and edit configuration files is "pretty bad." That said, all but one student managed to install Tor successfully (note that these students have a higher level of computer skills than many of our anticipated Tor users).

All users were concerned about whether or not Tor was enabled. The SwitchProxy plug-in on FireFox browsers on Mac platforms gave users both the ability to tell when Tor was working and to enable or disable it. Windows users did not have such an obvious indicator and many were skeptical about whether or not it was working.

Users appreciated being able to test Tor by visiting a website that presented their IP address,[8] but some were skeptical that Tor was still working after they visited another site. However, this was only helpful to users who knew what their IP address was to begin with.

[8] Such as www.whatismyipaddress.com