Tor User Experience Report

Recommendations on enhancing the
user experience of the Tor Browser Bundle

05/06/2013

Jeff Mau, George Rosamond

Funded by the Information Security Coalition

Table of Contents

Introduction
- How this project started
- Author biographies
- The value of the User Experience Design process

Preliminary Research
- Insights from previous papers
- Expert interviews
- Tor Browser Bundle installation experience

Opportunities
- Areas of opportunity to enhance the user experience
- Concept sketches of potential solutions

Prototyping
- Prototype to think through selected solution
- Testing with real users
- Revisions based on test findings

Recommendations

Appendix

Introduction

How this project started

In 2012, the Information Security Coalition awarded a grant to Jeff Mau and George Rosamond to explore ways to enhance the user experience of the Tor Browser Bundle (TBB).

With an approach based on understanding people first, we aim to bring a fresh perspective into making the current Tor software more usable. Additionally, we explore ideas to reimagine what using the Internet anonymously might be in the future.

We have created a hidden website to provide details on our efforts:

L7PLHLIAAOB6PUQW.onion

Author Biographies

Jeff Mau

Jeff Mau is Associate User Experience Director at Roundarch Isobar, a leading agency in the design and development of digital software solutions. Previously the head of Experience Design at Telenav, he led the creation of Scout, a highly rated navigation and discovery app.

Jeff holds a Master of Design Methods degree from the IIT Institute of Design, widely recognized as the top program in Innovation and Strategy. He holds a BFA in Photography and Design from Kansas City Art Institute.

Also active in educating the next generation, Jeff teaches courses in Design and Innovation at IIT Institute of Design in Chicago, California College of the Arts in San Francisco, and CEDIM in Monterrey, Mexico.

His specialities include Strategic Planning, Concept Development, User Experience Design and leading multidisciplinary teams through delivery of large-scale initiatives.

www.jeffmau.com

George Rosamond

George Rosamond is a Unix systems administrator with a concentration on anonymity, circumvention and privacy systems. He has operated an array of Tor bridges and relays for many years.

George is also a founder and coordinator for the New York City *BSD User Group. In addition to internet freedom projects, he manages colocation services with Que Air Data Services.

www.queair.net

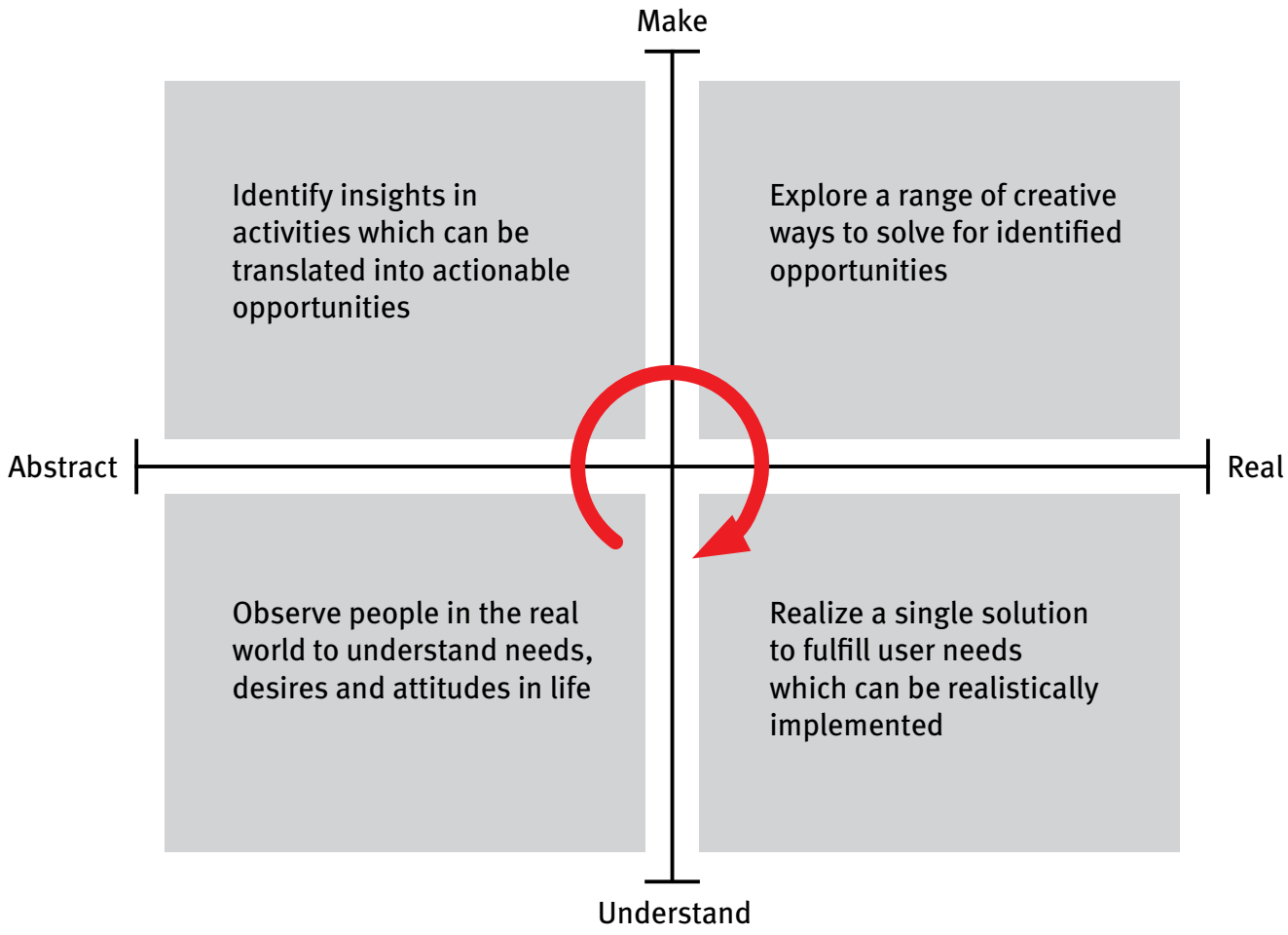
The Value of the User Experience Design Process

Central to the creation of any product, service or offering is the notion it will be used by a person.

All too often, the expert creating the solution is not the only type of user who may use the solution. With this we encounter feature rich, technically sophisticated software which is mindboggling to the average user who wants to accomplish a simple goal.

By starting with understanding people, the user experience design process brings focus to reframing problems to create solutions.

If done well, a design can fulfill unmet needs and desires in a way that aligns with the end user's point of view.



Preliminary Research

Insights from Previous Papers

Through insights from previous papers written on the usability of Tor and challenges with internet security in general, we discovered a clear path to enhance the user experience design of Tor.

"Eliminating Stop-Points in the Installation and Use of Anonymity Systems: a Usability Evaluation of the Tor Browser Bundle"
Greg Norcie, Kelly Caine, L Jean Camp
Presented at Hot PETS Symposium July 13, 2012, Vigo, Spain.

Identification of "stop points" as barriers to installing and using Tor were essential to brainstorming on ways to streamline the Tor user interface. Key stop points include:

The ability to discriminate between anonymized and non-anonymized browser windows while using Tor.

The download and installation process is unclear, with users misinterpeting the zip archive for the executable application.

The recommendation to explain "why" certain behaviors are required in the software.

"Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability"
Jeremy Clark, P.C. van Oorschot, Carlisle Adams
Published in SOUPS '07 Proceedings of the 3rd symposium on Usable Privacy and Security Pages 41-51.

Analysis of the challenges using multiple Tor-related tools including TorPark, Vidalia, FoxyProxy and TorButton led us to explore ways to simplify the Tor user interface.

Exposure to how Tor works may be difficult for novice users to understand.

The recommendation to use familiar, non-technical language is critical.

The recommendation to integrate Tor into the browser became reality with the Tor Browser Bundle.

Expert Interviews

A critical path for this project was to interview experts who had completed work on Tor before this effort. From academic research to activists encouraging internet freedom initiatives, we made sure to understand the context in which Tor is used around the world.

Jeremy Clark, University of Ontario
Our conversation with Jeremy reinforced the need to understand the full range of user types who benefit from Tor. Additionally, Jeremy encouraged us to think of anonymity for all forms of internet traffic such as instant messaging, email and Skype. The notion of Tor as a virtual private network was introduced in this interview.

Peter Fein, Telecomix
Peter's focus on helping people acquire tools to gain internet freedom was enlightening. Keeping the Tor code small and light enables delivery via email and USB devices. The need to provide pseudonymity online was particularly insightful in thinking about providing controls over the routing circuits.

Mike Perry from Tor Project, Kathleen Brade and Mark Smith from Pearl Crescent, Carolyn Anhalt
As we are interested in our research delivering an impact, this discussion was critical to relating our insights to current development activities.

Key insights from our interview include the belief that the browser must be a safe place and that Tor can play a critical role in securing the user. Additionally, much feedback comes into the Tor Project via bug reporting and development channels. The idea to streamline Tor by integrating Vidalia was introduced in this interview, correlating from our own observations.

An important consideration emphasized in this conversation was that many Tor users function in sensitive environments, such as internet cafes, where they want to remain indistinguishable from any other user.

The current redevelopment work is focused on an immediate need for streamlined distribution. The team shared the latest Vidalia-less Tor Browser Bundle aimed at keeping the installation file small enough to send as an attachment through email systems such as Gmail.

The Tor Browser Bundle Installation Experience

We documented the Tor Browser Bundle (TBB) installation experience on OS X. We also reviewed Onion Browser on iOS, Orbot on Android, Freegate, Ultrasurf and xB Browser.

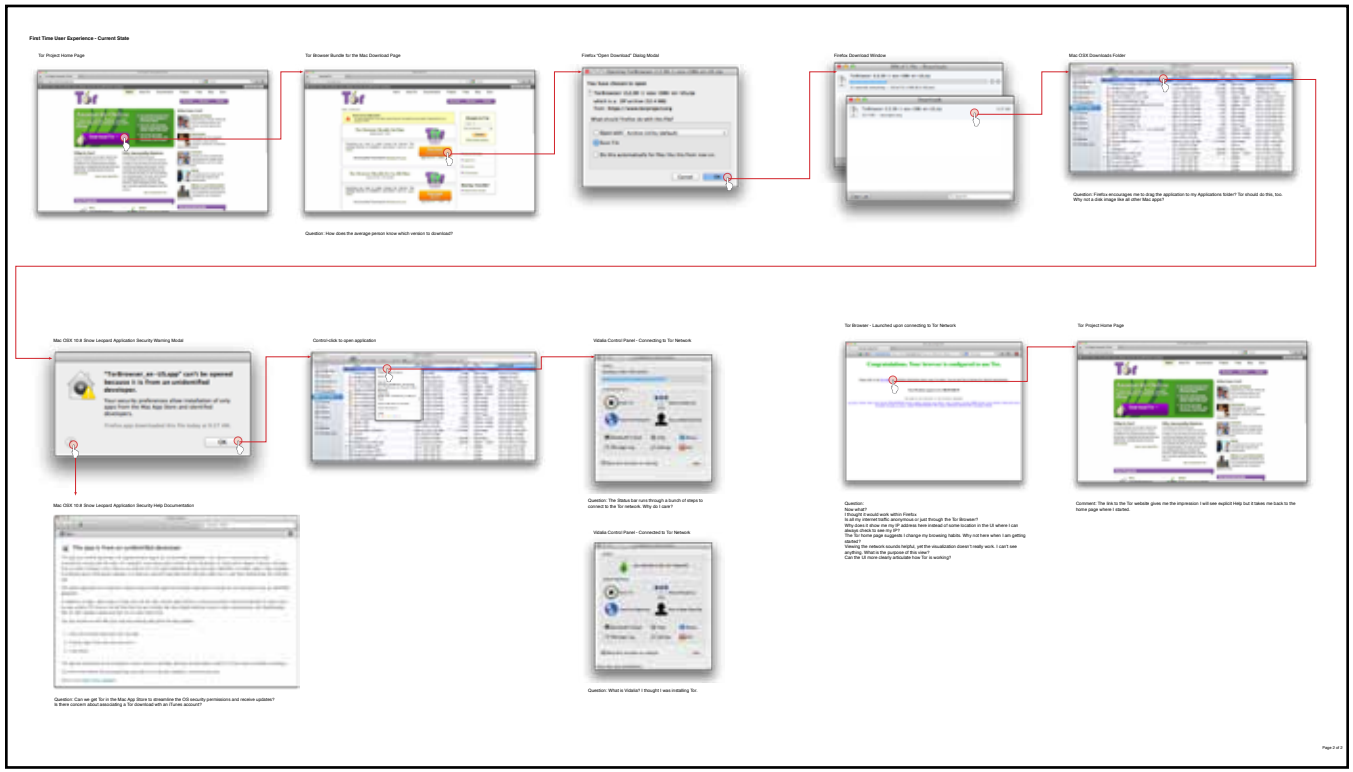
Key findings of TBB include:

The download process was cumbersome due to uncertainty around whether to select the 32 or 64 bit version.

Installation required several steps to open the .zip file. Other applications use a .dmg file to streamline this process.

Opening TBB launches Vidalia, yet users expect to see Tor. The name change is perplexing.

The check page provides a link to learn more about Tor, yet it returns the user to the home page with no additional information on browsing safely.



Opportunities

Opportunities

Articulate how Tor works

When the Tor check page loads, it encourages safe browsing techniques yet simply links to the Tor Project homepage for more information. This is an overly broad next step for users interested in understanding more about Tor and anonymity in general.

The opportunity exists to surface best practice content to the user and reduce the effort required to learn how to best use Tor.

Integrate Tor into the browser

During our user test sessions, users expressed confusion in seeing two separate windows while running Tor. It is not clear which window is “safe” or how making changes in the Vidalia control panel will affect the browsing session.

The opportunity exists to combine the Tor software controls into a Tor version of Firefox to reduce the learning curve in using Tor as well as clarify where the safe browsing will occur. Also, there may be additional visualizations and controls which may help further user confidence in controlling their anonymity online.

Virtualize Tor as a VPN-like tool

Through interviews with Tor experts, we heard that many people use multiple applications over the Tor network including instant messaging, email and secure shell. While many activities can be handled through the browser, there is a need to anonymize all types of sensitive internet traffic.

The opportunity exists to reimagine Tor as a VPN-like tool where any application that runs within a Tor “sandbox” is protected.

Concept: Articulate how Tor works

The first opportunity identified was enhancing the communication when Tor is installed. While tools like JonDonym's ip-check.info offer too much detailed information for average users, the Tor check page offers too little.

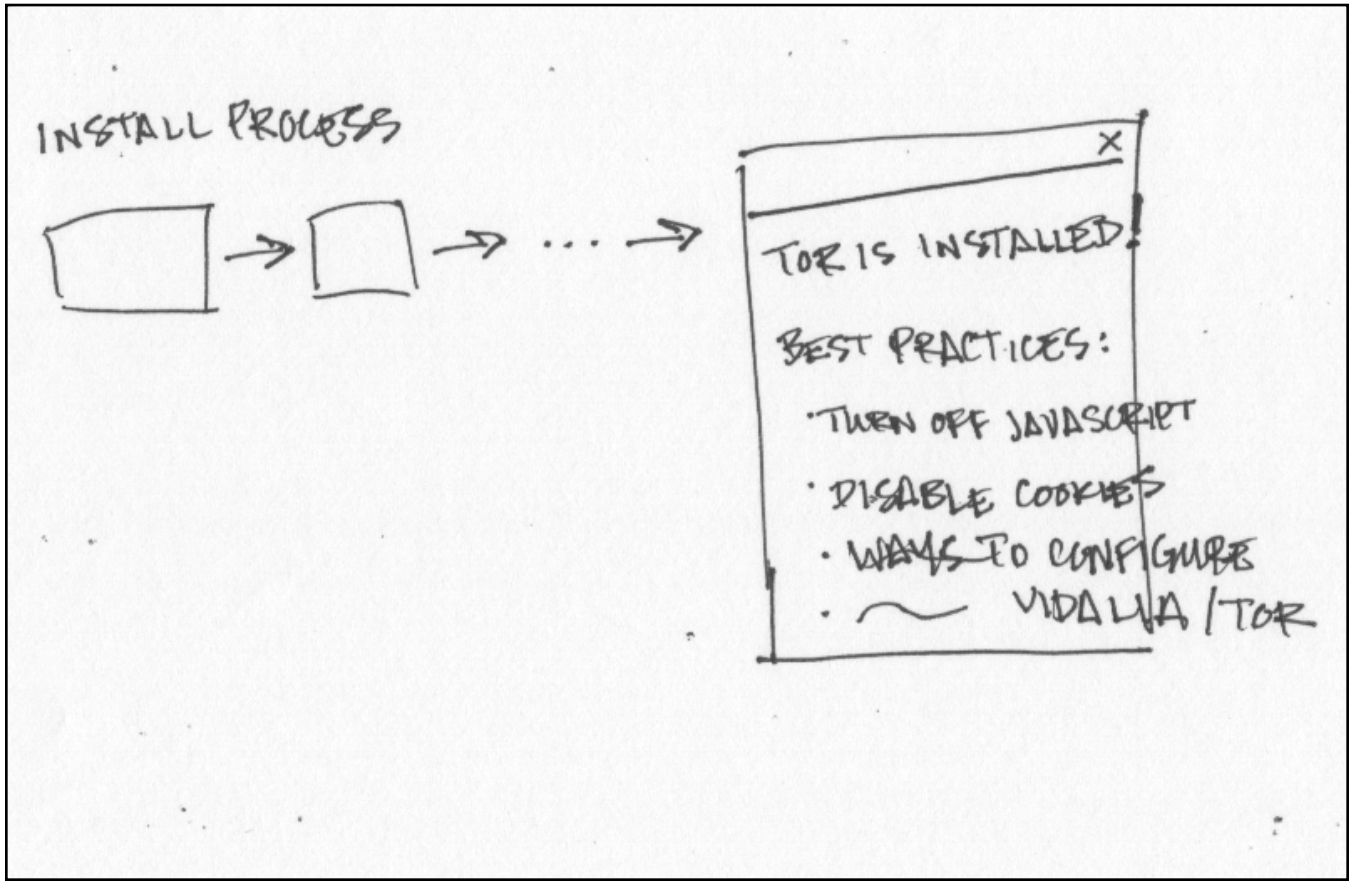
The primary goals:

More clearly communicate what it means when Tor is installed

Provide more detailed information to the user about how to use Tor appropriately

The design features:

An enhanced check page with details about best practices for browsing safely



Concept: Integrate Tor into the browser

The second opportunity identified was visualizing anonymity status in the browser.

The primary goals:

Educate the user on how Tor works through visualization of status and activity

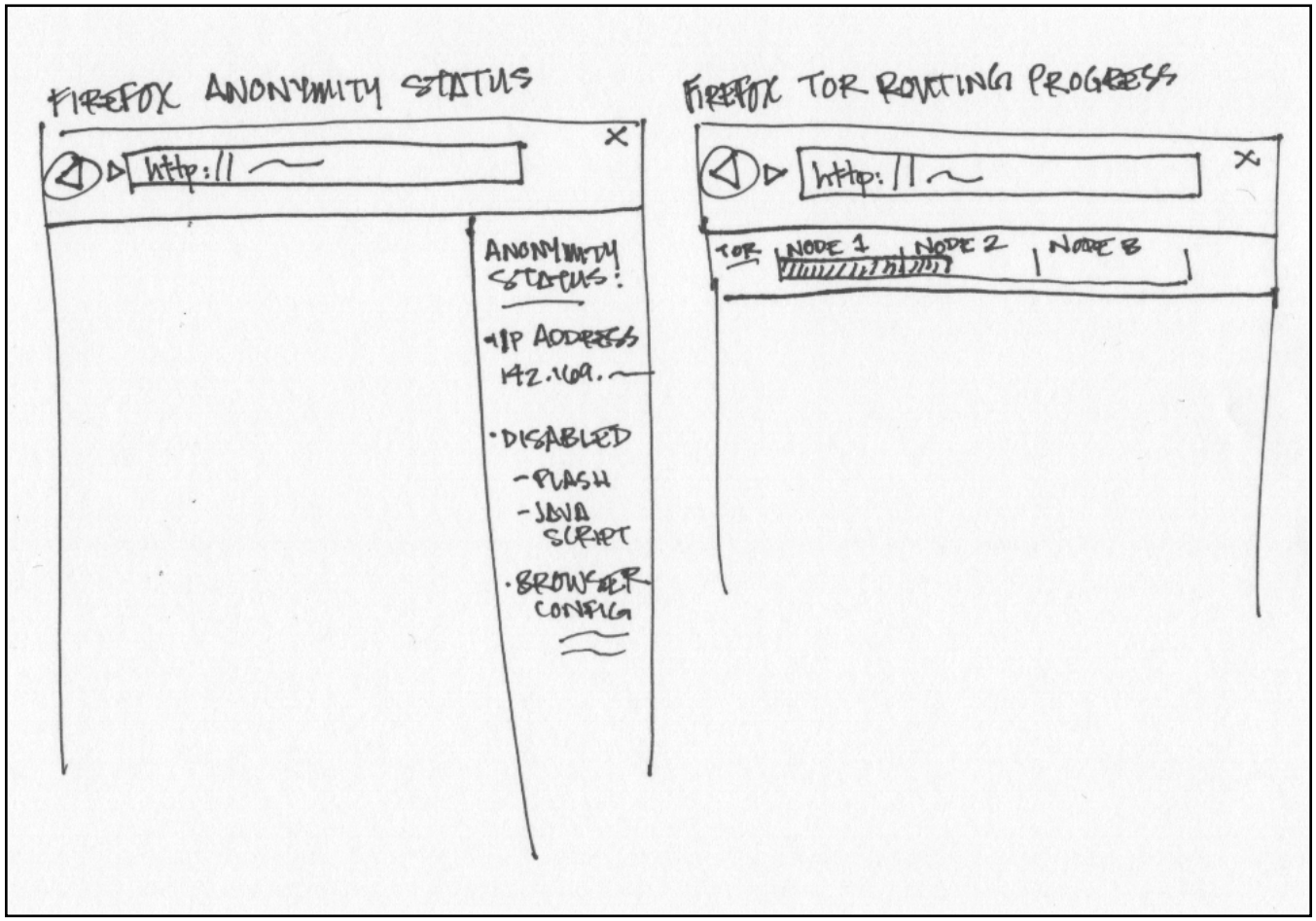
Bring Tor into the browser to eliminate the need to monitor both Vidalia and the browser

Clarify which window on the desktop is protected

The design features:

Details on personally identifiable information

Browser configuration to expose user to best practices in controlling anonymity



Concept: Virtualize Tor as a VPN-like tool

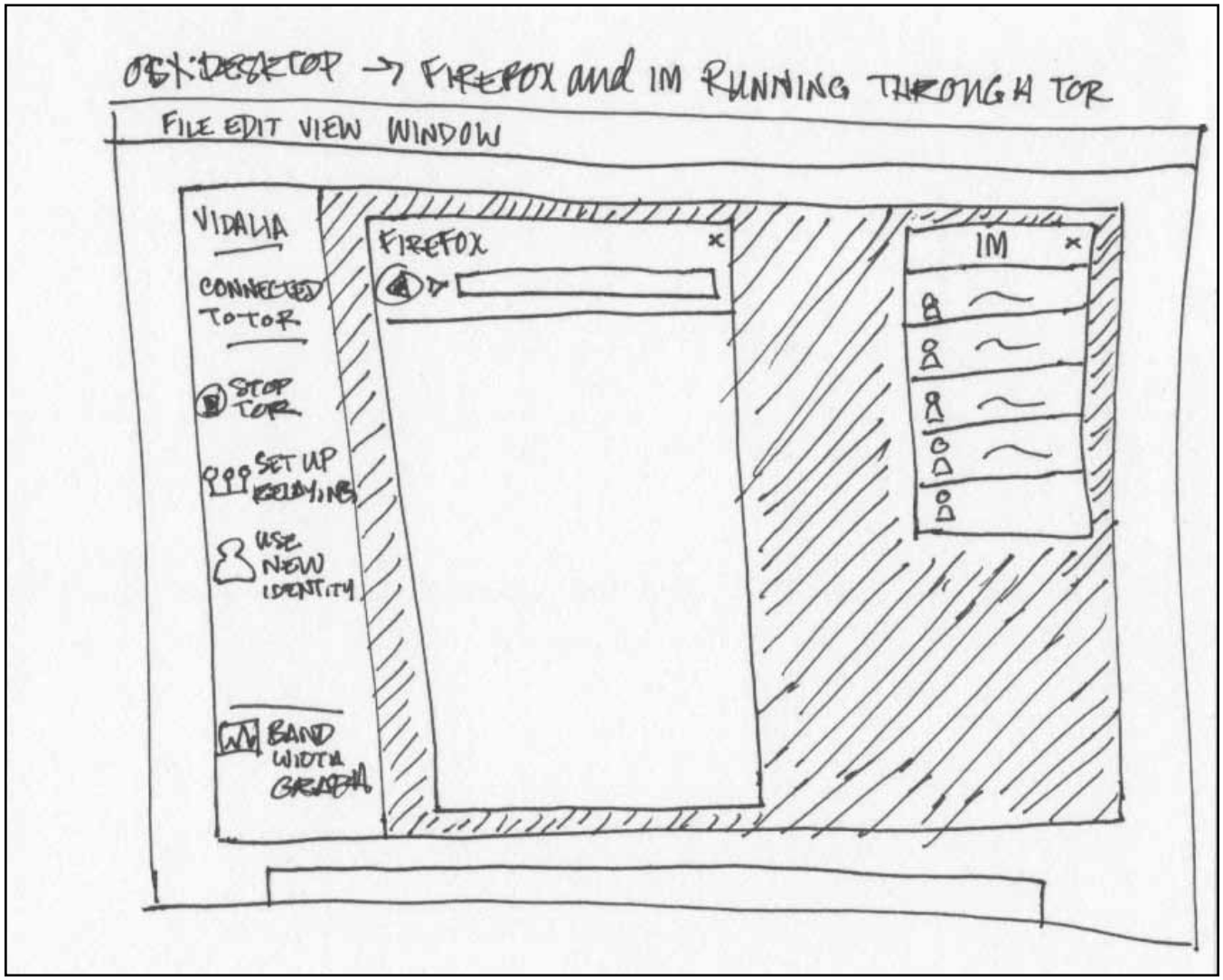
The third opportunity identified was reimagining Tor as a VPN-like tool.

The primary goals:

Redirect all relevant applications through the Tor network

The design features:

A Vidalia style control panel with an extended window which contains protected applications



Prototyping

The Initial Prototype: Vertical Panel

The initial prototype introduced a vertical panel along the right side of the browser window. Vidalia was left untouched.

The primary goals:

Provide status on user anonymity

Educate the user on personal information and software configuration as part of the user interface

The design featured:

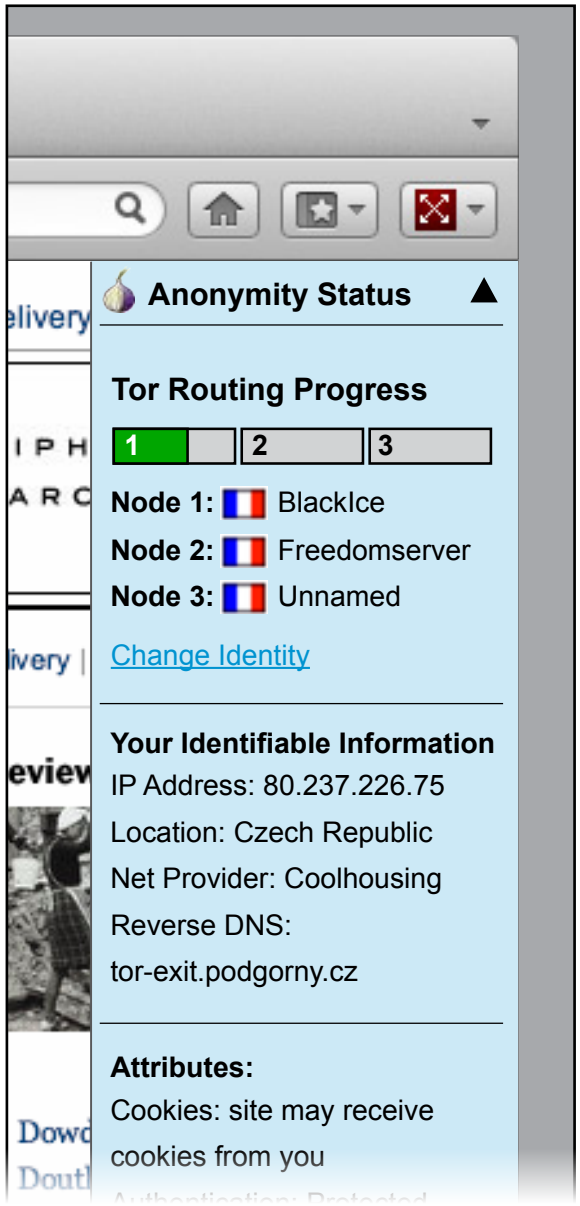
Routing progress always visible

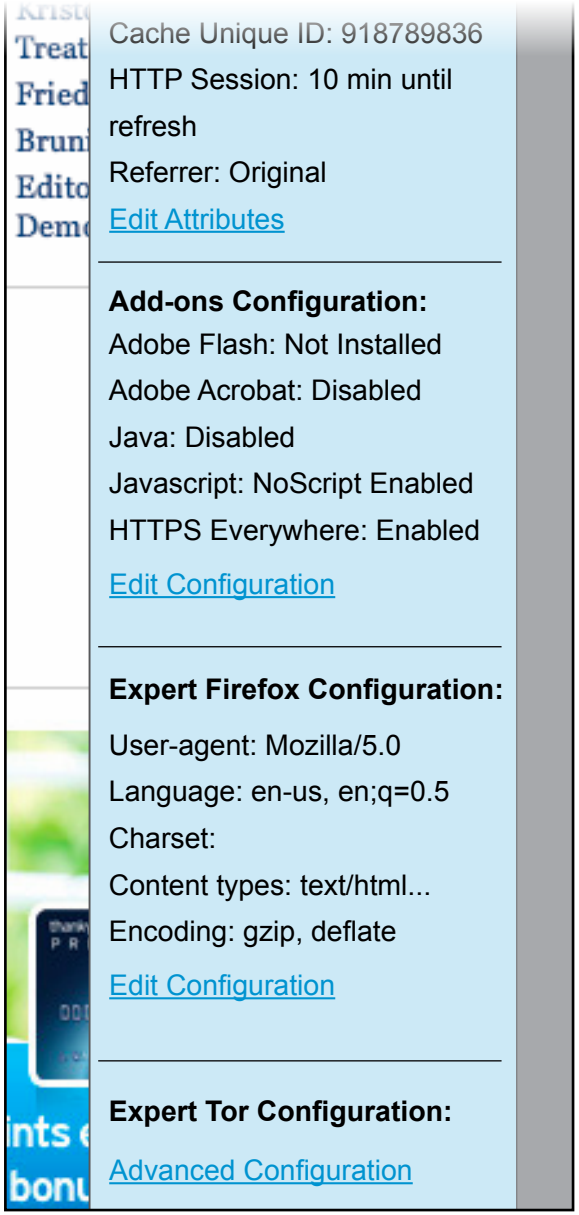
Personally identifiable network information surfaced

Easy access to control Tor and browser configurations

Panel can be minimized when desired

The Initial Prototype: Vertical Panel (detailed view)





Testing with Real Users

In November 2012 we tested the first interactive prototype with real users in New York City. User types ranged from a lawyer with little technology expertise to social activists with strong value systems around internet freedom to software engineering experts who fully understand computer networks and their associated risks. Key insights included:

Too much information
Details on cookies, plug-ins, add-ons and expert configuration were viewed as curiosities without any motivation to modify the configuration.

Viewing routing progress is critical to feeling safe
When users could see the routing progress update in real time as circuits are established, users expressed a feeling of confidence that their internet browsing was being anonymized and that Tor was "doing its job."

"I downloaded the Tor Browser Bundle and I got a Vidalia"
Users expressed confusion around the branding of the software where they were convinced of the need for Tor but received an additional application which was never mentioned during the acquisition process.

The safety of using multiple applications is confusing
When Vidalia runs as a separate application, users expressed concern that it is hard to tell which browser on the computer is functioning with Tor. Users would often open multiple windows across two browsers and not realize one is anonymous while the other is not protected.

Does the circuit reset with every page load?
Coupling anonymity status within the browser window implies that as the user loads a new page, Tor will open a new circuit.

Nomenclature is key to understanding the technology
Using terms like "anonymity" rather than "privacy" are critical to accurately communicate what the software does and how it is working. The more accurate we can make this language, the greater the user's trust in Tor keeping thier internet activity safe. This point becomes particularly important when translating the user interface into other languages.

New visualizations of status will increase confidence
The current network map, bandwidth graph and other visualizations require study to understand. Reimagining visual methods of user activity and Tor network status will provide the user finer comprehension of using Tor safely.

The Refined Prototype: Horizontal Bar

The refined prototype revised the design as a horizontal bar across the top of the browser window. Vidalia was removed.

The primary goals:

Provide status on user anonymity

Focus on the essentials of browsing safely

The design features:

Circuit routing progress always visible

Vidalia controls are incorporated into the user interface

Start/Stop Tor button is presented as a primary control

Additional controls are grouped under an “Advanced Settings” button to reduce the perceived complexity of configuring Tor.

The Refined Prototype: Horizontal Bar (detailed view)

Recommendations

Recommendation: Integrate Tor into the browser

Integrate Tor controls into a customized Firefox browser.

Bring focus by displaying only critical controls and visualize user anonymity status.

Provide advanced controls for configuration a layer deeper to reduce the learning curve for most users.

Redesign any functionality which is not working clearly e.g. the Network Map.

Simplify function labeling for ease of understanding and localization.

Provide a mechanism to retract the Tor panel from view.

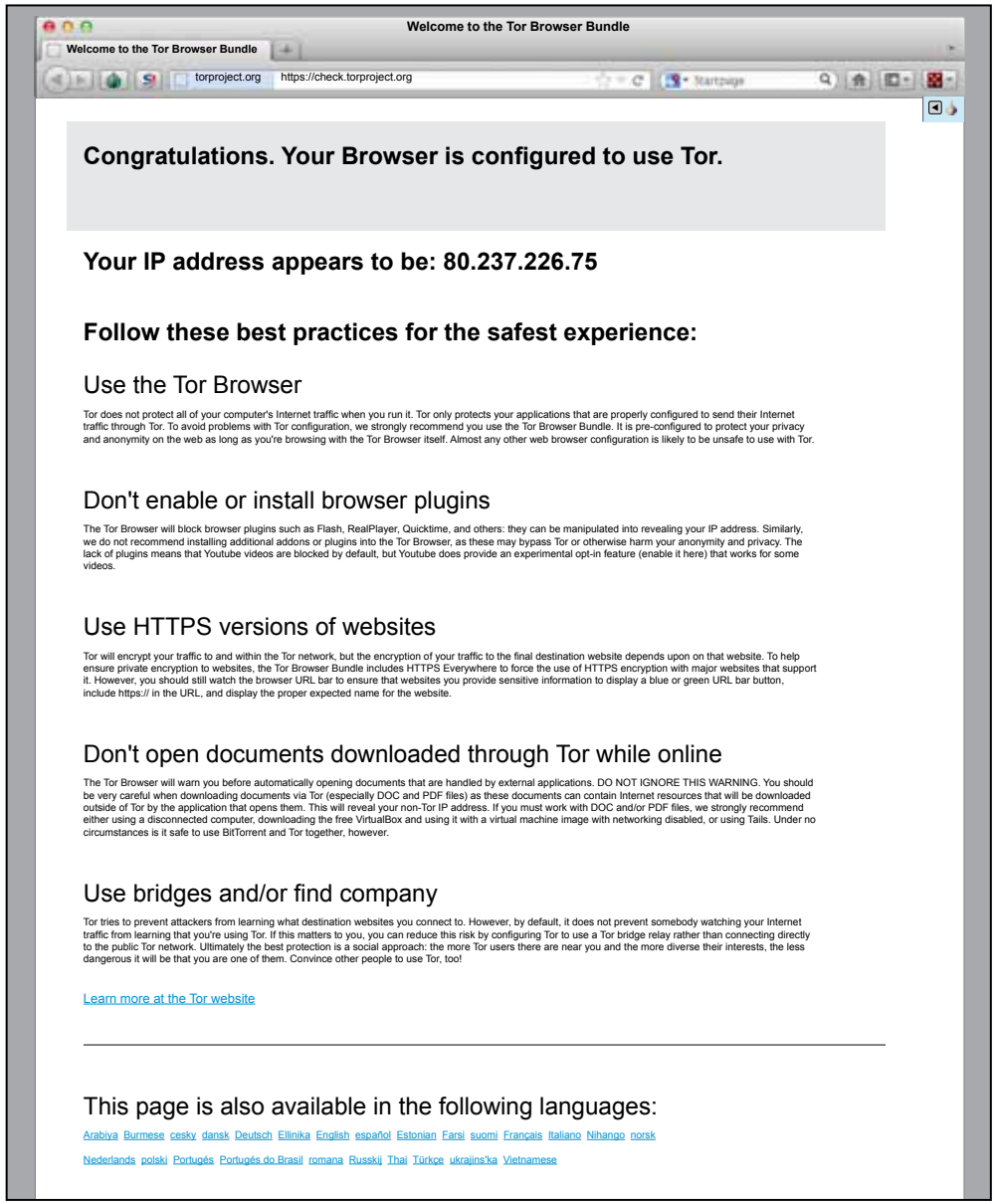
Remove the separate Vidalia application.

Recommendation: Share best practices on the check page

Communicate best practices for browsing safely using Tor on the check page.

At a minimum, link directly to best practices currently provided on torproject.org.

At a maximum, consider redesigning the check page to include best practices.



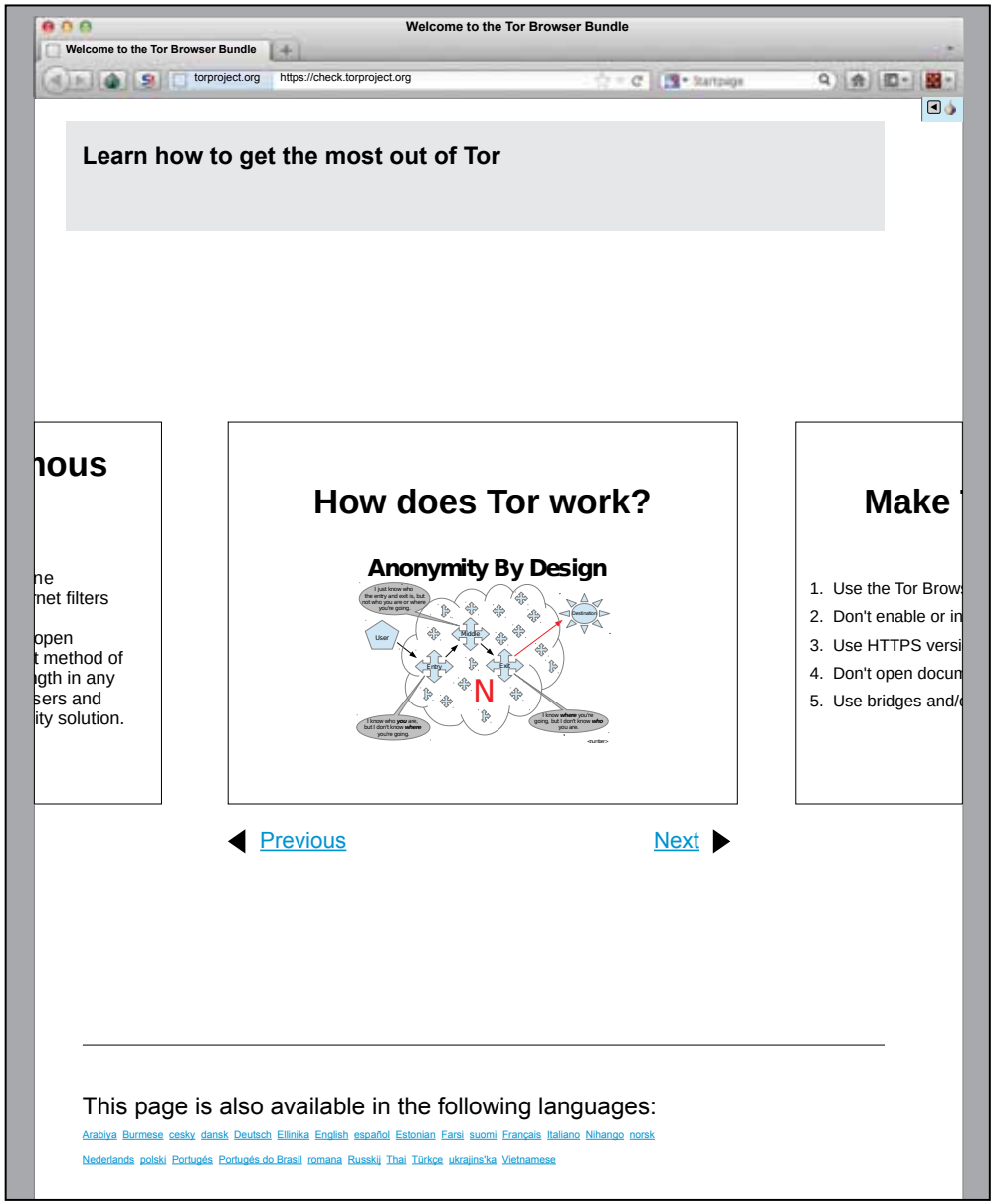
Recommendation: Create an online tutorial

Communicate best practices for using Tor on the check page.

Create an online tutorial with the following goals:

- Show Tor is working
- Show how Tor works
- Learn more
- Get involved

In the example provided, we have created a slideshow to walk users through the steps to take advantage of best practices.



Recommendation: Simplify installation of Tor

Simplify the installation process by creating a Disk Image file for download and installation on OS X.

Disk Images can be set to provide a shortcut to copy the Tor Browser Bundle application to the user's Application folder.

Firefox and many other applications do this today.

Appendix

Secondary Research

Papers Referenced

"Eliminating Stop-Points in the Installation and Use of Anonymity Systems: a Usability Evaluation of the Tor Browser Bundle", Greg Norcie, Kelly Caine, L Jean Camp. Presented at Hot PETS Symposium July 13, 2012, Vigo, Spain.
http://petsymposium.org/2012/papers/hotpets12-1-usability.pdf

"Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability", Jeremy Clark, P.C. van Oorschot, Carlisle Adams. Published in SOUPS '07 Proceedings of the 3rd symposium on Usable Privacy and Security Pages 41-51.
http://dl.acm.org/citation.cfm?id=1280687

Expert Interviews

Participants

Jeremy Clark, University of Ontario
Interviewed October 17, 2012

Peter Fein, Telecomix
Interviewed December 14, 2012

Tomás Touceda, Vidalia developer
Conversed via email February – March 2013

Mike Perry from Tor Project, Kathleen Brade and Mark Smith from Pearl Crescent, Carolyn Anhalt
Interviewed March 27, 2013

Tor Project Redesign

User Interface Specification

Author: Jeff Mau (jeff@jeffmau.com)
Version: 1.0
Modified: 08/26/2012

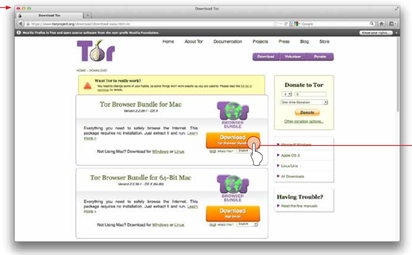
Section: First Time User Experience

First Time User Experience - Current State

First Time User Experience - Current State

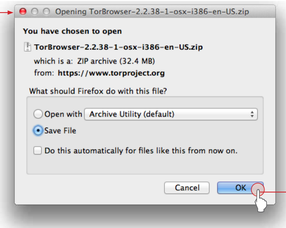
Tor Project Home Page

Tor Browser Bundle for the Mac Download Page

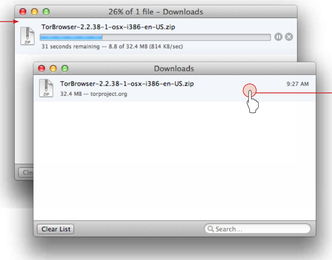


Question: How does the average person know which version to download?

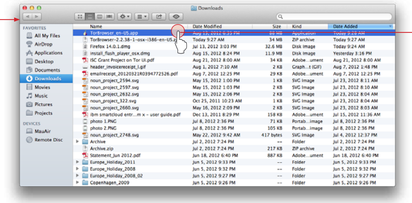
Firefox "Open Download" Dialog Modal



Firefox Download Window

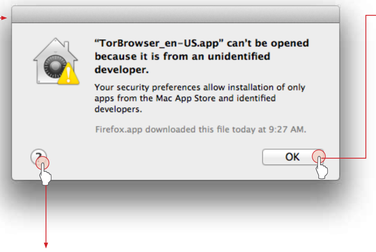


Mac OSX Downloads Folder

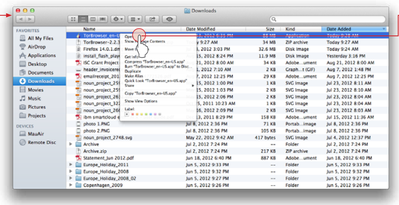


Question: Firefox encourages me to drag the application to my Applications folder? Tor should do this, too. Why not a disk image like all other Mac apps?

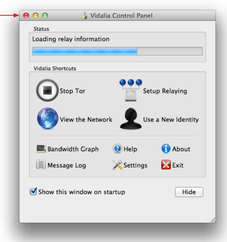
Mac OSX 10.8 Snow Leopard Application Security Warning Modal



Control-click to open application

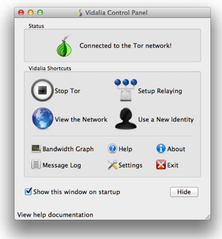


Vidalia Control Panel - Connecting to Tor Network



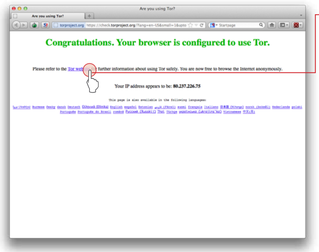
Question: The Status bar runs through a bunch of steps to connect to the Tor network. Why do I care?

Vidalia Control Panel - Connected to Tor Network



Question: What is Vidalia? I thought I was installing Tor.

Tor Browser - Launched upon connecting to Tor Network

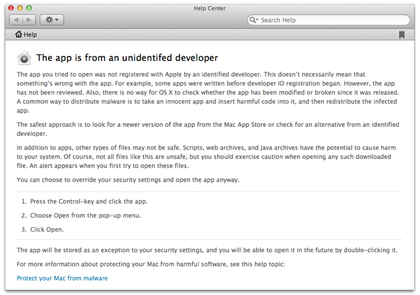


Question:
Now what?
I thought it would work within Firefox
Is all my internet traffic anonymous or just through the Tor Browser?
Why does it show me my IP address here instead of some location in the UI where I can always check to see my IP?
The Tor home page suggests I change my browsing habits. Why not here when I am getting started?
Viewing the network sounds helpful, yet the visualization doesn't really work. I can't see anything. What is the purpose of this view?
Can the UI more clearly articulate how Tor is working?

Tor Project Home Page

Comment: The link to the Tor website gives me the impression I will see explicit Help but it takes me back to the home page where I started.

Mac OSX 10.8 Snow Leopard Application Security Help Documentation



Question: Can we get Tor in the Mac App Store to streamline the OS security permissions and receive updates?
Is there concern about associating a Tor download wth an iTunes account?

Welcome to Anonymous Web Browsing with Tor

1. Tor can help you maintain anonymity online
2. Tor can also assist you in bypassing internet filters

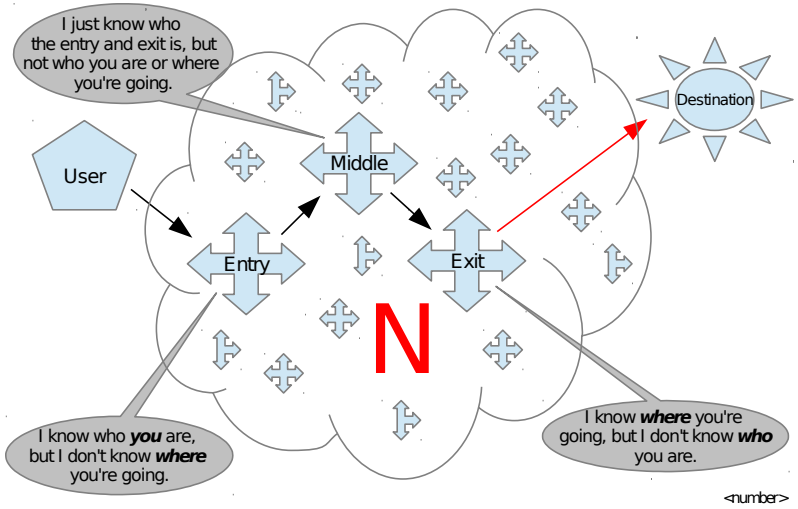
Tor is a public anonymity network based on open source software. It provides the most robust method of maintaining anonymity online. And the strength in any anonymity solution is numbers. The more users and Tor nodes, the stronger Tor is as an anonymity solution.

Anonymity loves crowds.

Online Tutorial (2 of 6)

How does Tor work?

Anonymity By Design



Make Tor Work for You

1. Use the Tor Browser
2. Don't enable or install browser plugins
3. Use HTTPS versions of web sites
4. Don't open documents downloaded through Tor while online
5. Use bridges and/or find company

Help Others Access Tor

Configure a bridge:

Learn More About Tor

- **Tor Project Overview**
  https://www.torproject.org/about/overview
- **Tor Blog**
  https://blog.torproject.org/blog/
- **Tor Documentation**
  https://www.torproject.org/docs/documentation.html.en
- **Tor Project FAQ**
  https://www.torproject.org/docs/faq.html.en
- **Contacting Tor for Support**
  https://www.torproject.org/about/contact.html.en

Help the Tor Project

The Tor Project is run by and for its users. Each and every user can contribute in some way.

https://www.torproject.org/getinvolved/volunteer.html.en

- Run a bridge or a relay
- Answer others' support questions
- Contribute funds
- Tell your friends that anonymity is not suspicious
- Tell the Tor Project what you like about it, and don't like

Thanks!

Jeff Mau
jeff@jeffmau.com

George Rosamond
george@queair.net