Anonymous surfing with Tor and Privoxy

SECRET AGENT

Internet users typically reveal their IP addresses, and this lets companies compile a profile of your Internet activities. Tor and Privoxy can help protect your privacy. **BY KRISTIAN KISSLING**

The epidemic of Internet-based market research continues: many companies routinely investigate their customers' Internet surfing habits – a cheap and transparent form of spying. And in some repressive countries, the government may even be watching where you surf.

Privoxy [1] and Tor [2] puts the spies off your trail. A browser typically talks directly to a remote target, most commonly a website, and the web server that hosts the site logs the corresponding access data. The Tor client prevents your requests from going directly to the target; instead the requests are forwarded via a proxy running on your home machine through a number of nodes to a so-called exit node, which then talks to the target machine (Figure 1). The server version of Tor acts as one of the intermediate nodes in the chain. The name "Tor" is an acronym for *The Onion Router*. Private users will more typically run Tor as a client, commonly known as an the Onion Proxy.

This structure poses one problem: if the data you request passes through various privately operated nodes before reaching your machine, any Onion Router operator could theoretically log your traffic. This is why a secret key is negotiated between your Onion Proxy at home and every node on the path to the exit node. The key prevents unauthorized nodes butting in on the conversation en route.

By encrypting data in multiple layers, only the Onion Proxy on your home machine is capable of accessing the data – this protection system also prevents node operators from decrypting the passing traffic. The result of this scheme is that the data is very much like an onion – covered in multiple skins of encryption. The exit node breaks through the skin and passes the data to the final target, although the exit node has no way of knowing which machine the request originally came from. None of the Onion Routers knows the Onion Proxy, and this means that Onion Router operators have no way of knowing whose data is passing through their nodes.

On the way back from the target, the information is repacked and stays encrypted until the proxy running on your home machine strips the encrypted layers to reveal the data. This makes it impossible for third parties, including the provider, to know what data you request or send; the person running the target machine just gets to see the IP address of

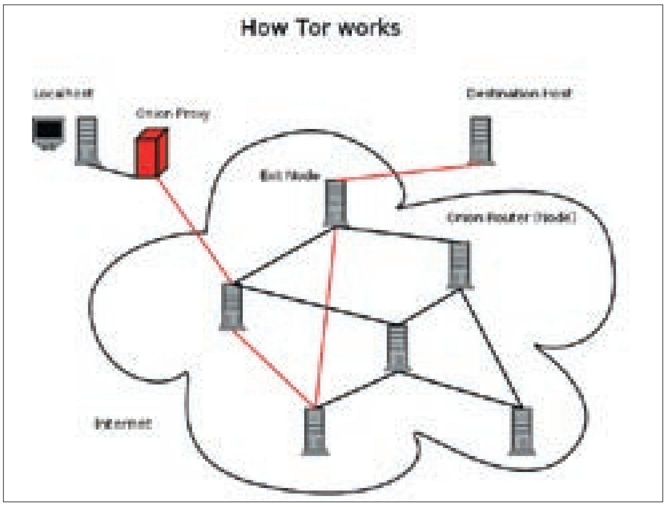


Figure 1: Tor forwards a web request through a series of intermediate nodes to obscure the identity of the user.

the exit node, which could be anywhere in the world.

Installing Tor

Tor is still a fairly young program, as the version number shows; it doesn’t have an interface at this time of writing. Suse users can download the source code for the stable version 0.1.0.16, and start by installing the Automake tools. If you have Suse 9.3 or 10.0, Autoconf and Automake are included. You additionallly need the GCC and GCC-C++ compilers. YaST automatically loads additional required libraries. Don’t forget to install the Openssl-devel, and Zlib-devel header files, along with the Libevent library [3].

Users with Suse 9.3 can't use YaST to install Tor; instead, download the source code from [2] and follow the standard installation steps: *./configure, make,* and *make install*. This should work out fine. Suse 9.3 also needs a new entry in */etc/ld.so.conf* to be able to locate the library. Add the path */usr/lib*, and then (working as root) run *ldconfig* to update your path information.

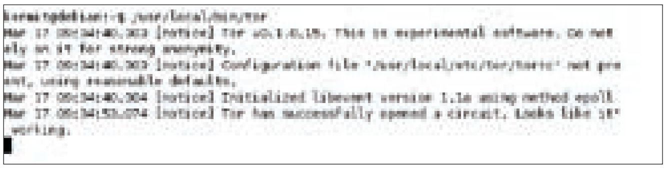
Things are slightly simpler for Debian users; just add the following entries to your */etc/apt/sources.list*:

```
deb http://mirror⏎
.noreply.org/⏎
pub/tor sarge main
deb-src http://⏎
mirror.noreply.org/⏎
pub/tor sarge main
```

Then become root and run *apt-get update* to tell the package manager about the new software residing at the specified address. You can then simply type *apt-get install tor* to install.

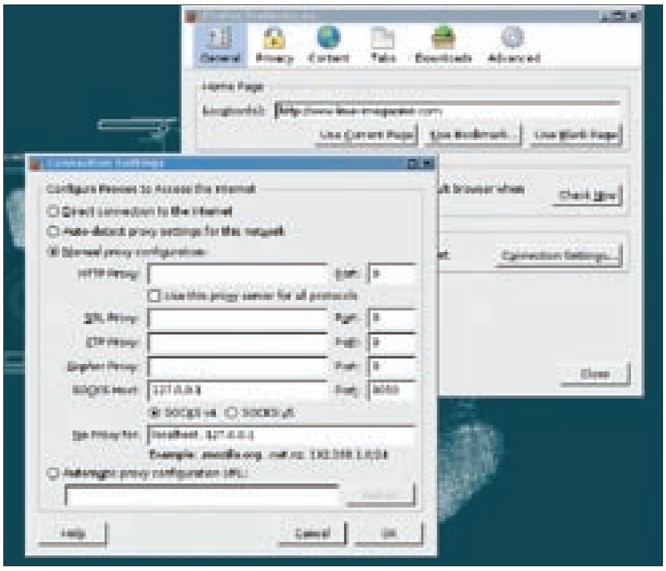
Here We Go...

Let’s give Tor a trial run. Pop up a console window and enter *tor*. After a short while, you should see a terse message that says “*Tor has successfully opened a circuit. Looks like it's working*” (Figure 2). If you are still not



```
kermit@debian:~$ /usr/local/bin/tor
Mar 17 00:34:40.303 [notice] Tor v0.1.0.16. This is experimental software. Do not
ely on it for strong anonymity.
Mar 17 00:34:40.303 [notice] Configuration file '/usr/local/etc/tor/torrc' not pre
sent, using reasonable defaults.
Mar 17 00:34:40.304 [notice] Initialized libevent version 1.1a using method epoll
Mar 17 00:34:53.074 [notice] Tor has successfully opened a circuit. Looks like it'
 working.
█
```

Figure 2: Tor has successfully opened a circuit, and told you about it.



Configure Proxies to Access the Internet
○ Direct connection to the Internet
○ Auto-detect proxy settings for this network
● Manual proxy configuration:
HTTP Proxy: Port: 0
□ Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
Gopher Proxy: Port: 0
SOCKS Host: 127.0.0.1 Port: 9050
● SOCKS v4 ○ SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
○ Automatic proxy configuration URL:

Figure 3: Configuring Tor as the proxy server for your browser.

convinced and want to make very sure, just Google for *my ip*. This takes you to a few pages that not only tell you your computer's IP, but other details like the country you are probably in, your operating system, and the browser you use, or even the web pages you visited recently.

To bamboozle these pages, first tell the browser to route all traffic via the Tor Onion Proxy. If you have Firefox, just go to the *Preferences*, and select *Connection Settings* | *Manual Proxy Configuration*. Enter *127.0.0.1* as your *SOCKS Host*, and *9050* as your *Port* (Figure 3). Now select the *SOCKS v4* entry and finish the configuration: your browser will now route all traffic to port 9050 first, and Tor will forward it onto the Internet. Mozilla users need *Edit* | *Preferences* | *Advanced* | *Proxies* for this.

Now, when you query your IP address, the results should look a lot different from the previous result set: the web server now thinks you live in Germany (Figure 4) – looks like Tor really is working.

If you have Suse, and want to launch Tor automatically when you start your machine, become root and add a line for */usr/local/bin/tor &* to your */etc/rc.d/boot.local* file; on Debian, a file named */etc/rc0.d/K20tor* ensures that Tor will launch automatically whenever you boot your machine. Tor has one problem that most encryption and anonymization programs have in common: encryption tends to slow down communications with remote web servers noticeably.

GLOSSARY

Chroot: *A security measure that maps the root directory for Privoxy to* /var/lib, *thus preventing would-be attackers from accessing directories farther up the filesystem tree.*

Privoxy for Dessert

Tor does not take all the risk out of browsing. As you may be aware, your browser needs to look up the target machine's address by sending a request to a DNS server; the server then resolves the host name (such as *www.linux-magazine.com*) to the IP address (212.227.104.121). The DNS server then sends the resolved IP address back to the browser. If somebody were to check the DNS server's logfiles, they could find out which machine had looked up *www.linux-magazine.com* and when. Privoxy can prevent this from happening by using Socks 4a, which, unlike Socks 4 and Socks 5, does not need to convert hostnames to IP addresses first.

Privoxy is a filtering proxy for HTTP that is often used with Tor. You can read all about using Privoxy as a web filter in the October 2005 issue of Linux Magazine [4].

Installing Privoxy

Users with Suse 9.3 and 10.0 can simply run YaST to install Privoxy. If you have Debian, just type *apt-get install privoxy*. After you complete the install, Suse will launch Privoxy automatically each time you boot your machine; to prevent this from happening, you need to launch YaST, go to the *System* tab, and click the *Runlevel Editor* button. To disable the *Privoxy* service, click *Disable*. Suse Linux runs Privoxy in a **Chroot** jail.

On Debian, Privoxy typically launches automatically after the install; if not, you can launch the client by becoming root and giving the */etc/init.d/privoxy restart* command.

The next step is to tell Privoxy to forward Socks requests to Tor. To forward Socks requests, Suse users need to open */var/lib/privoxy/etc/config* and enter the following line below item *5. FORWARDING*:

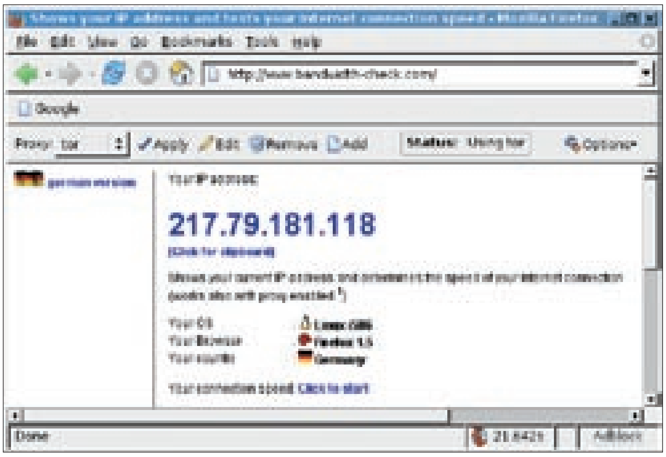
```
forward-socks4a / ↩
127.0.0.1:9050 .
```

Note the dot following the port; if you forget this, no forwarding will take place. You need to modify the same file for Debian, however, in this case the file resides below */etc/privoxy*.

Now update your proxy settings for Firefox and Mozilla to reflect the changes. Enter *127.0.0.1* as the IP address, and *8118* as the port in all cases, and then surf to the website that showed your IP address previously. If your IP address is shown properly, Privoxy is working properly; and if you see the wrong IP address instead of the correct address, Tor is also working.

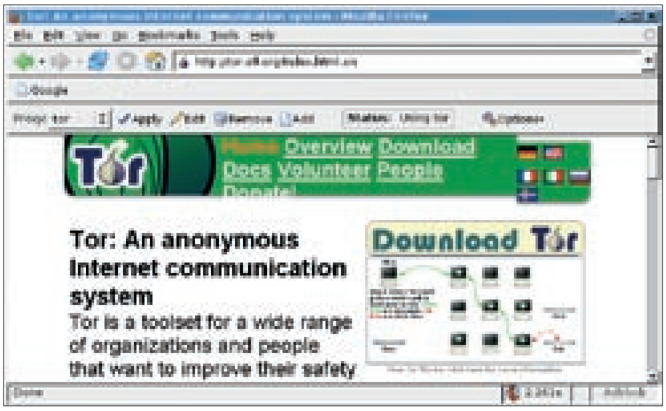
Quick Change

Previously, if you used your browser in mixed mode, that is, anonymously in some cases and open in others, there was no alternative to switching



http://www.bandwidth-check.com/
Proxy: tor
Status: Using tor
Your IP address:
217.79.181.118
Your OS Linux
Your Browser Firefox 1.5
Your country Germany

Figure 4: The website thinks you live in Germany, as the exit node contacting the server is running on a German server.



Tor: An anonymous Internet communication system

Tor is a toolset for a wide range of organizations and people that want to improve their safety

Figure 5: The Firefox "Switch Proxy" extension gives you an easy solution for enabling and disabling a collection of proxies.

the proxy on and off manually. Thank goodness this has changed: there is now an Switch Proxy extension for Mozilla and Firefox, which you can install by double-clicking the *Get more extensions* link in the *Extensions* window [5]. After relaunching the browser, you should have a new status bar for *Switch Proxy* (Figure 5).

To configure Tor and Privoxy as a new proxy, click *Add*, select the *Standard* entry, and then click *Next*. A window appears, letting you configure your new proxy settings. Don't forget to assign a name to these settings, just to be able to identify them later. When you are finished, click *Ok*. Use the list next to the *Proxy* entry to toggle between various proxy configurations.

Becoming a Microsoft Agent

While we are at it, what reason is there for you to tell everyone that you use Linux and prefer the Firefox browser? There isn't a good reason to reveal this information, especially some of the less well-behaved pages then slam the door on Linux users.

The User Agent Switcher [6] extension helps you change this. After you install the switcher and relaunch your browser, select *User Agent Switcher* in the *Tools* menu, and opt for *Internet Explorer 6* (or *Opera 8.5* if you prefer); the User Agent Switcher should now identify you as using Internet Explorer – luckily, this does not mean that you will be installing the usual security problems that come with the real Internet Explorer. ■

INFO

[1] The Privoxy project: *http://www.privoxy.org/*

[2] Tor: *http://tor.eff.org/*

[3] Libevent as Suse-RPM: *http://linux01.gwdg.de/~pbleser/rpm-navigation.php?cat=Libraries/libevent/*

[4] "Doorkeepers: Privoxy and Web-cleaner content filters," by Thomas Leichtenstern; Linux Magazine #59, 2005; p. 54.

[5] The Switch Proxy extension for Firefox and Mozilla: *https://addons.mozilla.org/extensions/moreinfo.php?application=firefox&id=125*

[6] The User Agent Switcher for Mozilla and Firefox: *http://chrispederick.com/work/useragentswitcher/*