Tor and the Tor Browser Bundle

Hints, tips, and tricks for effective use

L V Lammert
St. Louis Unix User's Gropu
Main Meeting

11 December 2013

Outline

- Tor
  - Brief history of Tor
  - Simple architectural overview
  - Installing Tor for client use
  - Overview of the toolset provided by Tor
  - Some practical usage examples
- The Tor Browser Bundle
  - What is TBB?
  - Obtaining and installing
  - Hints, tips, and tricks for effective use
- Sources and Resources

Tor: Brief history

- Originated in 1995; funded by the Office of Naval Research (ONR)
- DARPA funding kicked in around 1997
- Alpha version released “in the wild” late 2002
- EFF financially supported from 2004 to 2005
- DARPA and ONR funding lapsed in 2006
- An anonymous North American NGO and the Broadcasting Board of Governors are currently primary sponsors ($1+ million each)
- Used by Edward Snowden to divulge information about NSA’s PRISM program to the press

Tor: Simple architectural overview

- Client proxy encrypts multiple layers based on chosen path; sends to Entry Node
- Entry Node decrypts its routing layer; forwards to next node
- Node decrypts its routing layer; forwards to next node
- Number of hops varies depending on original client's routing choices
- Exit node decrypts the original packet; sends traffic to original target host *in the clear*
- Effectively the traffic appears to originate from the exit node
- There are caveats:
  - Client-side scripting can be used to reveal the originating host
  - Exit nodes could become compromised; sniffed
  - Compromised nodes can be used to perform timing analysis; determine origin

Tor: Installing for client use

- Do you trust your repos? If so, apt-get yum or zypper it.
- For the paranoid, grab the source tarball and compile it!
  - https://www.torproject.org/download/download.html.en

Tor toolset

- tor
  - Core service
  - Can be configured for all roles (***client***, entry, node, exit)
- torify
  - Wrapper to tor-ify another program
  - Doesn’t work with everything, but worth a try
- tor-resolve
  - DNS resolution via tor
- tor-gencert
  - Used to generate certificates for directory authorities

Tor: Practical usage examples

Demo time!

- torify wget http://ipecho.net/plain
- torify ssh
- torify Firefox
- torify ? (hint: not everything works)

The Tor Browser Bundle

What is it? From the Tor Project Web site:

“The Tor Browser Bundle lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.”

TBB: Obtaining and Installing

https://www.torproject.org/download/download-easy.html.en

Pick your OS and bits, download, and install!

But wait, there’s more. . .

TBB: Obtaining and Installing

Upon first launch, TBB will have scripting ENABLED by default. This is NOT recommended, and should be disabled immediately!

For the uber-paranoid, re-start TBB after disabling scripting to negotiate a different path and exit node.

TBB: Hints, tips, and tricks

- Do disable scripting and restart before “serious” usage.
- Don’t enable scripting unless you are willing to give away your IP, identity, or anything a script may access!
- Lack of scripting may make some sites unusable. Deal with it, or compromise your privacy by enabling scripts for that site.

TBB: Hints, tips, and tricks

Demo Time!

- Installation
- Verify IP change
- Disable Scripting
- Interface tour
- Browse some sites?
- Accessing hidden .onion sites?
- Keep up to date: Download TBB with TBB!

Wrap-up

- Tor is the core software which can be client, entry, node, and exit.
- torify can make many (not all) applications tunnel through Tor.
- Tor Browser Bundle contains “all you need” to browse anonymously.
- Make sure to disable ALL scripting and plugins as these can leak information.
- Utilize “endpoint shifting” to further obfuscate your Tor traffic.

Sources and Resources

Original Presenation from CIALUG, kristau.net: https://docs.google.com/presentation/d/1nxzYhwv4REy5qmuUV_5w97Ehxw5rX0LsDOBzTAtgNx4/edit#slide=id.p

- http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29
- http://en.wikipedia.org/wiki/File:Onion_diagram.svg
- http://www.onion-router.net/History.html
- https://www.torproject.org/about/sponsors.html.en
- http://en.wikipedia.org/wiki/Onion_routing
- https://ssd.eff.org/
- Tor and the NSA: http://goo.gl/KeW44