



Paranoid Browsing

By Aaron Grothe
NEbraskaCERT



Paranoid Browsing

- What is Paranoid Browsing?
- Why should I Paranoid Browse?
- How to be more Paranoid.



What is Paranoid Browsing?

- Paranoid browsing is where you want to make sure that you make it harder for people to connect your browsing to you



Why Should I Paranoid Browse

- You're looking up something medical that you want to make sure doesn't make it to the googleplex
- You're a whistleblower trying to make sure that something is traced back to you
- You want to learn more about tor or tails
- Because you want to and/or Because you can



Historical Paranoid Browsing

- This is how I used to do research
- Had a machine with two removable drives
- Would put drives into both Drives and boot off a cd-rom then DD the master to the use disk
- Shutdown machine remove CD and master drive and then boot and start browsing



Historical Paranoid Browsing (Cont)

- Would use a set of Open Proxies such as Proxies for all to do most of the browsing.
- Rules
- Always use at least two proxies in different countries with different laws and procedures and languages
- Pretty simple to do along the lines of
`http://firstproxy:portnumber/http://secondproxy:portnumber/
http://thirdproxy:portnumber/http://www.sitetoexamine.com`



Historical Paranoid Browsing (Cont)

- Worked pretty well. Harder to find „safe proxies“ nowadays as you never know who is running one
- Has largely been replaced by ToR and VPNs



Paranoid Browsing Today

- Will want to use tor (The Onion Router) and a decent VPN for security
- Technically you can get by with tor and a lot of people do or just a VPN
- A VPN is a service provider that you route your traffic through



What is TOR?

- TOR (The Onion Router) is a system that promotes internet anonymity and resists censorship
- Initial development sponsored by US Naval Research Lab
- Is constantly being evaluated and improved
- You connect to a machine on the tor network and your traffic is routed through the network and leaves from a different machine



3 Systems that use tor

- Whonix – Linux Distro using VirtualBox
- Tails – Live Linux Distro
- Tor Browser Bundle – Available multiple platforms (Mac/Linux/Windows)
- You can also install tor on your local machine and use it that way as well



Whonix

- System of Two VirtualBox Images (Workstation and Gateway)
- Workstation routes ALL traffic through Gateway so theoretically nothing can go out except via TOR



Whonix Pros

- Well segmented into Gateway and Workstation
- Theoretically ALL traffic on the workstation goes through tor on the gateway, allowing tools like IIRC and the like
- VirtualBox is free and cross-platform (Windows/Mac OS X/Linux)



Whonix Cons

- Gateway image has KDE on it so is quite a bit bigger than it needs to be
- Relies upon VirtualBox to make sure no traffic is sent out
- Using Debian Tools may try to set certain things such as Timezone which might lead to info leakage



Whonix Demo

- Lets do a quick demo of Whonix



Tails

- The Amenisiac Incognito Live System
- Live CD/USB image for browsing
- Fedora Based – routes through TOR



Tails Pros

- Easy to use, boot and go
- Celebrity endorsement – Supposedly Richard Snowden's choice of OS

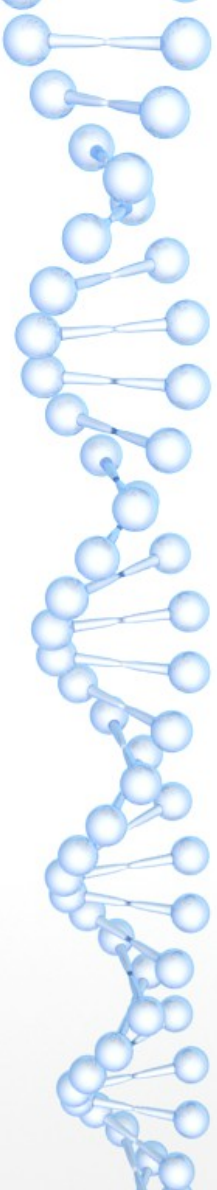


Tails Cons

- Supposedly is being actively looked into by the government
- I2P – Invisible Internet Project part has issues and is actively being investigated. Expect it to be dropped soon from Tails

Tails Demo

- Lets do a Demo of Tails





Tor Browser Bundle

- Software package that combines tor and a browser configured to use it



Tor Browser Pros

- Portable can be put on a USB stick
- Works cross-platform
- Easy to install/use



Tor Browser Cons

- Runs on local machine so possible cross-talk
- Has had some security issues in the past (flash)



Tor Browser Demo

- Lets do a Demo of the Tor Browser Bundle



Tor Drawbacks

- Will slow things down quite a bit
-
- Base Machine DL 39.59 Mbps/UL: 6.43 Mbps
- Whonix: DL 7.23Mbps/UL:5.2Mbps
- Tails Unsafe Browser: DL 19.64/Mbps/UL:6.4Mbps
- Tails Tor Browser: DL:7.91Mbps/UL:4.83Mbps
- Tor Bundle: DL: 6.4Mbps/UL: 2.8Mbps
- Done using speedof.me



Tor Drawbacks (Cont)

- Potential False sense of security
- Still need to use https as much as possible
- Rogue TOR endpoint was used and was able to capture many passwords as people through http over TOR was sufficient
- Potential attacks against tor
- Russia is offering 111k for anybody who can crack tor or weaken it
- Some protocols such as Bittorent's DHT can cause issues



Tor Drawbacks (Cont)

- Sabu of Anonymous was supposedly using tor for all of his traffic. The story is one time he didn't use it for IIRC and then the FBI had him
- Potential mathematical attacks of tor. If a sympathetic group got together and could control $\frac{1}{3}$ of the tor nodes they would be able to do some statistical analysis against it



VPNs

- Finding a good VPN
-
- TorrentFreak.com (2014 which VPNs take your Anonymity Seriously)
- - <http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/3/>



VPNs

- The VPN is your last line of defense. If you something goes wrong with your tor or something else you are counting on these people to not turn over everything they have on you :-)
- Some take great pains to do things like take cash or bitcoins to make it harder to connect a VPN account to you



Most Paranoid Scenario

- Using tails on a machine you paid cash for and don't use anything else
- Go to coffeeshop
- Connect to your VPN
- Use tor to browse Web
- Securely destroy machine when you are done browsing :-)



Couple of Other Cool Things

- <https://github.com/grugq/portal>
- P.O.R.T.A.L Personal Onion Router To Assure Liberty
- Uses a commercial router with alternative firmware to make sure your traffic goes through tor
- Got my router Monday but haven't had a chance to get it setup yet



Couple of Other Cool Things (Cont)

- Open Wireless Movement - <https://openwireless.org/>
- EFF project to create a series of open routers. If you run one you can get the ability to get some plausible deniability possibly
- Currently only supports one router type WNDR 3800, based on DDWRT so it should be possible to port to other routers as well



Couple of Other Cool Things (Cont)

- Onion PI – Raspberry PI plus tor
-
- <https://learn.adafruit.com/onion-pi/overview>
- Creates a tor wifi hotspot – nice for phones/etc.



References

- Historical References
-
- Internet Anonymity for Linux Newbies
- http://www.theregister.co.uk/2002/08/28/internet_anonymity_for_linux_newbies/
-
- Several other in series as well (good classic knowledge)



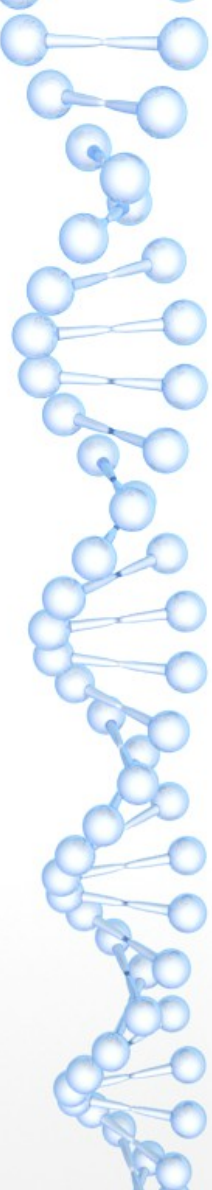
References

- Books
-
- Dagnet Nation by Julia Angwin (Excellent book talking about balance between privacy and convince)
- Little Brother/Homeland by Cory Doctorow – might as well hit Boing Boing and get your „Deep Surveliance“ button checked



References

- Tools Used
-
- Whonix – <https://www.whonix.org>
- Tails – <https://tails.boum.org>
- Tor Browser Bundle – <https://www.torproject.org/projects/torbrowser.html.en>



Other Tools

- Benchmarking Tool
-
- SpeedOf.Me – HTML 5 Network Benchmarking tool / doesn't use flash or java
-
- <http://Speedof.me>