Anonymity Matters

Intro to the Tor Network
Briar and other Tools that exist
Workshop: HowTo Hidden Service
FSFE Gruppe Berlin
26th July 2018
Tobias Diekershoff
Tobias Diekershoff
Berlin, Earth
FLOSS enthusiast and FSFE Supporter
Friendica Developer (Docs / Translations)
Mostly using Tor Browser for random links from contacts, just to add some noise.
Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.
Tor - Overview

Tor – The Onion Routing

- License: BSD 3-clause
- Homepage: https://torproject.org

Some numbers

- Relays: ≈ 6000
- Bridges: ≈ 1000
- Users: ≈ 2,000,000 / day (directly connected clients)
  Relays: USA 18%, UAE 14%, RU 12%, FR 7%, D 5%
  Bridges: RU 15%, IR 10%, USA 6%, IN 5%, VN 5%
- Bandwidth:
  advertised ≈ 275Gbit/s
  consumed ≈ 125Gbit/s
- .onion addresses: ≈ 100,000

Visualization Tor traffic
Source torflow.uncharted.software

data source metrics.torproject.org as of 2018-07-22
Tor - Who is using it?

Everybody
Dingledine said the United States Department of Defense funds are more similar to a research grant than a procurement contract. [...]
Tor - How it Works?

Network Proxy
- To use Tor, you need a proxy to the network
- Usually that listens at TCP 9050

Onion Routing
- developed mid 1990s US Naval Research Laboratories and DARPA
- Step 1: Establish route
- Step 2: Use the route

Hidden Services
- Services (webserver, IRC, XMPP, email ...) that run on servers in the Tor network
- .onion address
Tor - How it Works?
Tor - How it Works?

Clearnet internet-traffic using HTTPS / Credit: EFF (June 2017)
Visiting a clearnet page using Tor and HTTPS / Credit: EFF (June 2017)
Tor - Some Attacks against it

Eavesdropping

Traffic Analysis

Blocking Exit / Entry nodes

Use software / protocols over Tor that leak information

...
Tools - Tor Browser

- Based on the Firefox browser (ESR version)
- Bundled with the TorButton, NoScript and HTTPS Everywhere
- Automatically launches Tor background processes
- Homepage: https://www.torproject.org/projects/torbrowser.html.en
Tools - Operation Systems

GNU/Linux based operation systems aiming to provide a privacy friendly work space.

- Tails https://tails.boum.org/
  The Amnesic Incognito Live System.

- Whonix https://www.whonix.org/
  Whonix is a desktop operating system designed for advanced security and privacy.

- QubesOS https://www.qubes-os.org/
  A reasonably secure operating system.

Image credits — The named projects
Tools - Cellphones

**Orbot**
Network proxy to relay the traffic over the Tor network. (Android)

**Orfox**
Webbrowser using Orbot. (Android)

**orWall**
Force application through Orbot. (Android)

**Briar**
Secure messaging app. (Android)

**Onion Browser**
Webbrowser using the Tor network. (iOS)
Briar - Overview

Resilient P2P Messaging for Everyone

- OS: Android
- Available at F-Droid and Google Play or as APK from the homepage.
- License: GNU GPL v3 or later
- Sources: code.briarproject.org/briar/briar/tree/master
- Homepage: briarproject.org

Image Credits: Briar project
Briar - Features

- Messaging
- Private Groups
- Forums
- Blogs
- RSS Feeds Reader

Briar uses direct, encrypted connections between users to prevent surveillance and censorship.

Image Credits: Briar project
Conversation among two contacts

**Hi Bob!**
1 min ago

Hi Alice, thanks for telling me about Briar!

**Hi Bob!**
1 min ago

No problem, hope you like it 😊

**Alice**
2 mins ago

OK, I’ll start. Computers are terrible!

**No argument there - but how are they terrible?**
Carol 2 mins ago

Well, for a start, they’re terribly dull. They’re also terribly expensive, except the cheap ones, which are terribly made

**I was expecting this forum to be dull, and so far I haven’t been disappointed**
Bob 1 min ago

**Threaded conversation in Forums and Private Groups**

Briar - Features

Briar's main menu
Briar - Making Contact

Method 1: f2f Meetup
- Each scan a QR code from the other person's phone
- Briar establishes the connection via secure ways

Method 2: By a mutual contact
- Users may introduce two of their contacts
- If both agree, contact is established

Ending a Relationship
- If you end a relationship to a contact, they will see you as offline from now on for privacy reasons.

Introduce a new contact when meeting them f2f.

Image Credits: Briar project
Briar - Getting it

Briar can be downloaded via F-Droid, Google Play or directly at https://briarproject.org/download.html

Scan this QR code to add the Briar repository as source to your F-Droid. Open it in F-Droid, when the add new repository screen appears click Add. Once the updating process of the sources is finished you can install Briar.
Hidden Services - HowTo: Overview

Workshop

- Install Debian (stable) in a VM [prepared]
- Install Tor
- Install web2py
- Configure web2py to be used as a hidden service

Why web2py

No particular reason. Just it is easy in the dependencies, runs not on port 80 by default and ships with something to click in the browser.
Hidden Services - HowTo: Debian Installing Tor

- Install apt-transport-https, dirmngr packages
- Add Tor apt sources (here Debian Stretch) — /etc/apt/sources.list.d/tor.list

```
deb https://deb.torproject.org/torproject.org stretch main
deb-src https://deb.torproject.org/torproject.org stretch main
```

- Import gpg key for verification

```
gpg --keyserver keys.gnupg.net --recv A3C4F0F979CAA22CDBA8F512EE8E8BC9E886DDDD89
gpg --export A3C4F0F979CAA22CDBA8F512EE8E8BC9E886DDDD89 | sudo apt-key add -
```

- Install Tor

```
apt update
apt install tor deb.torproject.org-keyring
```
Hidden Services - HowTo: Configuration

- Open `/etc/tor/torrc` with your fav editor
- For the hidden service the config should be something along the lines
  - web2py runs on port 8000 by default, redirect to port 80 to ease access

```_sh	
SOCKSPort 9050
RunAsDaemon 1
ControlPort 9051
CookieAuthentication 1
ExitPolicy reject *:* # no exits allowed
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8000
```
Hidden Services - HowTo: Run it, Use it

- Get current web2px and unzip it
- If the `unzip` package is not installed, install it
- Run it

```
wget https://mdipierro.pythonanywhere.com/examples/static/web2py_src.zip
unzip web2py_src.zip
cd web2py_src
python ./web2py.py
```

- Start Tor

```
service tor start
```

- Look at `/var/lib/tor/hidden_service/hostname` for the `.onion` address
- Open `.onion` address in Tor Browser
Thanks!
Links

- Briar https://briarproject.org
- Briar, 34c3 - Thorsten Grote https://media.ccc.de/v/34c3-8937-briar
- EFF Visualization of HTTPS & Tor https://www.eff.org/pages/tor-and-https
- The Tor Project https://www.torproject.org
- QubesOS https://www.qubes-os.org/
- Tails https://tails.boum.org/
- Tor Detector https://check.torproject.org/
- Tor-Friendly Programs
- Tor instructions for Debian / Ubuntu https://www.torproject.org/docs/debian.html.en
- Whonix https://www.whonix.org/
- Slides https://git.fsfe.org/tobiasd/talks

Image Credit

- *Hacker* by xusenru (CCO)
  https://pixabay.com/de/hacker-kop%C3%BB%C5%A1on-licht-kerl-1725256/
Hidden Services - Links

- The Hidden Wiki
  http://zqktlw4fecnvo6ri.onion/wiki/index.php/Main_Page

- DuckDuckGo (to search the clearnet)
  http://3g2upl4pq6kufc4m.onion/

- not evil (to search the darkweb)
  http://hss3uro2hsxfogfq.onion/

- Aktion Freiheit statt Angst
  http://nnksciarcbrfsg3ud.onion/

- Bits of Debian
  http://4ypuji3wwrg5zoxm.onion/

- Qubes OS
  http://qubesos4rmmmz6n4.onion/

- The NY Times
  https://www.nytimes3xbfgragh.onion