Tor: It can do many things

Iain R. Learmonth

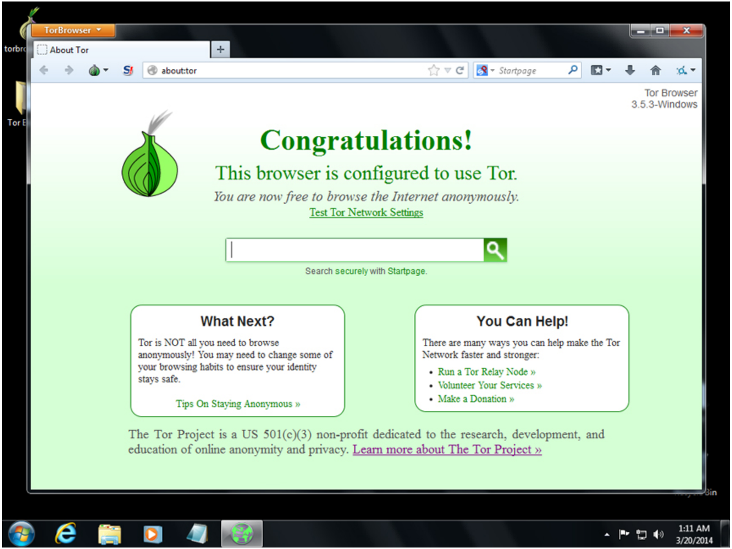
iain@erg.abdn.ac.uk
Electronics Research Group
University of Aberdeen

irl@torproject.org
Tor Project

TechMeetup Aberdeen
June 21, 2017

What is Tor?

- 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.
- Groups such as Indymedia recommend Tor for safeguarding their members' online privacy and security.
- Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online.
- Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers.



Tor Browser
3.5.3-Windows

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Image credit: torproject.org

What is Tor, really?

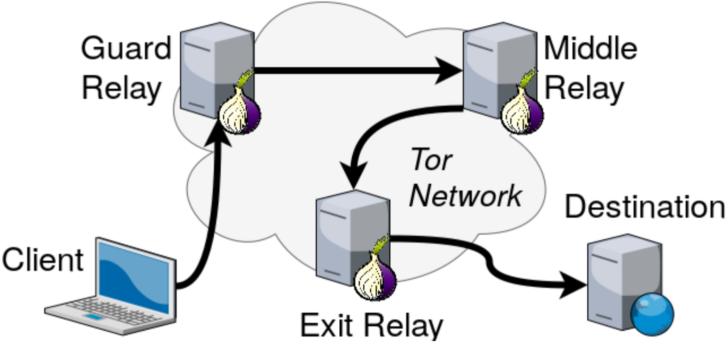
- An Encrypted Low-Latency Anonymising TCP Overlay Network
  - The Tor Protocol Specification[1]
  - The `tor` client software[2]
  - A network of servers: "relays" and "bridges"[3]

[1] https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[2] https://gitweb.torproject.org/tor.git

[3] https://metrics.torproject.org/networksize.html

A Typical Tor Connection Path



Encryption

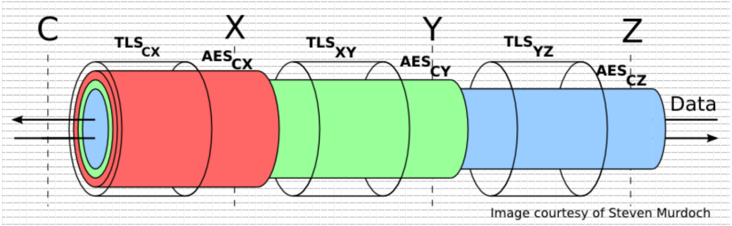


Image courtesy of Steven Murdoch

- There are a few layers of encryption
- TLS between hosts, for a single hop
- Layered encryption between the client and the {guard, middle, exit} relays
- The traffic itself may (hopefully) be using encryption also (to avoid exit relay sniffing attacks)

Bridges and Pluggable Transports

- Pluggable Transport Specification[4]

  "a generic mechanism for the rapid development and deployment of censorship circumvention, based around the idea of modular sub-processes that transform traffic to defeat censors"

[4] https://gitweb.torproject.org/torspec.git/tree/pt-spec.txt

Resilience

- As long as at least one Tor relay or bridge can be reached, the Internet is accessible unfiltered, uncensored and anonymously

Programmable

- Tor puts the clients in control
- Libraries exist for working with Tor
- Stem is a Python controller library for Tor[5]
- txtorcon is a Twisted-based asynchronous implementation for the Tor control protocol[6]

[5] https://stem.torproject.org/

[6] https://github.com/meejah/txtorcon

Exit Selection

- It is possible to define characteristics for your circuits
- This could include only using exit relays in certain countries

```python
import stem.process

tor_process = stem.process.launch_tor_with_config(
  config = {
    'SocksPort': str(SOCKS_PORT),
    'ExitNodes': '{ru}',
  },
  init_msg_handler = print_bootstrap_lines,
)
```

Listing 1: Set additional torrc options

Onion Services

- Onion services use .onion special-use domain name (RFC7686)
- They use a variety of path configurations (between 3 and 6 relays)
- As long as you can connect to Tor, you can host an Onion service
- NAT and firewalls have no relevance here

Ephemeral Onion Services

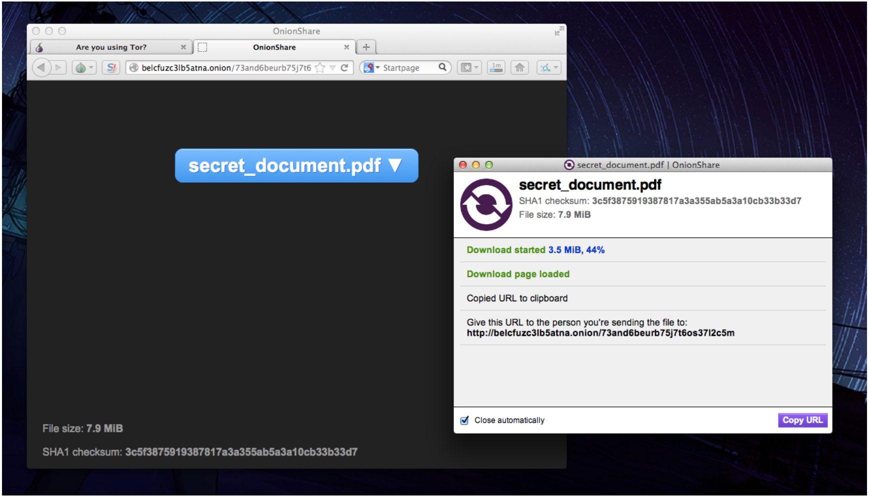
- To create a hidden service required running with the same user as the Tor daemon
- Ephemeral Onion Services can be created by using Tor's control port, removing this limitation

```python
from stem.control import Controller
from flask import Flask
app = Flask(__name__)

@app.route('/')
def index():
  return "<h1>Hi TechMeetup!</h1>"

print(' * Connecting to tor')

with Controller.from_port() as controller:
  controller.authenticate()
  # Create a hidden service where visitors of port 80 get redirected to local
  # port 5000 (this is where Flask runs by default).
  response = controller.create_ephemeral_hidden_service({80: 5000}, await_publication = True)
  print(" * Our service is available at %s.onion, press ctrl+c to quit" % response.service_id)

  try:
    app.run()
  finally:
    print(" * Shutting down our hidden service")
```

Listing 2: Ephemeral Onion Services Example

OnionShare

- OnionShare is an open source tool that lets you securely and anonymously share a file of any size
- It makes use of ephemeral onion services in order to allow for an end-to-end connection between the users


OnionShare
Are you using Tor?
OnionShare
belcfuzc3lb5atna.onion/73and6beurb75j7t6
Startpage
secret_document.pdf | OnionShare
Copy URL

secret_document.pdf ▼

File size: 7.9 MiB

SHA1 checksum: 3c5f3875919387817a3a355ab5a3a10cb33b33d7

secret_document.pdf

SHA1 checksum: 3c5f3875919387817a3a355ab5a3a10cb33b33d7

File size: 7.9 MiB

Download started 3.5 MiB, 44%

Download page loaded

Copied URL to clipboard

Give this URL to the person you're sending the file to:
http://belcfuzc3lb5atna.onion/73and6beurb75j7t6os37l2c5m

☑ Close automatically

Image credit: Micah Lee

Stealth Hidden Services

- HiddenServiceAuthorizeClient
- If configured, the hidden service is accessible for authorized clients only
- “Basic mode”: many keys for the same onion address are published
- “Stealth mode”: the server publish differents onion addresses with each different key

Stealth Hidden Services

- SSH Servers
- Family Calendar
- POP and IMAP Servers
- Weechat Relay
- Internet of ~~Things~~Onions

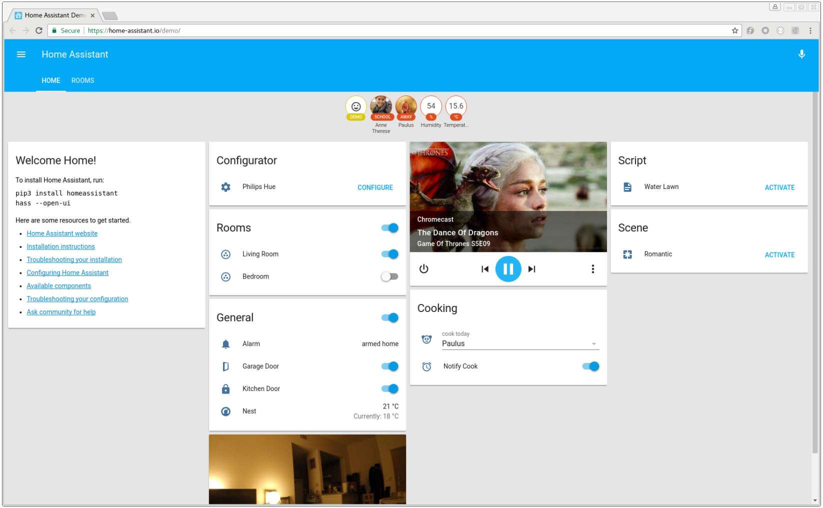
Image credit: User:Colin / Wikimedia Commons

Internet of Onions

- Home Assistant[7] is an open-source home automation platform to monitor, automate, and control various devices without the Cloud
- The backend is developed in Python and is communicating over Websocket with the frontend which is built on Polymer
- In June 2017, over 700 implementations are available including MQTT, MySensors, ZigBee, and Z-Wave
- Use of Home Assistant over Tor has been documented[8]

[7] https://home-assistant.io/

[8] https://home-assistant.io/docs/ecosystem/tor/



Home Assistant Demo

Secure | https://home-assistant.io/demo/

Home Assistant

HOME ROOMS

Welcome Home!

To install Home Assistant, run:

```
pip3 install homeassistant
hass --open-ui
```

Here are some resources to get started.

- Home Assistant website
- Installation instructions
- Troubleshooting your installation
- Configuring Home Assistant
- Available components
- Troubleshooting your configuration
- Ask community for help

Configurator

Philips Hue CONFIGURE

Rooms

Living Room

Bedroom

General

Alarm armed home

Garage Door

Kitchen Door

Nest 21 °C Currently: 18 °C

Chromecast

The Dance Of Dragons

Game Of Thrones S5E09

Cooking

cook today: Paulus

Notify Cook

Script

Water Lawn ACTIVATE

Scene

Romantic ACTIVATE

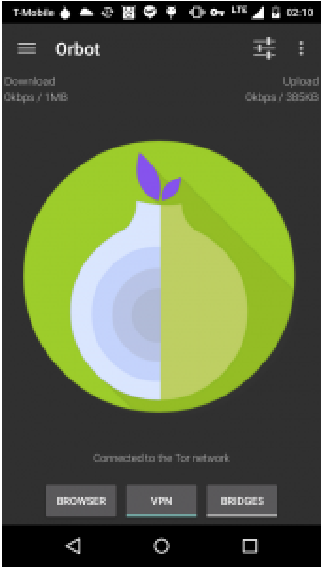
Image credit: User:Fabian.a / Wikimedia Commons

Mobile Apps

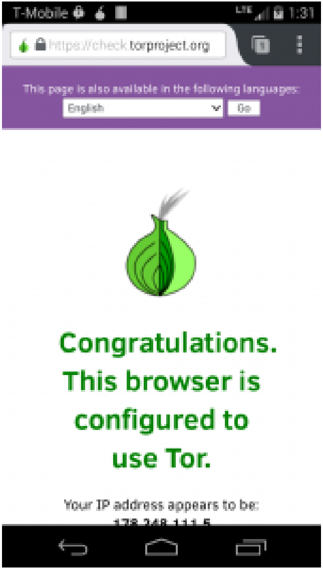
- Orbot[9] is a Tor client for Android
- Orfox[10] is a Tor Browser for Android

[9] https://guardianproject.info/apps/orbot/

[10] https://guardianproject.info/apps/orfox/



Connected to the Tor network



This page is also available in the following languages:

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 178.248.111.5

Image credit: guardianproject.info

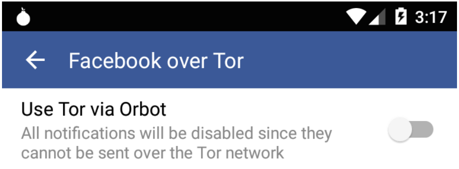
Integrate Tor into Your App

- NetCipher[11] is a library for Android that provides multiple means to improve network security in mobile applications
- It provides best practices TLS settings using the standard Android HTTP methods, HttpURLConnection and Apache HTTP Client
- It provides simple Tor integration, makes it easy to configure proxies for HTTP connections and ‘WebView‘ instances

[11] https://guardianproject.info/code/netcipher/

Facebook Tor Integration

- Facebook provides an Onion service at facebookcorewwwi.onion
- In April 2016 it had been used by over 1 million people monthly, up from 525,000 in 2015[12]
- Facebook added support for Orbot integration to their Android app



3:17

Facebook over Tor

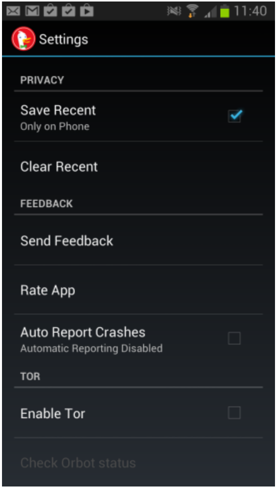
Use Tor via Orbot

All notifications will be disabled since they cannot be sent over the Tor network

Image credit: Facebook

[12] https://www.inverse.com/article/14672-facebook-s-dark-web-onion-site-reaches-1-million-monthly-tor-users

DuckDuckGo Tor Integration



PRIVACY

Save Recent ☑
Only on Phone

Clear Recent

FEEDBACK

Send Feedback

Rate App

Auto Report Crashes ☐
Automatic Reporting Disabled

TOR

Enable Tor ☐

Check Orbot status

Image credit: ghacks.net

There's even more...

- Globaleaks
  https://www.globaleaks.org/
- Magic Wormhole
  https://github.com/warner/magic-wormhole
- Open Observatory of Network Interference
  https://ooni.torproject.org/
- The Amnesic Incognito Live System
  https://tails.boum.org/
- Whonix
  https://www.whonix.org/

Thank you

GPG: A8F7 BA50 41E1 3333 9CBA 1696 **76D5 8093 F540 ABCD**

Slides available at:

`https://people.torproject.org/~irl/2017-06-techmeetup.pdf`