

TOR

How to be anonymous on Internet...

Marjorie DI BIN

M2CCI

2018 / 2019

English teacher : Virginia Gardner

Overview

- 🌀 What does it mean ?
- 🌀 Motivations of being anonymous
- 🌀 How to be anonymous ? ...with TOR
- 🌀 Effectiveness ?

What does it mean ?

- by default → we are “visible” on Internet



Your data



Who you are



What you buy



What you do

your opinions

- Anonymous → protect your identity and your data

Why ? motivations of being anonymous

- **to outsmart the authorities (dissidents)**
- **to prevent large companies from collecting a lot of personal data**
- **to protect my work or my sources (journalists, activist, alert launcher)**
- **to protect my data from the hackers**

Unfortunately some people want to be anonymous
to do illegal things
(terrorism, pedophilia, weapons or drugs sell, etc.).

How to do that ?

1. Internet - Darknet


Internet

Set of interconnected global networks providing the ability of :

- going on the web
- communicating : electronic mail, chat, etc.
- transferring data

Darknet

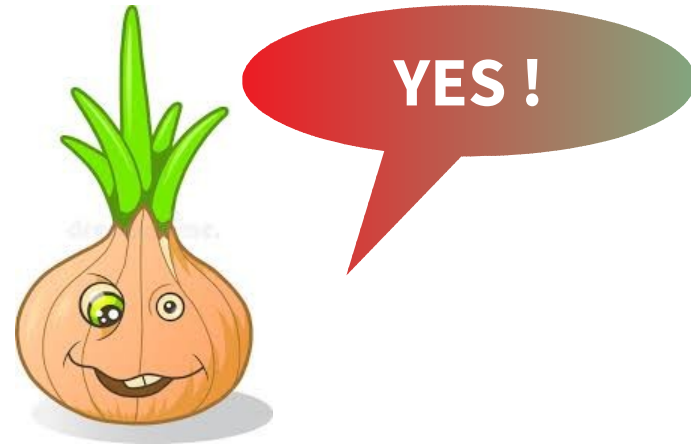
Several Darknets

- virtual, it is just a parallel network of Internet
- one of the most popular is called *Onion*
- to enter this one we have to use the software 

How to do that ?

2. with TOR

TOR The **O**nion **R**outer
“**You said Onion ?**”



History

- Was created by the American navy in the 90s
- since 2006 TOR is maintained by The Tor Project (<https://www.torproject.org/>)
- diversity of funding sources : universities, Firefox, American governmental agencies

How does Tor work?

1. Encrypted data

A story of layers...like onions !

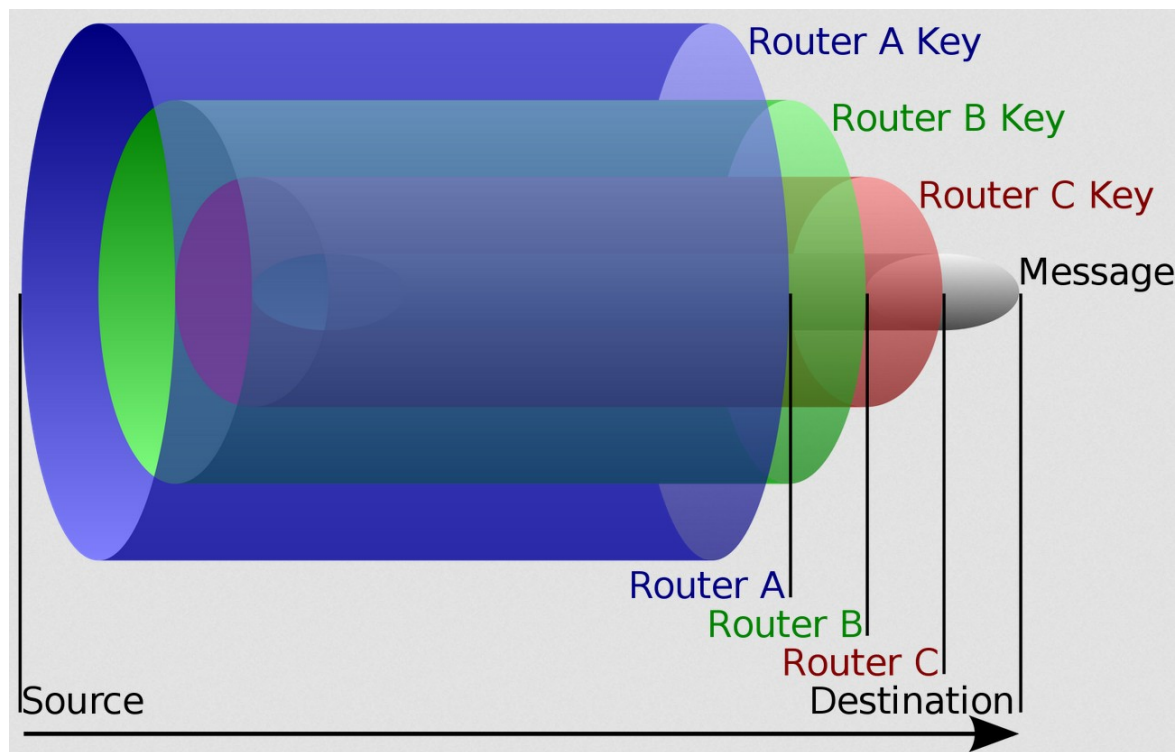
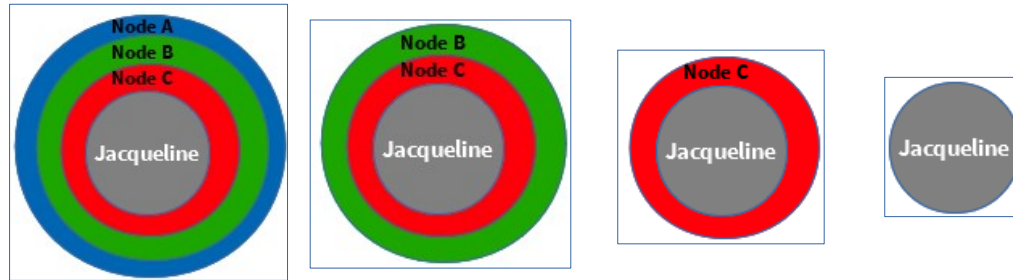


Diagram of the "Onion Routing" Principle.
English Wikipedia user HANtwister

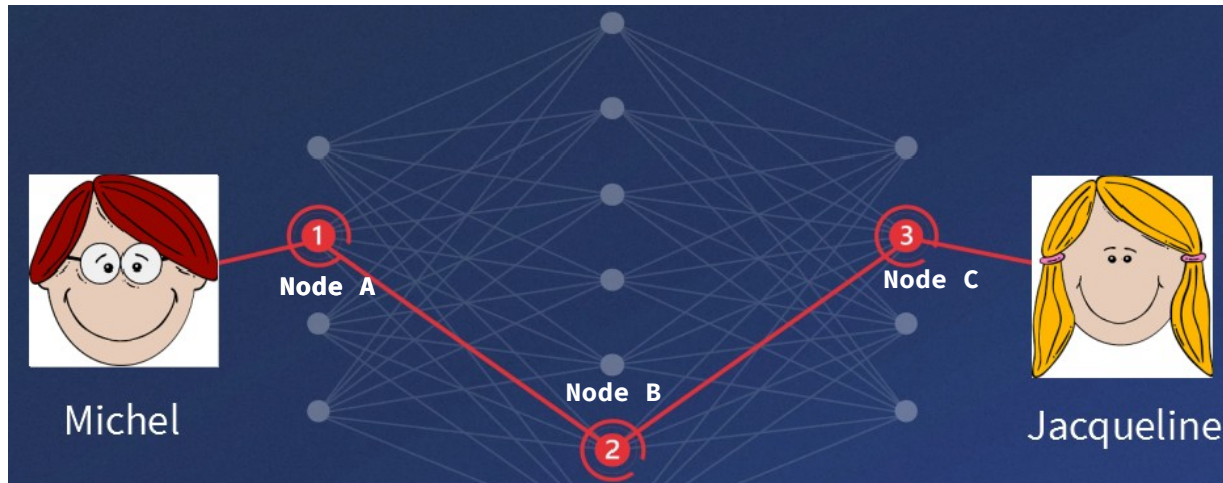
- at least 3 **nodes** = voluntary users computer
- A node/Router => provides its specif encryption key
- encrypted data are bouncing around the world

How does Tor work?

2. Through Tor nodes



The exit node
No more encryption
Be careful !
if it's a malicious
node, it can exploit
data (passwords,
nickname..) or
manipulate data
before sending them
back to Michel !



TOR : the dark WEB | Monsieur Bidouille

	Michel	Node A	Node B	Node C	Jacqueline	data
Node A						
Node B						
Node C						
Michel						

Spreadsheet “who knows what about communication”

Legend:

: known informations

To conclude

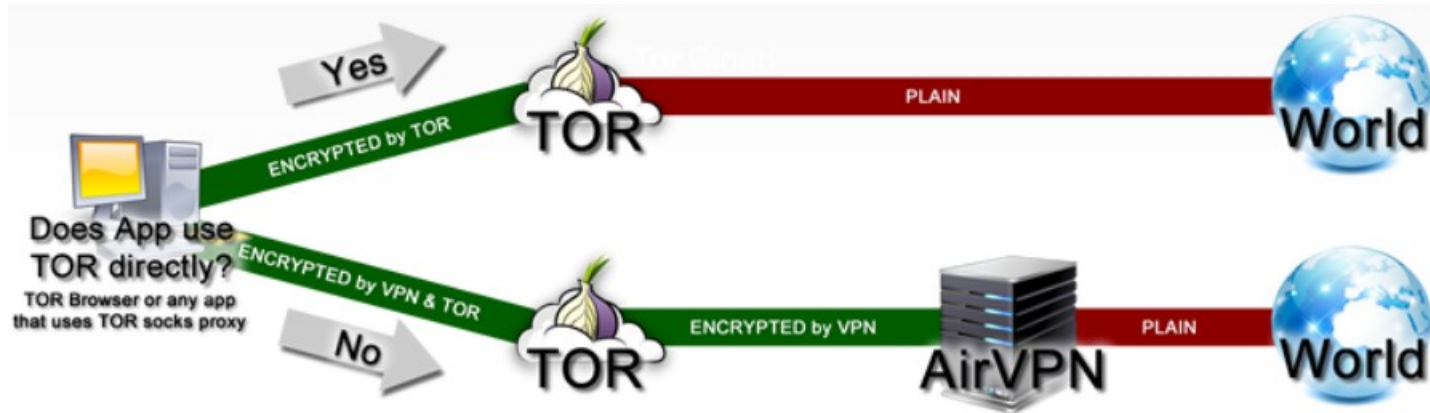
- Tor is described like a very good **privacy tool** out there.
Nevertheless, a number of **good practices need to be adopted** to be truly secured: Use only sites in HTTPS, or other encrypted services, use anonymous email addresses, pay in bitcoins, activate noScript on your browser, etc. Otherwise TOR is useless !
- **Negative points:**
 - ✓ navigation using this software is slow
 - ✓ some web services reject Tor users for policy reasons
 - ✓ Like all system, weaknesses have been already discovered but...
- Tor **is updated** to fix issues and deliver a new range of applications (examples: whistle-blowing platforms, untraceable messaging, etc.)

About effectiveness: another (best?) solution could be...

VPN with Tor (with AirVPN)

- combining the use of both helps make it harder for anyone online to identify you -

<https://airvpn.org/tor/>



Advantages: consolidates some main weaknesses of TOR

- Additional privacy layer: our VPN server will not see your real IP address but the IP of the Tor exit node
- Option to connect to web sites which refuse Tor connections
- Protection from Malicious at TOR exit nodes. All traffic is encrypted by the VPN client software before entering into TOR network, So browsing http websites can not be monitored on exit node.

Questions

Thank you!

