Topic 6 - Anonymization and Privacy

Eric Casanovas

Universitat d'Andorra

4th May, 2022

1 Introduction

2 Tor

Introduction I

Introduction II

- Privacy VS Anonymity VS Security
- Privacy refers to the use and governance of personal data
- Anonymity describes situations where the acting person's identity is unknown
- Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit

Privacy

- Privacy is important when you want to keep certain data and information about yourself exclusive to you and control who and what has access to it
- This is important when using apps or services that need your personal information
- An example can be bank services or social networks
- Privacy is an human right recognized in 1948 by the UN
- Privacy can be achieved using VPNs (not 100%)

Anonymity

- Anonymity is important when nobody knows who you are
- This is important to avoid censorship
- An example can be when you want to access (for example) webpages but you don't want that nobody knows that this is you ANonymity can be achieved using Tor (not 100%)

Privacy Anonymity Security

- Do you think that they are important? When? Why? All at the same time?

1 Introduction

2 Tor

What is Tor

- Tor stands for The Onion Router
- Is free and open-source software for enabling anonymous communication
- Released in 2002
- In 2006 was created the Tor Project, a non-profit organization to maintain Tor's development
- Tries to help its users achieve anonymity
- According to Tor Metrics there are more than 9k nodes

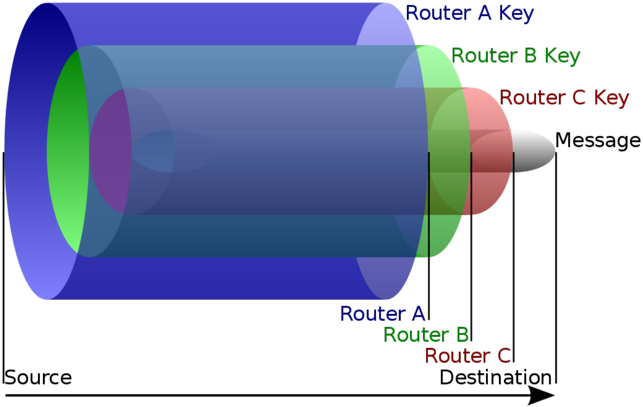
How Tor works I

- Tor uses the concept of the ‘Onion Routing’ method
- User’s data is first encrypted and then transferred through different relays present in the Tor network
- Creates multi-layered encryption and a hard-to-follow path to keep the identity of the user safe
- On each node, one encryption layer is decrypted
- In total, tor routing protocol uses 3 nodes:
  - Entry Guard
  - Middle Relay
  - Exit Relay

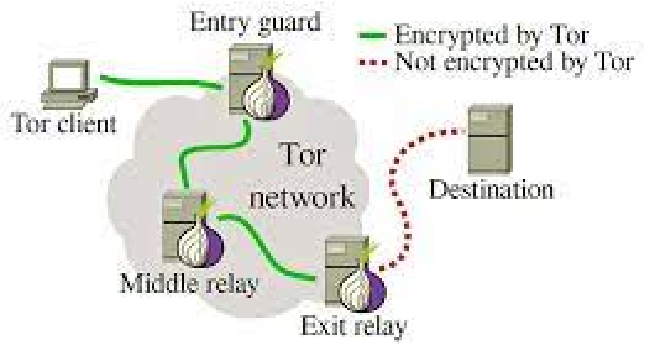
How Tor works II

- The **Entry Guard** knows the source and the middle relay, but not the destination
- The **Middle Relay** knows the Entry Guard and the Exit Relay, but not the source nor the destination
- The **Exit Relay** knows the Middle Relay and the destination, but not the source
- The **Destination** knows the Exit Relay but not the source (anonymity achieved)

How Tor works III



How Tor works IV



How Tor works V

- Tor protocol specification:
- https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

Pros

- Using Tor correctly the source IP address cannot be determined by the destination
- Can access websites without your internet service provider being aware of your browsing history
- Can bypass many kinds of censorship

Cons

- Very slow compared to VPNs and regular web browsing
- Possible to deanonymize by making a simple mistake
- Tor is legal, however using Tor may make your activity appear suspicious
- Some governments and network operators can prevent Tor from functioning
- Websites may refuse to function when you're using Tor, because tor relays are public

Alternatives

Tor is the most used tool, for this reason is the network that provides more anonymity (more users, more anonymous). But some alternatives are:

- I2P
- Freenet

Attacks to Tor

- Blocking: as nodes are public you can block connections
- AS eavesdropping: listening exit, guard nodes or both to deanonymize users
- Fingerprinting: clicks on a website, mouse fingerprint

How can we use tor I

How can we use tor II

Orbot:
Tor for Android
Anonymity Online
Download Tor

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

How can we use tor III

The END!