**Tor Directory Authorities and Relays**

There are 10 authorised DAs for Tor who constantly updated in validate the relays being used in the network and their capabilities

* This list is called the consensus
* The choose what relays are valid and when

Not centralised, so remember that there is a chance that an adversary could own a relay

Relay #1 is the guard relay

* Can see real ip address
* Forwards traffic to middle relay
* Can read traffic (ip) from client to middle relay

Relay #2

* Can see ip of guard and exit relay
* Forwards traffic to exit node
* Decrypts traffic from guard, re-encrypts traffic to exit
* Prevents guard and exit nodes form knowing each other

Relay #3

* Exit node is exit point at edge of Tor network
* Forwards data originally sent from client to its dst
* Can see data sent as it has to decrypt and forward it
  + If sensitive data is passed over unencrypted, then the exit nodes can sniff and inject malicious code

**Bridges**

Because all relays are published in the consensus, it would be very easy for an authority to block you from using Tor by blocking all the relays

* A bridge is an unpublished node that you would use to get around blocking or showing that you’re using Tor

Using a bridge doesn’t really hide the fact that you’re using Tor though to a well-versed adversary, monitoring the traffic can show that you’re using a Tor bridge

* Tunnelling to Tor through SSH or VPN or something else is recommended

**Pluggable Transports**

DPI can uncover that you are using Tor, would be Tors number one enemy

Even using a bridge won’t hide this because the bridge will have the same behaviours as other nodes

Pluggable transports transform the Tor traffic flow into something else so that when network analysis is performed, Tor traffic doesn’t seem to show up

Hex dumps of the client server hello to guard node is different from your typical client server hello which is why it can be distinguished when doing dpi or network analysis

**Torcc File**

Making changes in the Tor GUI will actually make changes to the Torcc file

Torcc-defaults contains default settings for Tor – not meant to be edited