Tor Bridge Exposure and Defense

Keeping our privacy on the Internet is more critical than ever given the pervasive surveillance we are all under that was exposed by Edward Snowden, and others. Tor is a privacy and anonymity tool that helps guard against this mass surveillance. It is used by more than two million users and has thousands of relays around the globe. However, access to Tor can be blocked by denying connections to the public IP addresses of its relays. To combat this, “bridge” relays are introduced. The IP addresses of these bridge relays are not public but distributed through various mechanisms designed at making the job of blocking all bridge IP addresses difficult.

Unfortunately, there are currently many ways that bridge relays can still be enumerated and effectively blocked. While, there have been proposed designs to cover some of these gaps, critical analysis is still lacking.

The aim of this thesis will be to explore the extent of the exposure Tor bridges are susceptible to, critically analyze some of the proposed defenses, and (ideally) implement and empirically evaluate a defense.

For further background, you might find this an interesting read. [https://blog.torproject.org/blog/research-problems-ten-ways-discover-tor-bridges](https://blog.torproject.org/blog/research-problems-ten-ways-discover-tor-bridges)

Practicalities

Promoter: Claudia Diaz
Daily supervisor: Tariq Elahi [tariq.elahi@esat.kuleuven.be](mailto:tariq.elahi@esat.kuleuven.be) office B01.29
Nature of the work: 20% literature, 50% theoretical work, 30% software
Number of students: 1 or 2