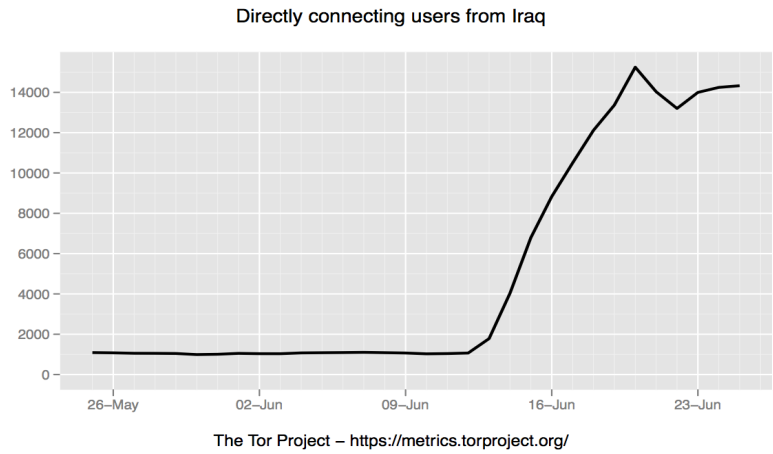
Tor handout.

About.

Tor (The Onion Router) is an open source software project that makes it possible to use the internet anonymously. Tor has an estimated 2.000.000 users.

Usage of Tor can be highly correlated with political events in a country. For example, the graph to the right shows the number of directly connecting Tor users when fighters from the Islamic State of Iraq and Syria (ISIS) took over a large part of north eastern Iraq around the tenth of June, 2014. Similar graphs exist for events in other countries.

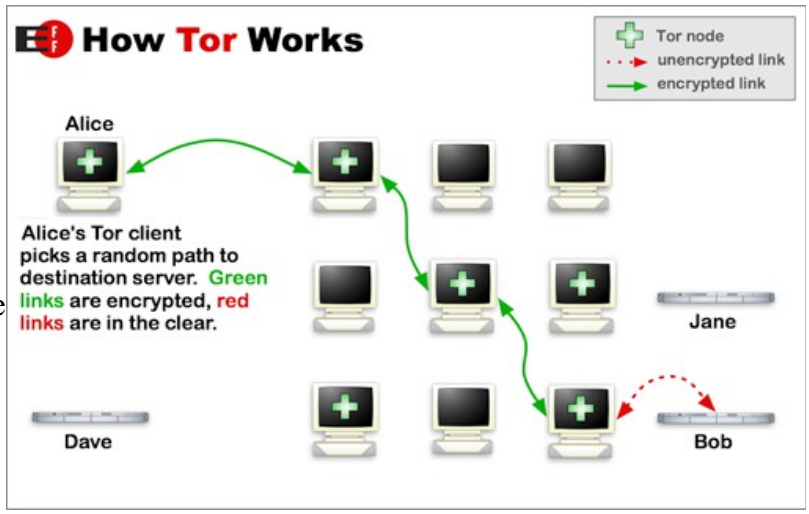


But Tor is not only used in the most oppressive countries. Tor can be used for sharing 'sensitive' content, like information about gay rights in Uganda, or whistleblowing in the UK. Many western journalists (e.g. Glenn Greenwald), activist and regular people use Tor on a daily basis.

How Tor works.

The Tor network consists of many Tor nodes. Client software (a component that we call Alice) can route internet traffic (like webbrowsing or emailing) through a circuit in the Tor network. These Tor circuits are connections through three Tor nodes and expire withing 10 minutes.

The following four steps give a high level overview of how a Tor circuit is constructed:



1 Alice learns about all available Tor nodes and selects three at random.

2 Alice connects to the first node she selected. The node generates a temporary (ephemeral) public-private key pair that it signs with its permanent key. The new public key is used to exchange a symmetric key.

3 Alice can now tunnel traffic through node1 to her second node, and again agree upon an ephemeral key.

4 Alice tunnels traffic through node1 and node2 to the third node and again exchanges ephemeral keys. Now she is ready to 'exit' the Tor network through the third node, and anonymously talk to Bob.

When Alice sends a message to Bob she encrypts the message with three layers of encryption using the three ephemeral keys that she agreed upon with the nodes. Each node decrypts ('peals of') one layer of encryption before forwarding the message to the next recipient. None of the nodes know who is talking to whom, and Bob also does not need to know who or where Alice is.

Circuits exist only for 10 minutes, after which the ephemeral keys are destroyed. Even if the Tor traffic has been recorded the content cannot be recovered by seizure of keys.

Tor hidden services.

The basic three hop circuit described above gives anonymity and location privacy to Alice when she initiates contact with Bob. However, Bob does not get location privacy. Bob might want to have location privacy if his service is sensitive. In addition, Bob might want to hide how popular he is or when he is active or inactive. For this purpose there are so called Tor hidden services. These are reachable only through the Tor network and extremely difficult to locate. The address of a Tor hidden service is a cryptographic hash of the public key of the service. E.g. The Pirate Bay is reachable as a hidden service on the following address: http://uj3wazyk5u4hnvtk.onion (reachable only using Tor). Because a public key is associated with each address, highjacking (acting as) a .onion address is more difficult than highjacking a .com address.

Attacks.

There exist two main attacks against Tor users.

The first is a correlation attack whereby an attacker watches an entrance and an exit node and observes the size and timing of the data-flows. From this the attacker might conclude that the entrance and exit are used in the same circuit and find out who Alice is reaching through the Tor network. This correlation can be made more likely to succeed through a number of different attacks.

The second attack is to censor access to Tor by blocking all the public nodes, or inspecting internet traffic and blocking traffic that is identifiable as Tor traffic. This is prevented using a concept called 'bridges', which are private nodes (as opposed to regular publicly known nodes). These private nodes bridge censored users to the regular Tor network. The traffic they produce is designed to not look like typical Tor traffic.

[1] https://torproject.org/