# Tor: Anonymous Internet communication

Steven J. Murdoch

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

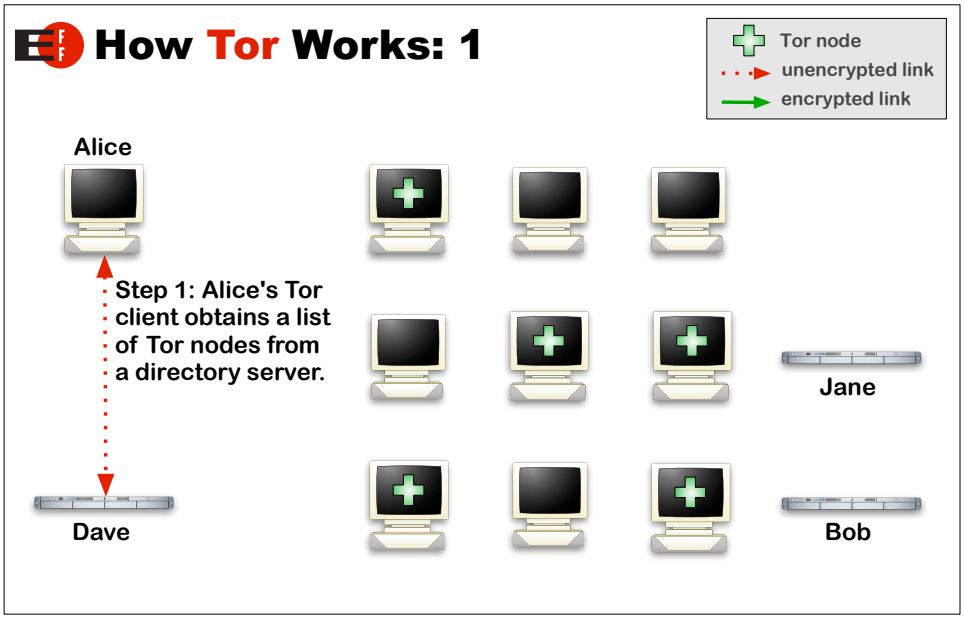
Encryption, as sometimes used with web browsing (SSL) and email (e.g. PGP), only hides message content, and not the traffic data: source, destination, size and timing. Traffic analysis is the study of such data to discover the behaviour and interests of groups and individuals. It is widely used to track people, for marketing, law-enforcement and by criminals. Anonymity systems protect the privacy of Internet users from traffic analysis.

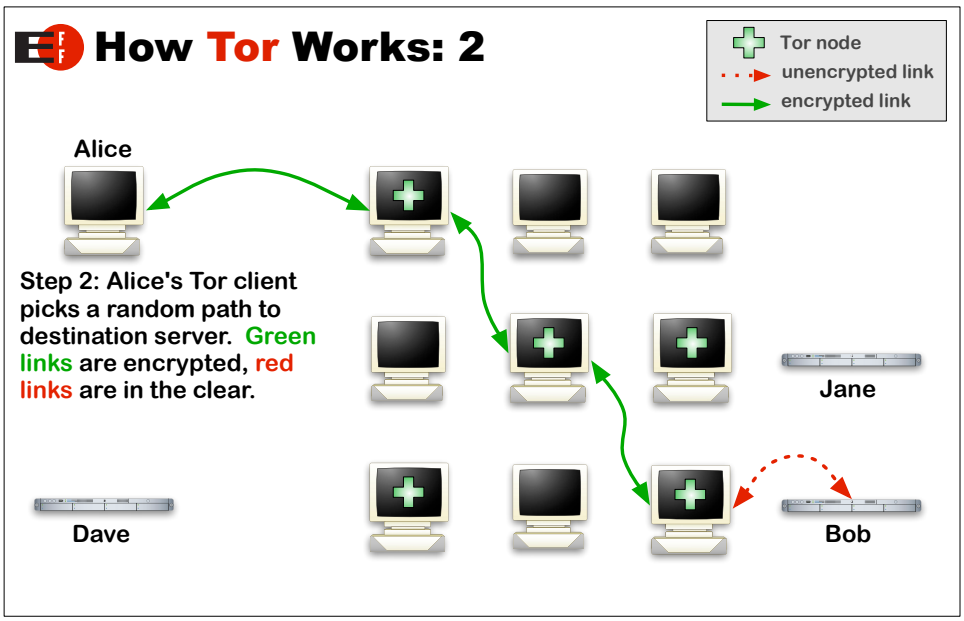
A wide variety of people require anonymity online. Survivors of abuse and rape, as well as those suffering from illnesses might want to participate in information sharing and support groups, without their employer or Internet Service Provider (ISP) finding out. Journalists can use anonymity systems to protect their informants, such as dissidents or whistle-blowers. Law enforcement organisations can use it to hide their surveillance patterns and avoid tipping off their targets. There are many more examples and this diversity is essential for anonymity, as each person hides within the crowd of other users.

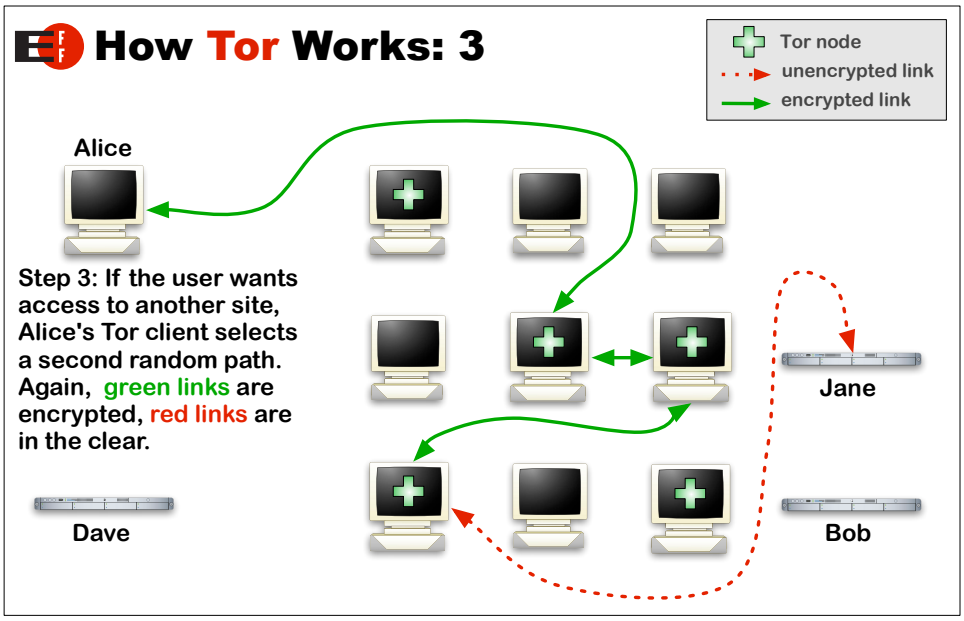
Tor is primarily used for anonymous web browsing, is estimated to have 200 000 users and is built from a network of around 500 servers run by volunteers. Messages are encrypted then sent through a randomly chosen path of 3 servers, and the traces they leave are erased. This makes it difficult for an attacker to follow a message from source to destination or vice-versa.

Tor's main weakness is that, unlike email anonymity systems, it does not delay messages. Attackers can use timing correlations to trace connections. This class of attacks and how to defend against them is the subject of ongoing research.

For more information see:
`http://tor.eff.org/`




Diagrams by Ren Bucholz, EFF

2006-07-06