Anonymous Communications and Censorship Resistance
Using Tor to defeat Internet surveillance

Steven J. Murdoch

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Abstract

When you use the Internet, you are being tracked. The websites which you visit know who you are; marketers track your behaviour and your preferences. Even criminals exploit the traces people leave online. Anonymous communication systems help defeat such monitoring. One such system, Tor, is used by over 500,000 people daily including law enforcement, human rights workers, military personnel, and ordinary citizens worldwide. While originally designed for enhancing privacy and safety, Tor is increasingly used for allowing its users to circumvent censorship, and access commonly blocked websites including social networking, reference and news. Anonymous communication systems introduce some unique challenges, but many of the problems faced by the Tor network mirror those which are found on the wider Internet. For this reason, the study of Tor and similar systems will be informative in general, and allow the testing of hypotheses which would be difficult to evaluate on larger systems.

What is Tor?

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, such as Tor, protect the privacy of Internet users from traffic analysis.

Tor is primarily used for anonymous web browsing, and is built from a network of around 1,500 servers (nodes) run by volunteers throughout the world. 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 between source and destination.

In addition to anonymity, Tor is used to circumvent national censorship systems. By hiding what websites a user is accessing, Tor makes it more difficult for countries to block access to certain websites. To make it difficult to block access to the Tor network, some Tor nodes (the "bridges") are not listed publicly, but their addresses are given out gradually.

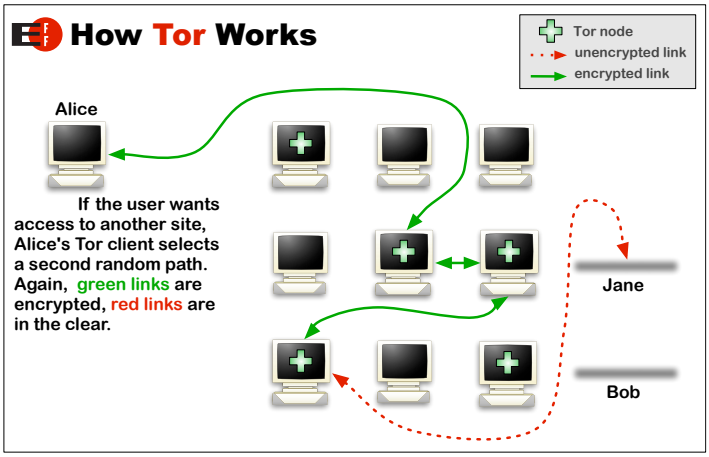


Diagram: Ren Bucholz, EFF

Why is anonymity needed?

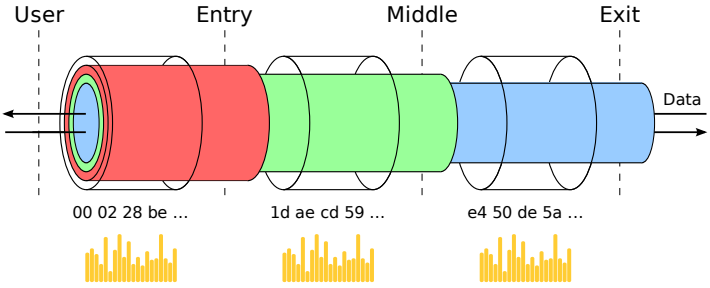
A wide variety of people require anonymity online. Survivors of abuse and rape, as well as those suffering from illnesses might want to participate in information sharing and support groups, without their employer or Internet Service Provider (ISP) finding out. Journalists can use anonymity systems to protect their informants, such as dissidents or whistleblowers. Bloggers discussing controversial topics can protect themselves and their families from retribution. 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.

Egyptian blogger Kareem Amer has been imprisoned since February 2007, serving a four year sentence

Canadian-Iranian blogger Hossein Derakhshan has been imprisoned since November 2008

Where more research is needed

Tor's weakness is that, unlike email anonymity systems, it does not delay messages. Encryption prevents attackers from tracking messages based on their content but they can use timing correlations to trace users. This class of attacks and how to defend against them is the subject of ongoing research. Promising defences I am investigating include adding extra messages ("dummy traffic") to disguise timing patterns.



Nested encryption hides content but not traffic patterns

Also, Tor is only one part of an Internet privacy solution. Modifications to the other system components users interact with are also needed to ensure that they do not leak identity information either. Enhancements to the Mozilla Firefox web browser are well advanced, but work on hardening the rest of the operating system is one of my active research topics.

Further information: `https://www.torproject.org/`

2010-10-26