An Anonymous Decentralised Messaging Application
Utilising the Whisper Protocol

Seán Durban
B. A. (Mod.) Computer Science
Supervisor: Dr. Donal O’Mahony
May 2018

Abstract

With the current extent of surveillance it’s difficult to guarantee any form of digital communication will remain private. Furthermore, current messaging applications may offer end-to-end encryption, which provides assurances to the message content being secure, but fail to preserve a user’s anonymity. They leak compromising information about the sender, recipients and the message itself from metadata. Centralised applications require a certain level of trust since servers handle the messages; this can present risks for both service and user. Ultimately a potential user should not have to choose a messaging application based on the application or company they trust the most and should have the ability to remain anonymous.

This project will propose a new form of messaging application which supports end-to-end encryption for both direct and group messaging by default. It will be decentralised and transparent, allowing for trust to be distributed in the system. It will also aim to maintain a user’s anonymity by being a dark system, where no compromising information is leaked from metadata. A messaging protocol called Whisper, from the Ethereum eco-system, is used to achieve this. Whisper has a unique approach to decentralised messaging and routing which has clear influences from other technologies such as Tor.

The application delivered is functional and provides a unique form of messaging. However, testing of the application was limited due to underlying issues with the Whisper network. As a result, it’s still unknown if it is a viable solution for mass usage or if anonymity can be truly guaranteed.