**Team 17 Project Proposal**

Ben Korza

Mark Fitzgibbon

Mitchell Caisse

**Need:**

As government spying and censorship becomes more common and/or well known it becomes harder to communicate without fear of prying eyes. This creates a need for a communication network in which its user can feel confident that their identities will remain unknown and that they are able to speak freely without fear of prosecution. This could be especially useful in protecting one’s conversations from eavesdroppers. It could even be used in organizing protests against corrupt powers.

**Approach:**

In order to meet this need we plan to create a communication network that will allow users to communicate anonymously and securely. In order to accomplish this we will create a distributed platform that allows users to do this. This platform will also involve a centralized name server which will assist users in determining its peers in the network. When a client first starts it will connect to the name server to determine its currently online peers. Once the client has its peers it will be able to communicate with others by using distributed messaging.

In order to keep message contents secret and the source and destination of the message anonymous, messages will be encrypted and bounced amongst peers. To send a message the client will first encrypt the message with the client it wishes to talk to’s public key. It will then broadcast the message to a set of its peers. The peer that receives it will determine if it is for it, by decrypting it with its private key, if it cannot decrypt it, then it forwards the message along to a set of its peers. Each client will have a list of messages it already received in order to prevent cycles from occurring.

Encrypting the messages using asymmetrical encryption allows the messages to be sent across the peers with no destination address and keep the contents of the message private as only the recipient will be able to read the contents. This allows the client who wishes to send the message to broadcast them, and hide their address, as even if the intended client is one of the initial peers, that client expects the messages to be broadcasted. He won’t know that the message came directly from the peer, keeping the source address of the message a secret.

**Benefit:**

The benefit of our implementation will be the fact that it uses a distributed network rather than connecting to a centralized server. This will make it harder to determine the original source of the messages. There will also be no central logs of all communications. A client will still be able to log conversation.

**Competition:**

The idea of an anonymous communication network is not new, however our Anonychat will still bring together a combination of things that does not currently exist on other products. Some anonymous communications include the Invisible Internet Project (I2P), an ongoing effort to build a free, open source, and anonymous internet. I2P includes a system to allow anonymous IRC communication, by simply allowing standard IRC protocol over the I2P network. Since I2P is designed at the network layer, it does restrict compatibility to only those on the I2P network to maintain anonymity, whereas Anonychat’s restrictions are to the application itself. Users will be able connect across any existing communication network. Freenode is an example of IRC using the standard protocol with SSL encryption to ensure anonymity. Freenode, being an IRC protocol, still will have direct connections that can indicate relations between users, while our Anonychat will implement a method to obfuscate intended targets of messages. In addition, Anonychat aims to be more directly peer to peer, requiring a central server only for initial connections to the Anonychat network. Competition also extends to peer to peer style communication network Skype, which uses a similar connection system we intend to implement (a central server to start, then p2p communication afterwards). A key difference between Skype and Anonychat is that Skype’s main focus is not anonymity, and uses P2P connections in a more direct method. Some projects in the IRC field, such as Quassel and Rust, are more direct competition in anonymity, but do not use the P2P connectivity we will attempt. Overall, our metric for success will be if Anonychat is able to reliably send messages through the distributed system with minimal chance for the messages to directly connect users.