**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 an anonymous communication network that is based upon the popular IRC protocol. We will define the word anonymous as a system in which each user does not know where a sent message originated. We will use an open IRC library, but only plan to implement the protocol’s most important functions. We first plan creating a distributed communication platform. This platform will allow several end hosts to communicate with each other without knowing where the complete message has originated from. To do this we plan to break messages into multiple parts based on how long the message is, encrypt the messages, and then distribute the message amongst peers. The current style of encryption we plan is up in air, but we are currently looking into a public-private key method. Since people can be identified in this method, we will need to research ways to circumvent this. We are also researching onion routing as a method of distribution.

The second phase will be to create a local IRC proxy that the user will run on their computer. This will be built on top of the communication platform, and will act as a local IRC server. This local server will forward the messages to all other clients connected. This will allow users to use this anonymous platform without modification to their current IRC clients.

**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 system is not anything new, and there have been numerous attempts to implement one. The Invisible Internet Project (I2P) contains an anonymous IRC protocol; however, I2P focuses more on an overall anonymous communication systems, whereas we are just focusing on a standalone communication program. Freenode is another anonymous IRC system, however Freenode still makes use of a centralized server, and uses SSL encryption rather than distribution for anonymity. A few others exists as well, such as Quassel and Rust, however these projects are no longer under active development and have taken different approaches.