**Team 17 Project Proposal, Anonychat**

Ben Korza, Mark Fitzgibbon, Mitchell Caisse

**Need:**

Many internet users desire a means of communication that guarantees privacy so that they can be confident their identities will remain unknown and their messages will be safe from prying eyes. This is especially the case nowadays as public concern increases about organizations which have been caught multiple times spying on users from both foreign and domestic networks. PRISM stands out amongst these cases, as here the NSA collaborated with companies like Google and Microsoft to collect data from their unsuspecting users. While PRISM cannot be circumvented through legal means, other companies, such as Facebook, have been accused of buying and selling user information. Therefore, this user need for anonymity should come as no surprise. The issue could be important among people who work at corporations as well, considering packet sniffers or other external programs can be used to intercept messages and identify information about them. Our Anonychat will attempt to resolve this need by implementing a system in which packets can neither be read from external programs nor traced with certainty.

**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 key benefit of our protocol is that anonymity is the central point of our design, where most communications normally add on such security features after message features are already implemented. The P2P nature of our protocol also means that there is no central point where communications must go through, and the central servers that will need to exist are simple and only show active connections to itself. The arrangement of our anonymity features allows the contents of messages, as well as connections between users, to remain unknown to any third parties of a conversation who may attempt to listen in.

**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, while Anonychat will use the P2P structure to hide interactions between users intentionally. Some projects in the IRC field, such as Quassel and Rust, are more direct competition in anonymity, but do not use the P2P model of connectivity we will attempt. Overall, our metric for success will be if Anonychat is able to reliably send messages through the distributed system with a minimal chance for the messages to directly be linked to users.