**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 spying on users in both foreign and domestic networks. PRISM stands out amongst cases of spying, as here the NSA collaborated with companies like Google and Microsoft to collect data from their unsuspecting users. Other companies, such as Facebook, have been accused of buying and selling user information. Therefore, this user demand for anonymity should come as no surprise. The issue could also 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 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 its target client’s public key. It will then broadcast the message to a set of its peers. The peer that receives it will determine if the message is meant for it by decrypting the message with its private key; if it cannot decrypt it, then it will forward 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. It also 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 target client is one of the initial peers, that client expects the messages to be broadcasted. The target client won’t know that the message came directly from the peer, keeping the source address of the message a secret.

**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. Our protocol keeps the contents of messages, as well as the connections between users, secret to any third parties who attempt to listen in. 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 contain data on active connections.

**Competition:**

The idea of an anonymous communication network is not new, however our Anonychat will still bring together a combination of things that are not currently provided by 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, 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 has 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 the 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). However, 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.