EMURA

## Developers:

## Gregory LeBlanc

## Norman Maclennan

## Steven Failla

Abstract:

The purpose of this application is to ensure the delivery of messages over the internet using a fully encrypted transfer mechanism. The application will have its own authentication server in which users will verify their information. Users will also be able to have fully encrypted file and image transfer. This application will use the most update encryption standard (RSA) – it will also use the SHA-256 hashing algorithm to hash the user’s private key. The key exchange process will be totally seamless, the user will not have to remember his or her public or private key, all they will have to remember is their password that they will use to login. The user will also be able to export his or her key pair – which can then be used for other purposes such as signing email. MORE NEEDED

Value:

Over the past 5 years, more emphasis has been put on security – especially when it comes to sending messages over the internet. Many people have fallen victim to their information being stolen by an unauthorized listener. There are many ways to secure your data when it comes to simple data transmission such as IM and email. This application wishes to **simplify** the operation and use of such technology. Our application will make the complicated process of securing IM chat a thing of the past – there will be no different in the setup of the program than any other Instant Messaging client that he/she has used in the past. A person’s information, whether it be a message they are trying to send to their significant other or a Department of Defense document, is very important, and our application takes care of the risk of someone being able to see this information. MORE NEEDED

Simplicity:

Simplicity is key when it comes to designing an efficient application (Probably don’t need this sentence). [Application name here] will be VERY simple. User creation will be only filling in a few lines of text and clicking a few “next” buttons. Once your username has been registered with our authentication server, the key generation process will take place. This should only last a few minutes. Once the user is logged back in they will see the standard “buddy-list” type screen. They will have many options from there to choose from. The GUI will be VERY self-intuitive. Any option will be clearly defined and the application will have a very detailed help menu. This program is designed for a person that is familiar with the basic operations of a computer, such as: clicking on an icon, doubling clicking on an icon, finding the start menu, understanding the meaning of “instant messaging.” We will also have a very detailed community webpage where users will find updates to [Application name here] and forums to discuss bugs and possible content for future releases.

Current Technology:

There currently are only two other fully encrypted instant messaging clients (See link: <http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients>). The current clients out there are: Brosix and BitWise communications. Brosix is an “Enterprise” only chat client – it is meant for Businesses to implement in their networks. They do have a free version but it is designed to be a trial version of the full product. BitWise communications has one free version and two paid versions – they also market heavily on enterprise communication. The main difference right away is [Application name here] will always be free and open source. That is something that we pride ourselves upon. This application will be different because it is not only designed for the business world – but is designed for the average security conscious user. We would like to create a community that prides itself on being secure and being private. The other two clients generally use the same encryption standard as our application ( because it’s becoming the industry standard ). More Needed

Requirements:

Minimal Hardware Requirements:

Operating Systems: Windows XP SP2 or greater

Linux Kernel Version 2.4.x or greater

Mac OSX Leopard or greater

Architecture: 32 OR 64 bit\*

Memory: 64 MB

* 64 bit Windows XP NOT supported

Software Requirements:

Java 6 or greater

An internet connection