Distributed Instant Messaging System
Requirements Document

Matthew Shea
Yi-Chin Sun

February 06, 2012

User Profiles

Primary Users

The target demographic for this system will be people of all ages interested in secure communications. Their expected education level could range from middle school to collegiate and beyond. Their computer usage could also range from occasional to frequent.

Stakeholders

Stakeholders in this project will include primary users as well as anyone in the community who is interested in cryptography and censorship-resistant design.

Constraints

Physical Constraints

Since we will not include voice recognition or alternative methods of text input other than keyboard as a function of the distributed IM system, individuals with visual or physical handicaps may be unable to utilize our program.

The program will require a keyboard or on-screen keyboard to operate effectively.

Environmental Constraints

Initially, the system will only be designed to operate on computers capable of running Java with the Swing user interface library. The design of the back-end should be flexible enough to allow interfacing with other systems, such as Android, in the future.

Requirements

Title:	Contact List
Requirement Number:	1
Requirement Type:	Interface
Description:	The system must have some means for the user to maintain a list of contacts.
Rationale:	Rather than sift through all users on the network, the primary user will only be interested in other users with whom he wants to communicate.
Source:	Popular Usage
Fit Criterion:	Space Efficiency, Effective Sorting
Dependencies:	None
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Chat Input
Requirement Number:	2
Requirement Type:	Interface
Description:	The system must have some means for the user to input text
Rationale:	The user would need to be able to communicate with other userss, and thus need a way to input text to be sent.
Source:	Popular Usage
Fit Criterion:	Space Efficiency, Feature Set
Dependencies:	RN3
Conflicts:	None
History:	**Created** (Yi-Chin Sun)

Title:	Chat History
Requirement Number:	3
Requirement Type:	Interface
Description:	The system must have some method of displaying the previous messages in the communication.
Rationale:	In order to facilitate a conversation, the system must implement a history system in order to review previously sent messages.
Source:	Popular Usage
Fit Criterion:	Space Efficiency, Ease of Reading, Distinction between Participants
Dependencies:	RN2
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Notifications
Requirement Number:	4
Requirement Type:	Interface
Description:	The system must be able to notify the user when a message is received, when the other user is typing, and the status of other users.
Rationale:	Since a user may engage in multiple conversations at once, the user must be alerted when a new message is received. Also, being notified if the other user is typing will facilitate in non-interruption of the other user's message. In addition, knowing the status of other users lets the user know who he/she can contact.
Source:	"When Conventions Collide", Popular Usage
Fit Criterion:	Ease of Distinction, Distinction between Statuses/Notifications, Visibility
Dependencies:	RN1
Conflicts:	None
History:	**Created** (Yi-Chin Sun)

Title:	Swarm Connection
Requirement Number:	5
Requirement Type:	Interface
Description:	The system must be able to accept input to change the swarm that the user is connected to.
Rationale:	Since the system back-end is supported by an extended DHT network, the system should allow the user to choose which swarm to connect to.
Source:	Popular Usage in Distributed Systems
Fit Criterion:	Usability, Simplicity
Dependencies:	None
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Status Update
Requirement Number:	6
Requirement Type:	Interface
Description:	The system must allow the user to specify their current status out of the following: Available, Busy, Away, Invisible
Rationale:	Users may want to make their current status available to the network in order to notify other users about their availability
Source:	Popular Usage
Fit Criterion:	Space Efficiency, Accuracy
Dependencies:	RN4
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Key Import
Requirement Number:	7
Requirement Type:	Interface
Description:	The system must have a utility to import encryption keys.
Rationale:	Since users are determined based on key rather than a password, the system must allow a user to import a key.
Source:	Common Sense
Fit Criterion:	Simplicity
Dependencies:	RN8
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Key Export
Requirement Number:	8
Requirement Type:	Interface
Description:	The system must have a utility to export encryption keys in some fashion, be it QR code, or a Base64 representation.
Rationale:	In the event that a user wishes to reinstall their operating system or upgrade, a user needs to be able to back-up the key that is used for the network.
Source:	Popular Usage
Fit Criterion:	Simplicity
Dependencies:	RN7
Conflicts:	None
History:	**Created** (Matthew Shea)

Title:	Account Creation
Requirement Number:	9
Requirement Type:	Interface
Description:	The system must provide a method for creating a user account in the swarm, including creating a user name and generating an appropriate key-pair.
Rationale:	Without some kind of account creation and keys, the user will be unable to participate in the network.
Source:	Common Sense
Fit Criterion:	Simplicity, Effectiveness
Dependencies:	None
Conflicts:	None
History:	**Created** (Matthew Shea)

Updated Schedule

A single modification was made: the deadline for the completion of the backend. The backend has proven more complex than originally anticipated, which demanded the deadline be pushed further back.

- 02/14 : Data Analysis Results and Prototyping Plan
- 02/23 : Prototype Demonstrations
    - Complete Interface Implementation
    - Complete Working Prototype
    - Complete Back-End
- 03/01 : User Test Plan
    - Select User Groups for Testing
- 03/13 : User Testing Begins
- 03/29 : User Testing Ends
    - Analyse Feedback
- 04/03 : Project and Supporting Documentation
    - Make Changes Based on User Responses
    - Finalise any Bugs and Features

Works Cited

Voida, A., Newstetter, W. C., Mynatt, E. D., & Tech, G. (2002). When Conventions Collide : The Tensions of Instant Messaging Attributed. *Names*(Vol. 4, pp. 187-194). ACM Press. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.12.8638