KEYCHAT

Technical Design Document

Prepared By:

Christopher Kvamme, Calvin Owens, Khalid Fallatah, Tyler Hargett,

Hunter Houston and Taylor Bishop

Table of Contents

1. Executive Summary
2. User Stories
3. Use Case Diagram
4. Database Models
    a. Database Diagram
    b. ERD
    c. Software Architectural Diagram
5. 'Paper' Prototypes
    a. Android
    b. Web
6. User Profiles
7. Task Analysis
8. O/A Matrix
9. Software Lexicon
10. Usability Test Outline
11. Usability Report

Executive Summary

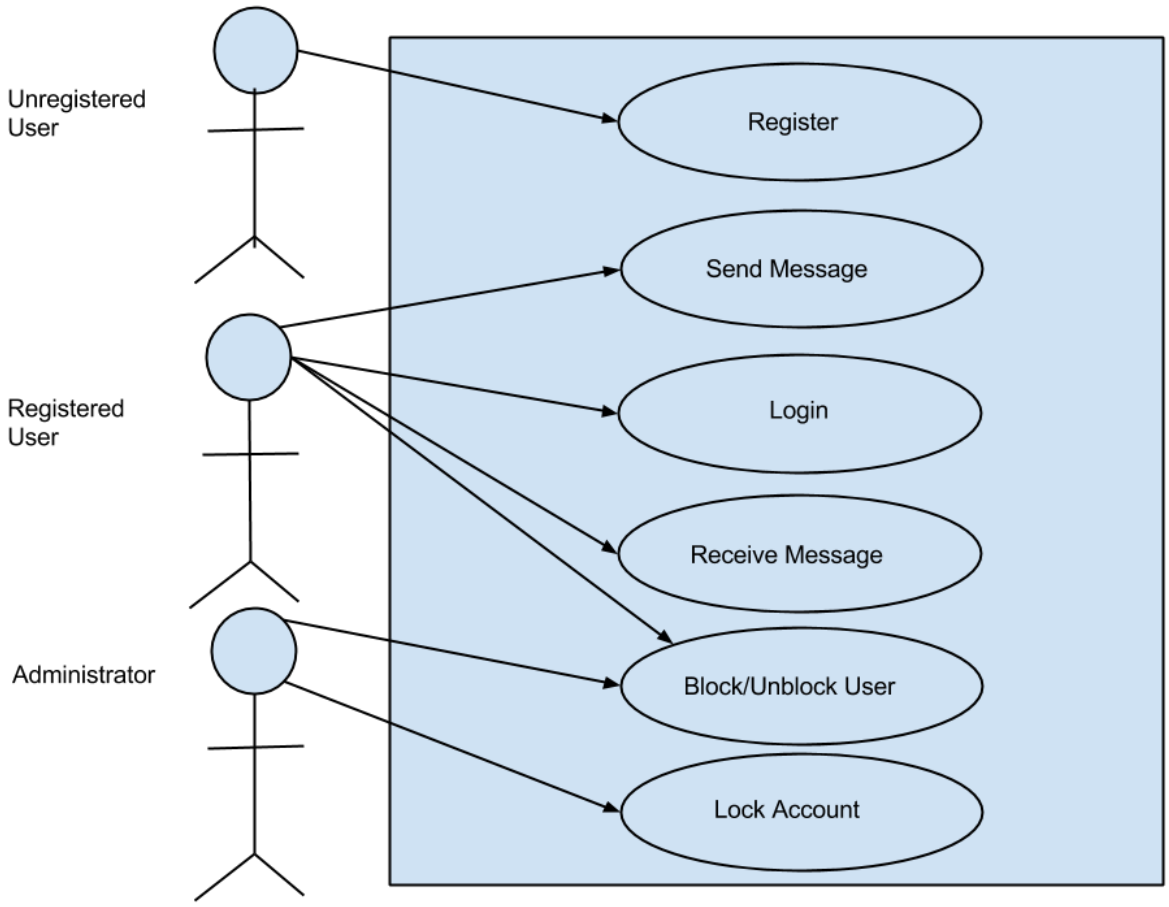
This document aims to provide detail on the current thinking regarding KeyChat and its implementation. KeyChat will be a secure, easy to use private messaging service. The service will be accessible on the web and via a limited Android application. The service is focussed on security and privacy.

This document is intended to describe a ‘snapshot’ of our current thinking. It is not final and in fact the information contained within the document may change dramatically. As we code we learn and make changes to the technological implementation. As we interact with the product we learn and update our user stories resulting in a dynamic set of features. Reader be warned: THIS DOCUMENT IS DYNAMIC. NO INFORMATION PRESENTED HEREWITHIN IS TO BE LOOKED UPON AS FINAL OR EVEN POTENTIALLY VIABLE AS THE PROJECT PROGRESSES.

User Stories

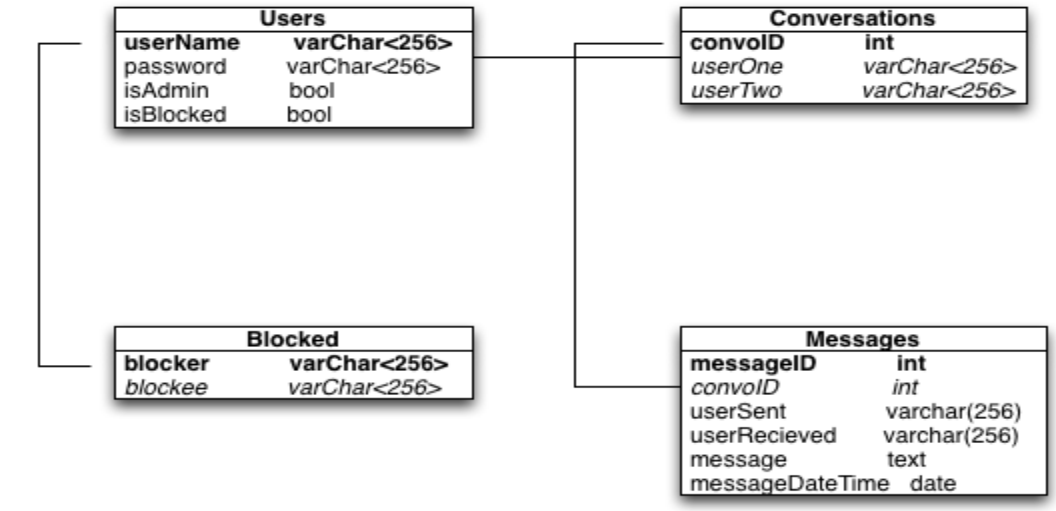
1. As a USER I want to login / register so I can use the service.
2. As a USER I want to logout so I can I can stop using the service.
3. As a USER I need to be able to permanently delete my account so I can leave the service and so no one else can use my username.
4. As a USER I want to send a message to another user so I can start a secure conversation with that user.
5. As a USER I want to see my previous conversations so I can quickly chat with that user again and so I can see what we were talking about previously.
6. As a USER I want my sent messages to be displayed to the receiving user within 5 seconds.
7. As a USER I want to be able to block users who have sent me a message so I can avoid spam / unwanted messages.
8. As a USER I don't want any private information to be displayed in my settings page so as to provide a secure and private setting.
9. As a USER I want to know the status of the security capabilities so I can be reassured that my messages are being sent securely.
10. As a USER I want to be able to flag an account as potentially compromised so I can be sure that the user is who they say they are / their account has not been compromised.
11. As a USER I want to know if the person I am talking to is online.
12. As a USER I want to close / delete previous conversations so I can delete / hide previous correspondence.
13. As an ADMIN I need to be able to delete an account so I can respond to a 'flag as compromised' request.

Use Case Diagram



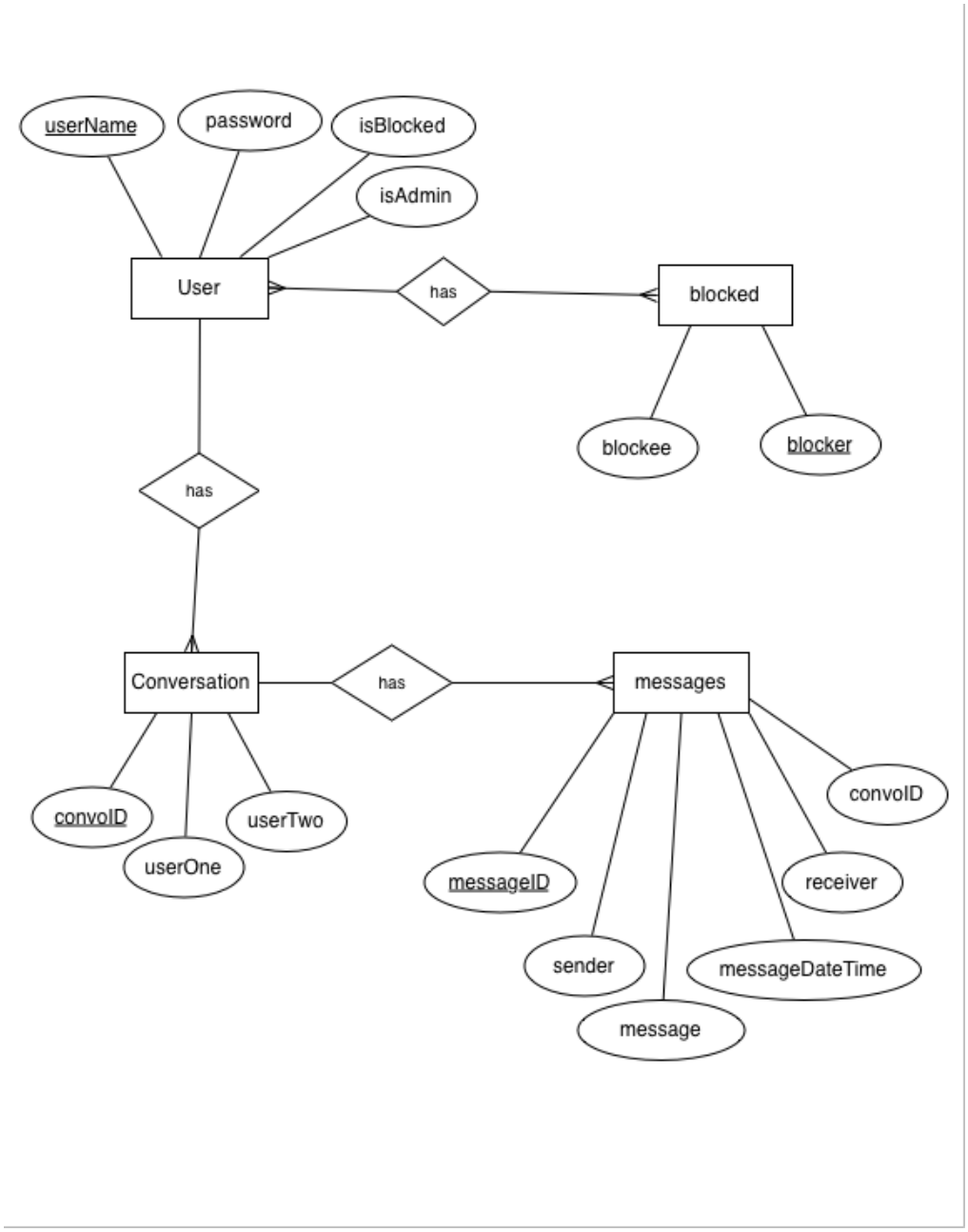
Database Models

Database Diagram



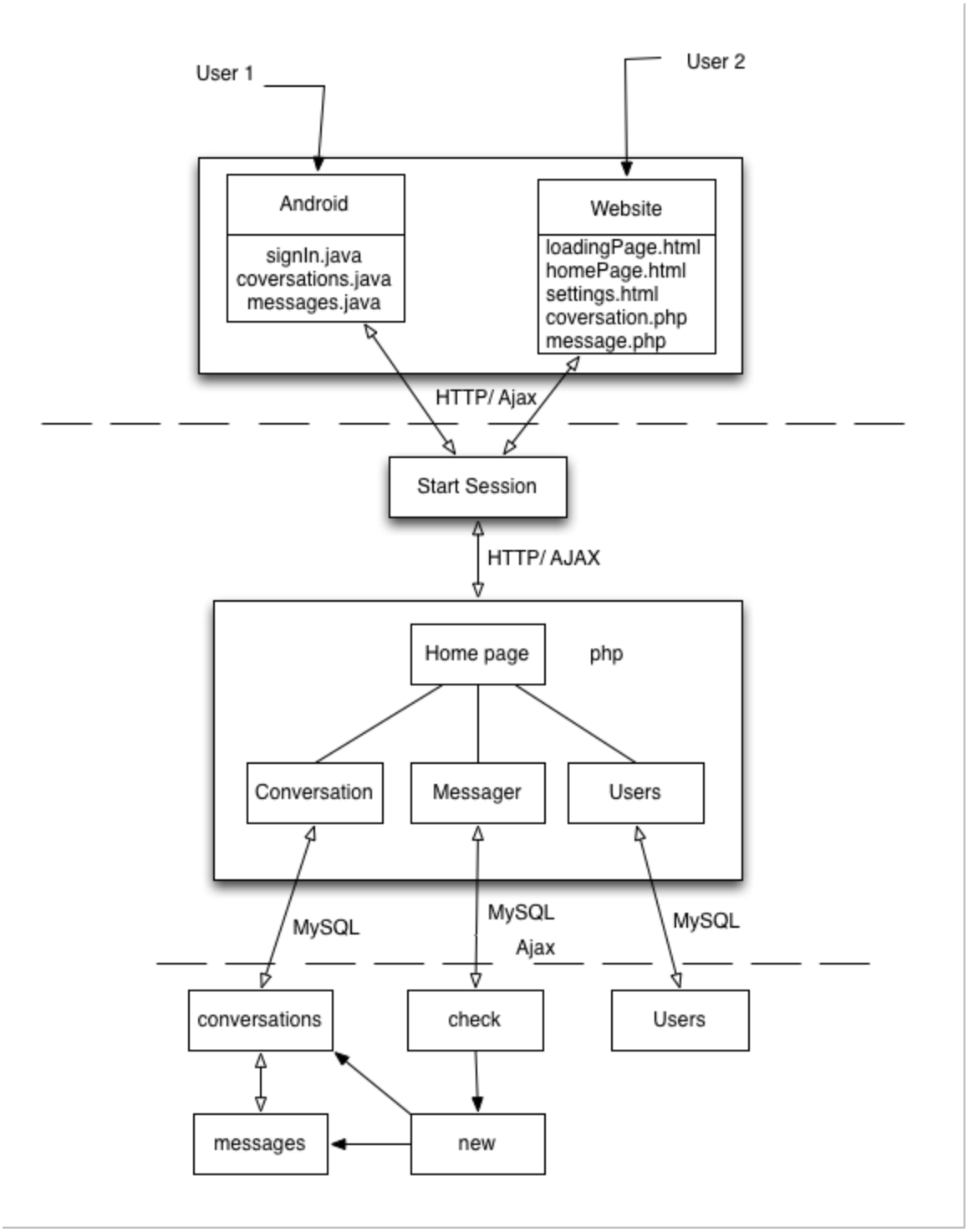
Database Models

ERD



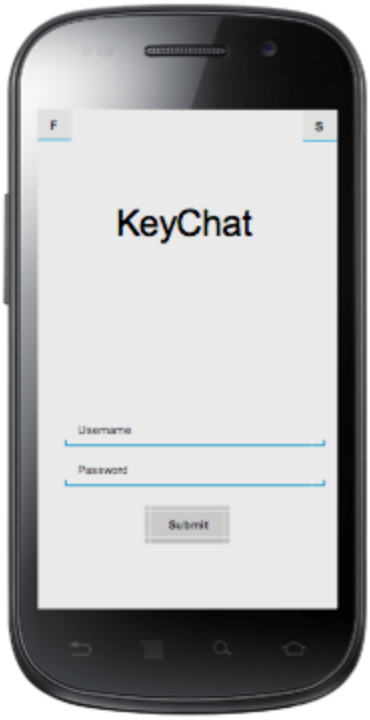
Database Models

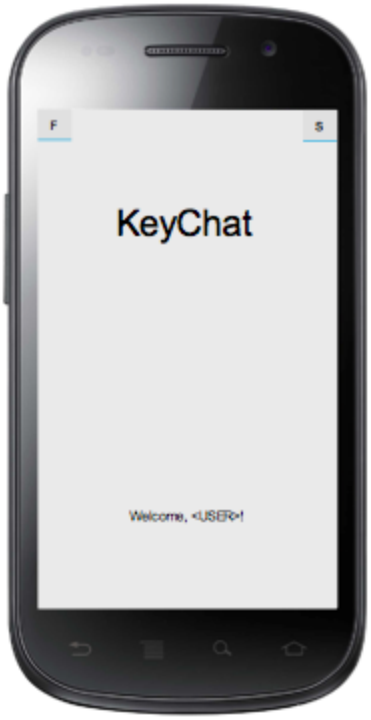
Software Architectural Diagram

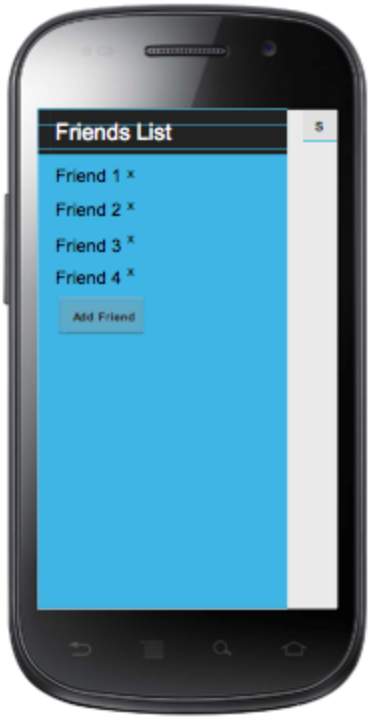


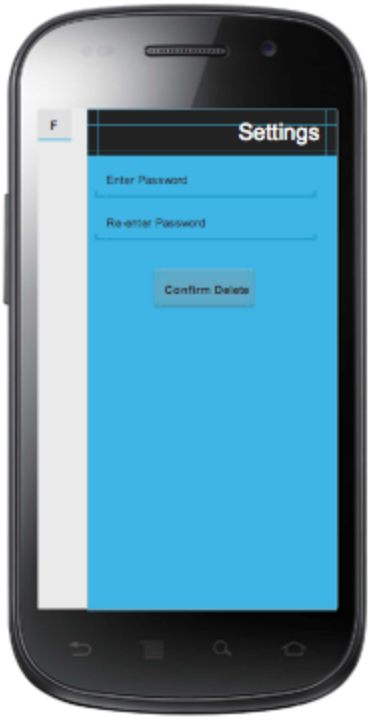
'Paper' Prototype

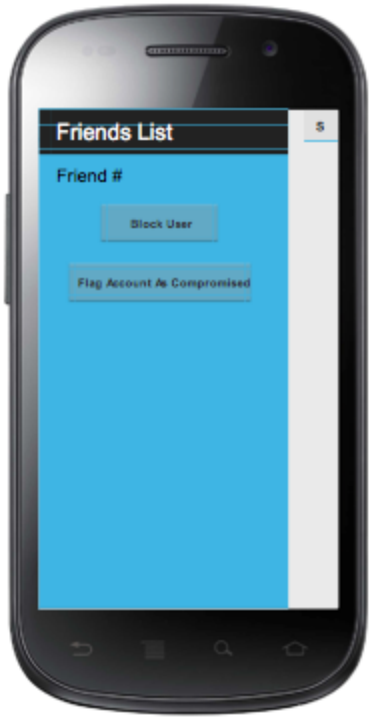
Android

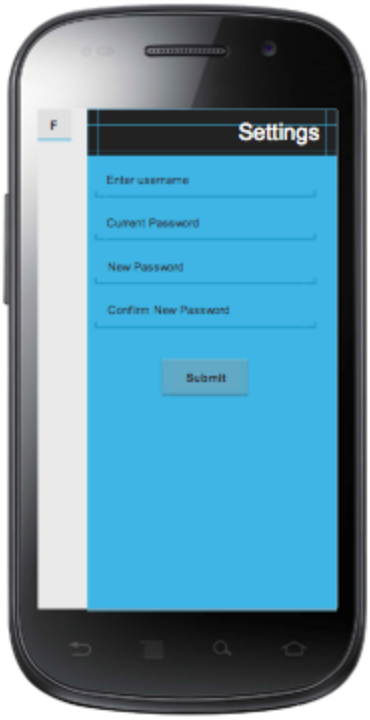


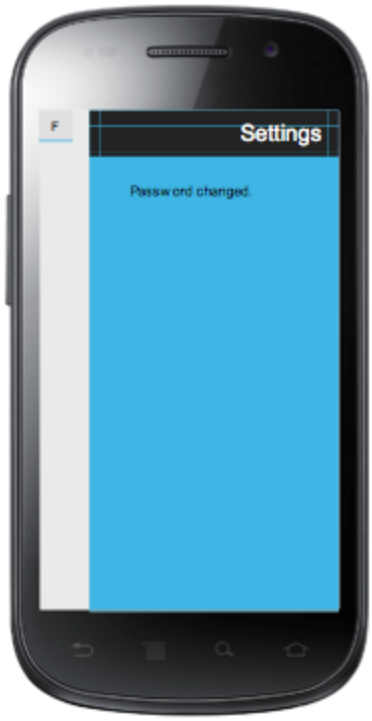








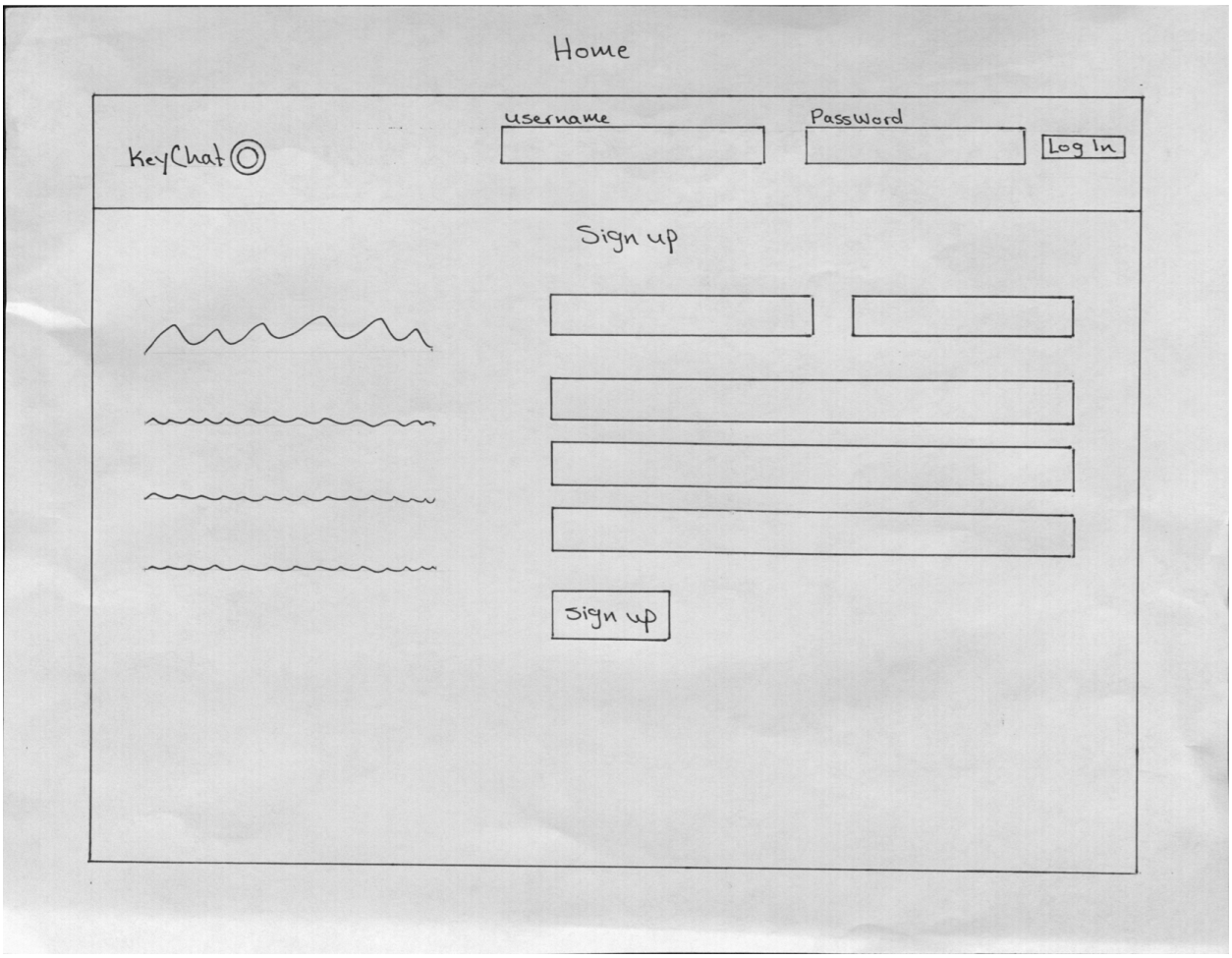


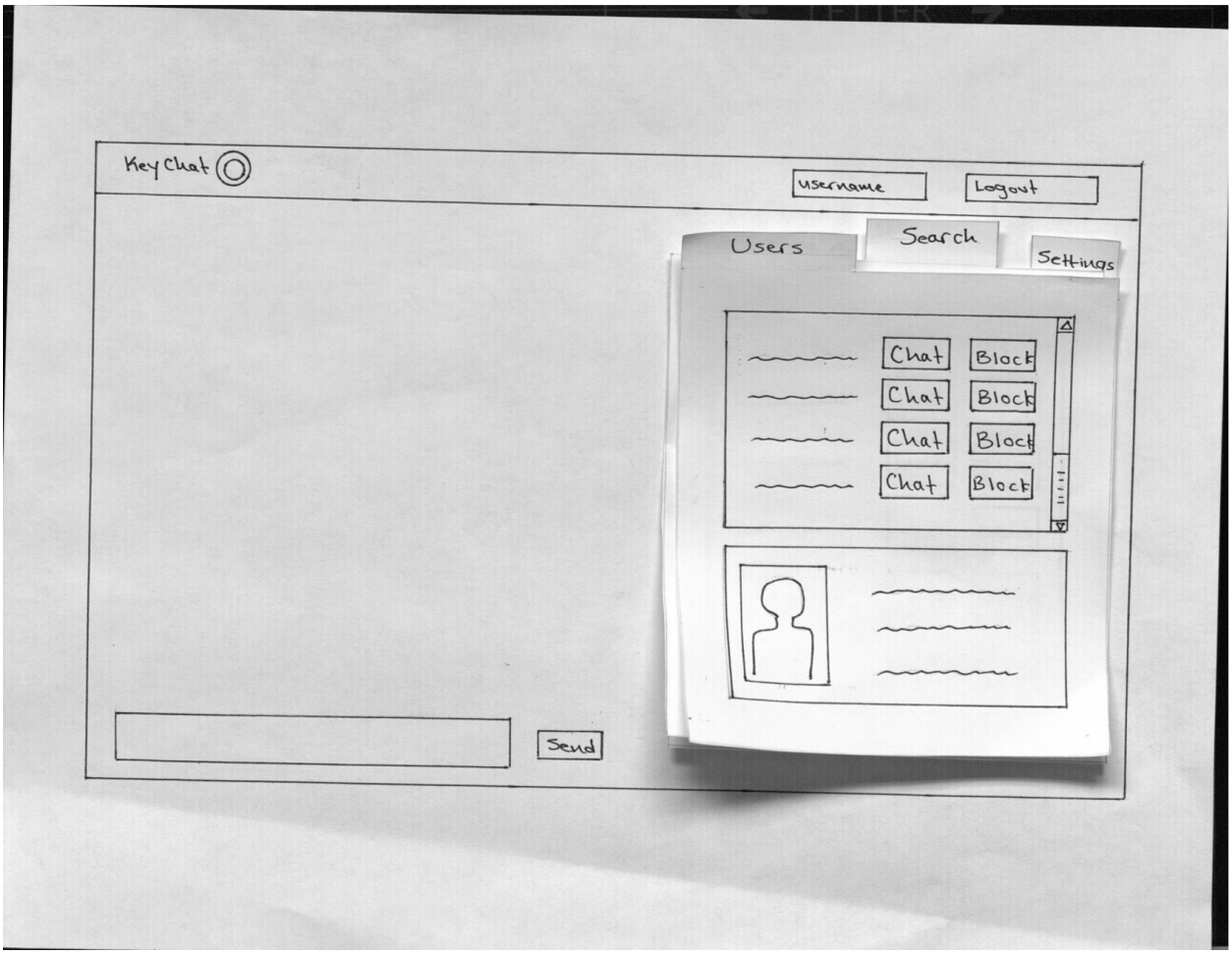

F
Settings
Password changed.

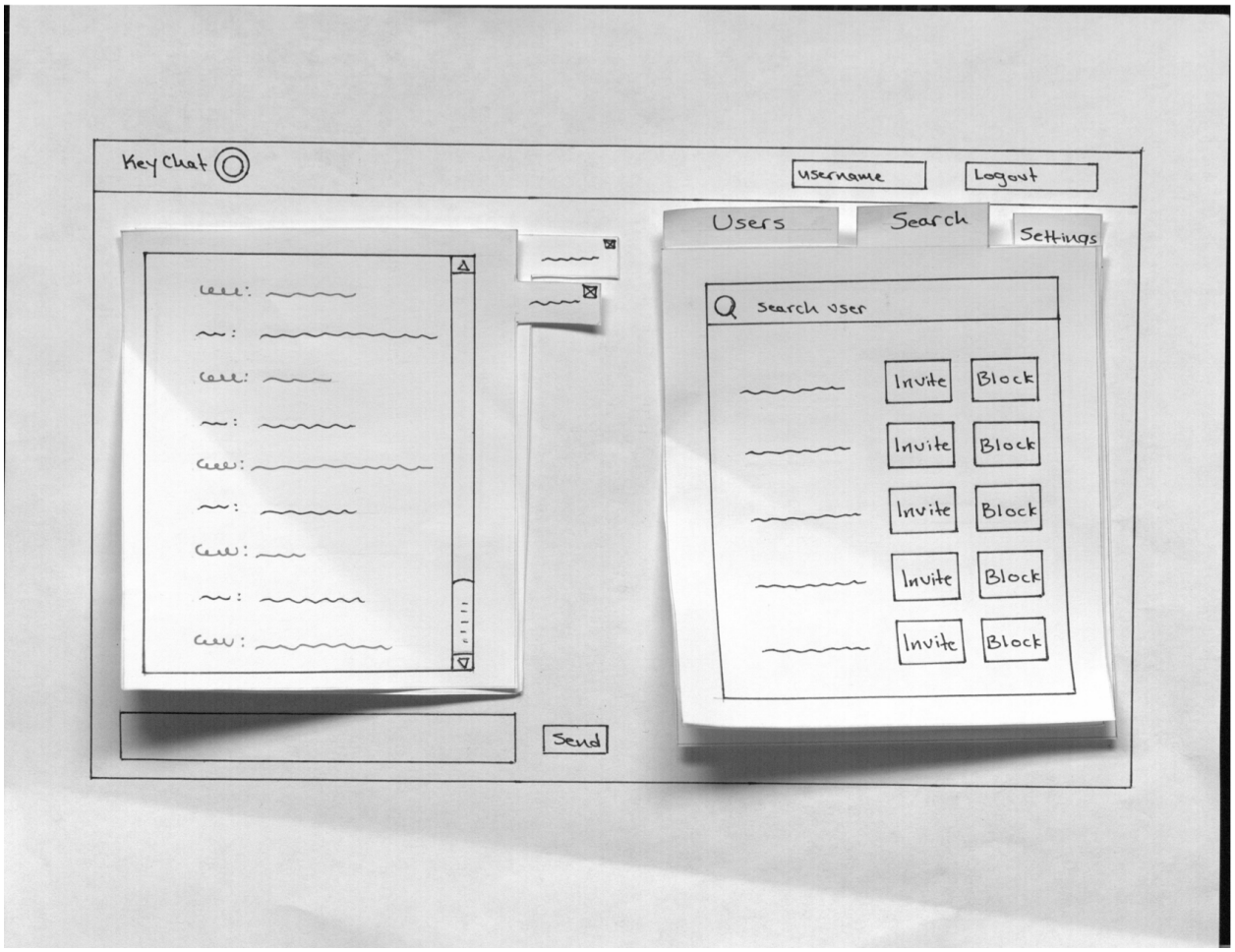

F
Friend #
S
lorem ipsum
solet damat
consectetuer adipiscing elit, sed diam
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123
Go

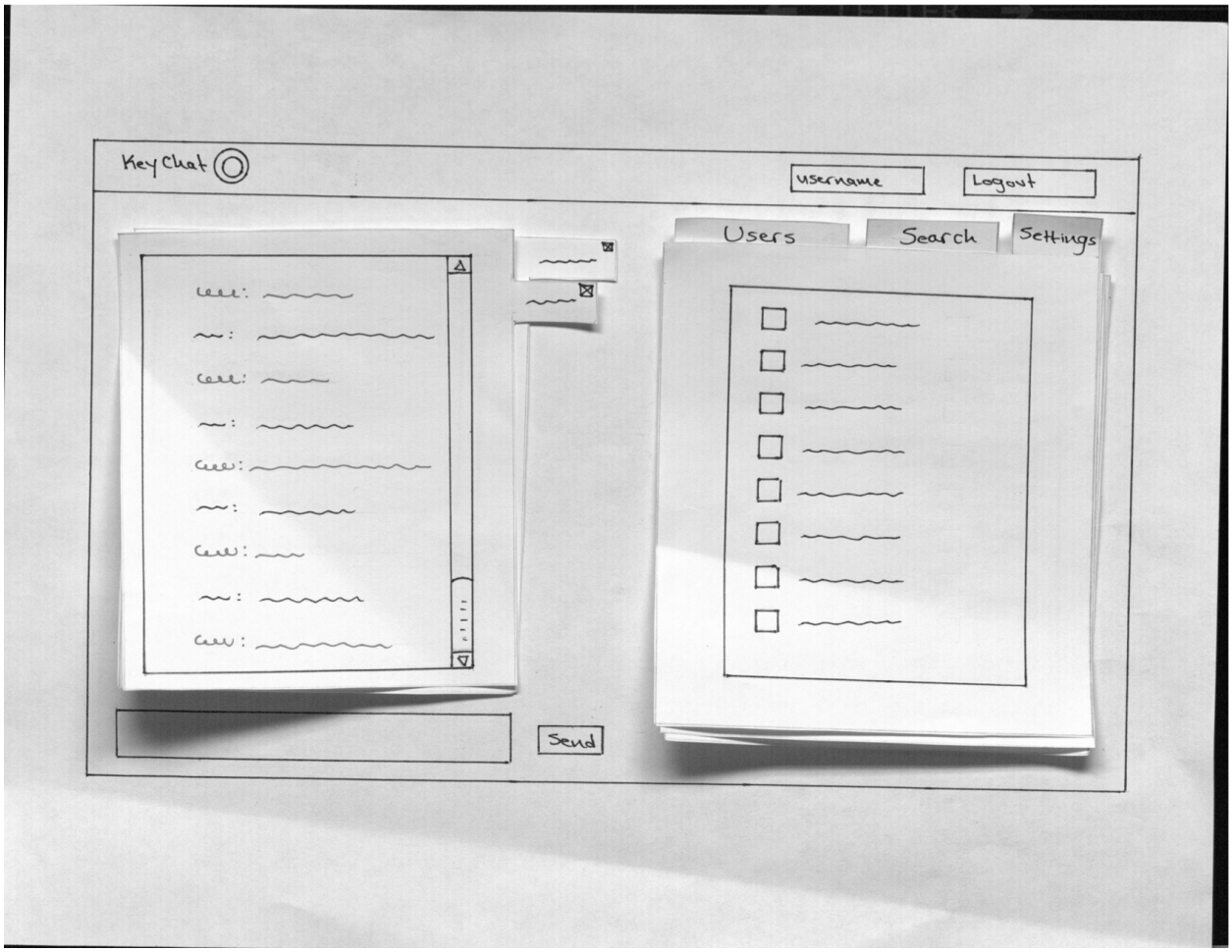
'Paper' Prototype

Web




KeyChat
username
Logout
Users
Search
Settings
Chat
Block
Chat
Block
Chat
Block
Chat
Block
Send


KeyChat
username
Logout
Users
Search
Settings
Search user
Invite
Block
Invite
Block
Invite
Block
Invite
Block
Invite
Block
Send

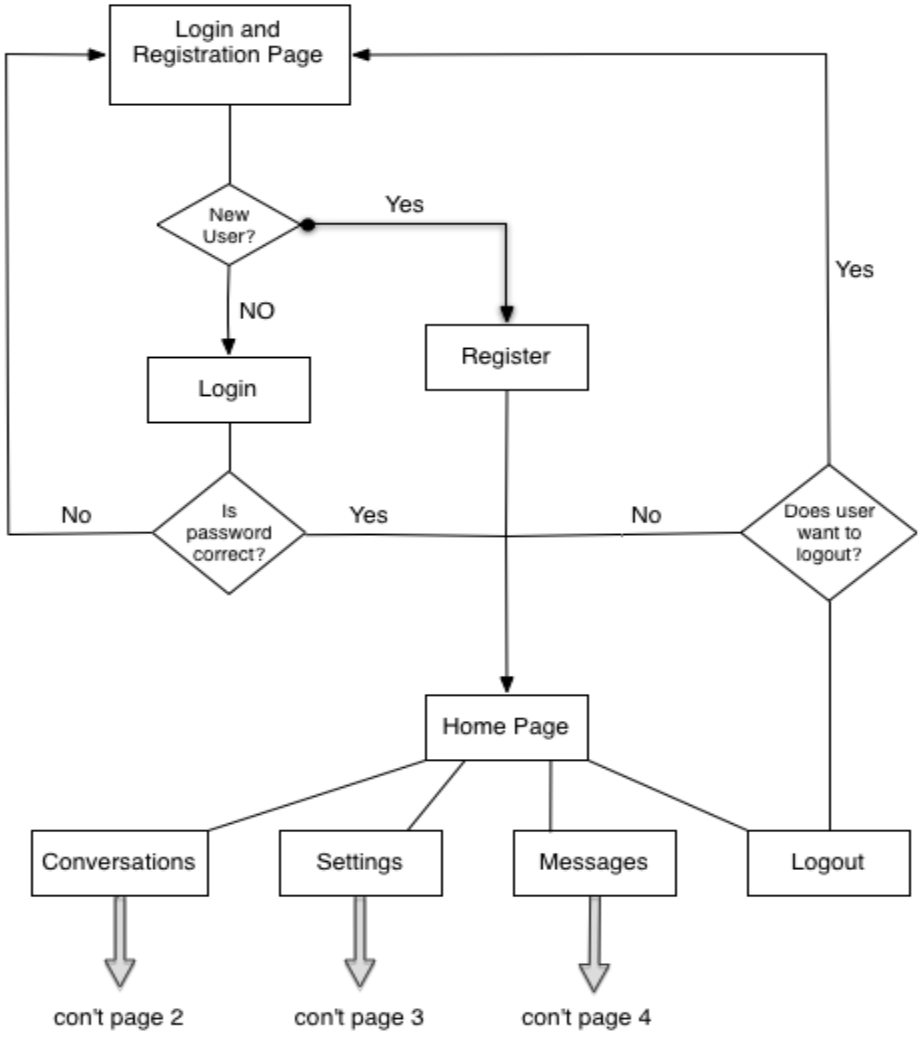

KeyChat
username
Logout
Users
Search
Settings
Send

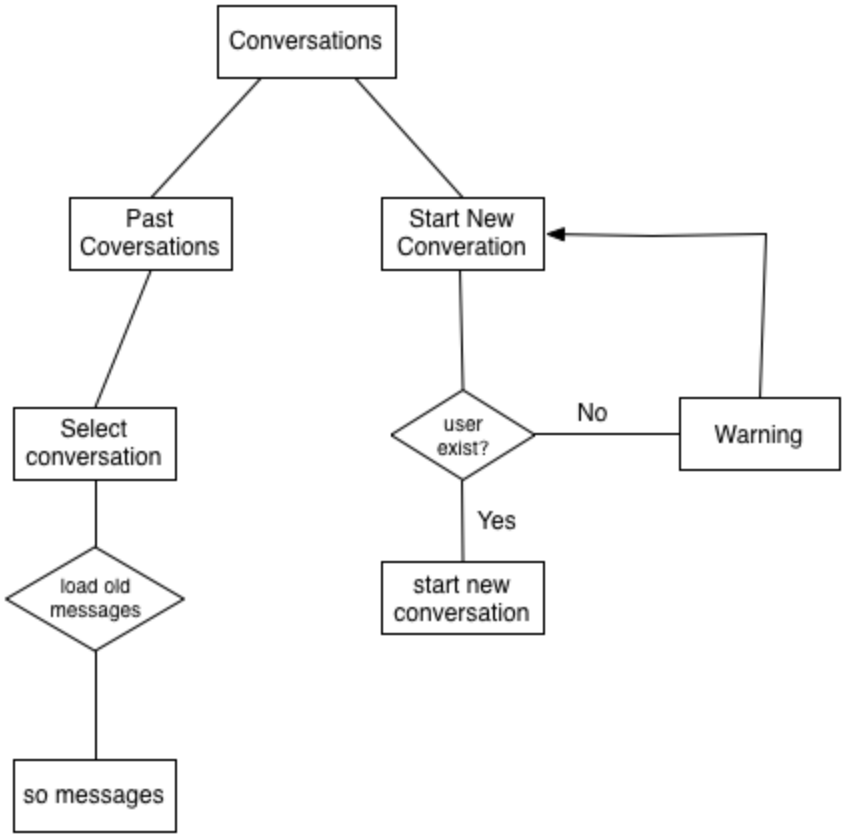
User Profiles

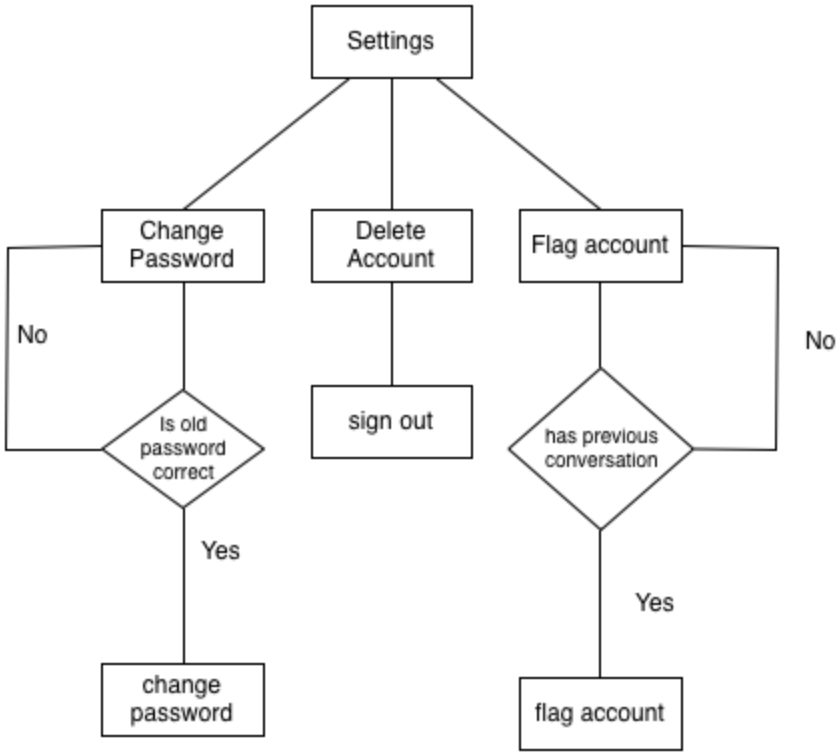
- "Hey this is cool" user
  - **Name:** Trey Kool
  - **Job description:** Student, low-level professional
  - **Job seniority:** None
  - **Education:** Due to interest, probably college educated or in college
  - **Salary:** Low
  - **Computer skill level:** High
  - **Task/Product skill level:** Spends a lot of time communicating over the internet, so high
  - **Motivation:** Thinks it's cool
  - **Likes/Dislikes about software:** Enjoys the idea of very secure communication, but is likely to get annoyed very quickly at features that would actually make the system bulletproof
- Criminal Lite
  - **Name:** John Stamos
  - **Job description:** Could vary widely
  - **Job seniority:** Could vary widely
  - **Education:** Due to interest, probably college educated or in college
  - **Salary:** Could vary widely
  - **Computer skill level:** High
  - **Task/Product skill level:** Likely high
  - **Motivation:** Engaged in some minor crime or other mischievous behavior, looking to protect self from incrimination
  - **Likes/Dislikes about software:** Feels the need to have secure communication, and will likely be willing to undertake some amount of features to make the system more secure than Trey Kool. Likely doesn't care enough to go very far though
- Real criminal
  - **Name:** Pablo Escobar
  - **Job description:** Could vary widely
  - **Job seniority:** Could vary widely
  - **Education:** Educated by the streets
  - **Salary:** Could vary widely
  - **Computer skill level:** High
  - **Task/Product skill level:** Likely high
  - **Motivation:** Is engaged in truly illegal or suspicious behavior that he/she wishes to conceal from wiretapping
  - **Likes/Dislikes about software:** Secure communication is very important to this user, and they will jump through a lot of hoops to make it more secure.

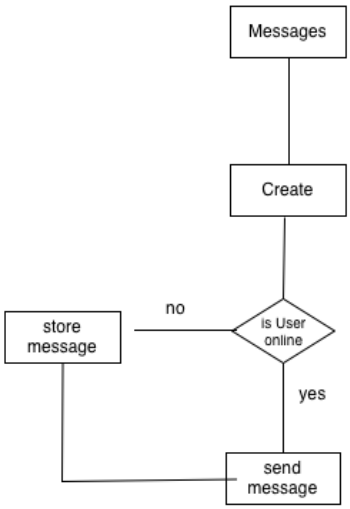
- Government whistleblower
    - **Name:** Eddy ‘Traitor’ Snowden
    - **Job description:** Likely works for government agency
    - **Job seniority:** Probably high
    - **Education:** Grad degree, probably technical
    - **Salary:** Could vary widely
    - **Computer skill level:** High
    - **Task/Product skill level:** High
    - **Motivation:** Needs to disseminate or receive information of interest to the highest agencies in government
    - **Likes/Dislikes about software:** This user could actually be a target of a high-level government agency, and needs to communicate in such a way as to avoid being found out by them. This user will undergo any inconvenience imaginable in order to more effectively secure his communication

Task Analysis




Conversations
Past Coversations
Start New Converation
Select conversation
user exist?
No
Warning
Yes
load old messages
start new conversation
so messages


Settings
Change Password
Delete Account
Flag account
No
Is old password correct
sign out
has previous conversation
No
Yes
Yes
change password
flag account


Messages
Create
is User online
no
store message
yes
send message

O/A Matrix

	Swipe	Tap	Open Keyboard	Submit	Type	Scroll	Open Page in Browser
Settings	x						
Flag Account		x					
Change Password		x					
Logout		x					
Main Page							
Login		x	x	x	x		
Register		x					x
Friends List	x						
Friend Name		x					
Open Conversation		x					
Conversation		x	x	x	x	x	
Message			x		x		

Software Lexicon

Perfect Forward Secrecy: A protocol in public key cryptography that ensures a compromised private key will not compromise the long-term set of public and private keys used

Encryption: A way to scramble data so that only a user who has the appropriate key can unscramble it

End-to-End Encryption: Encryption/decryption is done in the user's browser, so that data cannot be retrieved by an attacker even if they compromise the server

Privacy: Means that the data (In this case, text data) is not able to be decoded by an intrusive third party if it is sniffed and information identifying who a user is is kept to a bare minimum

Conversation: The text messaging feature, and crux, of the software - a conversation between two users during a session

Sign-up form: A form only available on the website (Not on Android) for potential users to create an account and start using KeyChat

Conversation window: Portion of the website dedicated to holding conversations with those on a user's friends list

User Search: Registered users can search for another registered user in the database

Profile: A registered user's account information, some of which is accessible to other registered users including user name

Settings: A page on both the website and Android where a user can change various

settings on their account such as password and disabling it

Flag Account: A registered user can notify the administrators of KeyChat that another registered user's account may be compromised by inputting their name and a brief description of why they believe is has been compromised

Usability Test

Number of Users: 4

Prospective user #1: Trey Kool
Prospective user #2: John Stamos
Prospective user #3: Pablo Escobar
Prospective user #4: Professor Raley as Eddy 'Traitor' Snowden

Outline of testing:

1. **Create An Account:** The user will create a new account for themselves
2. **Add user to friends list:** User will add a user to their friends list
3. **Message User:** User will go to Friends List, message the user they just added
4. **Delete Message:** Delete the message they just sent from the screen
5. **Logout:** User will log out then "exit" out of website/mobile app
6. **Login:** User will "open" website/app and login to their account
7. **Block Friend:** User will block the user they added earlier in the test
8. **Change Password:** User will go into Account Settings and change their password.
9. **Lock Account:** User will go into Account Settings and lock their account from further use

Types of Tests:

Summative: For users #1 and #2, we will be using the summative tests to look for errors in design and choices that the users may be struggling with.

Formative: For users #3 and #4, we will be using formative tests - having them think aloud and tell us what they think of the options in the design itself, as they are more knowledgeable with the concepts underlying the application and whose point of view will be invaluable.

Goals:

1. **Clarity of error messages:** Plain English error reporting in user interface should be easily understood from the most novice user to the most advanced while being able to accurately describe the problem that occurred.
2. **Ease of use:** The messaging UI should be natural and similar to other IM applications such as AIM and Windows Messenger, as well as the native messaging interface for iOS and Android.

Usability Report

ABSTRACT

The summative tests were non-quantifiable in nature: notes were taken from the standpoint of what should be a reasonable amount of time to complete each task, and “points” were docked for each - notes on the problems in design that may need altering for ease of use and understandability

Prospective User #1: “Hey this is cool” user

WEB:

-User seemed confused on what creating an account entailed

-”Search” and “User” button were inter-changed when trying to message a user on their Friend’s List

-User looked under Settings initially when trying to block user

ANDROID:

-User took longer than expected when asked to add a user after creating an account: Did not realize it was under the “F” for Friend’s List

-User searched for a Block feature when asked to Block friend just added

Prospective User #2: Criminal Lite

WEB:

-User spent quite some time looking between User and Search

ANDROID:

-User searched for a Block feature when asked to Block friend just added

-Finger came down on the “X” button next to friend’s name when asked to message friend

Prospective User #3: Real Criminal

WEB:

-User asked what the profile was for: mentioned that there should be no picture there, and no incriminating evidence that could link a user to his account on KeyChat

-User wanted more information on the encryption behind KeyChat and where it would be located on the page

-User asked what features would be under settings

-User mentioned that the Chat button seemed redundant; that to chat with a friend should be to simply click on their name

-User was curious about how messages were stored on the local machine, said they should absolutely not be, and also asked if cookies were saved when the website was exited

ANDROID:

-User asked whether messages would still be visible after exiting out of the app - hitting the home button or otherwise terminating the process. They seemed concerned by this

-User mentioned that there should be some sort of link to the webpage should they wish to read up on the encryption behind it - mentioned that unless they otherwise knew what it was before installing the app, they would have no idea what it was used for and the premise behind it

-User asked again whether messages would disappear from the screen or could otherwise be deleted from the screen, mentioned that a third-party could physically read the messages if they wished

-User asked whether accounts persisted on the back-end after accounts were deleted

Prospective User #4: Professor Raley

WEB:

-User noted that the web version and android version should be synchronized to match the features available in the product

-User mentioned that he was not sure what type of information was being provided when signing up. Noted that if cookies are not to be saved and login is not to be persisted, that the registration page should be separate from the front page

ANDROID:

-User mentioned that others may be unaware that the settings tab is on the right side - that there should be some type of identifying mark to it to make it obvious

-User was confused about deleting a message - how this was done and whether it deleted it on both sides of the conversation window

-User mentioned that it was unwieldy having “Flag Account As Compromised” in the Settings tab and forcing the user to type in the username they wish to flag

SUMMARY

The web and Android versions are unsynchronized and differ in the features they provide. Also, the paper prototypes show features that are currently nixed; signing in and registering are now completed with the same two input boxes(username and password). The registration page should be unmarried from the front page and detailed information on how users’ accounts are being protected should be readily visible when they visit the site. On Android, blocking and flagging other user’s accounts was not immediately obvious to some users. Otherwise, the vision of simplicity and ease-of-use has been accomplished.