Design
Jammed Alpha Release (1.0)
3.20.15

I. Confidentiality

- We ensure confidentiality in both network transmission of data and in data stored on the server's machine. All information sent between the client and the server is sent over a connection secured by Java's implementation of SSL, meaning that data sent over the network will be secure.

  In order to ensure the confidentiality of the data while it is stored on the server, we store it in an encrypted state. We only ever store the keys to this file on the client's local machine; they are never transmitted over the network. Therefore, if the client's machine is secure, the data stored on the server is also secure.

  The data is encrypted using the AES block cipher with CBC block cipher mode and PKCS5 padding. The key length used is 128 bits.

  Additionally, we generate a new IV every time the data is re-encrypted. We store this IV on the server with the encrypted user data. The IV length is 64 bits long.

II. Integrity

- Our system is concerned with the preservation of integrity across the network, as it is assumed that both the server and client machines are free from corruption. Therefore, in order to be assured that integrity was maintained, we relied on Java's existing SSL implementation and the MAC-then-encrypt policies underlying it.

III. Audit

- Our system performing auditing by writing to logs whenever the state of the server changes. There are two sets of logs that are maintained, the first is a general server log that only the server admin has access to and records all state changes on the server. The second set of logs are logs for each specific user that record state changes specific to that user. For the alpha release however, user specific logs are not implemented, and will be added at a later date.

A state change is defined by any action that alters the information on the server. These include receiving and sending data and login requests, user data and login changes, and other actions that will be implemented at a later time.

IV. Authentication

- ○ Design description here. Not needed for this sprint.

V. Authorization

- ○ Design description here. Not needed for this sprint.