M2 - Design

The 5 essential security elements for our system are outlined below. In this Alpha version, we aimed to deliver a system that preserved confidentiality and integrity. Confidentiality is achieved through the server not being able to see the messages between the clients through AES encryption. Each connection allows only the two clients in the conversation to have knowledge of the shared key. The server side will not be able to decrypt the message it is forwarding. The only content of messages known to the server is who it should forward to. So far, integrity is preserved since a message will be sent from one user to another without anyone else having permission to modify the recipient or the message content. This is enabled through signing the message using MAC.

In our following prototype, we intend to work on authentication. The current solution is that someone can be a client and log in with any username. Our next step is to have their account be password protected and have usernames be permanent to that user. Currently, we have different authorizations outlined for the server (and the server administrators) and the clients, but as we move to fleshing out different types of clients/users, this security element becomes more relevant. We currently are working on a logging system so we can audit our system. We intend to log information such as the number of login attempts and the IPs of those logins. Lastly, we will continue to strengthen confidentiality and integrity.

Authentication: The user is only able to access and use our application in case they have an account.

Authorization: Authorization is important in our system because we only want to allow a subset of our users to have access to certain assets and operations. For example, only a group chat administrator should be able to change group chat's color and add or remove members of the group to the users.

Audit: Audit is essential to our system because we need to make sure we are able to track who and when accesses our file system and database and with what privileges. This is to ensure that an unauthorized user cannot access our data regardless of the fact that some portions of it might be encrypted. In addition, such an audit provides a way for us to make sure that an unauthorized cannot make changes to the source code of our application either on the server-side or the client-side.

Confidentiality: Confidentiality of messages between intended users is a main priority in our system. This chat room was conceived as a way for users to send messages without the server side being able to see the content as well as prevent other users from accessing private direct or group messages.

Integrity: Proper file permissions corresponding to the role of the user will be maintained in our system. A group chat administrator will stay the administrator of the group until the permission is changed from the administrator's side. An encrypted message will be sent from one user to another through our server. No one else will have permission to modify the recipient or the message content as it is sending.