**Banking App Security**

Motivation and Problem:

In Cpts 321, my team and I created a banking app simulation. In its current state, this app is very insecure. By choosing this project I will be able to expand my knowledge regarding asynchronous key and token-based communication protocols. It will also allow me to gain experience with implementing database access control.

Description of the Contribution:

In order to increase the security of the app, there are a few things that I need to do. First and foremost, I need it implement a user login and password hashing function to limit what data each user has access too. I will also have to add database access control to prevent unauthorized access to the database. Because this app simulates a banking system, it would be transmitting sensitive information, so I will have to implement either an asynchronous key encryption or a token-based authentication, such as TLS/SSL, to provide secure data transmission.

Proposed Milestones

The first milestone would be to implement a basic user login functionality utilizing a salted password hash. The next milestone would be to add a token/ticket-based authentication protocol such as TLS/SSL to provide secure communication between the backend and frontend. The third milestone would be to add MFA to the login functionality. The fourth milestone would be to add Access Control to the database to prevent unauthorized access.

Proposed timeline to accomplish the milestones

* Login with password hash
  + Redesign and update user table in database: 1-2 days
  + Compare hash functions: 1-2 days
  + Add password hash function: 1-2 days
  + Validate password recognition: 1-2 days
* Database Access Control
  + Determine user groups and permissions: 1-2 days
  + Create database users for each group: 1-2 days
  + Test user permissions: 1-2 days
* Design and implement Client-side interface: 1-2 weeks
* Add communication authentication: 1-2 weeks
* Add MFA: 1-2 weeks