Implemented Changes since 4/13

Updated Database Security:

Since our initial presentation, we have made some modifications to any and all connection strings used to interface between the application and the internal database. Namely, we have updated the connections to use the SSL mode of connection when sending data. More specifically, we have changed all connection strings to contain the following: "`SslMode=Preferred`".

Regarding the security of static data (stored within the database) we have documented the configuration and instructions on how to encrypt a new database in the System Manager Documentation. Furthermore, we are manually encrypting any passwords that would allow access to the data using a Bcrypt hashing algorithm. These aspects combined with the SSL connection string mentioned above mean that the only possible route to access the data would be through correctly guessing a user password.

Updated Password Requirements:

To better address this weakness of security, we have implemented requirements for all user passwords. These requirements are as follows:

- Passwords must be at least 8 characters long.
- Passwords must contain at least 2 capital letters.
- Passwords must contain at least 1 special character.
- Passwords must contain at least 2 numbers.

Our goal is to make all passwords less susceptible to brute force attacks by forcing each password to be either unique/difficult to guess or by being sufficiently long that the time it would take to guess makes it impractical.