Patrick O’Brien, Marco Rojas

5/1/2019

CSC 160 Combo

Final Project Proposal

For our final project, we would like to design a program that serves as a tool that can perform various hashing functions, primarily working with the MD5 hashing algorithm. One tool would allow the adding of users to a password database lists, either with or without salt on the password. We would like to show good practice of working with a strong hashing algorithm for passwords in this area and display the use of SHA-256 as an alternative to MD5 here. We will also allow a user to login, and their credentials are checked against the database. Another tool would be a dictionary password attack tool that would use the hashes from a list of supplied words to attempt to determine the plaintext of a list of unknown hashes.

To accomplish our project, there are several objects, files, and arrays. We will have classes that create 5 classes: one object that creates MD5 hashes from strings like passwords; one that creates MD5 hashes with salt added to the password; two classes that do the same tasks but for the SHA-256 algorithm; and the driver class. We will use arrays and files in the driver class to store data throughout the running of the program.

Patrick will complete the MD5 object class. Patrick will work on the password database, where a user can log in and their login is checked by adding salt to the password and comparing to the stored hash of the salted password in the database.

Macro will complete the MD5 password with salt object class. Marco will work on allowing a user to check a password against a list of known passwords and return whether the password has a match or not.

Both of us will work on the dictionary attack, comparing the hash each of the passwords on a long list of popular passwords, against an unknown hash to determine its identity with a string search.