John Ryan

CMPT 220

Professor Rivas

22 November 2016

Milestone

One of the biggest problems in today’s digital society is the threat of being hacked or having your identity stolen. One of the easiest ways into a person’s personal life is through an 8-digit combination that too many people take for granted the fact that it is known only to them. Having a person’s password can lead to stolen personal information, money, and many other much worse things. Sadly, people do not generally help themselves when it comes to making a password. All too often, you see someone’s password include their name, address, birthday, general words, or other personal attributes. Leaving such things in your password makes you vulnerable to hacks. The most common type of hacking recently has been dictionary hacking. This type of hacking takes a long time but is generally successful when it comes to passwords not intended to protect the user. Dictionary hacking usually uses a computer program which can make up to 1000 attempts at your password a minute by going through a list of common words, phrases, or letter combinations (Gil). Sadly, even I am guilty of not having a unique password or even different passwords for different accounts. Thus, the program I want to create consists of a random password generator that allows the user to personalize their password in a way that does not include personal information. With many websites requiring different things such as a symbol or numbers and letters, this program will allow the user to select the desired length, then choose the number of letters, numbers and symbols they would like.

The way I plan on approaching this project is first by creating three arrays, which consist of numbers 0-9, letters, and different symbols, respectively. Then I have prompted the user to input the number of characters he would like the password to be. Following that, the user is asked individually how many numbers they want, how many letters they want, and how many symbols they want. With this information, a for loop is created for each of the individual characteristics, the length of how long the user input. For example, if the user wants 4 numbers to be in his password, the loop will run four times. In the for loop, there will be a math.random function multiplied by the length of the original array. Then, these numbers serve as index numbers for the original array, and a new array is created. For example, if the user wants 3 letters, and the three random index numbers are {3,25,2}, then the new array using these index numbers is {c,z,b}.

At this point, that is all I have written thus far. My next course of action includes finding a way to join the three arrays I have created and then randomly arrange that array so that it is not three consecutive numbers, then two consecutive letters, then four consecutive symbols. Also, I want to make parameters for the inputs by forming an if else statement to catch if the user puts in something that violates the parameters. For example, if the user were to put in a letter instead of a number for the input, then it should send an error message to the user. Also, if the user puts in three numbers that do not equal the total characters that they originally wanted, the program will throw an error message.

In making this project, I hope to create a program which helps prevent people from making generic passwords and being subject to hacking or theft. I hope to further develop this program and hopefully make it more secure with the selection of the characters and also the final randomized array.

Bibliography

Gil, Paul. "What Is 'Brute Force' Dictionary Hacking?" *Lifewire*. N.p., 16 Sept. 2016. Web. 11 Nov. 2016.

UML Diagram

