Faculty of Engineering and Applied Science

Software Project Management - SOFE-3490U

Lab 2 - Graphical Password Strategy

Group Member 1

Name: Luke Hruda

Student ID: 100654666

Group Member 2

Name: Brittney Desroches

Student ID: 100649514

Group Member 3

Name: Peter Levine

Student ID: 100546643

Date: February 5th, 2020

Lab Section CRN: 74014

Introduction

Personal security is a top priority when it comes to personal devices and while the regular typed in password is relatively effective given that the password is complex, those unaware of the importance of a long, secure password may be easily hacked. The Graphical Password Strategy is an easy way to boost the complexity and increase the security of devices while still being simple enough for users to understand. Using a graphical password system increases the security against the traditional means of hacking, including brute force search, dictionary search, social engineering, and spyware attacks. With this system, the group hopes to create a viable system to increase the security of the user's devices while also making the user interface more simple for the users. The graphical password system also overcomes a variety of boundaries some users might have, like language or illiteracy, because of the visual component of this password system. This in turn though does create a problem for users with limited vision. With a Graphical Password Authentication system, the overall goal is to increase security and user-password retention.

Objectives

For the Graphical Password Authentication system, there are a number of metrics required to build a secure password system. These metrics include security, reliability and speed.

The first objective is to be more secure than a standard text-based password system. For a traditional text-based password system, where only numbers and characters are allowed, there are thirty-six possible options for a single space of the password. The inherent strength of a password that is eight characters long would have over two-trillion combinations.

$$36^8 = 2{,}821{,}109{,}907{,}456$$

This eight-character password is then run through a hashing algorithm (usually MD5) where it is converted into what would be considered gibberish to the average person, where it is stored in a database. The password "password" would appear as "5f4dcc3b5aa765d61d8327deb882cf99" if put through an MD5 hashing algorithm. If we were to change this to a system where an arbitrary one hundred images, where the user was to select a sequence of eight images, this changes to ten quintillion options.

$$100^8 = 10,000,000,000,000,000$$

Initially, this is already one thousand more possible combinations for a sequence of eight images versus eight characters. This would allow for an increase password security against brute force attacks, as even if the MD5 hashed sequence of images are acquired by a malicious third party, they will have no way of matching the hash sequence to the images.

The second object of the login system will be to support users who use identical passwords. Where despite there being a large number of combinations for passwords, there will always be a chance that two users of a system will select the same sequence of images for their password. The signup service will work in conjunction with the database responsible for storing user data will ensure no two users will be allowed to use the same username/email login. As the

username or email will be the primary identifier for an account, duplicates of which will not be allowed.

The third objective for the system is to have high usability, allowing users a variety of distinctly different images to select from. A bad example of this is if all the images were different bodies of water, the user would have an incredibly difficult time remembering which images they select, let alone the correct sequence of them. Each image in the set will have to have a unique aspect in them to allow the user to remember their specific images. An example of this would be a user picking a password sequence of:

A Dog -> A Dump Truck -> A Fridge -> A Fork

Ensuring that in the set of pictures, there is only one photo of a Dog, a Dump Truck, a Fridge, and a Fork in the set of images, will allow the user to remember the images they select based off of the main object in the frame of the photo.

The fourth objective will be that once the graphical password is entered and the user presses submit, the sequence of images will authenticate in the same time frame like a traditional text-based password.

The fifth objective will be the longevity of the system. Images will be stored on the server-based storage system to ensure they will always be available so long as the client and the system host are connected to the internet.

Project Measures of Success

The primary goal of this project is to create a password system that is more secure than a text-based password and more user-friendly. The main metric used to measure the success of implementing these goals is customer satisfaction. To ensure high customer satisfaction, the project must meet the customer's expectations with a high degree of quality. Additionally, the project should stay on schedule and achieve a final budget within reasonable bounds to what was set by the customer and project management at the start of the project development.

During project testing and prior to deployment the project should perform with reliability and quickness, as defined in the initial business case. The systems database will store the hashed image identifier combination required for each user's password. Finally, the engineers working on this project should be satisfied with their contributions and not work under a time crunch or feel pressured due to management factors outside of their control.

Equipment

The graphical password application will be hosted attached to whatever website it is incorporated into. To program the system, we will use the standard web development languages of HTML5, Javascript, and CSS. A web server will be required to host this application, with a storage system attached to it to store sequences of images, and user login information. For a user to access the system, they will have to use their own personal computer.