

A prototype of Hotel Management System with a Secured Graphical Password to Avoid Shoulder Surfing Attack

Deshinta Arrova Dewi¹ and Alberto Santiago Ayong Angue Nchama², Lai Mei Yoon³

^{1,2,3} Faculty of Information Technology and Sciences (FITS), INTI International University, Nilai, Negeri Sembilan, Malaysia.

Corresponding Author: deshinta.ad@newinti.edu.my

Abstract

This paper mainly focuses on two things: secured graphical password and hotel management system. The aim of this study is to propose a new Hotel Management System that is secured from a shoulder surfing attack using a graphical password. This graphical password has been introduced by previous research and this paper offers a contribution to implement it into a hotel management system. Hotel management system has been chosen for this study because they are considered as people second home whereby personal information resides in hotels and the confidential information of the Hotels themselves are registered and kept in the Management System. The Management System has to deal with day to day activities, therefore, it has to be secured and the best way of doing so is to set a password. Passwords are used to authenticate real users from attackers, the most common Computer Authentication Method is to make use of alphanumeric usernames and passwords. There are significant drawbacks to this method because passwords are easily guessed by the attackers. To overcome this problem, the use of Graphical Password Authentication is introduced for Hotel Management System as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication and significantly able to avoid shoulder surfing attack. The PHMS is developed using SQL server 2014, the ASP.NET and the C# programming language for a recreation of the secured graphical password.

Keywords

Graphical Password Authentication, Shoulder Surfing Attack, Hotel Management System

Introduction

A large number of Hotels are still using alphanumeric passwords methods in their Management Systems and that makes their systems vulnerable to hacking because alphanumeric password method is no longer a secure method of protecting a system. The proposed graphical technique is an improvement of the alphanumeric password and it is based on using colors during the registration and verifications phases (Varghese, L., Mathew, N., Saju, S., & Prasad, V. K. (2014). The string proposed in this technique, it is composed of sixteen characters divided in eight lower cases letter from “a to h” and eight numbers from “1 to 8” (nevonprojects, n.d).

During the registration phase, firstly the user is asked to provide all necessary registration details requested by the system, and the most important detail will be the e-mail address. Secondly, the user is asked to enter his or her alphanumeric password from the characters provided. Thirdly, the user will be asked to select a color which will have to remember from several provided.

When a successful registration is done, the user can try to log in by providing the e-mail entered in the registration phase. After a successful authentication of the email address, the user will proceed with the graphical password where will have to enter his or her alphanumeric password previously chosen by selecting the characters using the chosen color in the way that the system will present them.

As a response, the Prototype of Hotel Management System (PHMS) display a circle composed of eight equally sized sectors. The colors of the arcs of the eight sectors will be different, and each sector is identified by the color of its arc, e.g., the red sector is the sector of the red arc. Initially, sixteen characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the “clockwise” button once or the adjacent sector counter clockwise by clicking the “anti-clockwise” button once (nevonprojects, n.d).

This concept has been introduced by the previous researcher in Varghese, L., Mathew, N., Saju, S., & Prasad, V. K. (2014). This paper recreates the previous graphical password and attaches it as a feature extension for the PHMS. Accordingly, the PHMS contains features as follows:

For Manager:

- Login (with Graphical Password): The manager does not have to register in the system, because a default email Id, pass-color and password as set for him/her, but can still change or update the pass-color and password whenever needed.
- The following access are defined: Add Rooms, Add Staff, Add Expense, Approve Booking, Check In Guest User, Check Out Guest User, View Booking, View Expense, Manage Staff and Log Out

For Employee / Staff:

- Login (with Graphical Password): As it is explained previously, the manager is the one in charge of registering the staff in the system. The staff will have to make use of the email id, pass-color, and password that the manager will provide to him/her when trying to log in the system. The staff member will only gain access to the system if the details entered match the ones entered during the registration.
- The following access are defined: Check In Guest User, Check Out Guest User and Log Out

For Guest User:

- The following access is defined: Register, Login (with Graphical Password), View Profile, New Booking, View Booking Status, Cancel Booking, and Log Out.

The objectives of this paper are defined as follows:

1. To study the requirement of hotel management system with a secured graphical password.
2. To recreate the graphical password based on previous research and integrate with the hotel management system.
3. To conduct testing towards the prototype of the hotel management system.

Methodology

In this paper, the following methods are carried out to fulfill the above objectives:

1. Requirement Gathering and Quick Design

At this stage, literature reviews that related to hotel management system and graphical password are conducted. Afterward, the data collection through questionnaire and interviews are performed to obtain more insights about the requirement of PHMS. The findings at this stage are used as guidance in developing the PHMS.

2. Development and Refinement of the PHMS

The PHMS is developed using SQL server 2014 as back-end technology (database). The front-end system development uses ASP.NET technology and the recreation of the secured graphical password using the C# programming language. The following interfaces are presented as results of the development.

Figure 1 is the user's main login page that allows three types of users to enter the PHMS. Figure 2 that shows the interface for guest registration when a guest attempts to log in. Figure 3 shows users login page after registration.



Figure 1. Users Main Login Page



Figure 2. Guest User Registration Page

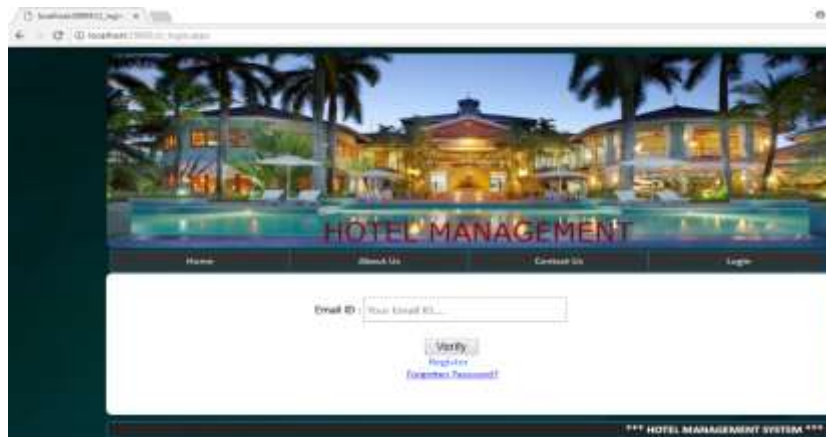
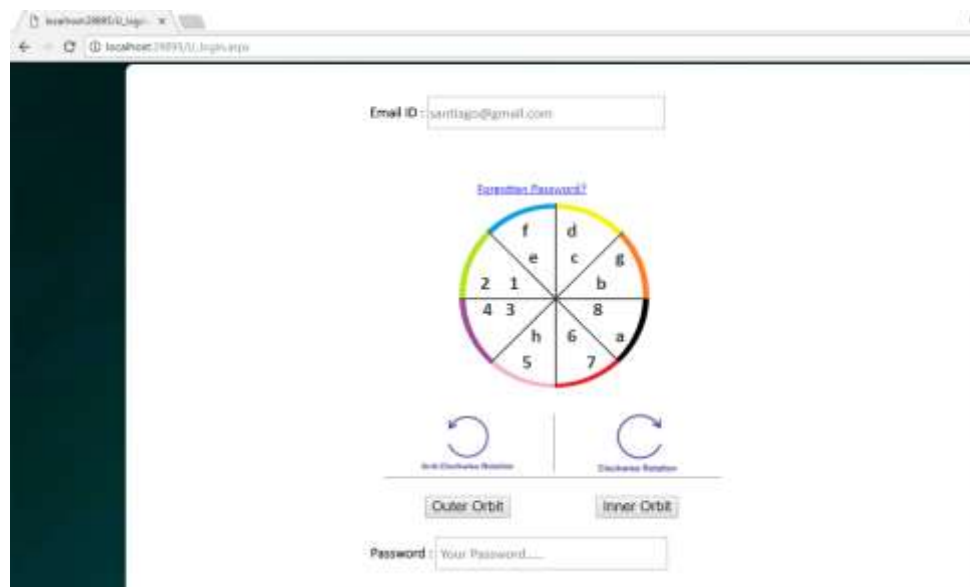


Figure 3. Users Login Page

The following figure 4 the secured graphical password that is created based on works of previous research. The secured graphical password is attached in the PHMS to an extension of security feature to avoid the shoulder surfing attack.

4.



Figure

Graphical Password Authentication

The circle in the graphical password consist of eight sectors whereby the colors of the arcs of the eight sectors are different. Each sector is identified by the color of its arc, e.g., the red sector is the sector of the red arc. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the “clockwise” button once or the adjacent sector counter clockwise by clicking the “anti-clockwise” button. By having this kind of techniques, the password character is entered into the text box without typing via the keyboard. This method is proven to be able to avoid the shoulder surfing attack.

3. Testing towards the PHMS development

The testing that has been carried out in this study consists of black box testing, unit testing, and integration testing. The one that is presented in this paper the unit testing results that involves modules with a secured graphical password.

Results and Discussion

There are two main parts is presented in this section: the results of data collection to study the requirement of the PHMS and results of unit testing after the development of the PHMS.

Part 1: Results of data collection before the development of PHMS

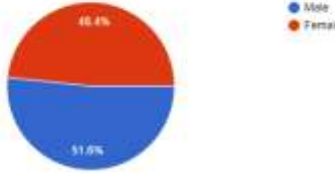
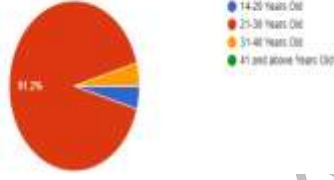
<p>91 respondents</p>  <p>Question 1: Kindly specify your gender as provided below:</p> <p>In this questions, the author had 91 respondents and 48.4% are male while 51.6% are female.</p>	<p>91 respondents</p>  <p>Question 2: Kindly specify your age as provided below:</p> <p>The author had 91 respondents, 91.2% are from 21 to 30 years old, 4.4% are from 14 to 20 years old and the rest 4.4% are from 31 to 40 years old as well.</p>
---	---

Table 1. Results of Question 1 and Question 2

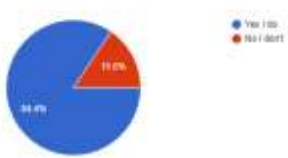

<p>90 respondents</p>  <p>Question 3: Do you make use of the hotels' reservation system to make bookings?</p> <p>According to the findings, the author had 90 respondents to this questions and 84.4% of them make use of hotels' reservation system while the rest 15.65 does not make use of those systems.</p>	<p>87 respondents</p>  <p>Question 4: If your answer from the previous question is YES. How often do you use the hotels' reservation system to make bookings?</p> <p>There are 87 respondents to this questions and 55.2% make use of the reservations systems sometimes while 26.4% make use of them irregularly and the rest 18.4% of respondents make use of those reservation systems every single time they reside in hotels.</p>
--	--

Table 2. Results of Question 3 and Question 4

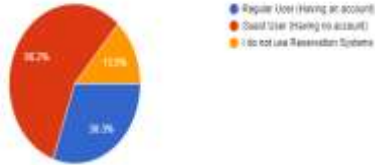
<p>89 respondents</p>  <p>Question 5: If you make use of the hotels' reservation system. How do you make bookings as? Most of the reservation systems provide the customers two options to make the bookings as. For this questions, the author had 89 respondents and 56.2% of them make a booking as guest users while 30.3% make bookings as regular users and the rest 13.5% stated that they do not use reservations systems.</p>	<p>Question 6: Have you (Either the regular user or guest user) ever experienced any misuse of your personal information by the management system of a hotel? If your answer is Yes, please specify.</p> <p>All of the respondents stated that they have not experienced any misuse of their personal information while one of them misunderstood the question and stated that, once they misunderstood his requirements by providing him a two beds room while he requested a three beds room.</p>
--	---

Table 3. Results of Question 5 and Question 6


<p>Question 7: If you own an account for hotels' reservation system. Has your account ever been hacked due to lack of security in the system? If your answer is Yes, please specify.</p> <p>➤ There are 62 respondents to this question and 60 of them stated that their accounts have never been hacked while 1 of them is unaware whether or not his/her has been hacked and the last one stated that he/she does not own an account.</p>	<p>91 respondents</p>  <p>Question 8: How safe do you think that your personal information is with the type of password provided in the hotel reservation system that you have ever used?</p> <p>There are several types of passwords and each hotel management system has implemented one of them of security aspects. The author had 91 respondents to this questions and 34.1% of them have never thought about the security of their personal information while using those systems. 31.9% stated that their personal information is pretty safe; 19.8% stated that their personal information is no safe at all while the rest 14.3% assured that their personal information is strong safe with the type of password provided in the system they have used.</p>
---	--

Table 4. Results of Question 6 and Question 7

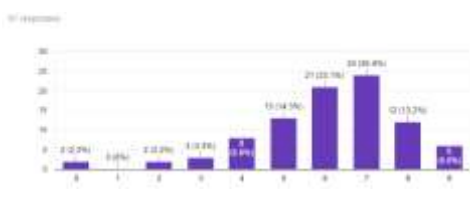
 <p>Question 9: If you were to rate the hotels' reservation system on a scale from 0 to 9, what would be your rating?</p> <p>The author wanted to know how good the hotel's reservation system is by asking the customers to provide their ratings in a scale from 0 to 9, bearing in mind that the rating 0 is the worst and 9 is the best. There are 91 respondents in this question, 2.2% rated 0; 2.2% rated 1; 3.3% rated 2; 8.8% rated 3; 14.3% rated 4; 23.1% rated 5; 26.4% rated 6; 13.2% rated 7; 6.6% of the respondents rated 8, and 6.6% of the respondents rated 9.</p>	<p>Question 10: If you were to suggest a feature to improve the security of hotels' reservation system, which features would it be?</p> <p>To know the aspects where the hotel's reservation system has to be enhanced, the author asked for suggestions from the customers and some of the highlighted suggestions have done with a better way of making payments online; more secure and strong password methods, and a more secure database design for keeping customers data with encryption.</p>
--	---

Table 5. Results of Question 6 and Question 7

Part II: Results of unit testing towards PHMS after development.

Unit testing is the type of testing can be considered the first step where the developer carries out different tests on the different functions or units of the system. This is very important as the developer needs to make sure each module works perfectly before it can be integrated into the main system. Errors and problems encountered during testing can be easily corrected.

The following tables 6 and 7 show the unit testing that consists of secured graphical password in the unit. Table 6 depicts the results of unit testing towards registration module. Table 7 depicts results of unit testing towards login module. Both modules employ the secured graphical password and this makes both modules as critical that need extra attention.

No	Test Field	Expected Result	Actual Result
1	Name	Users can enter any username they want. It can be a mixture of letters, numbers and other characters. All usernames must be unique. The field cannot be left empty, otherwise, an error should be given	Same as expected
2	Contact Number	Users can enter any contact number they want to and it can be from any region around the world. The field cannot be left empty, otherwise, an error should be given	Same as expected
3	Email ID	Users can enter their email. Anything other than a valid email will be rejected by the system	Same as expected
4	Address	Users can enter any address they want and it can be composed of any set of letters, numbers, and characters without error-prone	Same as expected
5	Password	Users must only enter a password composed of numbers from 1 to 8 and letters from a to h as it is required by the system	Users can still enter any letter, number, and character that it is

			supposed not to be accepted by the system
6	Password Color	Users can select their pass-color from the eight colors provided	Same as expected
7	Submit Button	Completes the registration process if everything is filled correctly, otherwise gives errors on specific fields. When everything is correct, it submits all the information to the database and takes the users to the login page	Same as expected

Table 6. The registration unit testing

No	Test Field	Expected Result	Actual Result
1	Email ID	Allows the users to enter their email id	Same as expected
2	Verify Button	Verifies whether the user email matches the ones in the database. When matching it takes the user to the password field, otherwise, an error message is shown	Same as expected
3	Anti-Clockwise Rotation Button	Allows the users to rotate the arc in an anti-clockwise direction	Same as expected
4	Clockwise Rotation Button	Allows users to rotate the arc in a clockwise direction	Same as expected
5	Outer Orbit Button	Allows users to select the letter or number located on the outer side of the arc	Same as expected
6	Inner Orbit Button	Allows users to select the letter or number located on the inner side of the arc	Same as expected
7	Password	Displays in an encrypted form the letters and numbers selected by the users using outer and inner orbits	Same as expected
8	Confirm Button	Takes the users to the main features page when the password has been correctly entered, otherwise it takes to Try Again button	Same as expected
9	Try Again Button	Allows users to reenter their password once again. After clicking, it takes users back to Confirm Button	Same as expected
10	Forgotten Password	Allows users to proceed to password reset form	Same as expected

Table 7. The login unit testing

Conclusions

The PHMS has successfully developed an alternative of hotel management system that integrates with the secured graphical password following the methodology mentioned in this paper. As a prototype, the PHMS has shown an alternative technique to prevent shoulder surface attack that may occur in the hotel management system. The idea of PHMS with the secured graphical password is applied as final year project in Bachelor of Computer Science (BCSI) in INTI International University, Nilai Campus, Malaysia.

References

Varghese, L., Mathew, N., Saju, S., & Prasad, V. K. (2014). 3-Level Password Authentication System. Department of Information Technology, Amal Jyothi College of Engineering, Kanjirappally, Kerala, India.

Arise, 2011, Authentication Schemes for Session Passwords using Color and Images. Retrieved from <http://airccse.org/journal/nsa/0511jnsa08.pdf>

Noveonprojects, (n.d.), Security projects ideas. Retrieved from <http://nevonprojects.com/graphical-password-to-avoid-shoulder-surfing/>

Ralph Heibutzki, (n.d.), Safety & Security Tips for Hotel Management. Viewed 12 September 2017, <http://work.chron.com/safety-security-tips-hotel-management-7983.html>

C.R. Kothari, 2014, Research Methodology: Methods and Technologies. Retrieved from <http://dspace.tiss.edu/jspui/bitstream/1/7047/1/Research-MethodologyMethods-and-Techniques-by-CR-Kothari.pdf>

Systemanalysisanddesigns, 2017, Systems Analysis and Design. Retrieved from <http://www.systemanalysisanddesigns.com/characteristics-of-a-system/>