IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Color Grid Based Authentication Session Using Hash Technique

Prof. Renuka Nagpure[1], Harsh Desai[2], NinaadSuvarna[3], Dipen Desai[4], Simranjeet Singh Chawla[5]

Department of Information Technology, Atharva College of Engineering, Mumbai, Maharashtra, India[1,2,3,4,5]

Abstract: Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced 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 colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, we proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

Keywords: Authentication, cryptographic hash function, graphical password schemes, session passwords.

I. INTRODUCTION

The most common method used for authentication is textual password. The vulnerabilities of this method like eavesdropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as fingerprints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow.

There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices.

In this paper, two new authentication schemes are proposed for PDAs. These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication schemes use text and colors for generating session passwords.

Literature Survey: A graphical authentication scheme [1] has already been proposed where the user has to identify the pre-defined images to prove user's authenticity. In this scheme, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre-selected images for authenticating the user from a set of images. However, this system is vulnerable to shoulder surfing.

Pass face [2] is a technique in which the user sees a grid of nine faces and selects one face previously chosen by the user. Here, the user chooses four images of human faces as their password and the user has to select their password image from eight other decoy images. Since there are four user selected images it is done for four times.

II. METHODOLOGY

Existing System: Currently there are no such authentication schemes except for plain text username and password scheme.

Proposed System: Authentication technique [3] consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or selects the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen to the user. The system verifies the password entered by comparing with content of the password generated during the registration process.

During registration, user should rate colors as shown in figure. The user should rate colors from 1 to 8 and he/she can remember it as "RLYOBGIP". Same rating of colors can be given to different colors. During the login phase, when the user enters his username an interface is displayed on the screen based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 10. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

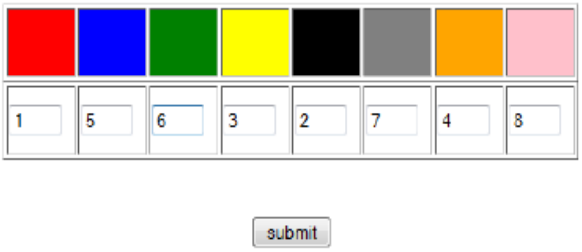
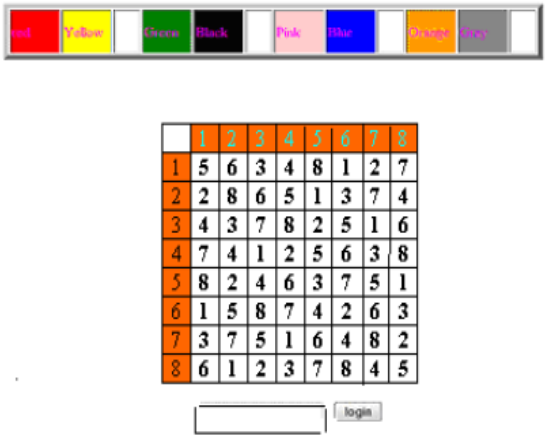


Figure above shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represent row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure above ratings and figure below login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e 3. The same method is followed for other pairs of colors. For figure below the password is "3573". Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.



This system will be developed for a Financial Broker who has all the financial information about the clients stored in the software. After Secured Login into the System User of the software will be able to access the following modules.

1) Secured Login
2) Add / Update / Delete / View Clients Information
3) Add / Update / Delete / View Clients Assets Information
4) Add / Update / Delete / View Clients Liabilities Information
5) Generate Assets Reports
6) Generate Liabilities Report

In addition to the above security we will include Hash Encryption Algorithm as well for enhanced Security.

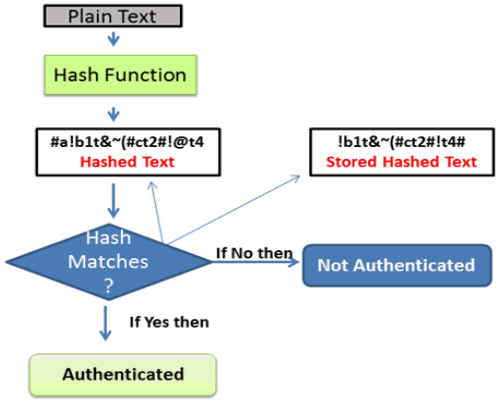


Fig: Flow Chart Example of Has Work

Cryptographic Hash Function: A cryptographic hash function [4] is a type of hash function which is considered practically impossible to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the message, and the hash value is often called the message digest or simply the digest.

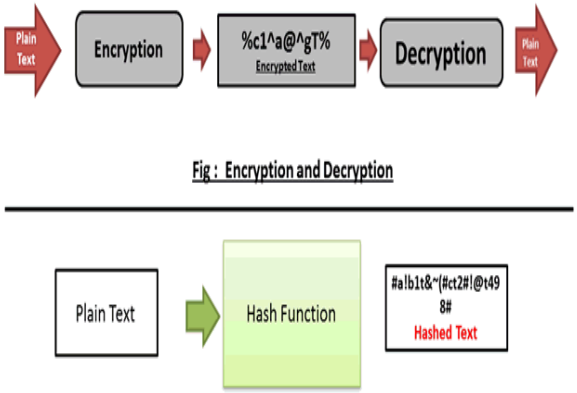


Fig: Hashing Concept

The ideal cryptographic hash function has four main properties:

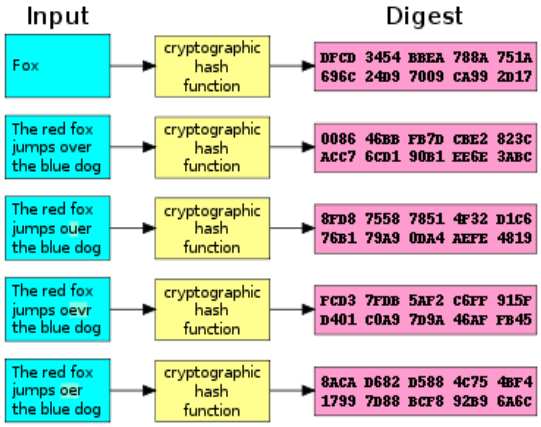
- Easy to compute the hash value for any given message.
- Infeasible to generate a message from its hash.
- Infeasible to modify a message without changing the hash.
- Infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information regarding security applications, notably in digital signatures and message authentication codes (MACs). They can also be used to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called fingerprints, checksums, or just hash values.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

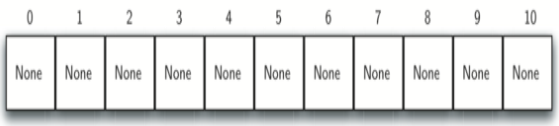


III. HASHING TECHNIQUE

In this, we attempt to build a data structure that can be searched in O (1) time. This concept is referred to as hashing.

In order to do this, we will need to know even more about where the items might be when we go to look for them in the collection. If every item is where it should be, then the search can use a single comparison to discover the presence of an item. We will see, however, that this is typically not the case.

A hash table is a collection of items which are stored in such a way as to make it easy to find them later. Each position of the hash table, often called a slot, can hold an item and is named by an integer value starting at 0. For example, we will have a slot named 0, a slot named 1, a slot named 2, and so on. Initially, the hash table contains no items so every slot is empty. We can implement a hash table by using a list with each element initialized to the special Python value None. Figure shows a hash table of size m=11. In other words, there are m slots in the table, named 0 through 10.

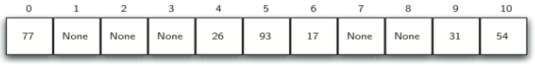


The mapping between an item and the slot where that item belongs in the hash table is called the hash function. The hash function will take any item in the collection and return an integer in the range of slot names, between 0 and m-1. Assume that we have the set of integer items 54, 26, 93, 17, 77, and 31. Our first hash function, sometimes referred to as the "remainder method," simply takes an item and divides it by the table size, returning the remainder as its hash value (h(item)=item%11).

Table below gives all of the hash values for our example items. Note that this remainder method (modulo arithmetic) will typically be present in some form in all hash functions, since the result must be in the range of slot names.

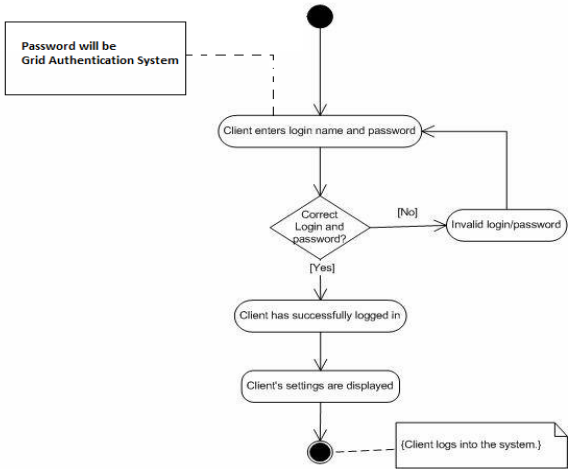
Item	Hash Value
54	10
26	4
93	5
17	6
77	0
31	9

Once the hash values have been computed, we can insert each item into the hash table at the designated position as shown in Figure below. Note that 6 of the 11 slots are now occupied. This is referred to as the load factor, and is commonly denoted by λ=number of items table size. For this example, λ=611.



Now when we want to search for an item, we simply use the hash function to compute the slot name for the item and then check the hash table to see if it is present. This searching operation is O(1), since a constant amount of time is required to compute the hash value and then index the hash table at that location. If everything is where it should be, we have found a constant time search algorithm.

You can probably already see that this technique is going to work only if each item maps to a unique location in the hash table. For example, if the item 44 had been the next item in our collection, it would have a hash value of 0 (44%11==0). Since 77 also had a hash value of 0, we would have a problem. According to the hash function, two or more items would need to be in the same slot. This is referred to as a collision (it may also be called a "clash"). Clearly, collisions create a problem for the hashing technique.



IV. SECURITY ANALYSIS

As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

PDAs because it is difficult to capture the interface in the PDAs.

Dictionary Attack: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session. In hybrid textual scheme, the randomized colors hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of colors. Even by knowing session password, the complexity is 8x4. So these are resistant to shoulder surfing.

Guessing: Guessing cannot be a threat to the pair based because it is hard to guess secret pass and it is 36x4. The hybrid textual scheme is dependent on user selection of the colors and the ratings. If the general order is followed for the colors by the user, then there is a possibility of breaking the system.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368. In the case of the Hybrid Textual Authentication Scheme the complexity depends on colors and ratings.

V. RESULTS

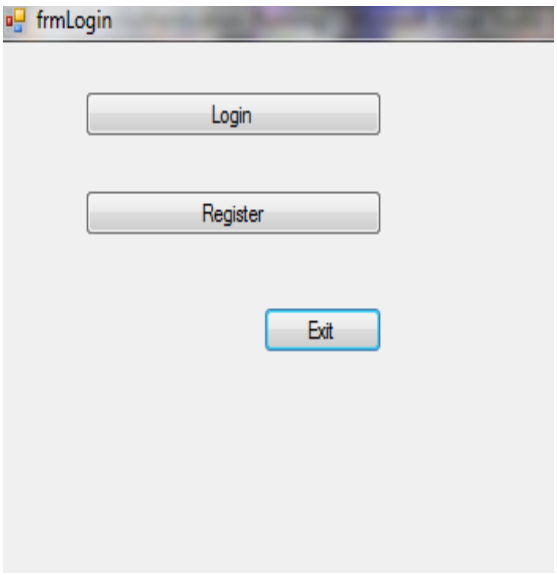


Fig: First Page of Login and Register

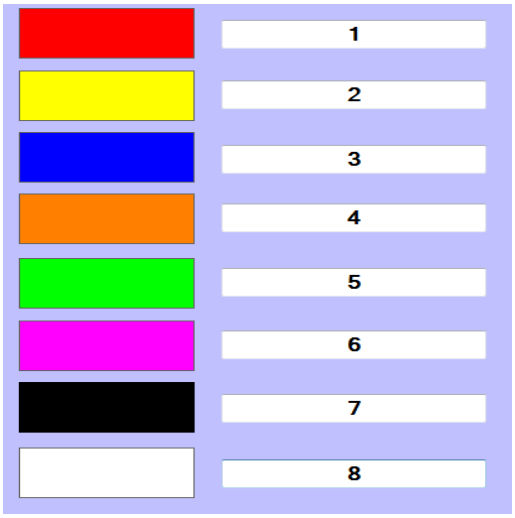


Fig: Registration Giving Rating to Colors

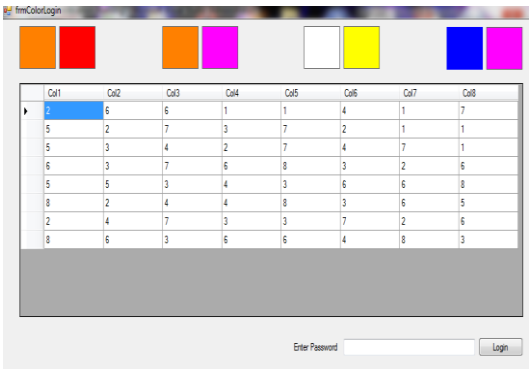


Fig: Generation of Color Grid

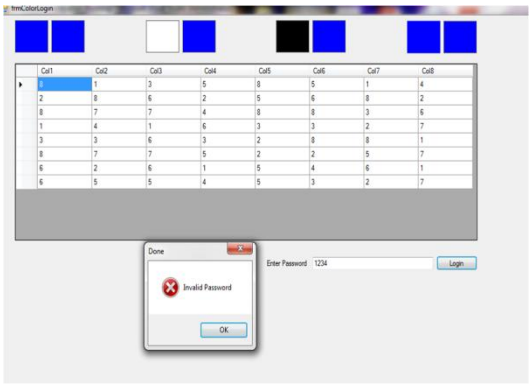


Fig: Invalid Login Attempt

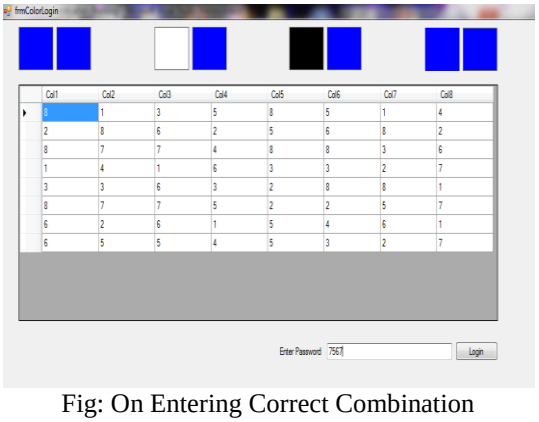


Fig: On Entering Correct Combination

DOI 10.17148/IJARCCE.2016.5496

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

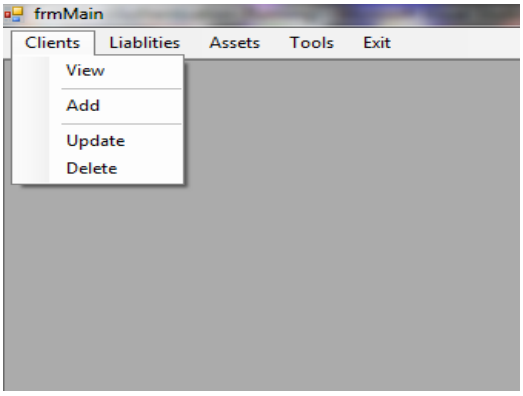


Fig: Finance Application

VI. CONCLUSION

In this project, two authentication techniques based on text and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration; during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

REFERENCES

[1]. R. Dhamija, and A. Perrig, "Déjà vu: A User study Using Images for Authentication", in 9th Unisex Security Symposium, 2000.
[2]. Real User Corporation: Passfaces. www.passfaces.com
[3]. Authentication Schemes for Session Passwords using Color and Images International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[4]. Scheier, Bruce, "Cryptanalysis of MD5 and SHA: Time for a New Standard", Computerworld, retrieved 15 October 2014.