Dynamic Cryptographic Algorithm to Provide Password Authentication using Cued Click Points

P. Ashok
Department of Computer Science and Engineering, Sri Sairam Institute of Technology, Chennai, India

Article Info

Article history:

Received Feb 21, 2017
Revised Jun 26, 2017
Accepted Jul 19, 2017

Keywords:

Authentication
Authentication protocol and password based authentication
Cued Click Points
Encryption
Password
Security

ABSTRACT

Nowadays, password based authentication is one the most common way of authentication for most of the user logins. However, the advancement in technology also posing many threats for the password authentication systems. Everybody will be keen to know others password. But there exists a very few who is very keen to devise a new authentication. In this paper, we have proposed a more advanced password authentication method yet a simple one which gives a tough competition for the attacker to break the password. For this, we are providing a special key-display interface to assist the modified cued click point's technique which helps in the more sophisticated dynamic authentication method. This interface helps to break the single password into a combination of 4 passwords and also adds three more password strings to the current password which is entered. It also uses a special one way encryption algorithm called Nesting 93 which is developed explicitly for this system. It helps to prevent almost any kind of attacks.

Corresponding Author:

P. Ashok,
Department of Computer Science and Engineering,
Sri Sairam Institute of Technology ,
Chennai, India
Email: ashokit009@gmail.com

1. INTRODUCTION

Security has been the most annoying problem in the recent years. Especially providing access to an authenticated user is definitely not as easy as it looks. All the users may want to have a more secured authentication system but no one seems to be compromised with the usability of the system. While making the authentication scheme more complex can be considered as one way but it is very important to have the complexity in the attacker side and not in the user side itself. To address this problem, we provide the combination of the password field and the key interface along with the modified cued click points which helps to produce a more sophisticated authentication scheme.

Cued Click Points (CCP) was generally designed to minimize pattern and to minimize the usefulness of hotspots for attackers. Instead of 3 click points on one image, Cued Click Points uses single click on three dissimilar images [1-3]. In modified CCP, instead of using click points on images we use Click Points on the key interface which was provided and this helps to break the password into a combination of 4 passwords. Also a one way encryption technique has been explicitly developed for this system. All these days we have been using one way hashing algorithm. It is a logical algorithm that helps in mapping information of whimsical range to a byte string of a specified size (an hashing function) which has been designed to also be a one way function, that is a function which is not feasible to transpose. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a "rainbow table" of matched hashes. This makes it a disadvantage for the system.

Another way of encrypting your password that has been used widely but more insecurely is encryption using key values. For encryption algorithms, a key specifies the transformation of plaintext into cipher text, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

2. LITERATURE SURVEY

Password authentication scheme using session based passwords in which it uses two session techniques for generating session bases passwords one is using the set of pairs of hidden passwords and the other is using the color rating while setting the password but both uses the grid structure to generate the password [4-6]. Knowledge based authentication scheme which uses a combination of both text and graphical passwords and persuasive cued click points assist in choosing the graphical passwords [1], [7- 8]. A study on various authentication schemes and provides a graphical authentication technique using recognition and recall based techniques [9]. A web based password authentication scheme which resolves the problems in the traditional password authentication or digital signature using Single-Block Hash Function [10]. Deals with secure authentication and transaction protocol by combining digital certificates and dynamic password by realizing the mutual authentication that exists between the client and the server [11].

3. VIEW ON CUED CLICK POINTS

Cued Click Points (CCP) a cued-recollect graphical password technique where users click on any one point in an image for the sequence of images. The upcoming image which is shown to the user is based on the previous click point. The results were positive. Performance was very excellent in terms of speed accuracy and number of mistakes. Users preferred cued click points to Pass Points saying that choosing and remembering only one point in one image is easier, and that seeing each image triggered their memory of where the respective point was located. Cued click points appears to allow greater security than Pass Points; the workload for attackers of CCP can be arbitrarily increased by augmenting the number of images in the system.

Recognition may it be through images or others is the easiest way for human memory where pure or complete recollect is most difficult as the data must be accessed from memory with no triggers [12]. Cued recollect through images falling somewhere between these two since they offers cue which should showcase context and trigger the stored memory.

4. EVOLUTION OF THE SYSTEM

The disadvantage of the cued click point system is, it is very tedious to click the images every time when you login to the system and it's too time consuming. There comes the system to overcome the disadvantage. The image that has been used for cued click points has been modified as keypad system in the proposed system interface.

The system has been developed so as to provide flexibility to the users in all possible way and to increase the work of the hackers. The entire encryption technique resides inside the key interface of the system.

5. IMPLEMENTATION

In this, the proposed system consists of a password field along with the special key display interface. This interface consists of ten set of keys numbered from 0 to 9. Each key is assigned to a set of twelve digit alpha numeric character and the constraint that has been specified to every single user of the system is that, the user has to select at least three to five clicks in the key interface each time when the user wants to login to the system. The clicks in the interface are made along with the password. User can just type the password in the password field and that password can be an alpha numeric one. But the other constrain is the password should eventually begin with an alphabet.

The flexibility given to the user in this system is the user can have the click points anywhere in the password. May it be at the last or at the middle or in between the password? The entire encryption of the system resides inside the keys. The keys that are typed also belongs to the password, i.e., the keys selected belongs to your password but the keys that have been selected will not be visible in password field.

If suppose your password is "crypt124" where the numerical have been clicked through the mouse in the key interface, the numerical values that have been clicked will not be visible in the password field even as a hidden text. Here comes the other advantage of preventing our system from being attacked from brute force attack.

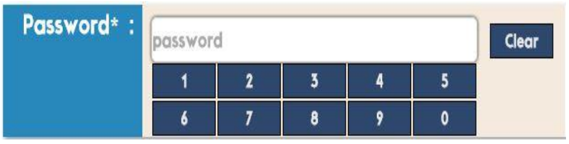

Figure 1. A special key display interface for our system

This system breaks the user's conventional single password into a set of four passwords and also adds a set of three strings while entering using the interface. So typically it sends seven set of strings to the encryption process in spite of the single password which is given by the user. This seven set of strings is taken as the input for the one way encryption algorithm called One-time Data Division (ODD).

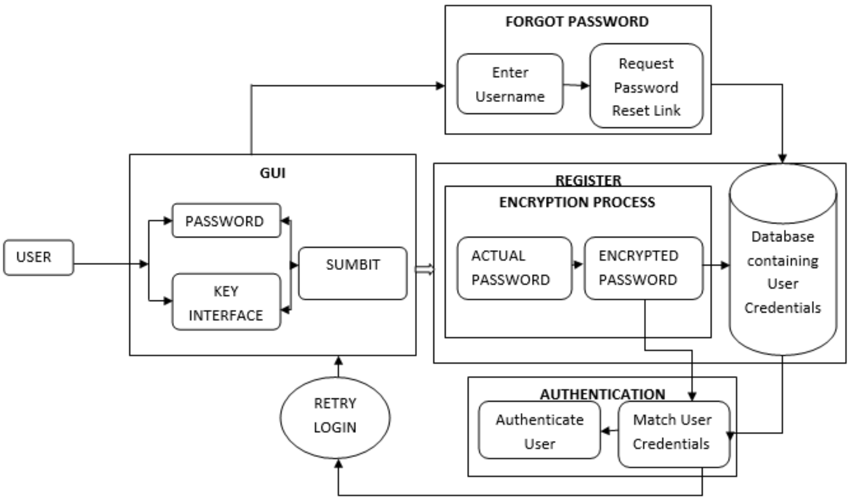

Figure 2. Architecture diagram of the system

Let us take a look at what happens when the user enters the password in a step by step process:

For example if the user enters the password as "cryptopassx3y2z1" then in this password the numeric characters 3,2 and 1 are the numbers which should be used in the interface.

a. User enters the password "cryptopassx" in the password field.
b. User clicks the key '3" in the key-interface while the content in the password field is still "cryptopassx". Now the current input to the system is "cryptopassx" and the six digit alpha numeric string which is assigned to key "3"
c. Now the user again enters "y" in password field along with "cryptopassx". Now the password in password field is "cryptopassxy".
d. Now the user clicks "2" in the interface while the content in the password field is still "cryptopassxy". Now the current input to the string is of four strings two from password field and two from the interface.
e. Again the points 3 and 4 are repeated.
f. Finally when user enters the submit button the current password field content "cryptopassxyz" will also be taken as the input. Therefore totally seven strings will be passed to the encryption algorithm. Four from the password field and three from the interface.
g. This seven set of strings will be used in the encryption algorithm called "One-time Data Division (ODD)" which is developed explicitly for this system.

After the encryption process, we will get an encrypted string which consists of all the 93 printable characters available except the blank space. This encrypted password is made of up of exactly 256 characters which will be stored in the database. So whenever the authentication occurs, the encrypted password from the user is compared with the encrypted password stored in the database. This is a one way encryption algorithm so it cannot be decrypted to its original form. If the user lost his password, then he can only reset the password by requesting a password reset link through the username.

6. ONE-TIME DATA DIVISION (ODD) ALGORITHM

It is named as "One-time Data Division (ODD)" since it uses the Divide as well as Nest concept which can be inferred from the name itself. 93 is derived from the fact that our final encrypted password consists of 93 printable characters in the ASCII value range from 33 to 125 which includes all the numbers, characters & special characters.

6.1. Core of the Algorithm

The Divide and Nest concept is that each password string gets divided into a single character and the alpha numeric string is inserted or nested between those characters and then combined and the process goes on for the rest of the string then it goes through a set of several transformations which remains the core of the algorithm.

This algorithm produces a string of 256 characters which is a combination of all the 93 printable characters except the blank space. Since this is a one way encryption algorithm, even the system administrator doesn't have any rights to access the user profiles and the user profile is highly secured.

This encryption algorithm can be easily customized for individual organization and instead of six digit alphanumeric characters we can use alpha numeric string of different lengths which increases linearly with 2. As the length increases, the complexity increases and the pattern formation becomes further strong.

6.2. Steps Involved

Steps involved in the One-time Data Division (ODD) algorithm:

a. The system receives a set of seven strings as input, four from the password field and three from the key interface
Let,

(i) The four set of password
strings -> p1, p2, p3 and p4

(ii) The three key values -> c1,
c2, c3

(iii) I1, I2, I3 etc. be theintermediate string formedduring the encryptionprocess.

b. Initially p1 and c1 is combined or nested or joined in a special way to produce an intermediate string I1.
p1⋈c1 —> I1
c. This I1 along with p2 and c2 is combined or nested using a special count value to produce I2.
P2⋈ c2 —> I2
d. The step three is repeated for p3 and c3 to produce I3.
P3⋈ c3 —> I3
e. An I4 is produced from I3 and p4. **I3⋈ p4 —> I4**
f. The currently formed string I4 is changed into a set of numbers using its equivalent ASCII values.
g. This ASCII value string is turned into a special string using a lossy data compression technique making it impossible to revert it back to the original string.
h. The resultant string is then converted to the final encrypted password which consists of exactly 256 characters.

7. CONSTRAINTS WHILE ENTERING THE PASSWORD

a. Each password must contain exactly 3 to 5 keys from the interface.
b. The beginning of the password cannot contain a key from the interface i.e., the password begin from the normal characters.
c. Once the user enters the wrong password, then using backspace is not advisable so a CLEAR button is provided to delete the password completely and retype it again

8. RESULTS

This password authentication scheme has been successfully developed and tested under various user credentials. Since the authentication is due to the textual password scheme combined with the modified cued click points it produces 100% success rate in authenticating each user. Generally textual data are relatively easier to compare than the graphical one while authenticating because of the accuracy in textual data.

9. ILLUSTRATION OF SYSTEM

If password is crypto123graphy, then password will be stored as:

```
!eotqAKlcmokCxqopVo^Q-Uq+Ue]`ssotqAKo@pVo^Q2c]o#Un[o]+Ue]`U!mokCxsgpVo^Q+&Y+Ue]`cM`ynero=mokCxo!Wo#Un[aEotqAK@:mokCxsLpVo^Q-=A+Ue]`!AotqAKlI`yner]#pVo^Q-wWo#Un[!]otqAKq=mokCxow[+Ue]`:#otqAKRW`ynerW_Ao#Un[AA+Ue]`]uotqAKu;mokCxw%pVo^Q+U]+Ue]`S/`yner(mpVo^
```

10. DATA FLOW IN THE SYSTEM

A data flow diagram (DFD) is a graphical representation of the “flow” of data through an information system, showcasing its process. A data flow diagram is periodically used as a primary step for creating an overview of the entire system, which could be further, is expanded. Data flow diagrams can also be used for the envisagation of data processing (structured design).

A DFD shows what kind of data will be an input for and output from the system, where the data will enter in and get out to, and where the data will be saved and stored. It does not show the information about the timing of process or information about whether processes will operate in sequence or in parallel (which is shown on a flowchart).

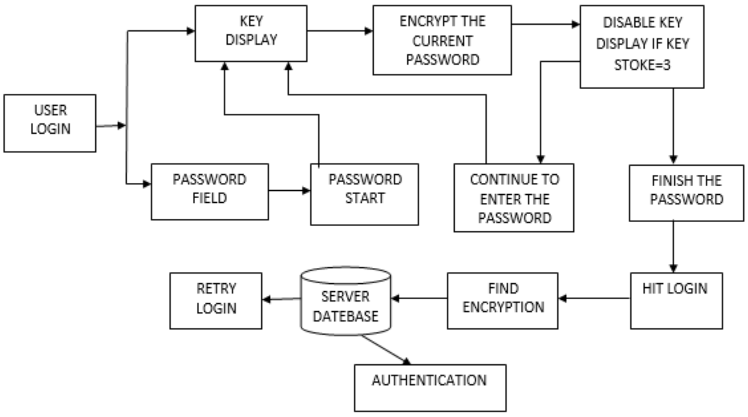

Figure 3. Block diagram showing the flow of data

11. SUPPORT FOR RECOVERY

Recovery to your account can be provided but the password cannot be recovered even by the administrator. The password once stored can be reverted back to its original password since we have used the concept of one way encryption. Added to it we have used a concept of lossy data compression technique where we have neglected the unwanted data and through which some of the data s lost. So the system can provide a support by sending a password reset link to the registered mail address. Clicking on the link would open a new page for password resetting. Using that page password can be resettled for the specific account.

12. CONCLUSION

The significance of selecting an environment appropriate Authentication method is perhaps the most important decision in designing secure systems. This method stands superior to the other password authentication system. It provides more security with less complexity and saves more time. The modified CCP technique along with the interface helps in providing a more sophisticated authentication mechanism with the textual passwords. Since it uses a special one-way encryption algorithm, even the administrator doesn’t have any access to the user profiles. If the user forgets his password then he can only reset the password by requesting a password reset link using his username from the administrator which will be sent to the registered e-mail id. And also the algorithm can be customized to produce various different encrypted passwords. This customization of the encryption algorithm makes it very useful for various organizations suiting its requirements

13. FUTURE WORK

The idea can be extended by removing the mandatory three to five key constraints and giving the user, the freedom to choose any number of keys. This choice of keys makes it much more complex for the attacker to guess or hack the password which in turn provides a stronger and a better authentication system. Also we can provide the user with password reset link in the registered mobile number too.

REFERENCES

[1] Smita Chaturvedi; Rekha Sharma, “Securing Text and Image Password using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption Standard”, *International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2015.

[2] Sonia Chiasson; Elizabeth Stobert; Alain Forget; Robert Biddle; Paul C. van Oorschot, “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism”, *IEEE Transactions on Dependable and Secure Computing*, volume 9, no. 2, March/April 2012

[3] Binitha V. M., “Persuasive Cued Click Based Graphical Password with Scrambling For Knowledge Based Authentication Technique withImage Scrambling”, *IOSR Journal of Computer Engineering (IOSR-JCE)*, e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 13, Issue 2 (July-Aug. 2013)

[4] Sanket Prabhu; Vaibhav Shah, “Authentication using Session Based Passwords”, *International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2015.

[5] S. Balaji; Lakshmi.A; V.Revanth; M. Saragini;V.Venkateswara Reddy, “Authentication Techniques for Engendering Session Passwords with Colors and Text”, *Advances in Information Technology and Management*, vol. 1, no. 2, 2012

[6] M. Sreelatha; M. Shashi; M. Anirudh; M. D. Sultan Ahamer; V. Manoj Kumar, “Authentication Schemes for Session Passwords using Color and Images”, *International Journal of Network Security & Its Applications (IJNSA)*, vol.3, no. 3, May 2011

[7] Smita Chaturvedi; Rekha Sharma, “Securing Image Password by using Persuasive Cued Click Points with AES Algorithm*”, International Journal of Computer Science and Information Technologies (IJCSIT),* vol. 5 (4), 2014

[8] S. Chiasson; A. Forget; E. Stobert; P. Van Oorschot and R. Biddle, “Multiple Password Interfernce in Text and Click- based graphical passwords in ACM Computer and Communications Security (CCS), Nov 2012

[9] S. Jayashri; M.V.Ishwarya; K. RameshKumar, “A Study on Authentication Protocols”, *International Journal of Emerging Technology & Research*, volume 1, issue 4, May-June 2014.

[10] Shi-Qi Wang; Jing-Ya Wang; Young-Zhen Li, “The Web Security Password Authentication based the Single–Block Hash Function”, *International Conference on Electronic Engineering and Computer Science*, 2013.

[11] Jing Liu; Qingyu Chen; Jianwei Liu; Jianhua Chen, “Design of Secure Authentication and Transaction Protocol based on Digital Certificates and Dynamic Password”, *International Conference on Computer Science and Service System (CSSS)*, 2011

[12] P. R. Devale; Shrikala M. Deshmukh; Anil B. Pawar, “Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme”, *International Journal of Soft Computing and Engineering (IJSCE*) ISSN: 2231-2307, volume-3, issue-2, May 2013