International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Authentication Schemes for Session Passwords Using Color and Images

Harnee K P [1], Nivetha J[1], Pavithra D[1], Selvapriya R[1], Ms. K. Veena[2]
[1]UG Scholar, [2]Assistant Professor,
Department of Computer Science and Engineering, Akshaya College of Engineering and Technology,
Coimbatore, Tamil Nadu, India

Article Info
Volume 8, Issue 2
Page Number : 542-548

Publication Issue
March-April-2021

Article History
Accepted : 18 April 2021
Published : 24 April 2021

ABSTRACT

Authentication is the first and the most important step in information security. It is used to authenticate the user identity. Where user need to memorize their password and remember at login time. Normally user use textual password to provide security, but textual passwords are vulnerable to many cyber-attacks, Such as - dictionary attacks, shoulder surfing etc. Graphical password schemes are used to overcome these problems. A Session password is a new technique based on the graphical password in which we using combination of text, color and images to solve the problem of security. Every time session password can be used to create password for user authentication, by this technique we can overcomes the attacks like shoulder surfing, dictionary attacks. We can use this method for PDAs (Personal Digital Assistants). A multitude of graphical based password scheme which have been proposed as alternative to text based password scheme, motivated by the promise of improved password memorability and thus usability. This paper presents a detailed evaluation of the various Authentication schemes which provides high level of security and provides security to your folder. It consists of three authentication methods like text, picture and colors for providing higher security.

Keywords : Authenticatin, Colors, Credentials, Password, Graphical Password, Images.

I. INTRODUCTION

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system. The authentication process always runs at the start of the application, before the permission and throttling checks occur, and before any other code is allowed to proceed. Different systems may require different types of credentials to ascertain a user's identity. The credential often takes the form of a password, which is a secret and known only to the individual and the system. Three categories in which someone may be

authenticated are: something the user knows, something the user is, and something the user has.
Authentication process can be described in two distinct phases - identification and actual authentication. Identification phase provides a user identity to the security system. This identity is provided in the form of a user ID. The security system will search all the abstract objects that it knows and find the specific one of which the actual user is currently applying. Once this is done, the user has been identified. The fact that the user claims does not necessarily mean that this is true. An actual user can be mapped to other abstract user object in the system, and therefore be granted rights and permissions to the user and user must give evidence to prove his identity to the system. The process of determining claimed user identity by checking user-provided evidence is called authentication and the evidence which is provided by the user during process of authentication is called a credential.

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, 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. Our main aim is to provide security to the confidential website and web application in computing devices through session passwords by using techniques like Pair based and Hybrid based authentication.

II. Related Work

a. Graphical Password Scheme using Color Login

In Dec 2009 author H. Gao proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidental login is high and password is too short. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. The advantages of this system is that it reduces the login time, session passwords are also generated to improve security. The disadvantage of this system is that it the possibility of accidental login is high and password is too short.

b. Hybrid Textual Authentication Scheme

In this paper M.Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed. As the color rating given by the user, the password will generate. First color shows row number and second shows column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it becomes very hectic to user. The benefit of this system is that it is flexible and simple to use.

c. Graphical Password Based Authentication for Mobile Systems

A hybrid graphical password based method is advised, which is a mixture of recognition and recall based methods having many advantages as compare to existing systems and more suitable for the user. In this system the user draws the selected object which is then stored in the database with the specific username. Objects may be symbols, characters, auto

shapes, simple daily seen objects etc. Then the user draws pre-selected objects as his password on a touch sensitive screen with a mouse. Then the system performs preprocessing. Then after stroke merging, the system constructs the hierarchy then the next step is sketch simplification, then the three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching. The plus point of this system is it's a combination of recognition and recall based technique, hence provides flexibility. This system performs some complex actions like pre-processing, stroke merging. So it can be a weakness of this system.

d. Password Authentication using text and colors

Authors proposed a system in which password scheme uses colors and text for generating session password. They have introduced a session password scheme in which the passwords are used only once for each session and when session is completed the password is no longer in use. In this system two session password schemes pair-based textual authentication scheme and color code-based authentication scheme are introduced In the pair based textual authentication scheme the user submits his password during the registration. The password should contain number of characters. When the user enters login an interface containing of a grid is showed during the login phase. The grid is of size 6 x 6 and it contains of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. Depending upon the password which is submitted during the registration phase, user has to enter the password. Users have to consider his password in terms of pairs. In the color code based scheme, the user has to get his password with the help of colors. During registration phase, user should fill up all his information and also rate colors. The merit of this system is it provides much better security. Demerit of the system is sometimes users may consider wrong password as they are supposed to consider the password in terms of pair.

e. Graphical Password as an OTP

In Graphical password as an OTP proposed by authors, she used the scheme of OTP. As there are many drawbacks of using alphanumerical passwords, people tend to forget the password, or they may write the password somewhere. Hence they have developed authentication methods that use pictures as passwords known as graphical password to solve this problem. They have provided an additional layer of security by generating one-time password(OTP) which is send to the users mobile. Using the instant messaging service available on internet, user will obtain the One Time Password (OTP). The OTP will be the information of the items present in the image to be clicked by the user. The users will authenticate themselves by clicking on various items in the image based on the information sent to them. The main aim of this system is to avoid Shoulder surfing attack. It also aims to avoid other attacks like dictionary attack, brute force attack and guessing attack. The OTP is sent on the user's mobile number from the database. The positive point of this system is it provides better security as it avoids shoulder surfing by using OTP. Negative point of this system is user must click within the tolerance of their chosen pixels and also in correct sequence.

f. Color Shuffling Password Based Authentication

Authors proposed a scheme which mainly focuses on shoulder surfing. In this system, they proposed a new click based color password scheme called Color Click Points (CCP). It can be viewed as a combination of Pass-Points, Pass faces, and Story. A password consists of one click-point per Color for a sequence of Colors. The next Color displayed is built on the previous click-point. In this proposed scheme, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Afterward, we examine the security and usability of the proposed system, and show the resistance of the proposed system to shoulder surfing

and accidental login. The benefit of this system is that it reduces the login time & it is an efficient system.

g. Authentication by Drawing Signature Using Mouse

Syukri has designed a technique where in authentication is actually done by drawing digital signature using a mouse. The technique includes two stages, in stage one registration is to be done and the other stage is verification. During registration stage user draws his signature with a mouse, after which the system extracts the signature area. It takes the user signature as an input and performs the normalization process after which extraction of the parameters of the signature is done in the verification stage. The disadvantage in this technique is forgery of signatures. Drawing with mouse is not familiar to most of the people and it is also a bit difficult to draw the signature in the same perimeters during registration time.

III. SYSTEM MODEL

Persuasive Cued Click Points: An authentication system works by having the user select the images, in a specific order. The Persuasive Technology guides and encourages the user to select stronger passwords (i.e. click-points), but not entirely impose system generated passwords. The proposed system consists of two modules; user registration and user login. The registration phase, in which user registers a unique username and the graphical password in the database, is followed by user login phase. During login, the user is asked to provide the username and correct graphical password. Upon successful verification of the user profile from the database, the user is now able to encrypt/decrypt his files.

Disadvantages

Graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spy ware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness. So this approach is that such systems can be expensive and the identification process can be slow.

a. Proposed System

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. 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. This system uses AES algorithm for generating password. The proposed authentication schemes use text, image and colors for generating session passwords.

AES Algorithm

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm,

this key needs to be expanded to get keys for each round, including round 0.

AES is based on a design principle known as a substitution– permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order array of bytes, termed the state. Most AES calculations are done in a particular finite field. For instance, 16 bytes, are represented as this two-dimensional array. The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of rounds are as follows.

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future- proofing' against progress in the ability to perform exhaustive key searches. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix – Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The 16 input bytes are substituted by looking up a fixed table (S- box) given in design. The result is in a matrix of four rows and four columns. Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes.

It should be noted that this step is not performed in the last round. The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike

Steps

1) The user register themselves by giving their details and choosing image point and password from the grid.
2) System stores these details.
3) User login with the details and have to choose the correct color code and image point and correct password from the grid.
4) System uses AES algorithm for authentication.
5) After successful authentication, user can get access to the system.

IV. PROPOED SYSTEM IMPLEMENTATION

a. User Registration Panel

The user has to register themselves with their mobile number, email id and the color code used while login process. Then the image panel will be opened and the user have to choose an image and have to choose the coordinate. Then a 5x5 matrix was displayed and it consists of numbers and letters. The user have to choose a password from the grid and click ok button. Now the user is successfully registered.

b. Login Panel

On running the application, a login form turn up, allowing the user to enter the username and password. If the user is already a registered one, then clicking on "login" button after filling username and password block. System will check the given data from database, if username exist then proceed to grid phase where there is a 5x5 grid displayed with mix of numbers and letters where the user have to choose the correct password. After successful validation of password color phase will be displayed. In Color Phase, there is displaying five colors (Red, Blue, Black, Yellow, Pale yellow) and user need to rate the color in between (0-9) value must be same as user gave while register. System will check the given data from database, if data match then proceed to Image phase where the user have to select the correct image coordinate otherwise no authentication is done.

V. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this project, two authentication techniques based on text and colors are proposed. These techniques are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the schemes can be up-scaled to make it more resistant to shoulder surfing attacks. To achieve higher levels of maturity and usefulness in graphical password authentication we introduced these methods. These schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness. These techniques can also be developed as ATM application where the person standing outside the transparent door could guess the ATM pin with the same Debit card or can be used against the key loggers in cyber cafe or windows application such as a folder locker or an external gateway authentication to connect the application to a database or an external embedded device.

VI. REFERENCES

[1]. Dec 2009, H. Gao proposed paper on “graphical password scheme using color login”.

[2]. In May 2011, M. Sreelatha proposed Hybrid Textual Authentication Scheme.

[3]. Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India “Graphical Password Based Authentication Based System for Mobile Systems”.

[4]. Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM Nagpur university, M.I.E.T Bhandara, “Password Authentication Using Text and Colors”.

[5]. Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, “Graphical Password as an OTP”.

[6]. In 2017 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalankar Institute of Technology, Mumbai, “Color Shuffling Password Based Authentication”

[7]. Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.

[8]. Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.

[9]. Chaitanya, G.K. and Raja Sekhar, K., 2021. Verification of pattern unlock and gait behavioural authentication through a machine learning approach. International Journal of Intelligent Unmanned Systems.

[10]. Saxena, N., Uddin, M.B., Voris, J. and Asokan, N., 2011, March. Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 181-188). IEEE.

[11]. Hintze, D., Hintze, P., Findling, R.D. and Mayrhofer, R., 2017. A large-scale, long-term analysis of mobile device usage characteristics. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1(2), pp.1-21.

[12]. Ibrahim, N. and Sellahewa, H., 2017, February. Touch gesture-based authentication: A security analysis of pattern unlock. In 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp. 1-8). IEEE.

[13]. Marques, D., Guerreiro, T., Duarte, L. and Carriço, L., 2013, September. Under the table: tap authentication for smartphones. In 27th International BCS Human Computer Interaction Conference (HCI 2013) 27 (pp. 1-6).

[14]. Løge, M.D., 2015. Tell me who you are and i will tell you your unlock pattern (Master's thesis, NTNU).

[15]. Aviv, A.J., Maguire, J. and Prak, J.L., 2016. Analyzing the impact of collection methods and demographics for android’s pattern unlock. In Proc. Workshop on Usable Security (USEC). Internet Society.

[16]. Syukri study based on Authentication by drawing signature using mouse, Journal of Computers, vol.5, no.5 May 2010.

Cite this article as :

Harnee K P, Nivetha J, Pavithra D, Selvapriya R, Ms. K. Veena, "Authentication Schemes for Session Passwords Using Color and Images", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 542-548, March-April 2021.

Journal URL : https://ijsrst.com/IJSRST2182109