Knowledge Based Authentication Schemes for Data Security

Rahul Ambekar, Mihir Kemkar, Kritika Jain, Sarika Priya, Amitabh Sahare

***Abstract*— The term authentication is used for accepting proof of identity given by a credible person who has first hand evidence that identity is genuine. A system accepts the exact authentication of individual and grants access to his assets.**

In modern era, humans are relying on the technology as a result a lot of crucial data is uploaded and stored on web giving its security a major concern as each access point is a potential intrusion point. In this paper we use two authentication schemes which generate session passwords collaborating texts with colours which are far beyond the disadvantages of textual and graphical passwords. Session passwords generate a new password in every fresh session thus securing the application efficiently.

***Index Terms*— Authentication, Data Security, Pair-based Authentication scheme, Color Rating Authentication Scheme ,CCP Authentication Scheme.**

I. INTRODUCTION

In today's technology-savvy online world, security requires utmost concern. Thus authentication is done to verify the accounts of every user considering their user id's and respective passwords. Now passwords commonly used are textual which are prone to hacking through dictionary attacks, eves dropping, guessing attacks, shoulder surfing, social engineering etc. Again textual passwords are long which are definitely easy to crack and difficult to remember thus hindering the security. Graphical passwords are an alternative to textual but having its own share of disadvantage of shoulder surfing, usability issues or taking. Another method used is biometrics also called as the inherence authentication scheme in which retina scan, fingerprints, digital signatures are considered but enormously increasing the cost and time, making it not a widely acceptable approach. So in order to overcome the problem we have proposed integrating three techniques based on the one element from the Multifactor authentication that is Knowledge factor. Session passwords is newly found technique which not only combines advantages of both textual with graphical but resists the disadvantage of shoulder surfing. This is because a new session password is generated on each login collaborating texts with images or colors thus securing the system efficiently. One session, One password. Once the session is terminated, the session password is useless. For every login process, user inputs different passwords. Creation of a new random password every time prevents hacking.

Manuscript received March 18, 2015.

Rahul Ambekar is a asst. prof. in computer department of Sinhgad Institute Of Technology of Savitaribai Phule Pune University, Pune, India.

Mihir Kemkar is a final year student in computer engineering in Sinhgad Institute Of Technology of Savitaribai Phule Pune University, Pune, India.

Amitabh Sahare is a final year student in computer engineering in Sinhgad Institute Of Technology of Savitaribai Phule Pune University, Pune, India.

Sarika Priya is a final year student in computer engineering in Sinhgad Institute Of Technology of Savitaribai Phule Pune University, Pune, India.

Kritika Jain is a final year student in computer engineering in Sinhgad Institute Of Technology of Savitaribai Phule Pune University, Pune, India

II. RELATED WORK

Textual-based passwords used in the previous years are subjected to various attacks as mentioned in the former section. Besides, many graphical authentication techniques have been evolved based on the requirements and their remains a potential intrusion point associated with the prior existing authentication methods which led to the betterment of system.

References from :

Dhamija and Perrig[1] proposed a graphical authentication scheme where the user has to identify the pre-defined. In this system, the user selects a certain number of images from a set of random pictures during registration.

Passface [2] is a technique where the user sees a grid of faces and selects one face previously chosen by the user. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is repeated for four times.

Blonder [3] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations.

Passlogix [4] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity of user. The results declared that pictures are most effective than the textual passwords. More graphical password schemes have been summarized in a recent survey paper [5]. Zheng et al [6] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.

III. PROPOSED WORK

So as there are numerous techniques proposed in the authentication schemes, it is very difficult to intrude any one of them. Thus in order to make a system more reliable we can integrate these authentication schemes and can create an application which can be difficult to intrude. Authentication technique consists of 3 phases: registration phase, login phase and verification phase.

A. PAIR BASED AUTHENTICATION SCHEME

During registration user is allowed to submit his password which can be referred as secret pass. Minimum length of the password is eight. The secret pass should contain only even number of characters and maximum length must till sixteen characters. This secret pass helps to generate the session password. During the login phase, when the user enters his

username an interface consisting of a alphanumeric grid is displayed. The grid is of size 6 x 6 and it consists of alphabets (A-Z) and numbers (0-9). These alphabets (A-Z) and numbers (0-9) are randomly placed on the grid and the interface changes every time when it is refreshed. User has to enter the password depending upon the secret pass by using alphanumeric grid. User has to consider his secret pass in terms of pair to enter the correct password. To enter secret pass, first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password which will be no longer useful after expiry of session. This technique is repeated for all pairs of secret pass .

FIG 1.0 PAIR BASED

B. COLOR BASED AUTHENTICATION SCHEME

At the time of registration, the user should rate colors for system defined word named as "BIGCROPS" and has remember the sequence rated for the word. It is important for a user to remember the sequence of the rating which he has defined for the default word "BIGCROPS". During the login phase, after the first authentication technique, an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 1×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains block of colors. The color grid consists of eight colors. Each color represents the row and the column of the grid. Depending on the ratings given to colors, we get the session password.

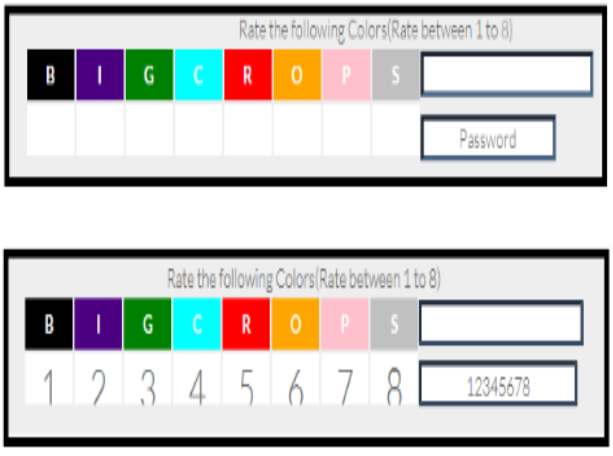

FIG 1.1 COLOR BASED

C. CCP AUTHENTICATION SCHEME

At the time of registration, user will select images (max 5) from the given system defined images and the user has a option of dividing the number into matrices which is called as splits. Number of splits will indicate the size of matrix in which the image is going to divide each and every image. User has to remember the sequence in which he clicks the images during registration and repeat the procedure during the login phase. Then user will give check- point for each image i.e. for example for a particular image split is 3 then that image will get divided into a 3x3 matrix and then check point can be combination of row and column e.g. (2,1),(2,2) etc. Images and respective checkpoint is stored in database.

FIG 1.2 (A) CCP WITHOUT GRID

FIG 1.2 (B) CCP WITH GRID

IV. SYSTEM ARCHITECTURE

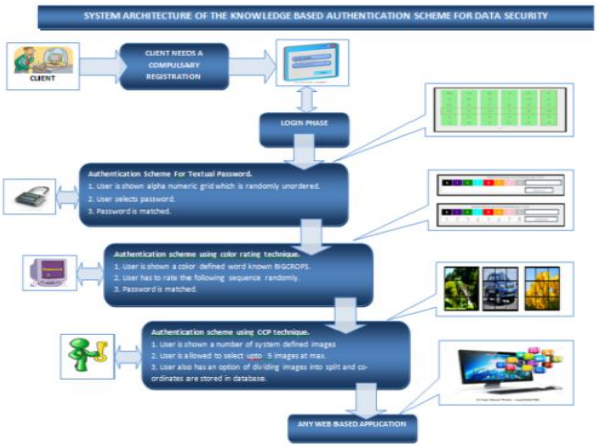

FIG 1.3 (A) SYSTEM ARCHITECTURE

The following is the system diagram which is based on the client-server architecture. In the following diagram we come to the conclusion that when the user is in the login phase, the user needs
to compulsory register for the given system before he is allowed access to his credentials. So, before approaching the login phase, user has to register by using the following three

techniques. After the registration phase, the data and the passwords which are entered by the user are stored in the database by using the Advanced Encryption Standard (AES) algorithm. During the login phase, the user enters the password through these techniques, the given password is validated and if the user is a authenticated person the system grants access to his credentials else the user is terminated.

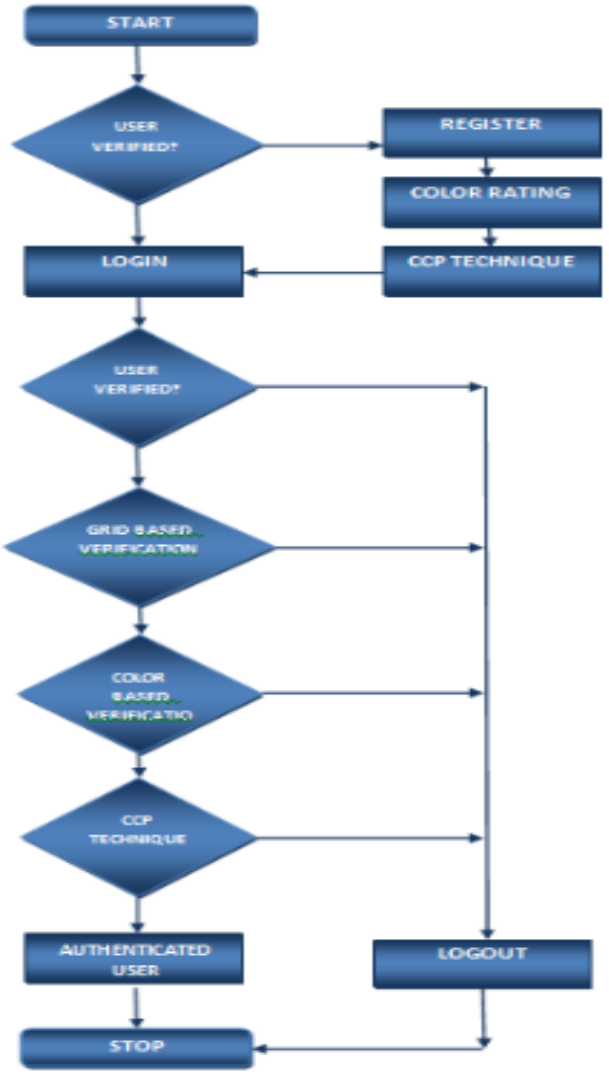

FIG 1.3 (B) FLOW CHART

V. ALGORITHMS USED

A. PAIR BASED AND COLOR BASED AUTHENTICATION ALGORITHM

Pair based authentication scheme uses a alpha numeric grid which consists of alphabets (A-Z) and number from (0-9). The alphabets and numbers are randomly ordered and are shuffled in the grid. This is achieved by using mainly three functions in the algorithm.

1. HashMap

HashMap contains values based on the key. It contains only unique elements. It maintains no order.

2. Shuffle

Shuffle method shuffles the content of collection every time it is called and generates different order of output.

3. Random

The random function helps us to generate the elements of alphanumeric grid.

B. CUED CLICK POINT ALGORITHM

The CCP algorithm is a case in which the user is shown a series of the system defined images and user has to select at max 5 images from the given images. After this process the user is allowed to enter the images into the split. A split divides image into 3x3 or 4x4 matrix which depends on the number of splits selected by the user. The user then selects each matrix from the given images and the co-ordinates of the following images are stored in the database. When the user enters the splits in login phase, the co-ordinates entered by the user are matched to the co-ordinates in database, if he is authenticated user, the system proceeds to the next level.

C. ADVANCED ENCRYPTION STANDARD ALGORITHM

AES is based on a design principle known as a substitution and permutation network, the combination of both substitution and permutation, is fast. AES consists three block of ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively in both software and hardware. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key for the encryption and decryption. All key lengths are sufficient to protect classified information up to the "Secret" level. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys – each round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

VI. SECURITY ANALYSIS

The proposed system is resistant to many types of attack. Due to dynamic password, many threats and risks such as dictionary attack, shoulder surfing, mouse and keyboard logger, personal digital assistant (PDA), etc are eliminated.

A. DICTIONARY ATTACK

Dictionary attacks consist of textual passwords. Here in this attack, different types of dictionary words are used by the hacker one by one and multiple attempts are made to authenticate. These attacks are eliminated as session passwords are generated each time.

B. MOUSE AND KEYBOARD LOGGER

Keyboard logger, also referred as Keystroke logger, is a key logging or keyboard capturing technique in which actions are

recorded (or logged) when the keys struck on a keyboard. Keyboard is unaware that their actions are being monitored. As there is a virtual keyboard displayed in the proposed system, this risk is eliminated.

C. SHOULDER SURFING

Shoulder surfing is attack where the user is observed while entering password in a system. As the proposed system uses the session password, the risk through shoulder surfing is eliminated.

D. GUESSING

Guessing is a technique in which the attacker guesses the password. In the following technique guessing isn't a threat as there can be 36x4 attempts to guess password.

E. BRUTE FORCE ATTACK

A brute-force attack, or exhaustive key search, is attack that can be used against the encrypted data. As the propose system makes the use of session password, the brute force attacks are avoided.

VII. CONCLUSION

In this paper, we have selected the important and efficient techniques which eliminate almost every possibility of breaching into a system. Thus by integrating all the three techniques into a single application we can ensure the security of any application. The nature of the system being flexible, we can integrate the proposed system into various fields and applications such as e-mails, social networking, fund transfer applications such as billing, banking, online shopping, for companies to store their confidential data etc. Thus the following system covers each and every potential intrusion point of a system thus making it completely secure.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9thUSENIX Security Symposium, 2000.
[2] Real User Corporation: Passfaces. www.passfaces.com
[3] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent,Ed. United States, 1996.
[4] Passlogix, site http://www.passlogix.com.
[5] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
[6] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.
[7] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.
[8] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.
[9] M Sreelatha, M Shashi, M Anirudh, MD 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, May2011.