Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

Review Paper On Graphical Password Authentication Techniques

Sharayu S.Ganorkar[1], Prof. H. V. Vyawahare [2]

[1]Computer Science & Engineering, Sipna C.O.E.T. Amravati
[2]Computer Science & Engineering, Sipna C.O.E.T. Amravati

Abstract — *Nowadays, user authentication is an essential attribute in the area of information security. The method of recognizing an individual commonly based on a user name and password. Passwords are the preeminent commonly used method for identifying users in computer and communication schemes. Text based password is a general authentication method used from early times. There are numerous authentication systems like biometric, textual, graphical, smart card etc. Graphical password is used as an alternative to textual/traditional alphanumeric password. Traditional alphanumeric password is tough to remember and generally forget by users as times passes, but in graphical password there are less likelihood to disremember password because people remember images more effortlessly than text based password. There are also fewer probabilities for hackers to take the graphical based password because hackers will not be capable to access the images uploaded by the user as password. Some graphical password schemes have been intended so far as it grows password usability and security.*
In this paper, we manner a wide survey of the current graphical password methods.

Keywords- *Graphical password, Text based password, usability, security, Attacks, Authentication*

I. INTRODUCTION

Data security and user authentication is a basic factor for information security. A password is a form of stealthy authentication that is used to regulate access to records. It is kept secret from unapproved users, and those desiring to increase access are verified and are approved or repudiated the access on the basis of the password. Authentication of user is simple component of any information system since it provides the facility to the user to access the method. Old security methods which are using from a long time afford less security for authentication than the advance security techniques. Passwords are used from early times itself as the distinctive code to identify the malicious users. Nowadays, passwords are used to bounds to access to guard computer operating systems, mobile phones, and others. A computer user may require passwords for many uses such as login to accessing e-mail from servers, personal accounts, retrieving files, networks, databases, web sites, etc. Normal passwords have some weaknesses such as hacked password, fail to recall password and stolen password. Conventional passwords have been used for verification but they are known to have complications in usability and safety. Recent days, another method such as graphical authorization is comfortable. Graphical password has been offered as different to alphanumeric password. Psychological readings have presented that individuals can remember images better than text. Images are normally easier to be recalled than alphabets and numbers, especially photos, which are even easier to be recalled than casual pictures. The main objective of graphical passwords is use for images or profiles to substitute text, since many intellectual and spiritual studies demonstrated that people accomplish extreme better when remembering pictures than words. The prime advantage of graphical passwords over text based passwords is the improved memorability.

II. LITERATIURE SURVEY

R Deale[1] executed Cued Click Points with Click Draw Based Graphical Password. A password includes of one click-point per image for arrangement of 5 images. The next image showed is on the basis of earlier click-point so users accept instant implicit response as to whether they are on the accurate route when logging in. An incorrect click leads down an improper route, with basic hint of authentication letdown only later the final click. A main usability enhancement over Pass Points is the fact that genuine users get instant response about fault when trying to log in. When they see an improper image, they know that the latest click-point was improper and can directly cancel this challenge and try again from the beginning. Few grid based schemes are proposed which uses recall method. In this scheme growing

security using undisclosed drawing in certain image during authentication procedure. Accurate password or inappropriate password is presented after final click.

Mohamed Sylla[2] implemented Combinatory Drag Design Graphical Password. In this Scheme one graphical keyboard is delivered to user for picking of a password. During collection of password user has to pick set of characters from the graphical keyboard. User must survey the arrangement for design of password.

Sobrado and Briget[3] established a graphical password method that compacts with shoulder suffering problem. In the first structure, the system will show amount of pass objects between several new objects. To be authentic, a user wants to identify pass-objects and click intimate the convex hull moulded by fully pass objects.

Hong et al. [4] later prolonged this methodology to permit user to allocate their individual codes to pass object modifications.

Nilesh Kawale [5] implemented a appreciation Based Graphical Password Scheme. In this system 3x3 lattice is used.

III. FUNDAMENTAL AUTHENTICATION METHODS

Authentication is a procedure which permits a user to approve his individuality to an application. Authentication methods are mainly categorized into three main areas, such as Biometric based, Knowledge based, and Token based authentication.

3.1. Token Based Authentication

A token is a portion of data created by the server containing information to individually detect the user. Token has a lifetime. The basic idea at the back of token based authentication system is easy. In this system, user has permission to pass their username and password in order to acquire a token which allows them to obtain exact resource without using their username and password. Once their token has been found, the user can obtain token which offer access to specific resource of time period to the isolated location. In token base authentication key cards, smart cards, credit card etc. are widely used to authenticate a system. Token based authentication works by confirming that every call to a server is convoyed by a signed token which the server confirms for authenticity and only then answer back to the request.

3.2. Biometric Based Authentication

Biometric authentication scheme uses behavioral characteristics of specific individual for verification. These characteristics are exclusive to individuals hence can be used to validate or detect a person. Here user can use his finger print, iris scan, palm scan, etc. as passwords for authentication. Biometric authentication systems equate biometric data pick up to stored, complete validate data in a files. If in both sections of the biometric data are same then authentication is established. Normally, biometric authentication is used to manage access to somatic and arithmetical resources such as buildings, rooms and computing devices.

3.3. Knowledge Based Authentication

Knowledge-based authentication is an authentication system in which the user is requested to response at least one secret query. In the knowledge-based authentication queries can be fixed i.e. static or active i.e. dynamic. In static knowledge-based authentication systems users allow to choice security queries i.e. questions and deliver answers that are kept in a computer and retrieved later, generally when a password wishes to be reclaimed or reset. While in dynamic knowledge based authentication, stage goes a further by producing questions that apply only to the future end user and do not essential earlier relationship with the customer. It is a mixture of text base password and picture based password. Picture based passwords also famous as graphical passwords which includes pictures or drawing passwords.

IV. GRAPHICAL PASSWORD TECHNIQUES

In this part, some prevailing graphical password techniques are discussed. Graphical based password techniques have been suggested to solve the boundaries of the text based password techniques, because pictures are easier to recall than texts. A literature review of papers about graphical password techniques shows that the techniques can be characterised into four groups as follows:

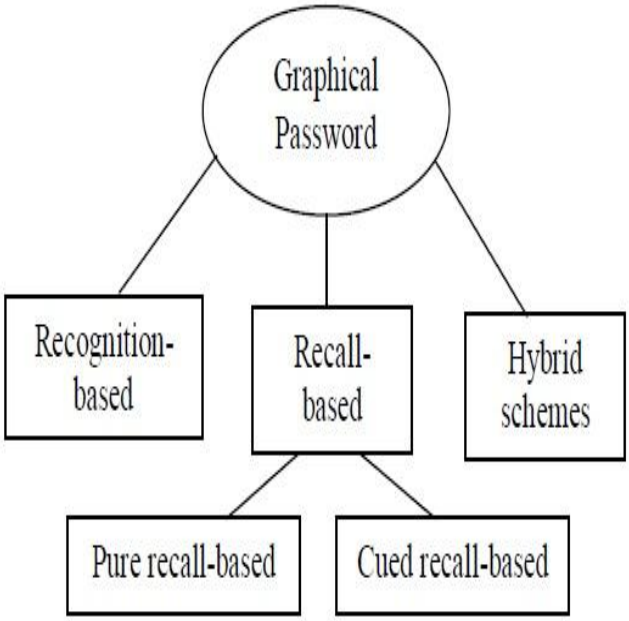

Figure 1. Classification of Graphical password authentication techniques

4.1. Recognition-Based Technique

In recognition based technique some images are shown to the user during registration. The user should select some images, icons or symbol from the collection of images. At the time of authentication procedure, the users requisite to identify their images, symbols or icons which are selected at the stage of registration between a group of images. In this technique users can remember their passwords even after 45 days. In Dhamija and Perrig technique [6] during registration user chooses certain amount of images from a group of arbitrary images. For the purpose of authentication user has to categorize those particular images in a sequence. In Pass face Technique [7] during registration human face database is shown to the user. User has to recognize known face.

4.2. Recall-Based Technique

In the recall base technique user has to recall something that has been created or designated at the time of registration. User can reproduce their password without any hint. This technique is very relaxed i.e. easy and convenient. It is more protected than the recognition based technique.

Recall based technique has two sub-categories:

4.2.1. Pure Recall-Based Technique: In pure recall based technique, clue is not provided to user to recall their password.

4.2.2. Cued Recall-Based Technique: In cued recall based technique, suggestion is provided to the user to recall their passwords. This technique is simple than pure recall based technique.

4.3. Hybrid Technique

In the hybrid technique, authentication may be grouping of two or more technique for greater advantages than individual techniques. It improves data analysis. Many single systems on both recognition-based and recall-based system are discussed and some of these schemes are joined to develop the hybrid technique i.e. schemes. In this technique, passwords are more unforgettable than text based passwords.

V. DESIGN AND IMPLIMENTATION ISSUES

Main design and implementation issues graphical passwords

5.1 Security:

Comparison of security issue in graphical password and text based password.

5.1.1. Brute Force Attack: In brute force attack complete key search is done. Brute force search have large password space. In this, each probable choice is taken into contemplation to break the password until the accurate one is found. It is more hard to bring brute force attack in contrast to graphical passwords than text-based password. A graphical password is fewer susceptible to brute force attacks than a text-based password.

5.1.2. Dictionary Attack: In the dictionary attack, an attacker tries to guess the password from a very large list of words, dictionary. Dictionary may be collection of various passwords. If user choose password, a word already present in the dictionary, then attack will be successful. In recognition based graphical passwords include mouse input as an alternative of keyboard input; it will be impossible to bring dictionary attacks against this type of graphical passwords. Graphical passwords are little weak to dictionary attacks than text-based passwords.

5.1.3. Spyware Attack: Spyware attack is type of malicious software. The goals of spyware attack are to collect data about user. Spyware attack is generally done by via a key logger or key listener. This malwares collects data without user's awareness and disclose this information i.e. data to an external source of attacker. It is still not perfect in recognizing the graphical password.

5.1.4. Shoulder Suffering Attack: Shoulder suffering attack refers to direct attack the user passwords by using straight observation methods. In this technique password can be identified by looking over a person's shoulder to get password. Shoulder suffering attack mostly occurs in crowded place i.e. public place. Graphical password is more open to shoulder surfing than text based password. Few recognition based technique are deliberated to fight shoulder surfing attack.

5.1.5. Social Engineering Attack: In social engineering attack, user gains the private data or information from the interaction. This attack is as well-known as Description attack. This attacker doesn't use any electronic technique for getting information. This attacker uses only human intelligence and tricky conversation to get the information as they wants.

In the above part, we have concisely studied the security issues with graphical password.

5.2. Usability

In the evaluation of graphical password numerous usability properties should be measured. These properties such as time to login, number of mistype password, number of forgotten after definite period of time during registration. Features are easy to use, easy to create, easy to learn. One of the main opinions for graphical passwords is that pictures are easier to recall than text sequences. A major analysis between the users of graphical passwords is that both the password registration and log-in procedure proceeds too lengthy, mostly in recognition-based approaches.

5.3. Reliability

The main design problem for recall-based systems is the reliability and correctness of user input acknowledgment. In this method, the error acceptances have to be custom sensibly-overly high acceptances may lead to several incorrect positives while excessively small acceptances may lead to various incorrect refusals. So, the more error tolerant the program, it is more accessible to attacks.

5.4. Storage

Graphical passwords need abundant storage space than that of text based passwords. Large amount of pictures may have to be sustained in a integrated database.

VI. CONCLUSION

In this survey paper, we discuss about graphical password authentication methods and exiting graphical password based methods. It fulfills both differing requirements i.e.it is easy to recall and it is tough to predict. Graphical password schemes offer a way of creating more human-friendly passwords. In this safety of the system is very extraordinary. Dictionary attacks and brute force search are infeasible. Passwords are easy to recall. Pictures are stress-free to recall than text strings. Then, we tried to survey on attack patterns and common attacks in graphical password authentication methods. Finally we have discussed different issues related to graphical password.

REFERENCES

[1] P. R. Devale Shrikala, M. Deshukh and Anil B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", International Journal of Soft Computing and Engineering, Vol.3, Issue-2 May 2013.

[2] Mohamed Sylla, Gul Muhammad, Kaleem Habib and Jamaludin Ibrahim, "Combinatory Drag-Pattern Graphical Password", Journal of Emerging Trends in Computing Information Sciences, Vol.4, No.12, Dec 2013.

[3] L. Sobrado and J.-C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[4] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management.Las Vergas, NV, 2004.

[5] Nilesh Kawale and Shubhangi Patil**.,** "A Reorganization Based Graphical Password System", International Journal of Current Engineering and Technology, Vol.4, No. 2, Apr 10, 2014.

[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9 USENIX Security Symposiums, 2000.

[7] Real User Corporation, "How the Pass face System Works", 2005.

