Volume-7,Issue-4, (April-17)
ISSN (O) :- 2349-3585

Graphical Password Authentication Technique: A Survey

Kanchan Poharkar[1] , Dr. S.A. Ladhake[2]

Department of Computer Science and Engineering, Sipna COET, Amravati

Abstract –At the present time, user authentication is one of the most crucial security issue. It is the most important aspect of cyber security. Text based password is a widespread authentication method. The auspicious alternatives of textual passwords is a graphical based password. These passwords contain images which are easier for humans to recall than the long stream of characters in text passwords. With the use of a graphical password user click on images instead of typing alphanumeric characters. Several graphical password schemes have been planned so far as it improves password usability and security. In this paper, we conduct an extensive survey of the present graphical password techniques.

Keyword- Text-based Password, Graphical Password, Authentication, Security.

I. INTRODUCTION

User authentication is an essential component in most computer security contexts. Studies about passwords shows that user can only memorize a limited number of passwords, they tend to write down them somewhere or will use the identical passwords for different accounts. Regular alphanumeric passwords have some limitations such as hacked password, fail to recall password and robbed password [1]. The text based password can be stolen by any dominant software. Phishing is another serious hazard to text based password. Phishing is the action of receiving secured facts such as username, password and other additional details by impersonating. Therefore, strong authentication is needed to secure all our applications. Predictable passwords have been used for authentication but they are known to have problems in usability and security. In Latest era, another method such as graphical authentication is presented. Graphical password has been proposed as substitute to alphanumeric password. Psychological readings have shown that people can memorize images better than text. Images are normally at ease to be recalled than alphabets and numbers, mainly photos, which are even at ease to be recall than random pictures. Graphical Password methodology is sometimes called as Graphical User authentication(GUA), because it is an authentication scheme that works by having the user select from images, in a exact order, presented in a graphical user interface (GUI). Graphical passwords have been used in authentication for smart phones, ATM machines, E-transactions. We can select only 26 alphabets and 10 numbers in the case of alphanumeric password, but in the case of graphical password the amount is not limited. In this paper, we conduct an inclusive survey of the surviving graphical password techniques. In this survey, we oversees the following issues.

• Comparison of security issues in graphical password and text based password.

• Major design and implementation issues of graphical passwords.

II. BASIC AUTHENTICATION TECHNIQUE

Authentication is a process which allows a user to confirm his identity to an application. Authentication methods are mainly classified into three main areas, such as Token based, Biometric based, and Knowledge based authentication.

A.Token Based Authentication

Token based authentication refers to “what you have”. Here key cards, smart cards, credit card etc. are widely used in order to authenticate to a system. Many of the applications are using token based systems for authentication e.g. ATM Machines

B.Biometric Based Authentication

Biometric authentication system refers to “what you are” type of authentication. It uses physiological or behavioral characteristics of a person for authentication. Here user can use his finger print, iris scan, palm scan, etc. as passwords for

authentication. A biometric scanning device takes a user's biometric data, such as fingerprint scan, and converts it into digital information a computer can interpret and verify. Biometric identification depends on computer algorithm to make a yes or no decision. The main disadvantage of these systems is they are very expensive.

C.Knowledge Based Authentication

The knowledge based authentication systems include the "what you know" type passwords to identify you, such as Personal Identification Number (PIN), password or pass phrase. It is the mostly used authentication system. These systems include both text based passwords and picture based passwords. Picture based passwords also known as graphical passwords involves images or sometimes also referred to drawing passwords. Also it is a tendency that human remembers images easily as compared to text and numbers. Also they provide good resistance to many attacks and provide large password space as compared to text based.

III. GRAPHICAL PASSWORD METHODS

In this section, some existing graphical password techniques are discussed. These techniques have been proposed to solve the limitations of the text based password techniques, because pictures are easier to remember than texts.Graphical password techniques can be classified into four categories which is shown in Fig.1

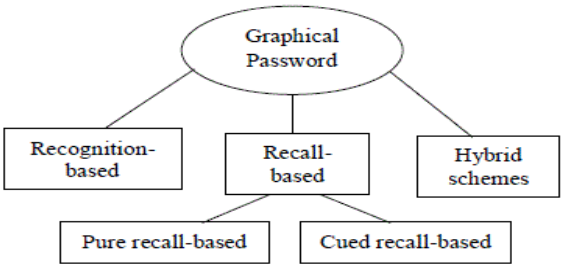

Fig.1 Classification of graphical based password technique

A.Recognition Based Technique

In this technique, users will select images, icons or symbols from a collection of images. For authentication process, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images. Researches were done to find the memorability of these type of passwords and it shows that the users can remember their passwords even after one month. Recognition based systems are also known as Cognometric systems or Searchmetric system. Recognition based systems have been proposed using usability and security considerations, and offers usability.

B.Pure Recall-Based Technique

In this technique, the user need to reproduce the password without any reminders, hints or gestures provided by the system. Pure recall-based methods are also known as Drawmetric Systems. Although this technique is very easy and useful, but it appears that users can hardly remember their passwords. Quiet it is more secure than the recognition based technique.

C.Cued Recall-Based Technique

In this technique, users are provided with the reminders or hints so that he or she can recall their password. Reminders help users to reproduce the password more precisely. This is parallel to the recall based schemes but it is recall with cueing. Cued recall-based system are also called Locimetric Systems as it is related to recognizing location. It is clicked based graphical password.

D.Hybrid Technique

In this technique, the authentication will be typically the combination of two or more schemes. Like recognition based and recall based or textual with graphical password schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing and so on.

IV. VARIOUS ALGORITHMS

A.Recognition based Algorithms

In this section, various recognition based algorithms are discussed.Cognitive Authentication is a recognition based algorithm designed to resist shoulder-surfing and spyware. Déjà vu [3] is a recognition based authentication algorithm which is proposed by Dhamijia and Perrig. In this, the user is provided with a random set of images. It is based on Hash Visualization Technique. PassFace is also a recognition based scheme. Story is another recognition scheme which is similar to PassFaces. Icons (GPI) is considered for solving the hotspot problem. Also another schemes for recognition based password are exit.

B.Pure recall based algorithms

In this section, various pure recognition based algorithms are Draw-A-Secret (DAS)[5] is the pure recall based graphical

ISSN:-2349-3585 |www.ijrdt.org

password algorithm which allows the user to draw their unique password. Passdoodle is a popular recall based system which allows users to generate a freehand drawing as a password. PassShapes is also a pure recall based scheme similar to Passdoodle in which geometric shapes are constructed from an arbitrary combination of eight different strokes and its password space is comparatively small because each stroke is produced from only 8 possible choices. Also other algorithms are present for pure recall based scheme.

C.Cued recall based Algorithms

Various cued recall based algorithms are as follows. PassPoint [2] Algorithm is a cued recall based system. This system agrees any natural image to be used which should be rich enough to have many probable click point. Cued Click-Points (CCP) is also cued recall based scheme in which the next image is exposed on the basis of the location of the previous click-point . Persuasive Cued Click-Points (PCCP) is another cued recall based system. It contains persuasive feature to Cued Click- Points. Random password which are selected to Cued Click-Points are persuasive. Another schemes for cued based technique are exit.

D.Hybrid systems

This schemes are the combination of two or more graphical password schemes. These schemes are presented to overcome the limitations of a single scheme, such as hotspot problem, shoulder surfing, etc. Some of the schemes of recognition based and recall based are joined to improve the hybrid schemes..“Click-a-secret” (CAS) which combines both recognition based and recall based schemes. This scheme allows input and record a secret though interaction with an image. Another hybrid scheme is PassHand and it is a combination of recognition-based graphical passwords and palm-based biometric technique which requires the processed palm images of human rather than usually using faces. Also other hybrid schemes are exit.

V. ATTACKS IN GRAPHICAL PASSWORD SCHEMES

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

A.Brute Force Attack

This is a cryptanalytic attack in which exhaustive key search is done. The main defense against brute force search is to have a sufficiently large password space. In this, every possible option is taken into consideration to break the password until the correct one is found. The password space of text based passwords is 94^N, where N is the length of password and 94 is the number of printable characters excluding “space”[6]. In graphical passwords it is complicated to trace every movement of the mouse or input device so the probability of success using brute force attack is more in textual passwords than graphical passwords. Recognition based graphical passwords be likely to have smaller password spaces than the recall based methods. It is more complex to carry out a brute force attack against graphical passwords than text-based password. Overall, a graphical password is less susceptible to brute force attacks than a text-based password.

B.Dictionary Attack

In this type of attack an exhaustive list of words example dictionary is used to break password. This dictionary consists of words which are most likely selected by the user as passwords. In this attack, an attacker tries to estimate the password from a very large list of words, dictionary. Dictionary will be the collection of all high probability passwords based on prior selections. Unlike brute force attack, dictionary attack uses a systematic key search to crack passwords, that considers only those possibilities which are most likely to succeed, but it cannot crack the password every time as in brute force attack. As recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. In some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. Overall, a graphical passwords are less susceptible to dictionary attacks than text-based passwords [6].

C.Spyware Attack

Spyware is a type of malicious software that goals to gather information about a person or organization without their knowledge, that may send such information to another entity without the user’s knowledge. Spyware attack is usually done by using a key logger or key listener. Spyware is ineffective

ISSN:-2349-3585 |www.ijrdt.org

for cracking Graphical password because it studies only key pressing and mouse clicking events which may not be similar permanently.

D.Shoulder Surfing Attack

This attack mostly occurs in crowded places where people are unaware of the people standing around him. Shoulder surfing is used to gain information such as personal identification number (PIN), password and other secrete data. Graphical password is more vulnerable to shoulder surfing than text based password. Few recognition based technique are designed to resist shoulder surfing attack.

E.Social Engineering Attack

This attack is also known as Description attack. It refers to psychological manipulation of people into performing actions and revealing confidential information. It performs various tricks for the purpose of gaining people's confidence and reveal their confidential information leading to different scams and frauds.

• Major design and implementation issues of graphical passwords

Security:

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

Usability:

One of the main opinions for graphical passwords is that pictures are easier to recall than text sequences. A major criticism among the users of graphical passwords is that the password registration and log-in process take too long, mainly in recognition-based approaches. For example, during the registration stage, a user has to choose images from a collection of images. During authentication phase, a user has to test many images to identify a few pass-images. Users may find this process long and monotonous. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less useful than text based passwords.

Reliability:

The major design issue for recall-based methods is the reliability and exactness of user input recognition. In this method, the error tolerances have to be set sensibly-overly high tolerances may lead to many wrong positives while overly low tolerances may lead to many wrong negatives. So, the more error tolerant the program, the more vulnerable it is to attacks.

Storage:

Graphical passwords need much more storage space than text based passwords. Large amount of pictures may have to be maintained in a centralized database.

VI. CONCLUSION

In this paper, we have conducted a survey of basic password authentication techniques and exiting graphical password based techniques. In this study, different algorithms from recognition-based, pure recall-based, cued recall-based, and hybrid schemes of graphical password authentication have done. 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] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords, School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada, ACM CCS'09, November 9–13, 2009

[2] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). Pass Points: Design and evaluation of a graphical password system.

[3] Dhamija R. and Perrig A., "Déjà vu: A User Study Using Images for Authentication", in Proceedings of 9th USENIX Security Symposium, 2000

[4] Sacha Brostoff, M. Angela Sasse, "Are Passfaces More Usable Than Passwords?, A Field Trial Investigation, 2000.

[5] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords". In 8th USENIX Security Symposium, August 1999.

[6] Arah Habib Lashkari."A new algorithm for graphical user authentication based on rotation and resizing"

[7] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, "Graphical passwords using images with random tracks of geometric shapes," 2008 Congress on Images and Signal Processing. 2008.

[8] S. Chiasson, P.C. van Oorschot, and R. Biddle. "Graphical password authentication using Cued Click Points". In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[9] Varenhorst, Passdoodles: "A lightweight authentication method". MIT Research Science Institute, July 2004.

[10] R. Weiss and A. De Luca, "PassShapes - utilizing stroke based authentication to increase password memorability".

[11] Ali Mohamed Eilejtlawi, "Study and development of a new graphical password system", May 2008. 12

[12] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results", In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

ISSN:-2349-3585 |www.ijrdt.org