JES
Journal of Engineering Sciences

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

Visual Cryptography and Secure Graphical Password Transaction in Online Banking System

J V N Raghava Deepthi #1, Unnam Ramya #2, Gurram Srivalli #3, Raya Divyasree#4, Pothineni Haritha#5

#1 Assistant professor, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#3 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#4 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#5 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)

Abstract: Graphical passwords have been used widely these days. Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as the weakest link in the authentication chain. As people can access their application anytime and anywhere, it increases the probability of exposing password to shoulder surfing attack. In this paper we proposed and examine a multifactor authentication scheme that improves the security of a graphical password system by integrating live video of a physical token that user carries with them. The physical token involves a digital pictures displayed on a physical user owned device such a mobile phone, the digital picture can be any image of the user like picture of palm, face etc. User presents these tokens to the system camera and then enters their password as a sequence of selections on live video of the token the user can remember easily. So this scheme has greater password space as user has to first select token and then clicks on live video.

Keywords—Graphical password, Dictionary attack, Brute force attack

I. INTRODUCTION

Text based passwords are the most widely used authentication method for decades. As Text based passwords consist of numbers and upper- and lower-case letters, these are considered strong enough to resist against brute force attacks. However, a strong text based password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is common case that users may use only one username and password for multiple accounts. Various graphical password authentication schemes were developed to solve the problems and weaknesses associated with text based passwords[21]. Based on some studies it is proved that humans have a better ability to memorize images with long-term memory than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as

the weakest link in the authentication chain. Therefore, a strong authentication scheme should be designed to overcome these problems and weakness in text based password. To overcome this problem, we proposed a novel authentication system based on graphical passwords to resist shoulder surfing attacks. In our system Authentication process is carried out by three techniques: CCP based Authentication, Doodle Based Intersection, PassBYOP. In CCP based Authentication technique[12], user have to select 5 images for password. Each image is divided into grid, from this grid user have to select one cell. The same process is applied to all five images. The password is formed by combining all selected cell from all 5 images. In Doodle based Intersection technique the user has to select one password containing doodles from doodle-grid. While entering password, for first symbol/letter (first doodle from password) user have to click on one doodle from row and one doodle from column whose intersection point is your password's first symbol/letter. Similarly user have to do for remaining doodles from password. In PassBYOP technique[1,2] user can set any real-time image as password. During registration process, user have to take any real-time image. This real-time image is get divided into row-column grid, and from these grid user have to select one block as his/her password. Next time while login, user have to take photo of same real-time image and have to select the same block he/she selected while registration process then feature extraction is performed on that block, and if the feature are matched with the registered image then only the user is get authenticated. The user can set their password using any technique as per his/her convenience. The Internet connectivity has converted the whole world into a global village and at the same time created many security problems[4,7]. For any organization, it is essential to protect its internal resources from security threats from all over the world. Security has three important goals - confidentiality, integrity and availability. Confidentiality refers to providing access to only authorized users, integrity refers to preventing from unauthorized changes and availability refers to providing access to authorized users at any time. Confidentiality can be provided by authentication and encryption. User authentication is the process of verifying the claimed identity of the user. By allowing only legitimate users, system access can be denied to the unauthorized users. There are three basic techniques for authentication– Knowledge based authentication, Token based authentication and Biometric based authentication [1], [2]. Knowledge based authentication technique uses something the user knows (e.g. passwords), Token based authentication technique uses something the user has (e.g. smart card) and Biometric based authentication technique uses unique, measurable characteristic of an individual (e.g. Iris, finger print). Among the three techniques, knowledge based technique is widely used for authentication which includes both text and image passwords [20]. Token based and Biometric based authentications are more secure than knowledge based authentication but, those techniques have their own limitations. Biometric authentication is not yet adopted

for all applications because of the expenditure involved for maintaining the special devices required for that. In the case of Token based authentication, token should always be carried for accessing the service and there is a possibility of losing the token or the token being stolen by some body. To avoid the usage of stolen tokens, an extended token based authentication uses PIN (Personal Identification Number) [7] in addition to tokens for authentication. In general, the three techniques can be used for different types of applications based on the security requirements. In the present situation, every user has to maintain number of user accounts either for office work or for personal work. Biometrics or Tokens can be used for applications with high security requirements and knowledge based authentication can be used for other applications. The traditional method used for knowledge based authentication is textual passwords. However text passwords have their own drawbacks like password which is easy to remember is easy to guess and password which is difficult to guess is also difficult to remember. To avoid this problem, users adopt non-secure strategies like reuse of passwords, or noting down the passwords, or simply forgetting the password. To deal with these problems, researchers have proposed graphical passwords [6] where user visualizes a picture or multiple pictures to create a password, such as selecting portions of an image. This system improves memorability and provides high resistance to brute force and guessing attacks. However, graphical passwords present have own problems like intelligent guessing [11], and shoulder-surfing attacks [3],[13],[14]. These attacks are effective because the portion of images selected as password by the user are also easy for an attacker to observe over shoulders of user or setting up a camera to record the password [3] and they are also predictable—as users always choose hotspots for e.g. eyes in a facial portrait[8],[19]. This issue is problematic .In order to address this issue, a new graphical password system, PassBYOP—Bring Your Own Picture, is proposed that provides security against observation attack ,it combines the user's Password with an image or physically possessed object[15]. This is achieved by using live video of a physical token, such as an object , a photograph, or even an image of a body part (e.g., a palm), for entering a graphical password. However, this scheme also have some drawbacks only a few features are extracted from the click on live video, as click on the video may not be accurately extracted instantly. So the whole security heavily relays on token selected only. And the token may be a part of user's public image which can be on social media websites also. So the scheme has smaller password space. In order to avoid this drawback we have proposed an Improved PASSBYOP in which token can be combined with an orientation of image so that same image if presented at a different angle will not be able to authenticate the user. So not only the token but also the orientation of the token presented is important. In second pass, more precise extraction of frames from live video with accurate feature detection will be done.

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

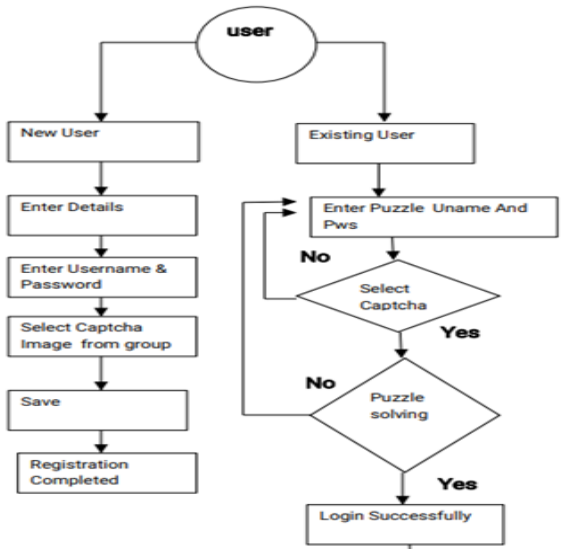
II. RELATED WORK

There are various research work is done in field of security and also in making authentication process more secure. In last few years there are lots of study on password authentication has been done in the literature. Among all of these proposed schemes, our focus is mainly on the graphical-based authentication systems[16]. To design this system we have studied the various papers who have worked on graphical password schemes. Reviews on some of them are given in this section. In order to defend the shoulder surfing attacks with video capturing, Fake Pointer [1] was introduced in 2008 by T. Takada. In addition to the PIN number, the user will get a new ”answer indicator” each time for the authentication process. The answer indicator is a sequence of n shapes if the PIN has n digits. At each login session, the FakePointer interface will present the user an image of a numeric keypad with 10numbers, with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow keys. During authentication, the user must repeatedly move numeric keys circularly as until the first digit of the PIN overlaps the first shape of the answer indicator on the keypad and then confirm a selection by pressing the space key. This operation is repeated until all the PIN digits are entered and confirmed. In 2011,Yang Xiang and Wazir Zada Khan[2] proposed a hybrid system for authentication. This hybrid system is a mixture of both recognition and recall based schemes. In this system during registration user have to select username and password in a conventional manner and then chooses the objects as password. After choosing the objects, the user draws those objects on a screen with a stylus or a mouse. Objects drawn by the user are stored in the database with his/her username. During authentication, the user has to first give his username and textual password and then draw pre-selected objects. These objects are then matched with the templates of all the objects stored in the database. In this system, the user will be authenticated only if the drawn sketch is fully matched with the selected object’s template stored in the database. In 2015, Hung-Min Sun, Shiuan-Tung Chen proposed a novel authentication system Pass Matrix[3], based on graphical passwords to resist shoulder surfing attacks. In Pass Matrix, a password consists ofonly one pass-square per pass-image for a sequence ofn images. The number of images (i.e., n) is user-defined. The user has to select one passsquare for all n images. During the authentication phase the user have to enter username then the system will provide one login indicator to the user .Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical baron its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the preselected pass-square of the image with the login indicator. The same process is followed for all preselected images. Finally, for each image, the password verification module verifies the alignment between the pass-square and the login indicator [7]. Only if all the alignments are correct in all images, the user is allowed to log into Pass Matrix. In 2015, Marcos Martinez-Diaz, Julian Fierrez [21]

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

published a paper in which authentication with free-form sketches is studied. Verification systems using dynamic time warping and Gaussian mixture models are proposed, based on dynamic signature verification approaches. The most discriminant features are studied using the sequential forward floating selection algorithm. Andrea Bianchi, Ian Oakley proposed a Pass BYOP [5] in 2015, a graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a system camera and then enter their password as a sequence of selections on live video of the token. Highly distinctive optical features are extracted from these selections and used as the password.

III PROPOSEDSYSTEM:



We present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Puzzle technology, which we call Puzzle as graphical passwords(CaPRP). CaPRP is both a Puzzle and a graphical password scheme. CaPRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaPRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaPRP also offers an ovel approach to address the well-known image hot spot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaPRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security. We present exemplary CaPRPs built on both text Puzzle and image-recognition Puzzle. One of them is a text CaPRP where in a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaPRP images. CaPRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear. The proposed system offers reasonable security and usability and appears to fit well with some practical applications for improving online security. This threat is wide spread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle

problem than it might appear. Puzzle Login(top of Puzzle technology Using mathematical problems).

IV Implementation:

Puzzle Login

The security and usability problems in text-based Login And password schemes have resulted in the development of Puzzle password schemes as a possible alternative. We can visualize the sum 1+2+3+...+n as a triangle of character . Numbers which have such a pattern of character are called Triangle (or triangular) numbers, written T(n), the sum of the integers from 1 to n time Using Factorial base Login Puzzle Solving.

Random Captcha Selection

A CAPTCHA is a test that is used to separate humans and machines. CAPTCHA stands for "Completely Automated Turing test to tell Computers and Humans Apart." It is normally an image test or a simple mathematics problem which a human can read or solve, but a computer cannot. It is made to stop computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts. It is named after mathematician.

Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of n individuals has the same probability of being chosen for the sample as any other subset of n individuals This process and technique is known as simple random sampling, and should not be

n	1	2	3	4	5	6
T(n) as a sum	1	1+2	1+2+3	1+2+3+4	1..5	1..6
T(n) as a triangle					...	
T(n)=	1	3	6	10	15	21

confused with systematic random sampling. A simple random sample is an unbiased surveying technique.

Image Puzzle Solving

we study how to prevent DoS/DDoSattackers from inflating their puzzle-solving capabilities. To this end, we introduce a new client puzzle referred to as software puzzle. Unlike the existing client puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithm in the present software puzzle scheme is randomly generated only after a client request is received at the server side and the algorithmis generated such that: 1) an attacker is unable to prepare an implementation to solve the puzzle in advance and 2) the attacker needs considerable effort in translating a central processing unit puzzle software to its functionally equivalent GPU version such that the translation cannot be done in real time. Moreover, we show how to implement software puzzle in the generic server-browser model.

OTP Generation

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

Online Bank

Online banking also known as internet banking, e-banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking that was the traditional way customers access banking services.

V Conclusion

Text passwords have been attacked in the recent years successfully. So, to improve the security of text passwords, several guidelines have been proposed to make these passwords hard to be guessed. But as we make these textual passwords difficult to be guessed by others, more they make difficult to be remembered by the user also. To overcome this drawback graphical authentication systems have been proposed recently. There are several graphical authentication techniques. But graphical passwords suffer from a drawback called shoulder surfing attack. To avoid this drawback Improved Pass-BYOP based graphical authentication system is proposed. In this paper we proposed and examine a multifactor authentication scheme that improves the security of a graphical password system by integrating live video of a physical token that user carries with them. The physical token involves a digital pictures displayed on a physical user-owned device such a mobile phone, the digital picture can be any image of the user like picture of palm, face etc. User presents these tokens to the system camera and then enters their password as a sequence of selections on live video of the token the user can remember easily.

REFERENCES

[1] A. Adams and M. Sasse, “Users are not the enemy,” Commun. ACM, vol. 42, pp. 40–46, 1999.

[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, “How to attack two- factor authentication internet banking,” in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.

[3] ARTigo, http://www.artigo.org/.

[4] F. Aloul, S. Zahidi, and W. El-Hjj, “Two factor authentication using mobile phones,” Proc. Comput. Syst. Appl., 2009, pp. 641–644.

[5] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords:Learn- ing from the first twelve years,” ACM Comput. Surveys vol. 44, no. 4, p. 19, 2012.

[6] G. E. Blonder, “Graphical passwords,” U.S. Patent 5 559 961, 1996.

[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567.

[8] S. Chiasson, R. Biddle, and P. vanOorschot, "A second look at the usability of click-based graphical passwords," in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–12.

[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–374.

[10] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based graphical passwords, Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398, 2009.

[11] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.

[12] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2013, pp. 2389–2398.

[13] B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam, "Secure, consumer- friendly web authentication and payments with a phone," in Proc. 2nd Int. ICST Conf. Mobile Comput., Appl., Serv., 2010, pp. 17–38.

[14] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009, pp. 889–898.

[15] A. Gelman, J. Hill, and M. Yajima, "Why we (usually) don't have to worry about multiple comparisons," J. Res. Educ. Effectiveness, vol. 5, no. 2, pp. 189–211, 2012.

[16] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in Proc.SIGCHI Conf. Human Factors Comput. Syst., 2010 pp. 1107–1110.

[17] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 657–666.

[18] S. Hart and L. Staveland, "Development of a multi-dimensional workload rating scale," Human Mental Workload. New York, NY, USA: Elsevier, 1988, pp. 139–183.

[19] H. Kim and J. Huh, "Pin selection policies: Are they really effective?" Comput. Security, vol. 31, no. 4, pp. 484–496, 2012.

[20] G. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vision, vol. 60, no. 2, 91–110, 2004

[21] Ms Grinal Tuscano et al. Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 5, Issue 3, (Part -5) March 2015, pp.60-64

[22]Ayannuga Olanrewaju O., Folorunso Olusegun, "Graphical-text Authentication of a window-based application",2011 International Journal of Computer Applications.

Authors Profile

J V N Raghava Deepthi, M.Tech., working as an Assistant Professor in the Department of Computer Science & Engineering, Qis Institute of Technology.

Unnam Ramya pursuing B Tech in Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, PrakasamDist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

Gurram Srivalli pursuing B Tech in Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, PrakasamDist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

Raya Divyasree, pursuing B Tech in Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, PrakasamDist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

Pothineni Haritha pursuing B Tech in Information Technology from Qis Institute of Technology Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist., JNTUK in 2016-20 respectively.

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254