Improved Pass-BYOP Based Graphical Authentication System Using Video Splitting Method

Garima Mathur
Research Scholar
Garima41mathur@gmail.com
SATI, Vidisha

Prof. Gagan Vishwakarma
Assistant Professor
Gagan.v.sati@gmail.com
SATI, Vidisha

Abstract— **Graphical passwords have been used widely these days. 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

The Internet connectivity has converted the whole world into a global village and at the same time created many security problems. 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 [2]. 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 [7], 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],[11]. 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.

II. Related Work

Graphical password based authentication systems are knowledge based system, which focuses on the fact that human can memorize and recognize images more easily than text password [1]. Graphical passwords are mainly classified into: recall based (*drawmetric*) scheme- based on drawing or sketching shapes on screen, recognition based (*cognometric*) scheme-based on selecting some known items from set of items and cued recall (*locimetric*) schemes-based on selecting regions of a known image [6]. Improved PassBYOP is related to locimetric scheme.

It is a multifactor authentication system that combines physical tokens with selection of frames from a live video. SIFT image processing algorithm [10] is used to extract distinctive features from an image that can be future used for comparison between images. There are also some techniques that can be used to extract features and to characterize the behavior from a video having multiple movements with multiple objects [5].

A. *Multifactor Authentication Scheme*

To boost security multifactor authentication [12] systems can be used, that combines two or more independent processes. Improved PassBYOP is a multifactor authentication system that combines token based authentication along with the selection of frames from a live video to create a password. *Aloul et al.* [16] used mobile phones as the hardware token for one-time password generation. *Dodson et al.* [9] proposed a challenge-response authentication system involving a user snapping a picture of a QR code with a mobile device. The data from this marker generate encrypted data that will be used during login.

However these tools are also susceptible to particular kinds of attack, such as Man-in-the-Middle schemes that alter messages transmitted between a user and the system [4].

B. *SIFT(Scale Invariant Feature Transform)*

SIFT is an algorithm which is used to detect and describe local features of image. From any given image interesting points of the object can be extracted to provide "feature description" of that object. It is important that the features extracted from the training image be detectable even there is a change in image scale, noise and illumination [10].

These features can also be used for object recognition. The recognition is preceded by matching individual features to a database of features from known objects using a fast nearest-neighbor algorithm, followed by a Hough transform to identify clusters belonging to a single object, and finally performing verification through least-squares solution. This approach to recognition can robustly identify the objects among clutter and occlusion while achieving near real-time performance.

C. *Matching Technique- SSIM (Structural Similarity Index Mapping)*

SSIM is a standard algorithm used for measuring the similarity between two images. SSIM is designed to provide an improvement over traditional methods such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which are proven to be inconsistent. Equation (1) is used to compute SSIM.

$$\mathrm{SSIM}(x,y)= \frac{(2\mu_x\mu_y+c_1)(2\sigma_x\,\sigma_y+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+_{c2})} \qquad (1)$$

Where,

μ_x: average of x

μ_y: average of y

σ_x^2: variance of x

σ_y^2: variance of y

σ_x , σ_y: covariance of x and y

$c_1= (k_1L)^2$, $c_2= (k_2L)^2$:two variables to stabilize the division with weak denominator

L: dynamic range of pixel values

K_1=.01, k_2=.03 by default

The SSIM formula is based on three comparison measurements between the samples of x and y: luminance (L), Contrast (C) and Structure (S).

The individual comparison functions are shown in (2), (3) and (4)

$$l(x,y) = \frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1} \qquad (2)$$

$$C(x,y) = \frac{2\sigma_x\,\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2} \qquad (3)$$

$$S(x,y) = \frac{\sigma_{xy}+c_3}{\sigma_x\,\sigma_y+c_3} \qquad (4)$$

$$c_3=c_2/2$$

SSIM is then weighted combination of-

$$\mathrm{SSIM}(x, y) = [l(x,y)^{\alpha}.c(x,y)^{\beta}.s(x,y)^{\gamma}]$$

$$\alpha ,\beta ,\gamma=1 \text{ by default}$$

The resultant SSIM index is a decimal value between -1 and 1.SSIM will result +1 only when the two data sets are identical, and -1 when data is completely different

SSIM (presented image, original image) is commonly used syntax for SSIM calculation.

III. Improved Pass-BYOP method for graphical authentication

A. *Pass-BYOP (Pass Bring Your Own Picture)*

This method is a multi-pass authentication [12] scheme which involves- A token which can be any image of the user like picture of palm, face etc. And a live video is to be clicked at any point of time the user can remember easily. So this Pass-BYOP scheme has greater password space as user has to first select token and then clicks on live video.

The PassBYOP transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multifactor authentication method. This makes PassBYOP *Resilient-to-Internal- Observation* [4],[15] meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communication between the authentication device and verification system.

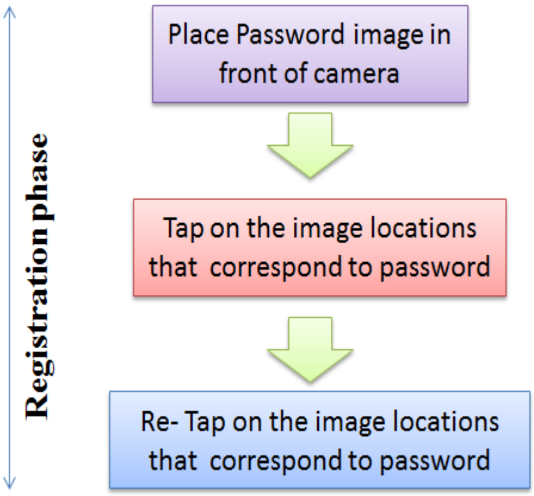
Registration phase
Place Password image in front of camera
Tap on the image locations that correspond to password
Re- Tap on the image locations that correspond to password

Fig 1: Figure showing registration phase of Pass-BYOP

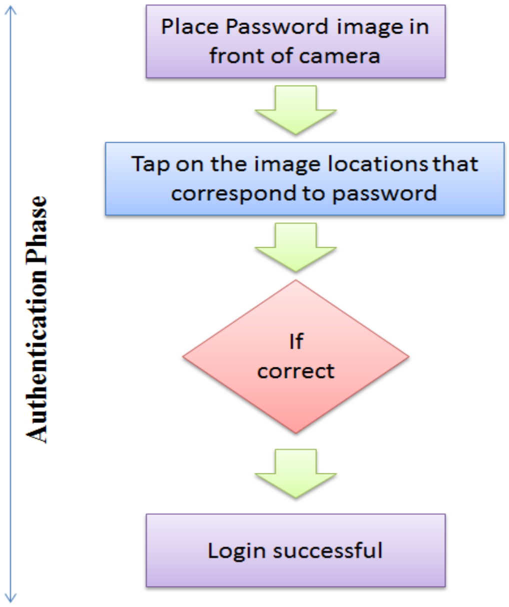
Authentication Phase
Place Password image in front of camera
Tap on the image locations that correspond to password
If correct
Login successful

Fig2:Authentication phase of Pass-BYOP

B. *Drawback of Pass-BYOP*

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.

C. *Proposed approach*

The 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 the second pass more precise extraction of frames from live video with accurate feature detection will be done. Selecting sequence of frames from thousands of frames will act as a password.

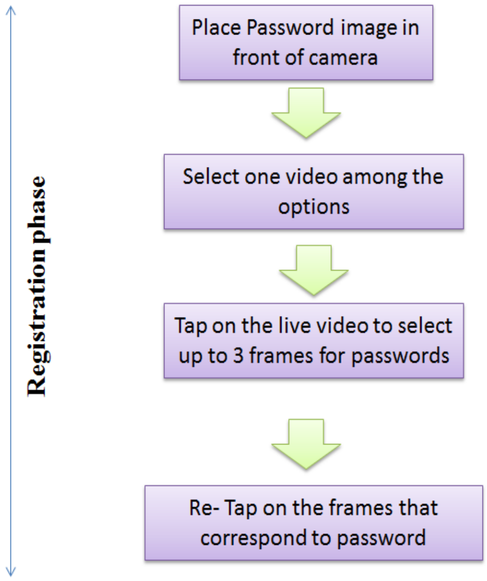
Registration phase
Place Password image in front of camera
Select one video among the options
Tap on the live video to select up to 3 frames for passwords
Re- Tap on the frames that correspond to password

Fig 3: Figure showing registration phase of improved Pass-BYOP

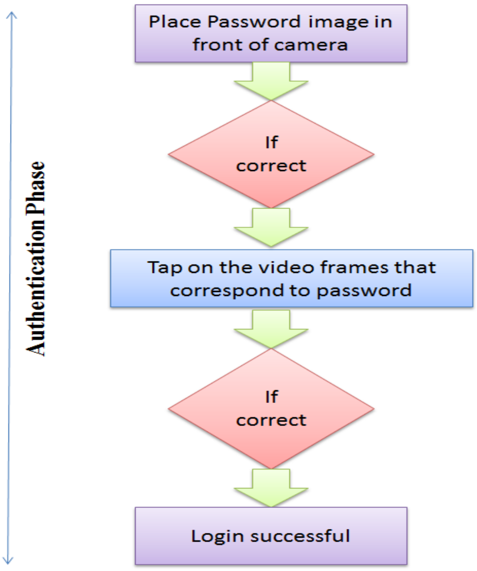
Authentication Phase
Place Password image in front of camera
If correct
Tap on the video frames that correspond to password
If correct
Login successful

Fig 4: Authentication phase of improved Pass-BYOP

During registration phase user have to place the token image in front of camera and then select frames of a live video to create the password .Selecting 3 frames out of thousands of frames will make it difficult to guess by an intruder and will boost the security.

During authentication phase user has to first recognize the pre-chosen token image, and then selecting 3 frames from the pre-chosen video, if correct password is guessed user will login successfully.

The Feasibility studies of Improved PassBYOP examine its reliability, usability, and security against observation. The reliability study suggests appropriate system thresholds of 90% of which must geometrically match originals in order to be judged equivalent. The usability study measures task completion times and error rates. Finally, the security study highlights Improved Pass-BYOP's resistance to observation attack shoulder surfing, camera based observation, or malware.

Comparison between Pass-BYOP and improved Pass-BYOP	
Pass-BYOP	**Improved Pass-BYOP**
1) Pass-BYOP is based on selecting an image from database during registration and its tapped regions only.	1) Improved Pass-BYOP is based on image selected from registration database and a frame of video selected from running video.
2) Complexity depends only on the number of blocks formed in an image during registration.	2) Complexity depends on image selected from database and largely on the frame of video selected during registration.
3) In an image there can be smaller number of blocks because if number of blocks increase then user will not be able to identify the block easily.	3) Even a small video consists of large number of frames. So, its complexity is high and make it difficult to crack but easy to remember for user.
4) Here tolerance range for selecting a point in any block is kept fixed. Those that felt outside the central 70x70 selection box will be discarded and remaining portion will be treated as password.	4) There is no such fixed tolerance range in improved pass-BYOP
5) Hotspot problem affects the performance of algorithm	5) Here hotspot problem is not considerable as compared to Pass-BYOP.

IV. Results

Objective results from login phase are shown in table 1.These data were tested for 50 users which are trying to guess password of another user .The possibility of guessing the secret image as well as video frames successfully is almost zero. However the possibility of guessing the secret image i.e. the token image is 2 because there may be a possibility that this image is available at any social networking site .The possibility of guessing the frame from a video and guessing both image and frame is zero.

Table 1

Tested by 50 users for guessing password of another user		
Success	Secret Image and video frame successfully guessed	0
Failure	Correct secret image	2
	Correct Video frame	0
	Correct Secret Image with correct video frame	0
	None correct	48

The PassBYOP authentication scheme provide resistance to observation and accuracy of 80% where as Improved PassBYOP provides an accuracy of 95% during registration phase and 99% during authentication phase.

TABLE 2

Accuracy of proposed scheme within 5 tries	
Registration Phase	95%
Authentication Phase	99%

The time analysis for authentication is shown in table 3

TABLE 3

Time analysis for authentication phase			
	Mean	**Median**	**Standard deviation**
Time (in sec)	173	118	41

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] 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

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

[3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, “A Shoulder Surfing Resistant Graphical Authentication System”,in IEEE Trans. on Dependable and Secure Computing,2015.

[4] 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

[5] S. Jain, G. Vishwakarma, and Y. K. Jain, “An Artificial Approach of Video Object Action Detection by Using Gaussian Mixture Model,” *Int. J. Eng. Trends Technol.*, vol. 42, no. 2, pp. 49–55, 2016.

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

[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, 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.

[9] 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.

[10] G. Lowe, “Distinctive image features from scale-invariant key points,” *Int. J. Comput. Vision*, vol. 60, no. 2, 91–110, 2004.

[11] Z. Zhao and G. J. Ahn, “On the security of picture gesture authentication,” in *Proc. 22nd USENIX Security Symp.*, 2013, pp. 383–398.

[12] B. Schneier, “Two-factor authentication: Too little, too late,” *Commun. ACM*, vol. 48, no. 4, p. 136, 2005.

[13] F. Tari, A. Ozok, and S. Holden, “A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords,” in *Proc. 2nd Symp. Usable Privacy Security*, 2006, pp. 56–66.

[14] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” in *Proc.Working Conf. Adv. Visual Interfaces*, 2006, pp. 177–184.

[15] Andrea Bianchi, Ian Oakley, and Hyoungshick Kim, “PassBYOP: Bring Your Own Picture for Securing Graphical Passwords” in IEEE Trans. On Human-Machine System, May /Aug. 2015.

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