International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 4 459 – 464

Authentication System Using Text Passwords Along With Persuasive Cued Click Points

Ms Anita Lahane
Asst Professor, Dept of Computer Engg
MCT's Rajiv Gandhi Institute Of Technology
Mumbai,India
anitalahane@yahoo.co.in

Samruddha Wagh
Student, Dept of Computer Engg
MCT's Rajiv Gandhi Institute Of Technology
Mumbai,India
samruddhawagh@gmail.com

Shreyans Jain
Student, Dept of Computer Engg
MCT's Rajiv Gandhi Institute Of Technology
Mumbai,India
shreyansjain3381@outlook.com

Mandeep Singh
Student, Dept of Computer Engineering
MCT's Rajiv Gandhi Institute Of Technology
Mumbai,India
mandeepsingh1018@gmail.com

Gurunath Vishwakarma
Student, Dept of Computer Engineering
MCT's Rajiv Gandhi Institute Of Technology
Mumbai,India
guruvishwakarma3@gmail.com

Abstract—This paper presents an implementation of a two level authentication using a combination of text passwords and persuasive cued click points on three or five images. The most common method for authentication is textual passwords. Though textual passwords are easy to remember, they are vulnerable to eavesdropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords have been introduced as an alternative to textual passwords. But same as textual passwords, shoulder surfing attacks make most of the graphical schemes vulnerable. To address this problem, textual passwords can be combined with graphical schemes in what gives a two level security without the use of additional hardware. This paper also presents an evaluation of the text based passwords and graphical password schemes which have been tested previously but failed, including usability and security evaluations.

Keywords--*Authentication, Persuasive Cued Click Points, shoulder surfing, social engineering.*

*****

I. INTRODUCTION

1.1 Graphical Passwords

Graphical passwords have become very popular in recent times, a graphical password is one that involves images instead of text thereby making them easier than a text-based password for most people to remember. Suppose an 11-character password is necessary to gain entry into a particular computer network. Instead of wq2q8KiJ89c, for example, a user might select images of Saturn (from among a screen full of real and fictitious planets), the country of Mexico (from a map of the world).Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. Even simple attacks like social engineering lead to fast results now that personal information is easily available on social media sites like Facebook.

1.2 Persuasive Cued Click Points

PassPoints based login requires a user to click on a pre-decided number of points on a single image but these systems can become very vulnerable as hotspot analysis can be done or if there is click point logger or mouse logger every click can be stored. A new alternative to PassPoints is Persuasive Cued Click Points wherein instead of clicking on the same image multiple times , there are a number of images which are pre decided either by the user or the system and each image will have a single user selected point whose suggestion will be given by the system ,on clicking which the next image will appear and this will continue till all the correct points have been clicked on the respective images. The images will be displayed in random order each time we try to login thus making it difficult for any hacker to analyse the clicks and thereby making it difficult to penetrate.

II. ANALYSIS

The below mentioned papers were thoroughly studied and it was found that Persuasive Cued Click Point based system

would be the best solution for our problem as compared to PassPoints or textual passwords.

The existing system involved only a single level authentication system using only Persuasive Cued Click Points provided higher success rates while logging in difficult to guess and crack the click points as compared to text passwords. Guessing attacks failed most of the time, hotspots and click point clustering failed most of the times, social engineering and phishing were also failing.[1] Still it offers some disadvantages such as more complexity at server end and while implementation, users faced difficulties while selecting passwords and remembering the positions of clicks at times, malware did record click points to some extent as the system involved only one type of authentication hence in the future an automated hacking tools could be developed.

Existing system presents a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration.[9]

Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in Fig 4.A drawback of this system is the vulnerability to shoulder surfing.

Figure 1 . Random images used by Dhamija and Perrig

In this system AES algorithm is used for encryption and decryption of the clicks generated on images. When the user clicks on image, x and y coordinates are generated and these coordinates are then encrypted in AES and stored in database. In this paper selecting password that is easy for user is a tedious task, discouraging user from making such choices. The user has to click on the image thrice. If the clicks are correct then the login is successful. And if the click points are wrong then the user is asked to validate 3 level click point.[5] Advantages of this approach are better security as compared to single level, Difficult to guess and crack the click points as compared to text passwords. Guessing attacks failed most of the time, capturing login instances won't affect the other login instances i.e. every time new instance is created hence last instance is not considered, it was easy for users to select passwords and remember the positions of clicks.

Still it offers some disadvantages such as more complexity at server end and while implementation, malware did record click points to some extent, shoulder surfing is one of the attack that can be performed very easily as this system works on single image, but provides best result with minimum overhead

III. PROPOSED SYSTEM

Hotspots and patterns formed by click-points reduce the security of click based graphical passwords, as attackers can use skewed password distributions to guess and prioritize higher probability passwords for more successful guessing attacks. Visual attention research shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain a problem.

The User registration Module will require the user to enter personal information along with a username and a password which would be textual. Every user as we know has different needs so it would be his choice whether to continue with just one text password or if he requires a two level authentication which would be highly recommended . The user would be given two options for the graphical password, he can either choose from one of the system provided default images or he may upload images according to his choice from his hard disk. Along with the image selection he would also be asked to select the click points on that particular image which would be securely encrypted with certain modifications from our end so that the encrypted data would not be very predictable or cracked by hackers.

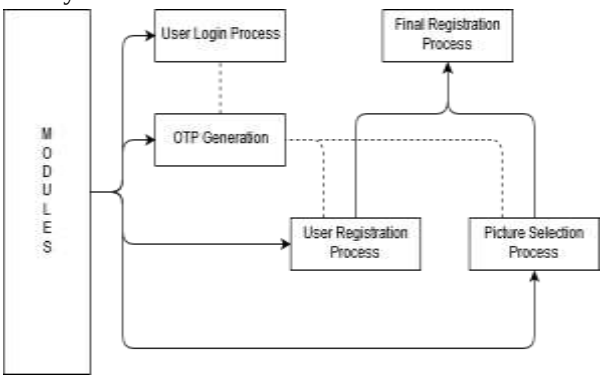

Figure 2. Basic architecture of the system

Once the user has signed up and is a registered user he will be allowed to login to the system by entering the username and text password, The images selected will appear in any order, irrespective of whether the selected point is correct or not the next image will appear and only at the end will the user be informed if the choice was correct or incorrect, this is done in order to make it difficult for any hacker to breakthrough in a few attempts, as he will feel he is making a progress in penetrating but actually he is only wasting attempts which is capped to 3 or 5 after which he will be barred.

In case the user forgets his textual password or Image based password ,he has the option of forgot password wherein he will receive an OTP on his Email as well as mobile number which he entered at the time of registration, this OTP will only be valid for a finite amount of time after which it will expire.

 ISSN: 2321-8169
459 – 464

Figure 3. Snapshot of GUI

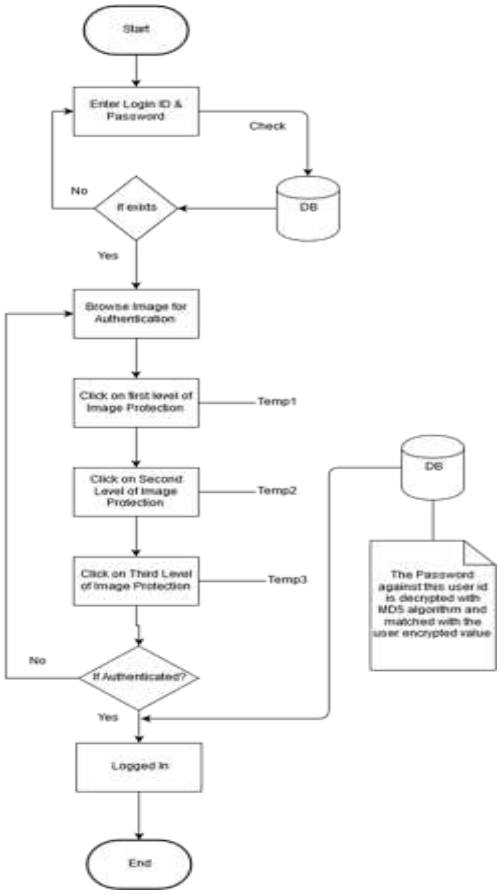

Figure 4.Login Process Flowchart

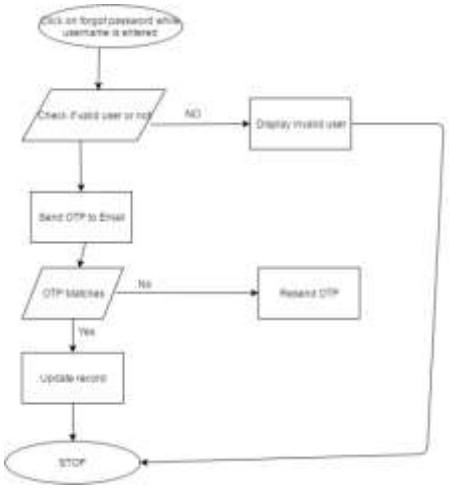

Figure 5. OTP process flowchart

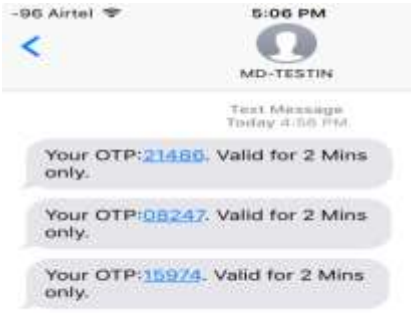

Figure 6.OTP received on SMS

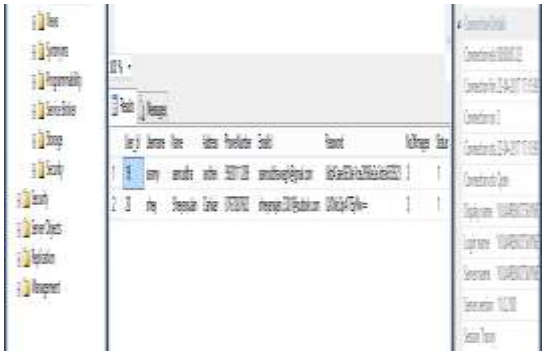

Figure 7. MD5 encrypted text password and image points

IV METHODOLOGY

4.1 MD5-TEXT

Message-Digest algorithms characteristics

Message-Digest (Fingerprint) algorithms are special functions which transform input of (usually) arbitrary length into output (so-called "fingerprint" or "message digest") of constant length. These transformation functions must fulfill these requirements:

1. No one should be able to produce two different inputs for which the transformation function returns the same output.
2. No one should be able to produce input for given prespecified output.

Message-Digest algorithms serve in digital signature applications for guaranteeing consistency (integrity) of data. Commonly used model is as follows (message-digest in cooperation with asymmetric cryptography):

Sender's side

Sender creates input message (M) and computes its message digest (sMD).

Then he uses his private key and encrypts message digest (esMD).

Encrypted message digest (esMD) is attached to the input message (M) and the whole message (M-esMD) is sent to receiver.

Reciever's side

Receiver gets the message (M-esMD) and extracts the encrypted message digest (esMD).

Then he computes his own message digest (rMD) of the received message (M).

He also decodes received message digest (esMD) with sender's public key and gets decoded message digest (desMD).

Then he compares both message digests (rMD ?= desMD).

When both message digests are equal, the message was not modified during the data transmission. All the Message-Digest algorithms take input message of arbitrary length and produce a 128-bit message digest.

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash.

MD5 hash algorithm consist of 5 steps:-

Step 1. Append Padding Bits

Step 2. Append Length

Step 3. Initialize MD Buffer

Step 4. Process Message in 16-Word Blocks

Step 5. Output

4.3 SECURITY

Any proposed authentication scheme needs to be evaluated in terms of possible threats. We begin by clarifying our target scenario for CCP and the particular
assumptions made about the system. We recommend that CCP be implemented and deployed in systems where offline attacks are not possible, and where any attack will be made against an online system that can limit the number of guesses made per account in a given
time period (this limit should include restarts as well).

A key advantage of CCP over PassPoints is that attackers need to analyze hotspots on a large set of images rather than only one image since they do not
know the sequence of images used for a given password. Secondly, using different subsets of images for different users means that an attacker must somehow gather
information about the specific subset assigned to the current user.

4.3.1 Guessing Attacks

Against PCCP the most basic guessing attack is a bruteforce attack, with expected success after examining half of the password space. However, asymmetrical password distributions could allow attackers to improve on this attack model.

4.3.2 Capture Attacks

Password capture attacks occur when attackers directly obtain passwords by blocking user-entered data, or by tricking users into disclose their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge based authentication schemes), capturing one login instance allows deceitful access by a simple replay attack. Shoulder-surfing: All three cued-recall schemes discussed (PCCP, CCP, PassPoints) are endangered to shoulder surfing although no published experiential study to-date has examined the extent of the threat. Observing the approximate location of click-points may reduce the number of guesses necessary to determine the user's password. A considerably more complicated substitute is to make user input invisible to cameras, for example by using eye-tracking as an input mechanism many images from the server instead of only one.

4.3.3 Malware

Malware is a major interest for text and graphical passwords, since keylogger, mouse-logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

All these security drawbacks could be overcome by using encryption algorithms.

V. TEST RESULTS

Figure 8. Password Complexity Validation

Figure 9. Random images appearing after wrong click

Figure 10. Successful login

 ISSN: 2321-8169
459 – 464

Test Case ID	Step Description	Expected Result	Actual Result	Pass/Fail
1	Basic Registration Process: To check integrated working of registration process.	Successful Registration	Registration is successful as long as all complexity conditions for the text password are satisfied.	Pass
2	Image Selection: Should accurately fetch the images from the memory and display in the viewport and display click box for the image.	Accurate in fetching image and displaying click box	Accurate in fetching image and displaying click box. Sometimes displaying difficult to remember boxes which can be refreshed for new box	Pass
3	Login Process: When text password is wrongly entered	Should display invalid username and password	Displays pop up window which displays the error message "Invalid username or password"	Pass
4	Login Process: Correct username and password but incorrect click on the image	Should display the image after text password entry and random images after wrong click.	Random images are displayed once there is a wrong click as expected and then no access is given.	Pass
5	Login Process: Correct username & password and correct click on all 3/5 images	Should successfully login and welcome message window should be displayed.	Application is very stable. After successful login, welcome image is displayed	Pass
6	Forgot password Process:On entering valid username, OTP must be sent to User's registered Email ID and mobile number using which he can reset entries.	OTP should be received on both Email and mobile within a few seconds	OTP in all test cases was successfully and quickly received on Email ,but there was a delay of few minutes while receiving the SMS OTP due to SMS Service provider's issue	Pass
7	Hacking attempts by unauthorized user	Should prevent unauthorized access.	We asked 5 of our friends to try and gain access, 2 of them were able to clear the text password stage by using social engineering but none of them were able to get past the click (graphical) password stage.	Pass

Average time taken for registration(3 images): 63 seconds
Average time taken for registration(5 images): 80 seconds
Average time taken for login: 23 seconds

VI CONCLUSION

The implemented system not only provides a user friendly login interface but also provides better security compared to the existing system of textual and graphical passwords with a reduced overhead ,the time required for the login process is a

little more than a normal login procedure. But for a safer security mechanism, this is a small compromise.

The future scope of this system could be stronger encryption algorithms ,gestures for portable devices and combination with existing systems such as biometrics or RFID's. Adding more number of images and increasing the number of clicks per image would significantly increase the level of security .

VII ACKNOWLEDGEMENT

We thank Prof. Ms. Anita Lahane for her support and for providing the necessary guidance concerning the implementation of our project. We would also like to thank Dr. S.Y Ket, HOD, Department of Computer Engineering, Rajiv Gandhi Institute of Technology and our Principal Dr. Udhav Bhosale for their support and facilities provided to us for the same.

REFERENCES

[1] Sonia Chiasson, P.C. Van Oorschot and Robert Biddle, ElizabeethStobert, Alain Forget, "Persuasive Cued Click Points: Design Implementation, and Evaluation of a knowledge based authentication mechanism", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.

[2] MadhuriAchmani, RadhikaDehaley, AnujaGoanlkar, AninditaKhade, **"** Two level Authentication System Based on Pair Based Authentication and Image Selection", in IJRADET Vol. 4 Issue 4, April 2016.

[3] Tara H R, Usha T, Ganeshayya I Shidaganti, "Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points", in IJERT Vol. 2 Issue 6, June 2013.

[4] Sonia Chiasson, P.C. Van Oorschot and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" in ESORICS, September 2007

[5] SmitaChaturvedi, Rekha Sharma, "Securing Image Password by Using Persuasive Cued Click Points with AES Algorithm." In IJCSIT Vol. 5 Issue 4, 2014

[6] Suresh Paigidala, C. ShobaBindu, "Improved Persuasive Cued Click Points for Knowledge-Based Authentication" in IJCSIT Vol. 4 Issue 6, 2013

[7] SnehalAmbade, ShubhamBhivgade,Saurabh Trivedi, S. B. Lanjewar,"Image Based Authentication Using Persuasive Cued-Click Point Technique" in International Journal of Software & Hardware Research in Engineering, Vol. 2 Issue 3, March 2014

[8] M Sreelatha, M Shashi, M Anirudh, Md Sultan Ahamer, V Manoj Kumar,"Authentication Schemes for Session Passwords using Color and Images" in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[9] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[10] Ms Anita A. Lahane ,Gurunath Vishwakarma,Samruddha Wagh,Mandeep Singh and Shreyans Jain, "Combination of Persuasive cued click points and textual passwords for two level authentication,"International Journal of Research In Science & Engineering Special Issue 7-ICEMTE March 2017 p-ISSN: 2394-8280 e-ISSN: 2394-8299.