International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-8, August 2014

Enhancement of Security Using Three Level Authentications

Mr. Amit Kashinath Barate, Mrs.Sunita S. Shinde, Ms. Prajakta Umesh Mohite

***Abstract*—The authentication system provides the secure environment for the resources. User authentication and identification have always represented the challenging aspects of security systems. The text based authentication and user identification are not sufficient to address to address these issues. The text based security is considered retrograde and obsolete for current security threats that easily undermine authentication, identification and non-repudiation. A crucial usability goal for authentication systems is to support users in selecting better passwords. Often users create memorable passwords that are easy for attackers to guess, whereas the strong system-assigned passwords are difficult for users to remember. Therefore, modern day researchers opt for alternative methods. Here a graphical password system with Onetime Password (OTP) is described. In the proposed work, a click-based graphical password scheme called Persuasive Cued Click Points (PCCP) is used along with pass point's password. In this system, a password consists of sequence of few images wherein a user selects one click-point per specific region of an image and on the last opened image user has to reselect the sequence of clicks for that specific image. Using the instant messaging service available through internet, user will acquire the One Time Password (OTP) after image authentication. A user will receive an OTP through Email for the sake of verification to the system. The OTP is generated using random algorithm hence a unique OTP is produced each and every time the user requests for logins. Thus in this system, in order to access information an user has to enter correct image password and also verify the OTP sent to him. Due to integration of three level authentications the security is enhanced in this system.**

***Index Terms*—Authentication, PCCP password, Pass points password, OTP, security.**

I. INTRODUCTION

One of the major functions of any security system is to control access of people in or out of protected areas, such as physical buildings, information systems and our national borders. Computer systems and the information they store and process are valuable resources that need to be protected. Access to computer systems is most often based on the use of alphanumeric passwords. However, users face difficulty in remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

- Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
- Passwords should be secure, i.e., they should be random and hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

To overcome the problems associated with text password based authentication systems, many researchers have proposed the concept of graphical password and developed the alternative authentication mechanisms. Graphical password systems are promising alternative to conventional password based authentication systems. For enhancing the security of system, multiple authentications can be one of the solutions. In this study, we propose to increase the security by using 3 level authentications by integration of text password, Graphical password (pass click points and percussive Cued click points) and automated one time generated password received through email or phone number given at the time registration by user.

II. GOAL OF PROPOSED WORK

Following are the main goals of this paper

- To enhance the security of the system
- To make password more stronger and user friendly
- To reduce probability of guessing of password

III. RELEVANCE

Security is a user's primary task and typically involves an extra step in addition to the main task, such as having to log in to read one's email. Users need security features to be as non-disruptive as possible, but still need them to work properly to preserve integrity and privacy.

To increase the security of system, graphical passwords are good alternatives to text passwords. Pass points passwords provides more security than text password, however, during password selection an user can select any pattern or hot spots in the image thus there is possibility of hacking for pass points password by attacker. Furthermore, the percussive Cued click point could add up to the pass point password to further improve the security. There is requirement to enhance the security at higher level and to fulfil this necessity integration of text password, graphical password and automated generated one time password is one of the solution.

IV. LITERATURE REVIEW

Ahmad Almulhem et al. have proposed an alternate method for the text passwords [10]. They suggested replacing text passwords by graphical passwords, which makes password

Manuscript received Aug 17, 2014.

Mr. Barate Amit K, Department of Electronics and Telecommunication, Shivaji University .

Prof Shinde S.S., Department of Electronics and Telecommunication, Shivaji University .

Ms. Mohite Prajakta U., Department of Electronics and Telecommunication, Shivaji University .

more memorable and easier for people to use. In addition, the graphical password is more secure.

Ahmet Emir et al. proposed the authentication system 'Pass Points Graphical Password' [11], which consists of a sequence of click points (say 5 to 8) that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no other role than helping the user remember the click points. Pass point makes password more stronger and significant password.

The introduction and evaluation of various methods for purely automated attacks against pass point-style graphical passwords system have been given by Paul C. van Oorschot et al.[12]. For generating these attacks, they introduce a graph-based algorithm to efficiently create dictionaries based on heuristics such as click-order patterns (e.g., 5 points all along a line). Some methods combine click-order heuristics with focus of-attention scan-paths generated from a computational model of visual attention.

Sonia Chiasson et al. have proposed and implemented the 'Persuasive Cued Click- Points system' [1], which is effective in reducing the number of hotspots (areas of the image where users are more likely to select click points) but still maintaining usability. Rather than five click-points on one image, CCP uses one click-point on each of a sequence of five images. The next image displayed is determined by the location of the previously entered click-points. The claimed advantages are that logging on becomes a true cued-recall scenario, wherein seeing each image triggers the memory of a corresponding click-point. Thus remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time.

V. PROPOSED METHOD

The objective of the current study is to enhance the security of system by integration of text password, graphical password (pass point click and Persuasive Cued Click-Points) and automated generated one-time password (received through an automated email or mobile to the authentic user).

A. Level 1 –text based password

Fig 1. Screenshot of text based password registration

This level contains the text password which may be alphabet, numbers or any characters. When the user registers for first time in a system, they create a user ID and text password. To login, a user has to reenter the text password which he had selected at the time of registration.

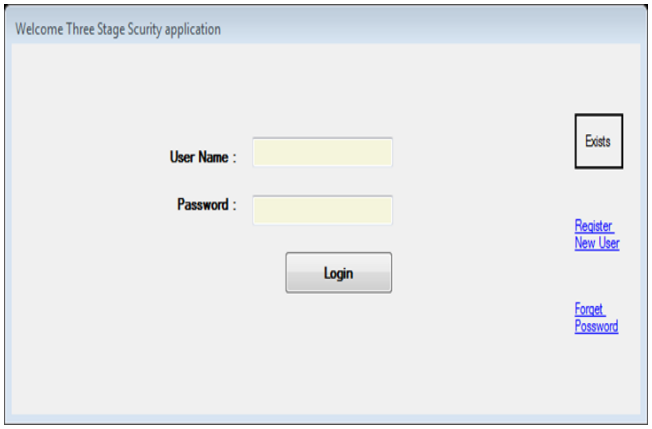

Fig 2. Screenshot of text based password login

B. Level 2 – image based password

This level contain graphical password which is main component or heart of this project of this project. It is an integration of Persuasive Cued Click-Points and pass point. The user has to select first image which he had selected at the time of registration. A click on this image will open the next image and each click on image will decide the next image. So for entering in the system he has to click on same location in correct sequence which he had selected at the time of registration. In proposed work, both the PCCP password and PassPoints password is made up of 4 click points each.

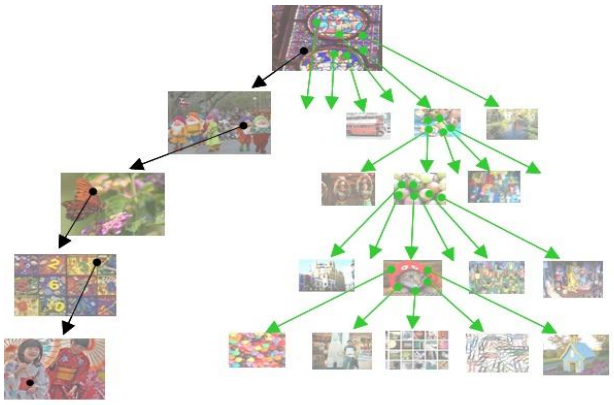

Fig 3. Example of PCCP password

After four correct PCCP clicks, the last image will open and on this image user has to click at four correct locations which is the pass point system.

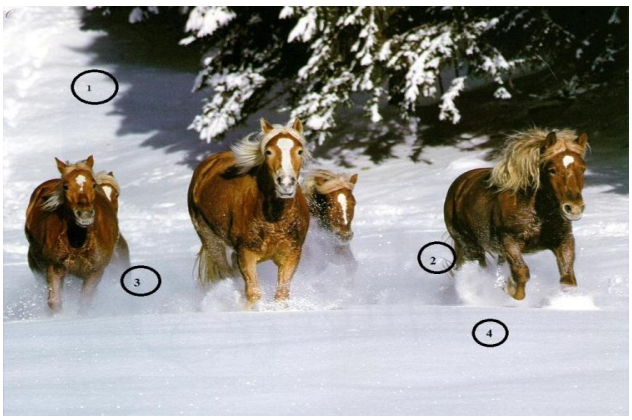

Fig 4. Example of pass points password

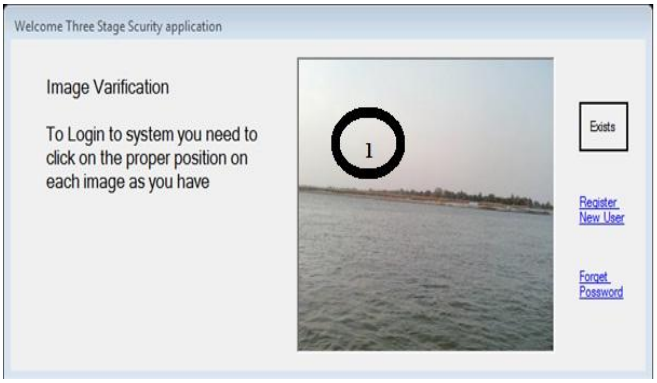

Fig 5. First click of PCCP password

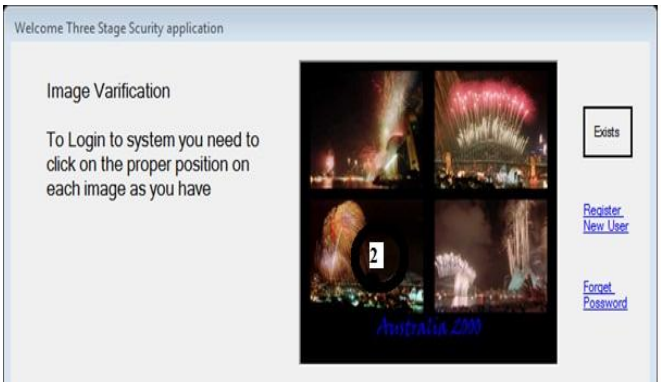

Fig 6. Second click of PCCP password

Fig 7. Third click of PCCP password

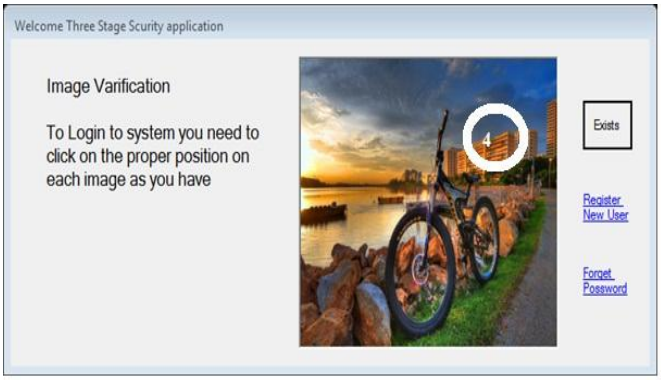

Fig 8. Forth click of PCCP password

Figure 5-9 shows how after entering the correct PCCP password last image will be open. On this opened image user has to enter the four clicks in correct sequence. If the users enter both text password and image password correctly; only then the user is permitted to the third level of authentication.

Fig 9. Four clicks of pass point password

C. Level 3 – (One Time Password)

After the successful clearance of the above two levels, the 3-Level Security System will then generate a onetime numeric password that will be valid only for one login session. The authentic user will be informed of this one time password through his email-id.

The notations used in OTP algorithm

Symbol		Represents
T	-	It is the Time value, the changing Factor.
Key	-	Shared secret between client and server.
Digit	-	Number of digits in an HOTP value.

Description of algorithm:

The OTP algorithms are based on an increasing time value function and a static symmetric key known only to client and server. In order to create the OTP value, a HMAC- SHA-1 algorithm was used. Since the output of the HMAC-SHA-1 calculation is 160 bits, we had to truncate this value to a smaller digit so that it can be easily entered.

The algorithm can be described in 3 steps:

Step 1:
Generate the HMAC-SHA-1 value
Let HMK = HMAC-SHA-1(Key, T) // HMK is a 20-byte

Step 2:
Generate a hex code of the HMK.
HexHMK=ToHex (HMK)

Step 3: Extract the 8-digit OTP value from the string
OTP = Truncate (HexHMK)

Fig 10. Screenshot of level 3 of authentication system

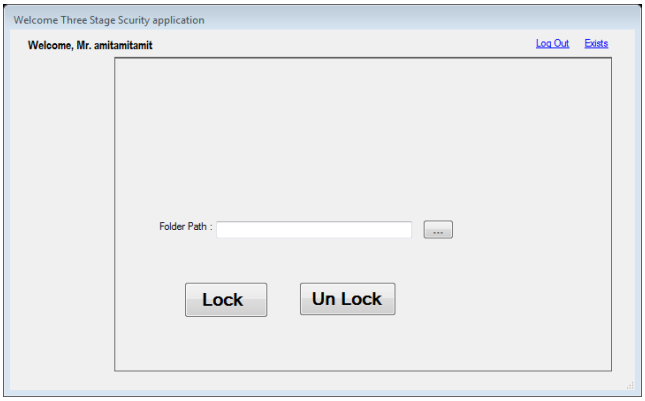

Fig 11. Screenshot of system when user enters all correct passwords correctly

After entering the all three password correctly a user will enter in the system. Figure 11 shows the system after entering all passwords correctly. From this window a user can authenticate any folder of any size. For authentication of a folder, user has to select path of folder and then click on the lock or unlock button.

D. Flowchart

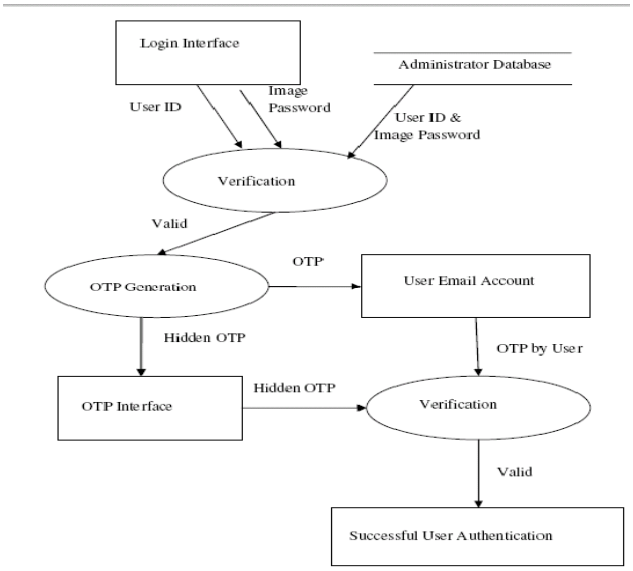

Fig 12. Flowchart of three level authentication system

Flowchart of proposed method is shown in the Fig. 12.

VI. Conclusion

- Three types of authentication systems are integrated together in order to enhance the security of the system.
- It will certainly be a great enhancement especially in the areas where high security is the main issue and time complexity is secondary. For instance, application of this system at a firm or industry or institute where it will be accessible only to some higher designation holding people, who need to store and maintain the crucial and confidential data secure.
- Image password present at the second level of authentication system is the main component of this system and is made up of combination of PCCP and pass point clicks password. This will significantly reduce the chances of guessing of password by attacker.
- OTP generation done by random number generator algorithm (used during password creation) is impossible to be exploited during an attack.
- This tool can be used for folder of any size, thus, there is no limit on size while authentication.
- It can be used to authenticate folders which may contain files of any type i.e. this system is able to provide security to all type of files.
- It can be used to authenticate the folders located even on external hard disks.

Acknowledgment

I would like to acknowledge and extend my heartfelt gratitude to my guide Prof. Sunita S. Shinde for her encouragement and support

References

[1] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, March 2012.
[2] World Research Journal of Human-Computer Interaction. ISSN: 2278-8476 & E-ISSN: 2278-8484, Volume 1, Issue 1, 2012, pp.04-08.
[3] International Journal of Pure and Applied Sciences and Technology, ISSN 2229 – 6107, Volume 1, Issue 2, 2010, pp. 60-66.
[4] Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.
[5] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006.
[6] FABIAN MONROSE AND MICHAEL K. REITER, Ch09.10346 Page 161 Friday, August 5, 2005, Graphical Passwords.
[7] Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget, Department of Computer and Information Science, Modeling user choice in the PassPoints graphical password scheme.
[8] Ahmad Almulhem Computer Engineering Department King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia, A Graphical Password Authentication System.
[9] P.C. van Oorschot, Amirali Salehi-Abari, Julie Thorpe School of Computer Science, Carleton University, Purely Automated Attacks on PassPoints-Style Graphical Passwords.

Authors

Mr. Amit K. Barate is pursuing M.E in Electronics and Telecommunication from Shivaji University, Maharashtra. He has completed the Bachelor's degree in Electronics and Telecommunication from Mumbai University, Maharashtra.

.**Prof. Sunita S. Shinde** has received the Bachelor's and Master's degree in Electronics Engineering from Shivaji University, Kolhapur, Maharashtra. She has teaching experience of 16 years. Her fields of interests are Wireless communication and Adhoc Networks. She is a life member of ISTE. She has written three books on Computer Networks.

Ms. Prajakta U. Mohite is pursuing M.E in Electronics and Telecommunication from Shivaji University, Maharashtra. She has completed the Bachelor's degree in Electronics and Telecommunication from Mumbai University, Maharashtra.

.