Dual Step Authentication

Mrunmai Vikas Khedekar[1] Vaishna Kumar[2] Prof.Mamta Meena[3]
[1,2]Student [3]Assistant Professor
[1,2,3]Department of Computer Science Engineering
[1,2,3]Atharva College of Engineering, Mumbai, India

Abstract— Computer and network security is most highlighted part of security wherein the attacker just needs to find the weakness of the security. The implementation thus provides the mechanism of combination of two unique techniques PCCP technique and IAES algorithm .The combination of this techniques provide strength to the security thus enabling the user for a secured access also thus proportionally the task of attacking is reduced by increasing the possible combination of attacks. The authentication mechanism mainly focuses on that point of security which are more prone to be attacked by any means of threat which are vulnerable for the user`s information, these mostly are sensitive information and the reliable service sector. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security. Text-based passwords alone are subject to dictionary attacks as users mostly use passwords which are easy to memorize. Two way authentication techniques protect the data by using both the text and graphical passwords. We suggest a hybrid user authentication approach combining text passwords, recognition-based graphical passwords, a two-step process, for increasing security, to encourage users for selecting more random, and eventually more difficult for guessing, click-points.

Key words: Persuasive Cued Click Point (PCCP), Improved Advanced Encryption Standard (IAES), Knowledge Based Authentication

I. INTRODUCTION

A. Introduction

A network attacker should not be able to act as a legitimate user. When entering the system the user needs to authenticate itself with a password. It is the first shield that defends the user from unauthorized users for secure and reliable authentication. The number of users having accounts is increasing with the developing technology. On that basis using different passwords for different accounts is dilemma. Hence, if the user for its convenience uses same password for all systems, it can get compromised if the attacker attacks the system. On the other hand, if different passwords are used for different systems, users have the tendency to forget the difficult password due to they write it down thus by gaining access over this log of the user the attacker performs its task. Security in transmission of digital images has its importance in today's image communications due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue.

B. Need

A password is a convenient and more reliable method of authentication for users entering a computer system. The system simply requires acknowledging before itself a proof from the user of its authentication to image itself as an authorized user. Although this authorization is implemented but at the same time its security is subjected to a number of attacks. The following are common security risks where a legitimate user may lose his or her password

1) Over the Shoulder attack:
When a person types in his or her password, someone might just steal the password by looking over the person's shoulder, or by indirect monitoring using a camera.

2) Brute Force Attack:
The password consists of a finite length which is a combination of 8 alphanumeric characters, the attacker can such programs that generates password to match it with the attacking to obtain a valid one. With the developed technology, the attack can be more effectively as the time of computation has decreased.

3) Sniffing Attack:
In the scenario where the network channel is not properly encrypted, it would fall prey to the network sniffer which is done by network sniffing tools. Also, malicious tools as key loggers could capture user's passwords during the authentication process.

4) Login Spoofing Attack:
In this attack the user sets up a fake authentication site ,which imitates as the real one. When the user starts the authentication process the attacker gains access to the user`s Id and password and accesses the original site with user`s password, thus acting as legitimate user.

C. Background

Graphical passwords have been proposed as alternatives to text passwords to improve both usability and security issues. Text passwords are the most popular user authentication method[2], but have security and usability problems. Alternatives such as

tokens and biometric systems[2] have their own drawbacks. In this system to mitigate the problems with traditional methods, advanced methods have been proposed using graphical passwords[2]. Greg Blonder first described the idea of graphical password in the year 1996. For Blonder,[2] graphical passwords are nothing but the predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. The major goal of this method is to reduce the guessing attacks as well as[2] encouraging users to select more random, and difficult passwords to guess. Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information of graphical passwords is available elsewhere Of interest herein are cued-recall click-based[6] graphical passwords. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include Pass Points[4] and Cued Click-Points[4][5].

II. REVIEW OF LITERATURE

A. Authentication

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized user`s information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. There are two types of authentications textual and graphical authentication.

1) Textual Authentication

A text password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource which should be kept secret from those not allowed access. The proposed scheme can be implemented with Smart Cards or USB tokens. It consists of three phases.

- Registration
- Login
- Authentication

2) Graphical Authentication

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI) [5]. For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA) [4].

- Recognition-based technique: In recognition-based technique [2] a user chooses images during the registration stage and is said to be an authenticated user only when he/ she identifies one or more images.

B. Techniques for Authentication

The methods of authentication rely differently on area designed for security and its aspect in authentication. This project works on two important techniques designed for authentication.

- Persuasive cued click points [2]
- Improved advanced encryption standard [2].

III. IMPLEMENTATION

A. Persuasive Cued Click Points (PCCP) with IAES

We propose a two-step authentication method to strengthen text passwords by combining them with graphical passwords. So to secure the image password IAES algorithm [2] is used in which the click points entered by the user is encrypted and decrypted by using IAES algorithm. In PCCP [2] a user click is taken as input. From the position of the user click the image is divided as 16 parts each of the image part is now known as grid. The user is prompted for input as user click from the 16 grids available [2]. This process is repeated, until the total number of input from the user is three clicks. Specifically, when users create a password, the images are slightly shaded except for a randomly positioned viewport [2]. The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information could be used by attackers to improve guesses and could also lead to the formation of new hotspots. The viewport's size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points.

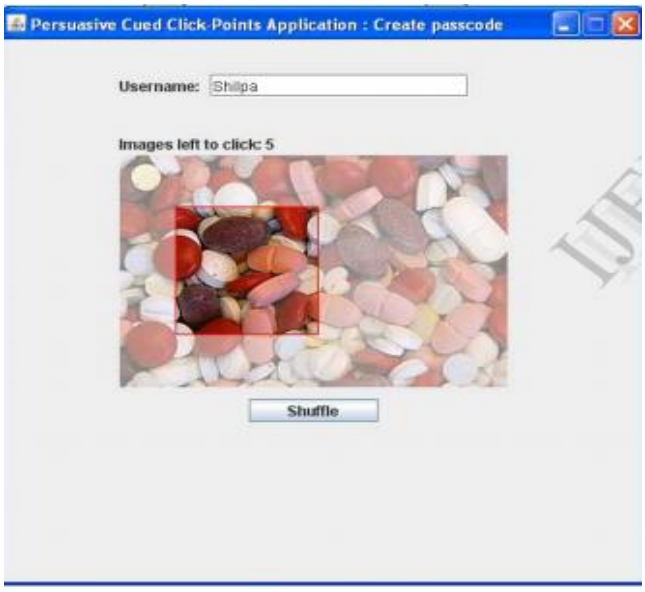

Fig. 1: Shuffle and Viewport

Users are required to select a click-point within this highlighted viewport and could not click outside of this viewport [2]. If they are unwilling or unable to select a click-point in this region, they could press the "shuffle" button to randomly reposition the viewport. While users are allowed to shuffle as often as they want. The viewport and shuffle buttons [2] only appears during password creation. During password confirmation and login, the images are displayed normally, without shading or the viewport and users were allowed to click anywhere.

1) Shuffles

During password creation, PCCP users may press the shuffle button Fig.1 [6] to randomly reposition the viewport. Fewer shuffles lead to more randomization of click-points across users. The shuffle button is used moderately [2].

2) Viewport

The viewport visible during password creation must be large enough to allow some degree of user choice, but
Small enough to have its intended effect of distributing click points across the image. The viewport positioning algorithm as shown in Fig.1[6] randomly places the viewport on the image, ensuring that the entire viewport is always visible and that users have the entire viewport area from which to select a click-point. This design decision has the effect of deemphasizing the edges of the image, slightly favoring the central area. A potential improvement would to allow the viewport to wrap around the edges of the image, resulting in situations where the viewport is split on opposite edges of the image [2].

B. Advanced Encryption Standard

Encryption specifies the process of plain text transformed into cipher text so that only legitimate user can recognize the meaning of encrypted data. AES is one of the successful and strongest encryption algorithms [1]. The concept of salt key is used in AES to improve the performance of encryption and decryption. In AES symmetric key cryptography is used. Symmetric key cryptography used the same key for both encryption and decryption part. The key data for AES is 128 bits or 192 bits or 256 bits with the rounds of size 10, 12, 14 respectively[1]. The size of key is also the same as the size of data of AES. Three different rounds are involved in the execution of AES. In this system AES 128 bits are used with improved features of [1] AES. For enhancement in AES salt key is added with the AES key so the possible combinations of password are enhanced. It proves that after adding the salt key with AES, it becomes the improved AES. IAES [2] is used for encrypting the text as well as graphical passwords of the users.

1) Salt key

Salt key is used in an improved AES. A salt key[2] is random data that is used as an additional input to a one way function that hashes a password. The primary function of salt is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow attacks. A new salt is randomly generated for each password. In a typical way, the salt and the password are processed and concatenated with a cryptographic [3] hash function, and the resulting the output is stored with the salt in a database. For later authentication hashing [3] permits, while defending against compromise of the plaintext password in the event that the database is somehow compromised.

C. Phases of Implementation

The methodologies in proposed system consist of phases of implementation with synchronized functioning of the techniques and algorithms. The phase of implementation is shown in fig.2:-

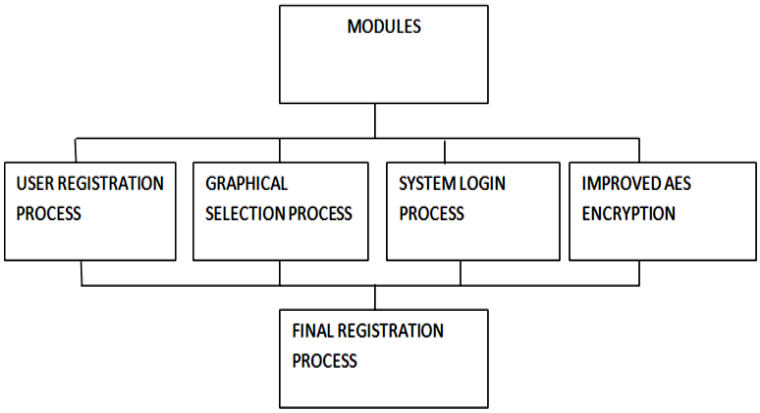

Fig. 2: Phases of validation

1) Phase 1: This is the first phase and the registration phase as shown in Fig.2 wherein the user inputs its basic information, this phase will consist of the activities as
   - Input of personal information
   - Input of text password
2) Phase 2: This phase shown in Fig.2 consists of graphical authentication of the user that comprises of
   - Selection of the picture for use to upload either from the system side or from the user side.
   - User input is taken on the picture as the click
   - On inputting the click, from the position the user has clicked the image gets divided into 16 parts.
   - After dividing the image the user is prompted for more clicks but these clicks are not on different images but on the same expanded version of the image.
   - After two more clicks the user is registered successfully.
3) Phase 3: The third phase as shown in Fig.2 is about to ease the task of the user from the two authentications
   - The user has to answer 10 questions
   - The questions could be based on like any of user defined questions.
   - This completes the registration process.
4) Phase 4: The user now starts with the next process of authentication, this is the login phase as shown in Fig.2.
   - The user will be prompted to input it`s user-id and text password, which are IAES encrypted[2].
   - If the user forgets the text password, it will be asked to renew its password.
   - After validating the text password, the user will be asked for graphical authentication.
   - User will be displayed a window of images.
   - User has to click on the correct registered image.
   - After clicking the valid image, the user will prompted for 3 clicks.
   - A viewport will be displayed, the user can move the viewport across the picture, the part of the picture displayed in the viewport will be clear the rest will be blurred
   - Then on inputting its first click according to its input co-ordinates will be displayed the enlarged image of the viewport and hence it will continue for two more clicks.
   - If the image is validated the logged-in successfully else not.
   - If user forgets its graphical password, there will be shuffle button through which the user can drag the viewport for new click after which the user will be again shown a 16-grid divided image and will be prompted for 2 more clicks for validation with IAES[2] algorithm.

IV. ARCHITECTURE

A. Implementation Architecture

The implementation architecture shown as Fig. 3 shows the phases of implementation wherein the database acts as a backend supporter who keeps the user and system validated. The data flow starts with entering the user valid id and it gets checked in the database for availability, if exists the user is asked for graphical authentication and if there is no availability the user is asked to change the id. After graphical authentication if the user is authenticated the password is stored with encryption and logged on else it is asked to browse images again.

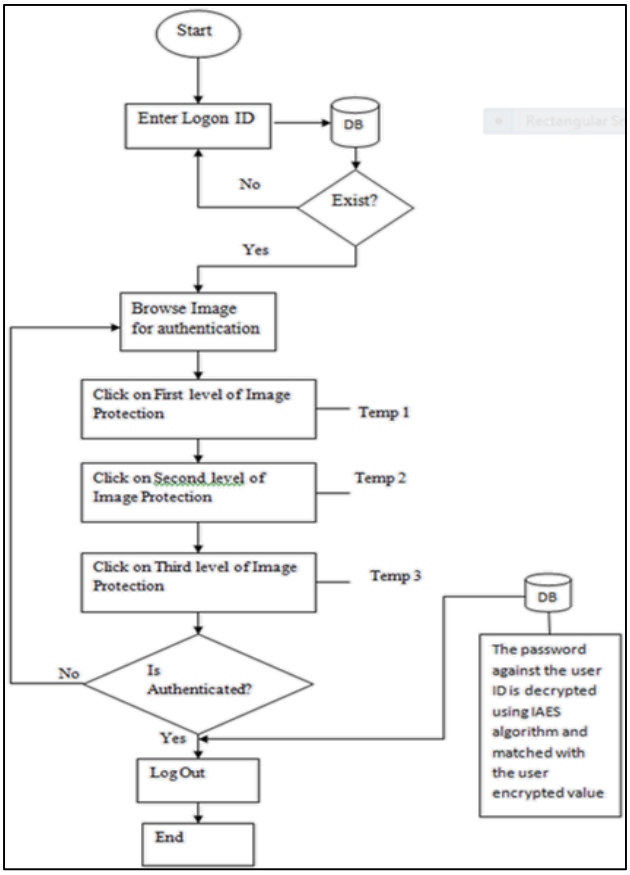

Fig. 3: Implementation Architecture

B. IAES Implementation

The working of IAES as shown in Fig.4 [2] is no different than from the traditional AES working [1]. Four different stages are used, one of permutation and three of substitution:

1) The IAES also comprises of the same stages of computation but the only difference is that a salt key is added, a randomly generated value which increases the potential of encryption [3].
2) Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block [3].
3) Shift Rows: A simple permutation [3].
4) Mix Columns: A substitution that makes use of arithmetic over [3].
5) Add Round Key: A simple bitwise XOR of the current block with a portion of the expanded key

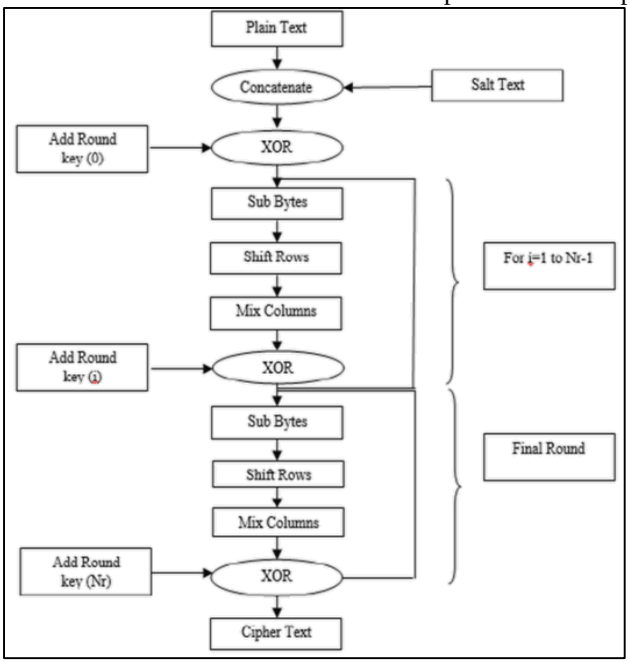

Fig. 4: Implementation of IAES

V. CONCLUSION

The implementation of this technique, a combination of Persuasive cued click point technique (PCCP) with the encryption of Improved Advanced Encryption Standard (IAES) provides the ability to the user to secure their information by providing an alternative to the existing system. The implementation practically erases the most prevailing form of attacks and has completely eradicated their forms .On the basis of the current computation, though through the speed of computation the attacker could not gain access of the system as the encryption provides a high range of combination. It thus provides a security shield for the attacks present. Referring to the comparisons of the techniques as shown in Fig.5 the combination of PCCP+IAES provides highest combination of possible attacks than the PCCP+AES, the only technique of only PCCP and CCP respectively although formed the basis for the improved techniques present today, they have been found vulnerable for user adaptability and to face the future attacks.

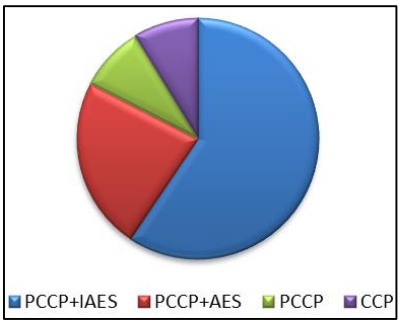

Fig. 5: Technique Comparison

REFERENCES

[1] Smita Chaturvedi, Rekha Sharma,Securing Image Password by Using Persuasive Cued Click Points with AES Algorithm,Volume5(4), IJCSIT (2014, Aug.).
[2] Smita Chaturvedia, Rekha Sharma ,Securing Text & Image Password Using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption Standard ,Volume 4(5), International Conference on Advanced Computing Technologies and Applications (ICACTA),Issue 2014.
[3] Cryptography and Network Security: Principles and Practice 5th edition, William Stallings, Pearson.
[4] Vaibhav Moraskar1, Sagar Jaikalyani2, Mujib Saiyyed3, Jaykumar Gurnani4, Kalyani Pendke5, Cued Click Point Technique for Graphical Password Authentication, Vol. 3, IJCSMC, Issue. 1, January 2014.
[5] P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar, Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme, Volume-3,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Issue-2, May 2013
[6] Ms. Shilpa. L. Dhapade, Implementation of Persuasive Cued Click-Points Techniques for Folder Security using Secure Hash Algorithm, Vol. 2, Issue 6, June – 2013.