Securing ATM Using Graphical Password Authentication Scheme

Sonia Rathi[1], Raunak Chitnis[2], Ramakant Yadav[3], Mrs. M.V.Bhosle[4]

[1]*(Department Of Information Technology, Marathwada Mitra Mandal's Institute of Technology, India)*
[2]*(Department, Of Information Technology, Marathwada Mitra Mandal's Institute of Technology, India)*
[3]*(Department Of Information Technology, Marathwada Mitra Mandal's Institute of Technology, India)*
[4]*(Department, Of Computer Engineering, Marathwada Mitra Mandal's Institute of Technology, India)*

ABSTRACT : In our day to day life ATMs are widely used and have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic with its attendant issues. But crime at ATMs has become a nationwide issue that faces not only customers, but also for bankers and this financial crime case rises repeatedly in recent years. To handle this issue, one solution can be the use of graphical password to overcome the problem of textual password.

In this paper, we present and evaluate our contribution, i.e., the iChess password. The iChess password is a multifactor authentication scheme. We present an iChess Chess board virtual environment where the user navigates and interacts with various objects. The series of actions and interactions toward the objects inside the iChess environment constructs the user's iChess password. The design of the iChess virtual environment and the type of objects selected determine the iChess password key space. Further for more security we are providing a random four digit number (flash code) on the respective users mobile which is new for every login.

Keywords – *Authentication, Graphical password, Usability security, Flash code*

1. Introduction

1.1 Need

Now a day's crime at ATMs has become a serious issue that faces a huge problem by all ATM users. As ATM has generated much relief to carry out the transaction whenever needed in any urgency. But a lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. The fraudsters can even get details from bank server if the user continues with the PIN served by bank. Once users ATM card is lost and the password is stolen, the users' account is unprotected to attack by criminals. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The current techniques of user authentication, which includes the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers) that suffer from various limitations. Passwords and PINs can be illegitimately acquired by direct covert observation. Even the passwords can be recognized through shoulder attack where the user will have no idea even if some unauthorized user kept eye on the password. When ATM cards are lost or stolen, an unauthorized user can often guess the password because many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Thus to overcome this existing system we have proposed more security to ATM system by using graphical password in the form of chess game through virtual environment and further authenticate through flash code.[1]

1.2 Basic Concept

To achieve the above needs for security of an ATM system we are providing authentication in the form of click based graphical password and further with a four digit random number (Flash code) on users mobile.

1.2.1 Click Based Graphical Password: In this the user needs to click on the given image or on the virtual environment say at 5 specific points of the image or virtual environment to set it as the user's password. Click based graphical passwords are more secure then the textual passwords because they are easy for the human to remember and hard for the hacker to know it because of its large size. [1]

1.2.2 Flash code: In flash code we are generating a four digit seed based random number and sending it to the user's mobile, which will be new for each new login.

2. Literature Survey

In this section we will study about the various graphical password systems that have been proposed for the purpose of the authentication. Various graphical password schemas had been proposed until now. The first graphical password was introduced by Blonder. Blonder's graphical password consisted of a predetermined image and user needs to click on that image or touch it various point on the image.

The graphical password have been divided into recognition based, recall based and also cued recall based password schemas:

1] Recognition based password:

Recognition based technique require the user to identify and recognize the secret, or part of it, that the user selected before. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in. Phishing attacks are somewhat more difficult with recognition-based systems as a correct set of images must be presented to the user before password entry. Shoulder-surfing seems to be of particular concern in recognition-based systems when an attacker is standing behind the user and sees or observes the images selected by users during login.[3][4]
Various recognition based password schema are explained below:

1]Passfaces: The recognition-based system studied most extensively to date is Passfaces . Generally during setting a password the user selects a set of human faces. A panel of candidate faces is presented during his/her login. Among the given set of decoys the user must select the faces he/she selected during setting the password. Passfaces simply works by having the user select a subgroup of x faces from a group of k faces. For authentication, the system shows p faces and one of the faces belongs to the subgroup q. The user has to do the selection many times to complete the authentication process. [5]

Fig.1 Passfaces

2] Story: The Story scheme, which requires the selection of pictures of objects (people, cars, foods, airplanes, sight-seeing, etc.) to form a story line. Story was proposed by Davis, Monrose and Reiter [2004] as a comparison system for passfaces. Users create a story by selecting a series of pictures. To log in, users are presented with one panel of images and they must identify their story images from among set of fake images. Images used for the story scheme can be everyday objects, places, or people. Story introduced a sequential component: users must select images in the correct order. To aid remembrance, users were instructed to mentally construct a story to connect the images in their set. [3][4]

3] Déjà Vu: Another recognition-based graphical password system is Déjà Vu proposed by Dhamija and Perrig, which authenticates the users by choosing pictures among the set of fake pictures. These pictures are presented in a random manner. Each picture is derived from an initial seed and no need to store the pictures pixel by pixel so only the seeds need to be stored in the server. Therefore, an authentication server does not need to store the whole picture; it simply needs to store the initial seed. [4][5]

2] Recall Based Graphical password: Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recall-based graphical password systems are occasionally

referred to as *draw-metric systems* because users recall and reproduce a secret drawing.
Some of the recall based graphical password schemas are explained below:

1] Draw-A-Secret (DAS): DAS, introduced by Jemyn is recall based graphical password schema and, is simply a grid in which the user draws their password using a stylus or a mouse. The user's drawings, which consist of one continuous or preferably many pen strokes using a stylus or a mouse are considered to be the user's password. The password space depends on the size and the complexity of the grid. Larger grid sizes increases the password space which becomes difficult for the attacker to crack the password. However, there are limitations in grid complexity due to human error. To recall where the middle points were becomes very hard to guess for the user if we have very large grid sizes. [1][6]

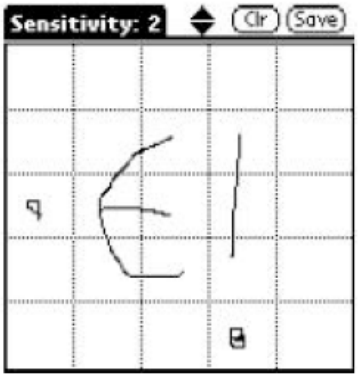

Fig.2 Draw-a-secret

Other recall based password schema's like as BDAS, YAGP, and PASSDOODLE etc. are the other systems developed from DAS.

3] Cued recall based graphical password:
Cued-recall based graphical password is the further development of recall based passwords i.e. the user to repeat or reproduce a secret that the user created before. Cued-recall systems typically require that users remember the target specific locations within an image. Cued-recall graphical password systems date back to Blonder's first graphical based password. Passpoints the successor of it launched research in the cued-recall subclass and hence sometimes called *click-based graphical passwords.* Various cued recall based graphical system is explained below: [2][6]

1]Passpoints: Cued-recall based password history is mostly dominated by passpoints. In passpoints the user needs to click on the five different positions or areas of the same image. Hence it is clicked based graphical password. The click is mouse based and user must remember the correct sequence or series of click points on that predetermined image for the next successful login. The below figure will explain the passpoint structure. [2][9]

Fig.3 PassPoints

2] Cued click points: It is a click-based scheme where users select one click-point on each of 5 images presented in sequence, one at a time; this provides *one-to-one cueing*. During the next login the user must remember that particular click point on the given image to unlock the next correct image, if the click is wrong the next opened image will be a fake one and not from the chosen series of images. This will stop current user authentication.[7]

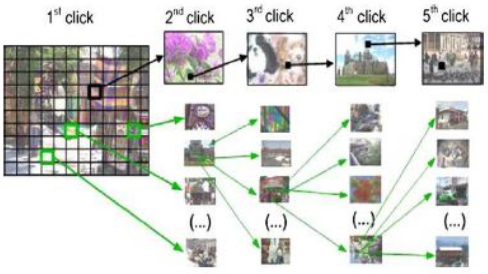

Fig.4 Cued click points

3] Persuasive Cued Click point: Persuasive Cued Click-Points (PCCP) is a variation of CCP

designed to persuade users to select more random passwords. It functions like CCP, but during password creation the image is dimmed except for a small square viewport area randomly positioned on the image. Users select a click-point from within this viewport, or may press a "shuffle" button to randomly reposition the viewport until a suitable location is found. On subsequent logins, images are displayed in their normal format with no dimming or viewport. Common wisdom that users choose the path-of-least-resistance here means selecting a click point within the first or first few viewports. The design intent of the randomized viewport positions is to flatten the distribution of click-points across multiple users, to reduce the effects of hotspots.[8]

Fig.5 Persuasive cued click points

2. System Architecture

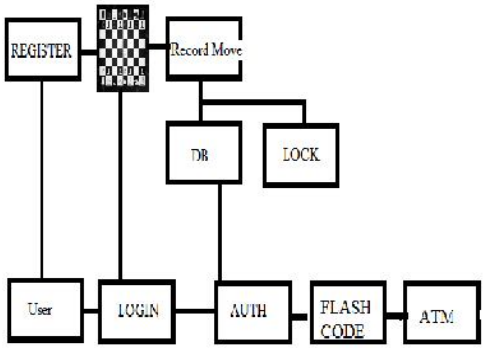

Fig.6 Proposed Architecture

Above given is the architecture of our proposed system. Here firstly when a new user enters the environment, the user must initially enter all his details in the registration form to get their unique identification number. The info consist of name, address, phone no, acc no etc. Phone number will be required further to get the flash code on their respective mobile. User who is already registered can directly does login. After registration the user will get their unique identification number which they have to memorize for every transaction. The user then play chess game to set their password which is stored in the database and locked by bank server.

At the time of login, user will enter unique identification number which is already received during registration then virtual environment of chess board will appear where user will enter password which is set through chess moves. Password will be crossed check from bank server database and if valid then user will be authenticated. After authentication user will get flash code on mobile which user have to enter it and further ATM transactions are carried out.[1]

3. Proposed Work

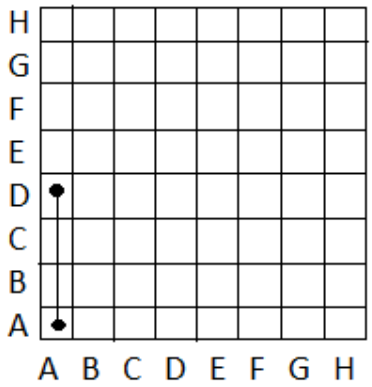

Fig.7 Chess Matrix

The movement of each piece in virtual chess board game will be stored in the form of 3D matrix. Each piece in the chess game will be given a unique id number. This id will determine that specific piece and his unique moves like rook moves any number of vacant space forwards, backwards, left, or right

in a straight line. It also takes part, along with the king, in a special move called casting.

For example in 8*8 matrix rook is at position AA in start of the game. It will be given a unique id say 1.If move the rook from its starting position AA to AD, it will be stored in the 3d matrix in the form (1,AA,AD) for each move we play.

4. Conclusion

To develop a system that gives major emphasis on ATM security by using Graphical Password in the form of Chess Game. We are also using Flash code technique for verifying user's presence.

4.1 Advantages

- 3D password's application provides protection of critical systems and resources.
- 3D password can combine many existing systems of authentication, providing an extremely high degree of security to the user.
- Our proposed system provides two layer securities for authentication and authorization.
- 3D graphical based password space size is very large due to which it becomes very difficult for the hacker to hack.

4.2 Disadvantages

- Shoulder surfing attack (A person standing behind you may be seeing your chess moves).
- Brute Force attack.
- Hotspots are created on the images during the password creation which makes easy for attacker to guess using the screen scraper technique.

5. Acknowledgement

We are very thankful to our professor Mrs. M.V. Bhosle of Department of Computer Engineering, MMIT Lohgaon, Pune, Maharashtra, India, for providing their support for this project. We would also like to thank our HOD Mr.K.S.Wagh for his un-ending faith and blessings.

References

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, *Three-Dimensional Password for More Secure Authentication,* School of Information Technology and Engineering, University of Ottawa, *VOL. 57, NO. 9, SEPTEMBER 2008*

[2] Chippy. T and R.Nagendran**,** *Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points*, International Journal of Communications and Engineering*, Volume 03– No.3, Issue: 01 March2012*

[3] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords*, School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada, ACM CCS'09, *November 9–13, 2009*

[4] Robert Biddle, Sonia Chiasson, and P.C. van Oorschot, *Graphical Passwords: Learning from the First Twelve Years,* Carleton University, Ottawa, Canada, ACM, *September 27, 2010*

[5] Amirali Salehi-Abari, Julie Thorpe, and P.C. van Oorschot, *On Purely Automated Attacks and Click-Based Graphical Passwords***,** Annual Computer Security Applications Conference, IEEE, *Version: Sept.15, 2008*

[6] Sonia Chiasson, Robert Biddle, P.C. van Oorschot, A Second Look at the Usability of Click-Based Graphical Passwords, Symposium On Usable Privacy and Security (SOUPS) *2007, July 18- 20, 2007, Pittsburgh, PA, USA. Volume 2, Issue 9, September 2013*

[7] Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul van Oorschot, Robert Biddle, *Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords,* ACSAC '10 Austin, Texas USA *Copyright 2010 Dec. 6-10, 2010, ACM 978-1-4503-0133-6/10/12*

[8] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot**,** *Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism*, IEEE, VOL. 9, NO. 2, MARCH/APRIL 2012

[9] Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memonc, *PassPoints: Design and longitudinal evaluation of a graphical password system,* International Journal of Human-Computer Studies 63 (2005) 102–127

[10] Aman Darren Davis Fabian Monrose Michael K. Reiter, *On User Choice in Graphical Password Schemes,* Usenix, The Advanced Computing Systems Association, *Volume 13 pages 11-11 27 July 2004*