ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Advanced Scalable Shoulder Surfing Resistance Password Authentication Scheme

Priti S. Katkade [1], Dr. Shubhas K. Shinde [2]

P.G. Student, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra, India1

Professor, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra, India2

ABSTRACT: The most common method is textual passwords that were used for authentication. Unfortunately, these passwords can be easily guessed or cracked. The next best techniques are graphical passwords. Since, there are many graphical password schemes that are proposed in the last decade, But most of them suffer from shoulder surfing which is also a big problem. Also, there are few graphical passwords schemes that have been proposed which are resistant to various attacks. In this paper advanced authentication scheme is proposed for any transaction. The scheme authenticates the user by session passwords. Session passwords are passwords that are entered and used only once. Once the session is terminated, the session password is no longer useful. For every login process, user input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. We proposed advanced scalable shoulder surfing resistance graphical password authentication scheme AS3PAS method which removes drawback of previous S3pas method. The proposed authentication schemes required less time for login process and uses co-ordinates of images for generating session passwords which reduces storage space in DB.

KEYWORDS: Advanced Scalable Shoulder-Surfing Resistant Graphical Password Authentication Scheme (AS3PAS).

I. INTRODUCTION

Authentication can be defined as one entity proving its identity to another. But how can one entity always know another is who they claim to be? This problem has remained unresolved for millennia. For centuries, we have used signatures to prove our identity, despite evidence that signatures can be copied and forged. Being certain of an entity's identity is usually practically impossible. System administrators and users rely largely on a text password authentication scheme for digital authentication. When first registering for a service, a user will provide the system with a sequence of text characters as their password. To later access the service, the user will have to provide the exact same text password. Text passwords remain popular because they have several advantages. They are easy to learn to use, easy to implement, can be easily changed if they are compromised or forgotten. Simple password and short password is easy to remembered but it can be easily hacked, while random and lengthy passwords are secured but hard to remember

To overcome these problem graphical schemes were used. In graphical password there is also problem for shoulder surfing. But here user is authenticated using session to enter the different password. When the session is over then that password is of no use for next session and current session gets terminated. Session password provides more security as every time the session start a new password is created.[1] so, here AS3PAS scheme is explained in detail how it works to get authenticate safely.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

II. LITERATURE SURVEY

Sr.no	Authors Name	Method /Techniques Used	Advantages	Disadvantages
1	Dhamija and Perrig	Proposed 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. Later, during login the user has to identify the pre selected images for authentication from a set of images[1][3]	The system is more secure than text based authentication scheme.	This system is vulnerable to shoulder-surfing
2	Jermyn	Proposed a new technique called "Draw-a-Secret" (DAS) where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. [2]	This system is more secure than then simple graphical authentication process.	This authentication scheme is vulnerable to shoulder surfing
3	Syukri	Developed a technique where authentication is done by drawing user signature using a mouse. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature.[5][6]	Drawing with mouse is not Familiar to many people, it is difficult to draw the signature in the same perimeters making it more secure.	The disadvantage of this technique is the forgery of signatures.
4	Haichang	Proposed a new shoulder-surfing resistant scheme where the user is required to draw a curve across their password images orderly rather than clicking on them directly.[7] This graphical scheme combines DAS and Story schemes to provide authenticity to the user	This authentication process is more secure because its shoulder-surfing resistant scheme	This scheme is complicated for the user of the system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

5	Wiedenback	Describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects.[4]	In order to make the password hard to guess large number of objects can be used making it indistinguishable objects to be more secure.	If fewer objects used it may lead to a smaller password space, since the resulting convex hull can be large.
6	Zhao and Li	Proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region.[2]	It has high level security since Protected by shoulder-surfing , hidden camera, and spyware attacks.	It takes long time for login process.
7	Zheng	Designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.[5]	The scheme has salient features as a secure system for authentication immune to Shoulder-surfing, hidden camera and brute force attacks.	The shapes chosen by the user may have normal meaning, the attacker will have more chance to attack the password.

TABLE 1: DIFFERENT GRAPHICAL AUTHENTICATION TECHNIQUES.

III. PROPOSED ADVANCED S3PAS SCHEME

Graphical based password authentication systems are now more secure than text based. So, after literature survey on all graphical based schemes we decided to make s3pas scheme more advanced. So its future scope was to implement s3pas totally by graphical way instead of printable pass character.

In the proposed AS3PAS system the user has to create its own region. The smaller the region the security is more. Clicking on three times on a given complicated image. During registration process the user is provided with the complicated images. What user has to do is, he has to click on image three times creating a triangular region. Now during logging process the valid user will click inside that region all the three times to get authenticate successfully. Cracker or invalid user will try to click on image but probability of clicking inside the region three times is very low and exits from the system if attempts exceed making system more secure.

AS3PAS generates the login image locally and transmits the image specification i.e. coordinates of image instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time. AS3PAS can be used in a high capability system to provide high level security by "Change image" technology. In that image will be changed if a user fails in clicking the correct areas, or inputs wrong session passwords for more than a certain no. of times [2]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV. EXPERIMENTAL RESULTS

Example: Step by Step Login Procedure for AS3PAS System:

Step 1: Registration Process:

- Initially User clicks on the complicated image for 3 times.
- It makes the users own triangular region as shown below.
- So, user's record is saved successfully in registration process

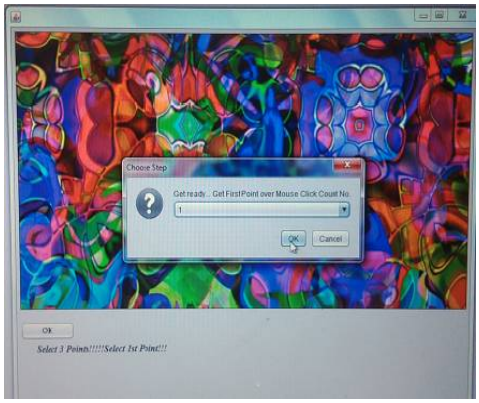

Figure 1: user selects 1st point while registration.

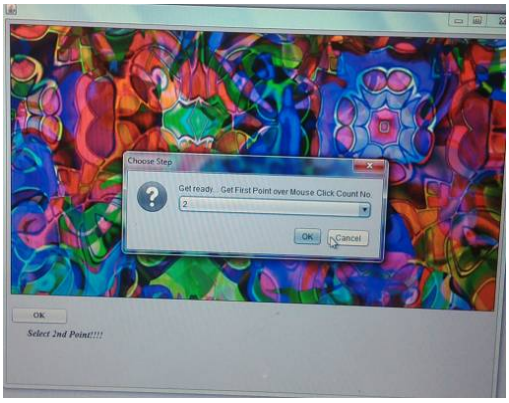

Figure 2: user selects 2nd point while registration.

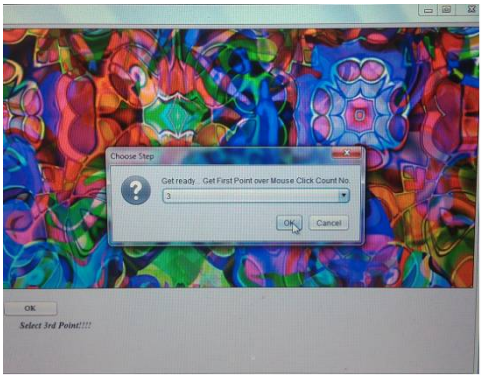

Figure 3: user selects 3rd point while registrations

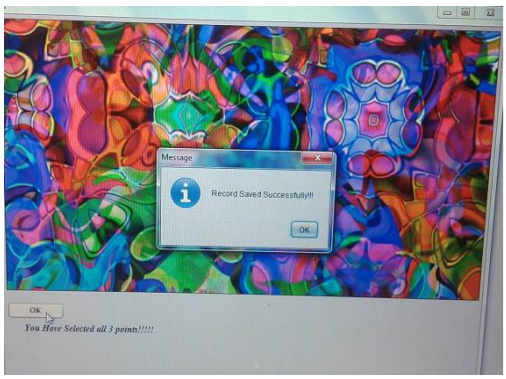

Figure 4: user's record saved successfully

In the proposed AS3PAS system the user is provided with the above complicated images as shown above. Initially user selects any complicated images to get register. Fig 1. Shows how user selects 1st point Fig 2 user selects 2nd point and Fig 3 likewise user selects 3rd point which makes his own triangular region. And at last his record gets saved at the backend. So instead of keeping entire image in the database the system stores only co-ordinates of images selected by the user.

Step 2: Login Process:

(A): If Valid user

- User now while logging process selects its region provided in registration process.
- He gives three points of region by clicking on image 3 times forming valid region.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

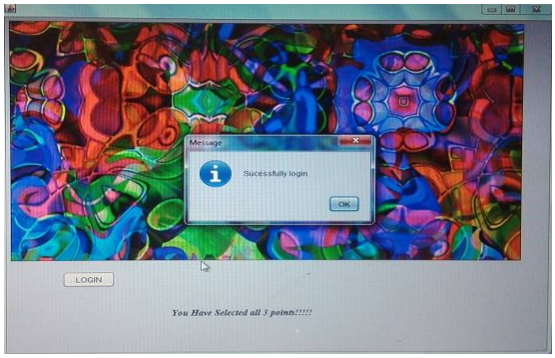

Figure 5: Valid user gets Login successfully

Step 2: login process:

(B): If Invalid user:

- Invalid User now while logging selects its region randomly.
- He gives three points of region by clicking on image 3 times.
- If he selects wrong points message will be displayed for him.
- If no. of attempts exceeds by invalid/valid user systems gets exit.

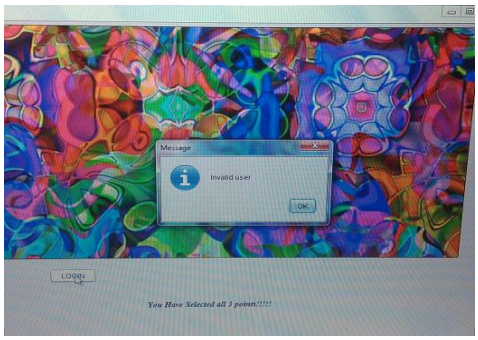

Figure 6: Invalid user gets Login Failed Message**.**

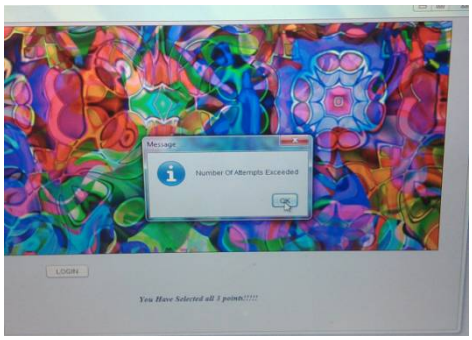

Figure 7: If no. of attempts exceeds systems gets exit.

After the registration process the valid user can enter the system anytime clicking within his own region for authentication. As shown in Fig-5. Login successful message to valid user. If the user is not valid he may enter the system. Now invalid user may attempt to click on image no of times to enter the system but it's impossible that invalid user gets authenticated as strong security features of AS3PAS. Fig-6 Shows how invalid user selects points by clicking on image anywhere within 3 times it gets login message failed but if attempts exceeds the system gets exit as shown in Fig-7.

V. ANALYSIS AND DISCUSSION ON PROPOSED SYSTEM

1 Shoulder Surfing Resistant

After an attacker observes or records one click on the screen from the user, the attacker cannot gain enough information of the user's password. That is it's not impossible to click within same region of valid user. This shows that a shoulder-surfing attack is mostly not possible.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

2 Brute Forces Search Resistant

The primary reason is that we adopt "change image" technology. If a user fails in clicking in the correct region, or a user inputs wrong passwords for 3 times, the system automatically changes the complicated login image. By doing this, there is no way for attackers to adopt brute-force search to break the password because the password will change after changing the image.

So, all the attempts toward the previous complicated login image become useless. The attacker has to start a new search in the new image. Therefore, we argue that "change image" technique makes AS3PAS immune to the brute-force search. [2]

3. Social engineering

Graphical passwords are not easy way to share the passwords with each other For example; it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

4. Dictionary attacks

Since graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords

VI. CONCLUSION

Thus after literature survey we decided to use AS3PAS, to provide a user more secure authenticated transaction. This Scheme can also be used to develop as windows application folder locker or as an external gateway authentication to connect the application to a database or an external embedded device.

REFERENCES

1. Priyanka S. Kedar and Vrunda Bhusari., "Using PBKDF2 Pair & Hybrid technique for Authentication", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May 2014.
2. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", in 21st International Conference on Advanced Information Networking and Applications Workshops, vol. 2. pp. 467-472, Canada, May-2007.
3. D. Aruna Kumari, "Implementation of Network Based Authentication Mechanisms", Advances in Information Technology and Management, volume-1, Issue-.2, April- 2012.
4. S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy., "Authentication Techniques For Engendering Session Passwords With Colors And Text", Advances in Information Technology and Management, Vol. 1, Issue- 02, May-2012.
5. Vaishnavi panchal, Chandan p. patil " Authentication schemes for session password", International Journal of Scientific & Engineering Research, Volume 4, Issue3, March-2013
6. Z. Zheng, X. Liu, L. Yin, Z. Liu., "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, Issue-5 May 2010.
7. V. Bhusari., "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

BIOGRAPHY

Priti S. Katkade is a PG student in Dept. of Computer Engineering at Lokmanya Tilak College of Engineering, Navi Mumbai, India. Her area of interest is networking and security. Also participated in AVISHKAR Research convention 2016 at district Level.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

	Dr. Subhash K. Shinde is working as professor in Dept. of Computer Engineering at Lokmanya Tilak College of Engineering, Navi Mumbai, India. He is having academic experience of 16 years at UG and PG level courses of University of Mumbai. He has guided many projects at UG and PG level. His areas of interest are Data Mining, Database, Computer Network