A Secure Intranet Email Application using KBAM
K. Purusothaman¹, R. Nithish Kumar², R. K. Dhanarajan³, V. Rajaramanan⁴
Assistant Professor⁴
Department of Computer Science and Engineering
Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Abstract:
This system, which will computerize the activities of A Secure Intranet Email Application Using Graphical password. The main feature of the computerized system is to keep track of all the information in more authenticated way where the information is not hided where as this package provide the security measures which will inform the receiving user where the information from the other user is altered or not. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

Keywords: component; formatting; style; styling; insert (key words.

I. INTRODUCTION:
An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it’s easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique which uses one click point on five different images. The next image to be displayed is based on previous click-point and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

II. LITERATURE REVIEW
Nowadays, user authentication is one of the important topics in information security. Strong text-based password schemes could provide with certain degree of security. However, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Graphical user authentication (GUA) has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. In recent years, many networks, computer systems and Internet-based environments try used GUA technique for their user’s authentication. All of GUA algorithms have two different aspects which are usability and security. Unfortunately, none of graphical algorithms were being able to cover both of these aspects at the same time. This paper presents a wide-range survey on the pure and cued recall-based algorithms in GUA, based on ISO standards for usability and attack patterns standards for security. After explain usability ISO standards and attack patterns international standards, we try to collect the major attributes of usability and security in GUA. Finally, try to make comparison tables among all recall-based algorithms based on usability attributes and attack patterns those we found.

Nowadays, user authentication is one of the important topics in information security. Strong text-based password schemes could provide with certain degree of security. However, the fact that strong passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. In recent years, many networks, computer systems and Internet based environments try used graphical authentication technique for their user’s authentication. All of graphical passwords have two different aspects which are usability and security. Unfortunately none of these algorithms were being able to cover both of these aspects at the same time. During our research, we could find eleven Recall-Based authentication algorithms which we tried to explain their lacks and attacks. Then in the last section, in order
to cover usability and security features at the same time, we try to make three different comparison tables.

This paper presents an integrated evaluation of the Persuasive Cued Click-Points graphical password scheme, including usability and security evaluations, and implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points.

User authentication is one of the most significant issues in computer and information security. Currently, the most prevalent and well-established authentication approach is based on the use of alphanumeric passwords. The first text-based authentication scheme was introduced in the late 1960s, and so far the most computer systems, networks and applications use this technique to authenticate their users. With the growth of users and services, this approach became susceptible to several vulnerabilities and drawbacks. In this paper, we analyze and evaluate modern authentication methods with the purpose of reviewing tendencies and assessing the user authentication in both security and usability.

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments. Although security researchers have made great strides in fighting these threats by protecting systems, individual users and digital assets, unfortunately the threats continue to cause problems. The principle area of attack is Authentication, which is of course the process of determining the accessibility of a user to a particular resource or system.

III. ANALYSIS AND DESIGN OF THE APPLICATION

A. EXISTING WORK:
Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

Blonder’s Scheme
Graphical password scheme in which user click on several different predefined locations on a predetermined image. During login, the user has to click on the approximate area of those locations. Basically the image helps the user to summon up their passwords and therefore this scheme is considered more suitable than unassisted recall. The problem with this system is that boundaries are predefined which results various attacks are easily possible.

Pass-Point Scheme
Pass-point graphical password scheme in which password consists of a sequence of 5 different click points on a given image. During password creation user can select any pixel in the image as a click-points and during authentication the user has to repeat the same sequence of clicks in correct order within a system defined tolerance square of original click-points. Pass-point used the robust discretization technique. The problem with this scheme is that HOTSPOT (area of an image where user more likely to select the click-point) and also pattern formation attacks are easily possible.

B. Drawbacks:
□ The blonder’s scheme in which user click on several different predefined locations on a predetermined image. The problem with this system is that boundaries are predefined which results various attacks are easily possible.
□ Pass-point graphical password scheme in which password consists of a sequence of 5 different click points on a given image. The problem with this scheme is that HOTSPOT (area of an image where user more likely to select the click-point) and also pattern formation attacks are easily possible.
□ Cued click point uses one click point on five different images instead of five click-points on one image. The problem with this technique is false accepted and false reject is possible.

IV. SYSTEM IMPLEMENTATION

ADMIN SESSION
• Admin Profile
• User List
• Change Password

DESCRIPTIONS:
In admin session the admin can view his profile and view, edit, and delete the user at any time. Then admin can change their password at anytime by giving the old password.

REGISTRATION SESSION
In registration process, the user can register their account by giving their personal details, they are, User ID, User Name Password, Re password, Phone, Email ID, Street, City, State, Country, Gender, Pin.

Graphical password generation
Discretization is used to just allow the correct click-points to be accepted in the region without storing exact click-point coordinates. Centered Desceretization offers centre tolerance such that during password creation an invisible grid is overlaid in such a way that the grid comes in centre with respect to selected click-point and the grid size used is 2r×2r.

It divides an image into square\ tolerance regions, to verify whether a login click-point comes within the same tolerance region as the original click-point.

During password creation the grid’s location is set for every click point and there is a identical tolerance area centered around the original click-point, by calculating the appropriate (x,y) and
grid offset (Gx,Gy) (in pixels) from a (0,0) origin at the top-left corner of the image. Later during user login, the system uses the originally recorded grid offsets to place the grid and determine the acceptance.

Password Creation Process:

1. Grid offset (Gx,Gy) used for grid positioning and can be calculated as,
   
   \[ Gx = (x - r) \mod 2r \]
   
   \[ Gy = (y - r) \mod 2r \] where r is tolerance value

2. A Tolerance area identifier (Tx,Ty) is given by,
   
   \[ Tx = (x - r)/2r \]
   
   \[ Ty = (y-r)/2r \]

LOGIN SESSION:
In this session member can login to their account by giving user name, password and graphical password.

Login Process:
First it retrieves the corresponding (Gx,Gy) for corresponding click point and calculate

\[ Tx = (x - Gx)/2r \]

\[ Ty = (y-Gy)/2r \] and checks the current click-point falls in the grid or not.

MEMBER SESSION:

Inbox

Compose mail

Sent Mail

User Profile

Change Password

DESCRIPTION:
In this session user can use this account as Email account. In this account user can compose mail, store the received mails in inbox, and user can view the sent mail details. Then user can change their account password. The mail is send by using SMTP protocol.

AES Encryption Module:
In this module while user is sending a message, secret key will be generated by the system and will be sent to receiver’s e-mail id. Receiver has to get the secret key for viewing the message. If the secret key is not valid receiver cannot view the message which was sent by the sender.

AES Decryption Module:
In this module before viewing the message user has to enter the secret key which was sent. The entered secret key will be verified and if it is correct then only user can view the message.

Change Password:
In this session user can change their password by giving old password.

V. SYSTEM ARCHITECTURE

VI. RESULT

a. Registration Phase

![New User Registration Form]

b. Graphical Password Phase

![Graphical Password Settings]
VII. CONCLUSION

In this project we did an Adding Persuasive features in Graphical Password to increase the capacity of KBAM. It’s to develop this project; we used J2EE as a front end and MY SQL as backend. A major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also it removes the pattern formation and hotspot attack since it provides the system suggestion. Also the proposed system removes the shoulder surfing attack.

VIII. FUTURE ENHANCEMENT

• In this project we can implement this with 2d images in future we can implement with 3d images or digital signature login process.
• In this project we prevent from some basic attacks, but in future we can try to implement with some high capacity attacks also.

IX. REFERENCES


