ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

A Novel Based Multilevel Graphical Authentication System

V. Priya dharshini[1], A.Gomathi[2], N.Saravanaselvam[3]

M.E student, CSE department, Sri Eshwar college of Engineering, Coimbatore, Tamil Nadu, India[1]

M.E student, CSE department, Sri Eshwar college of Engineering, Coimbatore, Tamil Nadu, India[2]

Professor, CSE department, Sri Eshwar college of Engineering, Coimbatore, Tamil Nadu, India[3]

Abstract: Graphical passwords provide a promising alternative to traditional alphanumeric passwords due to the fact that humans can remember pictures better than text. A simple graphical authentication system that consists of a sequence of 'n' images and the user has to select the click points associated with one of the 'n' image for login. The proposed mechanism is a more secure graphical password authentication which consists of a sequence of 'n' images in the grid format and the user is asked to select a precise image from the grid during registration. This authentication system employs the user's personal handheld device or E-mail as the second factor of authentication. In the login phase, the user enters the username to the website. The username transmitted to the database by the server and it displays a set of images in grid. A precise image is selected from the "n" images and is provided to the server. The server generates a random pixel value from the selected picture and sends it to handheld device. The user is asked to do five click points on the image according to the pixel value in some specific order within some time constraints (e.g. if there are 10 random pixel value user should enter [2], [4], [6], [8], [9] pixel value for successful login); the pixel value acts as a onetime password. The user is authenticated only if he/she selects and clicks on the correct pixel value. The inaccurate pointing of pixel value leads to the unsuccessful authentication and the login access get denied.

Keywords: Graphical passwords, Images, Pixel values, Authentication, Log in.

I.INTRODUCTION

Current authentication techniques are classified as token based and biometric based, knowledge based authentication. Biometric based authentication provides more reliable user authentication which uses iris scan, finger print or facial recognition. Token based techniques such as key cards, smart cards and bank cards are widely used. Token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards generally require a PIN number which is to be remembered by the user. Knowledge based authentication system can be text based or picture based. The picture based technique can be further divided into two categories: Recognition based and Recall based techniques.

1.1Types of Authentication

Three-factor authentication is an authentication system which includes all the three mechanisms and depends on what you have (e.g.: token), and who you are (e.g. biometric) what you know (e.g. password). To pass the authentication, the user must enter a password and provide a pass code generated by the token, and scan her biometric features (e.g. fingerprint or pupil). The major drawback of this approach the identification process can be slow and such systems can be expensive, unreliable. However, this type of technique provides the highest level of security.

Two-factor Authentication is more attractive and practical than three-factor Authentication and is based on token based and text based authentication system.

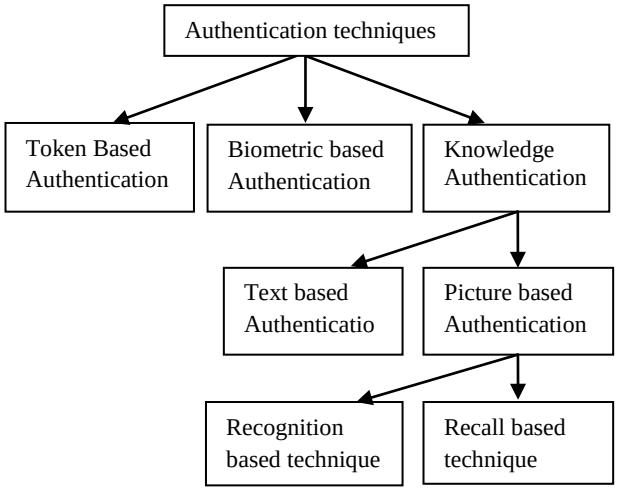

Fig. 1 Classification of Authentication Technique

II. PIXEL VALUE

Each digital image files stored inside a computer has a pixel value which describes how bright that pixel is, and what color it should be. During extraction, the image files are dividing into grids; it can be 16 by 16 grids or 8 by 8

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

grids. Each grid is being calculated its pixel value with compression algorithm. Then, all grids' pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire from an image. In this graphical authentication method, pixel value will be used as authentication key for a password.

Pixel value access control is a method to provide a new secure guard mechanism for access control on online or any web based system. It is used to avoid end user to key-in their password being capture by key logger software. With a pixel value access control secure system, an image will be used to authenticate their identity. The end-user required to select the image from the system or to upload their known image in order to log in to an online system. When the server receives the images, the system will extract pixel value from the picture and used its value as authentication value for respective user-name. The way to extract pixel value from an image is using Image compression techniques. There are various imaging compression algorithms and each compression techniques produce an output in quantitative value or known as pixels value. Those pixel values will be used to authenticate a password. The end users are authenticated and authorized to access their resource on the network without entering passwords. The end-user account is safe and Key-logger software got no keystroke capture.

Based on user-name – password concept and graphical password concept, pixel value and user access control is combination of both concepts. With pixel value user access control method, users should enter their user-name and upload their security image to the log-in page. The security image is just known by the user secretly, so it is called as *passpict*, and not to store on server. Server then, extract the uploaded image to get its' pixel value that will be used to authenticate a user. The pixel value is bringing to query for next authentication method. User-name and pixel value are being authorize from user database. The user will allow for access if the user-name and pixel value is successfully passing the authorize process. The user account details are cache in a database that containing user-name and pixel value.

IV. RELATED WORK

Authentication in the computer world refers to the act of confirming the authenticity of the user's digital identity claim. It is a fundamental component in most computer security contexts and provides the basis for access control and user accountability. Texts passwords are the most commonly used technique for authentication and have several drawbacks such as key-loggers, dictionary attack; shoulder-surfing and social engineering.

Two contradictory demands are to be satisfied by the text passwords. First demand is that the passwords have to be easily remembered by a user and the second is that have to be hard to guess by the attacker. Easily guessable and/or short text passwords are normally chosen by the user, which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password sometimes leads to an opposite effect as a user may tend to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. Another decisive problem is that users tend to reuse passwords across various websites.

To overcome the shortcomings of text-based password, two-factor authentication techniques and graphical password have been employed. Graphical passwords provide a promising alternative to traditional alphanumeric passwords due to the fact that humans can remember pictures better than text. In general, Graphical password method is a type of knowledge base authentication system and graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall. In recognition-based techniques, a user is authenticated by challenging them to identify one or more images they chosen during the registration. In recall-based techniques, a user should reproduce something that he or she created or selected earlier during the registration stage. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory.

Susan et al [2] proposed the Pass-Points graphical password scheme, in which a password consists of sequence of 5 to 8 different click points on a single image and the click points are chosen by the user. The image is displayed on the screen by the system. The image is not secure and has no role other than helping the user remember the click points. Any pixel value in the image is a candidate for a click point. Pass-Point comes over click based graphical password scheme. The main disadvantages of this scheme are HOTSPOTS and pattern formation attacks.

Sonia et al [3] proposed Cued Click Points which was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. By using of five click-points on one image, cued click points uses one click-point on five different images. The next image displaying is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of authentication failure is displayed after the last click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point.

Alireza et al [5] introduced the use of personal device in combination with the graphical password. In this approach some hint information is transmitted to the personal device such as hand held device, to determine the appropriate click points and their order, for each login session. The clue information is transmitted either through direct communication, indirect communications or photographic communication. This technique prevents the user from remembering the click points. But this technique has

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

several disadvantages like shoulder surfing, pattern formation attack etc.

V. PROPOSED SYSTEM

In this paper, we provide a promising secure graphical authentication system based on the pixel value based technique. Pixel value scheme is the one in which a given image password consists of a pixel values which may generated randomly for login. For password creation user selects an image from "n" images and for login the user have to click on the pixel value on selected image in some constraints. The proposed authentication system consists of sequence of "n" images and the user has to select the unique image. During login, pick the precise image from "n" images which is selected during registration and provide it to the server. The pixel values generated randomly from the image will be sending to handheld device or to E-Mail. The user has select five click points associated with that image in some correct constraints for successful login. The system leverages the user's cell phone or communication service for secure authentication which leads to prevent incremental guessing attacks. The proposed system consists of three phases.

A. Registration Phase

The user to get access to the website and to get privileged to access the services, the first is to register to the website. During registration, the user after selecting the user name is asked to select an image from the set of "n" images. The image selection can be done either from those chosen by the user or those generated by the system. In the final phase of registration user have to submit their mobile phone number or mail id to get random pixel values.

USER NAME 123@abc.com Sign in

IMAGE PASSWORD Forget Password?

Fig.3. Images in Grid format

User-name and pixel value are being validate from user database. The user will permit for access if the user-name and pixel value is successfully passing the validating process. The user account details are placed in a database that containing user-name and pixel value. Pixel value will be used as authentication key for a password. Pixel value from an image can be encrypted using Image compression techniques. The encryption and decryption are also performed by using AES algorithm.

B. Login Phase

In the login phase, the user submits the username to the website. The username transmitted to the database by the server is used as the key to retrieve the images associated with that user. One image among the "n" images is selected and is provided to the server. When the server receives the images; the system will extract pixel value from the picture and used its value as authentication value for respective user-name and send to the handheld device. The way to extract pixel value from an image is using Image compression techniques. There are various imaging compression algorithms and each compression techniques produce an output in quantitative value or known as pixels value. The user is asked to click on the image according to the pixel value within some time constraints which generated randomly and send to handheld device with as shown in figure 2. The user is authenticated if the user selects the correct pixel value. The incorrect pointing of pixel value leads to the unsuccessful authentication and the login access get denied.

Fig.4. Login Phase

C. Authentication Process

Passwords that should be confidential are readable easily when the key-stroke logs being retrieve by hacker. Pixel Value user access control method is not involving password key-in on a workstation. The password has been stored in server and it is a pixel value generated from extracted image file through image compression algorithm, in example Discrete Cosine Transform (DCT). The algorithm produces pixel value that used as password to authenticate a user access. It is kept secretly on database and even users have no idea what is the password. This authentication method brings a lot of benefits which is: First, key logger is unable to capture typing text when there is no password key in involving. Second, multilevel authentication will protect login page from brute force attack or dictionary attack.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

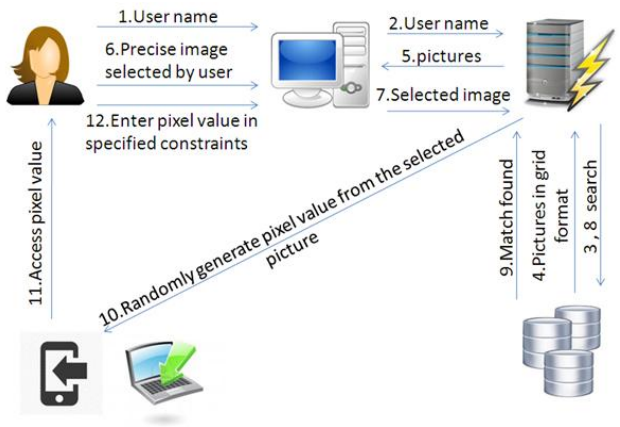

Fig.5. Authentication Process

The proposed system includes number of images and an image consists of five click points. During login, the user has to select the precise image and handover to the server .The server generates the pixel values and deliver to the handheld device. Since for each login session, pixel values of the image can generated randomly and transfer to the device. When authentication fails due to the incorrect pointing of click points the login access is denied.

VI.CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this paper, we propose a more secure graphical authentication system. The system combines graphical password scheme along with handheld device to form a novel method for multifactor authentication. This authentication system ensures the protection from threats such as key loggers, hotspot, and shoulder surfing etc…Random pixel value which also acts as a onetime password and provides more authentications.

REFERENCES

[1] Ahmad Almulhem, "A Graphical Password Authentication System," in 978-0-9564263-7/6/$25.00 IEEE, 2011.
[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", Int. J. Human-Computer Studies 63 (102–127,) 2005).
[3] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points", J.Biskup and J. Lopez (Eds.): ESORICS 2007, LNCS 4734.
[4] Aswathy, Theresa, Jenny,"A proficient multilevel graphical authentication system", Int.J.IJSETR 2013(1341-1344)
[5] Alireza Pirayesh Sabzevar and Angelos Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords," in IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008.

BIOGRAPHY

V.PRIYA DHARSHINI received her B.E Degree from Karpagam University, Coimbatore, Tamil Nadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest is Network Security.

A.GOMATHI received her MCA Degree from Anna University, Chennai, Tamil Nadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest is Data Mining.

Dr. N. Saravana Selvam has obtained his Ph.D. in Computer Science and Engineering from Anna University, Chennai in the year 2013. He has obtained both of his Post Graduate degree, M.E. (Computer Science and Engineering) and Graduate degree B.E., (Electronics and Communication Engineering) from Madurai Kamaraj University (Tamilnadu, India). He is currently serving as Professor & Head of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu. During his fifteen years of teaching profession, he shouldered a member of teaching, administrative and societal based assignments.He is a Life Member of ISTE, IAEng and IACSIT. Currently, he is specializing in the area of Network Engineering.