SURVEY ON GRAPHICAL PASSWORD AUTHENTICATION

Mr. J. Jelsteen[1], V.Selvapriya[2], S. Sufiya Muskan[3]

[1]Assistant Professor, Department of Computer Application, Sri Krishna Arts and Science College, India.

[2,3]BCA Student, Department of Computer Application, Sri Krishna Arts and Science College, India.

ABSTRACT

One method of computer security authentication is the use of a graphic password. The most crucial aspect of computer science nowadays is digital/computer security, which protects user or client data. And one of the hazards is shoulder-surfing, in which a thief can steal a password by watching directly or by recording the authentication session. The most popular and straightforward way for this authentication is the graphic password strategy. So, we recommend a fresh approach to address this issue. In order to defend against shoulder surfing attacks, we have created two ideas. initial, If the registration does not already exist, the user must register. Second, you need to enter a user ID and password that are both current. The key phrase is a collection of letters and digits. Third, the user must go through image-based authentication, where the user can select their own password, and this method has a higher probability of working against it. Your password should be chosen in accordance with the registration password; it must match when you log in. There should be numerous color-based passwords used in colour basis authentication, and you must keep track of the password order according to the colour. Similar to three-factor authentication, too. The proposed graphical password authentication method that is suggested here is hence secure to shoulder surfing and other likely attacks. To increase the security of the authentication method, image steganography—the practise of masking data within images—is implemented. The use of steganography techniques allows for the storage of text passwords within the images.

Keywords: Graphic password, Shoulder Surfing, Image Steganography.

1. INTRODUCTION

The issue with text-based passwords used in knowledge-based authentication mechanisms (KBAM) is well-known. An authentication system's objective is to assist users in choosing the best password. The graphical password is an alternative to alphabetic passwords. One method for ensuring the security of a digital device or vital information is the use of a graphic password. We all know that an image or an image-based password is easily stored or recalled by the human brain. Therefore, we suggest graphical passwords for users who can record random values with high levels of security and have no trouble remembering them. Data access point authentication controls customer security assurance. As a password, it employs a variety of shapes and [1]images. Scientists also assert that an image is easier for the human brain to recall than text. Images are easily processed by the human brain. Additionally, an image-based password is immune to social engineering, keyloggers, dictionary attacks, etc. Recent reports claim that a security team at a corporation executed a network password cracker and discovered roughly 80% of the passwords within 30 seconds. The graphical user authentication method is also known as the graphical password method (GUA). Persuasion is primarily used to control user choice in click-based graphical passwords, encouraging users to choose more random click points that are difficult to guess. The proposed system makes it more difficult for users to choose weak passwords that are easy for an attacker to guess, discouraging them from doing so. Instead of burdening users, it is easier to track the system's suggestions for a secure password, which is a feature lacking in most schemes. In this case, the persuasive feature is combined with the previous cued click point technique, which uses one click point on five different images. The next image displayed is determined by the previous click-point. For valid users, it provides implicit feedback in the form of changing the user's previous click-point if they are unable to recognise the image while logging, and the user can restart the password entry, whereas explicit feedback is provided after the final click point.

2. METHODOLOGY

GRAPHICAL PASSWORD AUTHENTICATION

Graphical passwords were first introduced by BLONDER in 1996..Graphical Password Authentication is intended for graphical passwords. Wherever they have presented some ineffective graphical password technique, for example, multiple-image based a user may be presented with a number of images, from which he or she must choose one or more[2]. The following grid-based scheme which is a simple object There are no more displays required. The Triangle scheme is next, which provides a protrusive surface. It's difficult to choose because the number of images shown is nearly identical. The calculation of the base is the most important aspect of this paper of the username As a result, this new scheme frequently resolves the existing system's numerous issues. This paper primarily focuses on the design of a graphical password system that is completely compatible with various authentication systems. Furthermore, the primary goal of this method is to achieve higher security with a simple technique that is difficult to guess by a hacker.

TYPES OF AUTHENTICATION

There are three types of authentication. They are the following

a. Pass Point.
b. Cued Click Point.
c. Persuasive Cued Click Points.

PASS POINT:

During this system, the user must select 5 points from a single image and repeat the same sequence of points from the single image[3] while selecting and logging in. The click events can occur on the same or a different image. Users can also choose an image sequence. There are four main modules in this system: image submission, image password point mark, pixel tolerance calculation, and authentication. Users can submit an image, then click on it to create a password, and the system will calculate the pixel tolerance for each pixel around it. The user must then click within the tolerances in the correct sequences while authenticating.

CUED CLICK POINT:

It has the same structure as the pass point, but the main difference is that it passes 5 points on five completely different images, one point per image. For a sequence of images, users click on one point per image. The image that follows is based on the previous click-point. We present the findings of an initial user study, which showed promising results. In terms of speed, accuracy, and number of errors, performance was excellent.

PERSUASIVE CUED CLICK POINTS:

PCCP could be used as an authentication method. PCCP is a great technology, but it has some security issues. Persuasive Technology assists users in creating more secure passwords. To avoid hotspots, the viewport is randomly positioned. Users are asked to select the highlighted portion of the viewport, but they are not allowed to select outside of the viewport. The user can change the position of the viewport by clicking on the shuffle button. Only during the password creation process is the highlighted viewport and shuffle button present. There is no shaded portion in the image during login and password confirmation, and users are free to click anywhere in the image.

ALPHANUMERIC PASSWORD AUTHENTICATION:

A password that is alphanumeric contains numbers, letters, and special characters (like an ampersand or hashtag)[4]. In theory, alphanumeric passwords are more difficult to crack than letters-only passwords. They can, however, be more difficult to create and remember. An example of an alphanumeric password is one that requires both letters and numbers. An alphanumeric keyboard is something like a computer keyboard. A character that is alphanumeric.

COMPUTER AUTHENTICATION:

Authentication is the process by which a user proves their identity to their system or server. Entering a username and password when logging into a website is a common example. There are various types of authentication.

a. Single-factor authentication (SFA).
b. Two-factor authentication (2FA).
c. Multifactor authentication (MFA).

Authentication allows legitimate users to access the computer. And if the authentication does not match, the unauthori sed person will be denied access. Authentication technique used by any digital system or site where the system or site needs to know who the actual authorised user is[5]. Even authentication is used to determine which resources the user has access to and which are denied access to, when the user can access the resource, and how much of the source the user can consume. Typically, server authentication involves the input of a username and password. Cards, retina scans, voice recognition, and fingerprints are examples of other forms of authentication. Client authentication typically entails the server providing the client with a certificate that a trusted third party, such as a bank, expects from the client. Authentication does not determine which activities or files a person may perform or view. Authentication merely identifies and verifies the identity of the user or system.

The primary goal of authentication is to grant authorised users access to the computer while denying unauthorised users access.

Passwords, physical identification, and biometrics are three methods used by operating systems to identify and authenticate users. These are explained further below.

PASSWORD:

A password is a secret text that is a combination of characters, numbers, and symbols that is used during authentication to verify the user's identity. A password is a vital secret key for digital devices or websites. To secure our vital information, users must create a username and password. All usernames and passwords have been saved on the server. When a user attempts to access information, the user must verify their username and password by comparing them to the login system.

PHYSICAL IDENTIFICATION:

Physical identification is used in organisations such as education departments, businesses, and government offices[6]. Now that technology has advanced, an organisation is setting up an authentication machine that will allow all authorised people in the organisation. For example, if an employee has an employee ID card to identify himself in their organisation, he must authenticate himself with it before beginning his duties. His ID card, which is known as physical identification, and this system will protect it against unauthorised individuals. Enter the organisation without permission. Physical security is something that any organisation must consider. safeguard against any threat. ATM smart cards, which are the best example of physical identification, are used in our daily lives.

BIOMETRICES:

In biometrics, bio stands for "human," and metric stands for "measurement." Biometrics, in its most basic form, is any measurement related to Human characteristics that distinguish one individual from others A type of unique security is biometric authentication. A technique that uses biological characteristics such as our voice, fingerprints, eye retinas, and so on[7].

SYSTEM OVERVIEW:

The graphical password-based authentication system is based on a click-based graphical password system that not only guides and assists the user in password selection, but also encourages the user to choose a more random distributed password. The proposed system is based on Persuasive Technology, which motivates and influences people to act in a certain way.

SECTION IN GRAPHICAL PASSWORD:

Graphical passwords are passwords that use images and different colours. Because people remember pictures better than words, graphical passwords are easier to remember. The graphical password is less vulnerable to brute-force attacks. Graphical passwords are more visually appealing and are used in place of text or alphanumeric characters. The graphical passwords are divided into six sections:

Scheme Based on Images:

The number of images will be provided in this scheme, and the user will be required to choose images as the password. From the grid, the For authentication, the user must select the actual images in the correct order. The password can be easily remembered by the user, as shown in the pictures.

Colour Base Scheme:

The number of colours will be provided in this scheme, and the user will be required to choose colours as the password. Different colours are used in this system to confuse imposters, but it is simple to use for authorised users. Because of the colours, the user can easily remember the password. It is impervious to shoulder surfing attacks. For authentication, the user must select the correct sequence of real colours. The password will then be saved in the database.

Recognition Based:

With this technique users set an image as a password during registration. User must reproduce or remember their own passwords, and thus no hints are given to remember the passwords. The user must select the specific number of images in this set as a password. During authentication, the user must correctly recognize these preselected image.

Signature Based Scheme:

The user's signature is used in this scheme for the password specified in the system. As it stands, no one's signature can be copied. A minor error in the signature can prevent access.

Pure Recall Based:

Users find it difficult to remember a pure recall authentication system. Some published results for pure recall authentication systems provide a higher level of entropy than text-based passwords. Users must draw the password on a grid or a blank canvas in order to use this scheme. The user must redraw the drawing so that it touches the listed sequence of coordinates. It is more secure than the recognition-based technique, but users struggle to remember their passwords.

Cued Recall Based:

During the registration phase of this scheme, the user must select multiple click points on an image in a specific order. Then came the user must select the same click points in the same order as the click points selected in the previous step. Phase of registration these techniques are simpler than pure recall-based techniques because they give the user hints to remember the password[8].

ADVANTAGES OF GRAPHICAL AUTHENTICATION METHOD:

- The system's security is extremely high.
- Graphical password schemes allow you to create more human-friendly passwords.
- Dictionary attacks and brute force searches are both impractical.

DISADVANTAGES OF GRAPHICAL AUTHENTICATION METHOD:

- They take up a lot more storage space than text-based passwords.
- The process of registering a password and logging in takes far too long.
- Shoulder Surfing: As the name suggests, shoulder surfing is the practise of peering over people's shoulders as they process information. Almost all graphical password schemes are vulnerable to shoulder surfing due to their graphic nature

3. CONCLUSION

Picture passwords can be used instead of textual alphanumeric passwords. Because most existing authentication systems have flaws, graphical passwords, in which users click on images to authenticate themselves, are the most preferred authentication system. Although authentication techniques generate passwords, they are vulnerable to attacks such as dictionary attacks, brute force attacks, and shoulder surfing.

A key usability goal of an authentication system is to assist users in choosing the best password. A user creates a memorable password that an attacker can easily guess, whereas strong system-assigned passwords are difficult to remember. As a result, modern researchers examined various alternative methods and concluded that graphical passwords are the most preferable authentication system. More security can be achieved by implementing encryption algorithms and hashing for storing and retrieving images and points. The proposed system combines the existing cued click point technique with new features. with the persuasive feature to influence user choice, encouraging users to choose more random click points is difficult to predict. The picture password is still in its infancy. More research is needed in this area.

4. REFERENCE

[1] Graphical Password Authentication. ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.

[2] Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015

[3] The Shoulder Surfing Resistant Graphical Password Authentication Technique. Mrs.Aakansha S. Gokhalea , Prof. Vijaya S.Waghmareb.

[4] A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K.

[5] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402

[6] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.

[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176,2000

[8] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar, Burak Erdeniz, “Towards Usable Solutions To Graphical Password Hotspot Problem”, IEEE INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE,2009.