International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 02 | 2021

Analysis of Different Graphical Password Authentication Techniques

[1]Ishita Popli, [2]Priya N.
[1]MCA student, Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, India
[2]Assistant Professor, Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, India

ABSTRACT

Authentication of users is very critical in the area of information security. Passwords have been adopted to enforce identity confidentiality. One of the important issues for the protection of knowledge is user authentication. There's a degree of convenience with a solid text-based password scheme. However, the difficulty of memorizing good passwords also drives their owners into writing or even saving them on paper. The password based on text is a common form of ancient authentication. Text-based passwords aim to target certain types of people, such as dictionaries, assaults, threats by brute force and social techniques etc. Graphical password protection is the preferred approach to text-based authentication. Computer systems and web-based platforms have used visual authentication techniques to authenticate their users in recent years. Many graphical password schemes were proposed to increase the accessibility and reliability of the password. This is divided into different techniques, based on recognition, cued-recall, pure recall and hybrid based.

Keywords: Authentication, Graphical password, Security, Text Passwords

1. INTRODUCTION

Protection of knowledge has been described as a major issue in recent years. Authentication is the main field of information security, which determines when user access to a specified device or resource can be permitted. Passwords are a usual and commonly used form of authentication. A password is a hidden authentication method for data access control. Unauthorized accounts are kept hidden and those who would like to get in are checked and password-based access is allowed or refused.

Passwords have been used as special code for identifying malicious users since ancient times. Passwords are used in modern times to block access to computing networks, cell telephones and others. For several purposes, computer users can need passwords such as logging in to their own accounts, accessing server e-mails, recovery of files, databases, networks, websites etc.

Usual passwords have disadvantages like password compromised, password forgetting, and password stolen. Therefore, to protect all our applications, strong authentication is needed. Conventional passwords were used for authentication, but accessibility and security issues are known to occur. Another approach is being implemented recently, such as graphical authentication. Psychological research showed that people are more able to recall pictures than text. Images are usually more easily remembered. Session codes are another way to provide greater protection. Passwords of session are passwords used only once. The session password is no longer useful after the session is ended. Users enter different codes for each individual login operation. For production of session passwords, the proposed authentication systems use text and color.

2. RELATED WORK

2.1 Graphical Passwords

Visual login is another name to alphanumerically authenticated password by clicking on the icons. It is a method of authentication where users have to pick such images in a particular order. The photographs are seen on an app for the visual user. This technique is called authentication of the graphical user. The passwords in texts can be stolen, compromised, and forgotten with demerits. Strong authentication technology is required in order to protect our whole application, but traditional password technical problems are not adequate for authentication. Nowadays a new methodology, i.e. graphical user authentication, is very common. Authentication for a graphical user is an alternative alphanumeric login form. Psychological experiments have shown that people can faster and longer memorize pictures than sentences.

2.2 Text Passwords

A word or string of characters is used to enter a facility and to authenticate the user. This character string is referred to as a password. It would be safe if passwords are kept hidden. You can crack passwords by watching the person's shoulder as he enters the password. This practice is called surfing by the shoulder. This tactic is used by attackers to rob the password from the user-typed physical view of the password. It can easily be broken if the password security is not high. It is simple to break small codes.

2.3 Graphical Password Methods

To address the disadvantages of the conventional word password technology, visual password technique has been introduced, as images can be stored better than text. A graphical password techniques survey reveals that the techniques can be divided into different classes -

2.3.1 Recognition-Based Technique

Users can select from a series of icons on the visual user interface in this technique. Upon checking, users choose their photos that are collected between collections of images at the time of sign up.

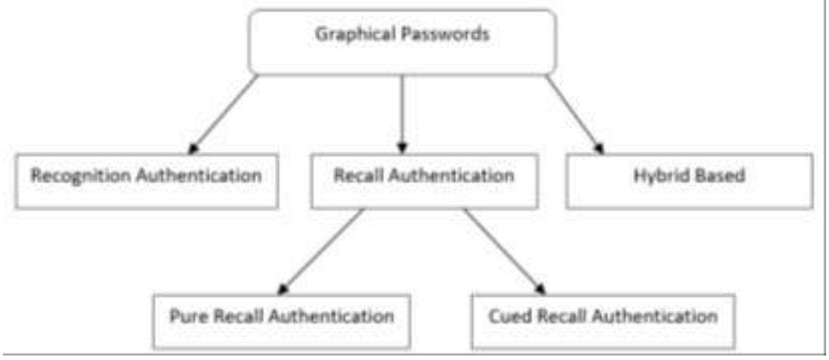
Graphical Passwords
Recognition Authentication
Recall Authentication
Hybrid Based
Pure Recall Authentication
Cued Recall Authentication

Fig.1. Categorization of Graphical password authentication techniques

2.3.2 Recall-Based Authentication

It's very fast and quick, but people don't seem to know their passwords. It is still safer than the recognition Authentication.

2.3.3 Cued Recall-Based Authentication

Users write their passwords in this technique without any suggestions or reminders. While this approach is easier and more practical, users cannot recall their passwords in this respect.

2.3.4 Hybrid Schemes

The variations of two or more authentication systems are used in this technique. This technique solves other systems' challenges, such as shoulder surf, spyware, etc.

3. BACKGROUND

3.1 Recognition Based Techniques

Cognometric systems are also known as recognition-based systems. Users of these programmers have to keep in mind the images together during registration and when logging in, they have to recognize their images from the image list. Various recognition-based systems were created with various picture styles, mostly such as clip arts, marks, faces, forms, etc.

In the challenge collection of password pics and videos, the user must recognize the password pictures. Random photos created by tiny initial seeds can be stored and transferred easily and art images are not unfavorable to document or communicate with anyone. This scheme has disadvantages as an obscure image and body size is difficult to recall, far smaller than text-based passwords.

Cognitive authentication is an algorithm based on recognition that resists shoulder surfing. If a user is in a portfolio picture, the user can step right or to the bottom edge of the panel. The total likelihood of the right response is calculated by the cognitive authentication scheme such that no possibility was entered after each round. Authentication is a positive when chance exceeds a certain threshold.

3.2 Pure Recall Based Techniques

Pure, graphic password reminder schemes are also known as metric drawing system, because the user remembers a grid edges drawn during registration. Users usually use this style of application to draw password to a grid. Remembrance is hard to remember, since the retrieval is without recalls or hints.

3.2.1 Passdoodle

This graphic password technique consists of the manual template or text drawn by any input system on user computer. The user has to record a matching doodle for authentication. As far as security is concerned, the hackers are much more confident and it would be hard to imagine.

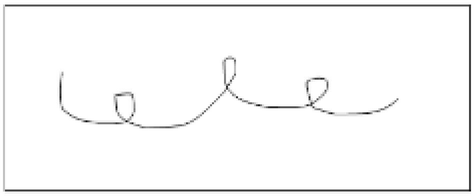

Fig.2. Example of Passdoodle

3.2.2 Draw A Secret

People are required to use pen or mouse to draw and build their password on a 2D grid. A continuous stroke or a few distinct strokes by "pen-ups" can be seen in the drawing, such that the next stroke continues in another cell. Using the same pattern along the grid cells is needed to successfully sign in. The computer stores the sequence of coordinates that users draw a grid cell password and create a DAS password encoded. The password length is the number of all coordinating pairs. By having a stroke in the same sequence used during registration, the user will redraw the picture for authentication.

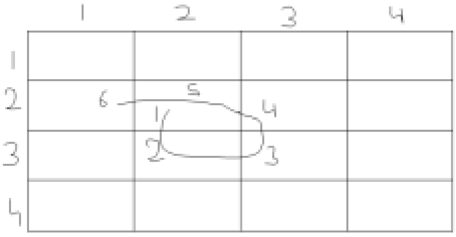

FIG.3. Draw a Secret method on a 4*4 Grid

3.2.3 Syukri Algorithm

The user drawing as a signature with the mouse is achieved through this authentication. The technique consists of two phases: registration and check. Users must sign with the mouse at the time of login, and the machine will remove the signature space. The data is then saved to the archive. In the check step, the user first enters and then removes the user's signature parameters. A geometric average and dynamic database modification are used for the testing of the scheme. The biggest benefit of this approach is that it is not necessary to recall the signatures and signatures that are difficult to counterfeit.

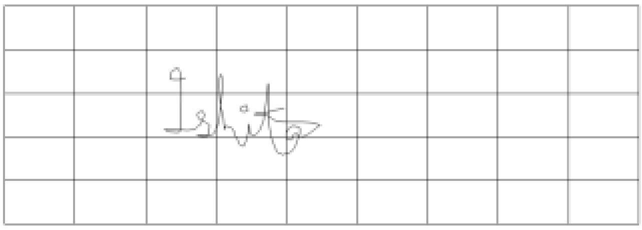

Fig.4. Example of Syukri algorithm

3.4 Cued-Recall Based Authentication

Users write their passwords in this technique without any suggestions or reminders. While this approach is easier and more practical, users cannot recall their passwords in this respect.

3.4.1 Blonder

The first visual password in which user has to click pre-determined areas, will show a default picture. Since the field of preset click regions is relatively limited, it takes a long password so it can be easy to keep long passwords safe.

3.4.2 PassPoint

In this, the picture could be dynamic, real world scenario and the areas, which were the weaknesses of the blonder algorithm, could not be determined. Users have to press on the icons of those places for registration. The user must press near the chosen points within any tolerance distance for authentication. The shoulder surfing issue is not removed entirely.

3.4.3 Passlogix v-Go

A chronologically specified password is produced in this technique. Depending on their surroundings, the user can choose his favourite background picture such as the dining room, kitchen and bedroom. Then, the user can enter the password by clicking on the objects in the scene. The operation can be the repetition in a space, for example, several things can be clicked in a kitchen to follow a certain meal recipe.

3.4.4 Drawing Geometry

There are a x b grids in this system, and every grid is divided into four diagonal lines. The reasonable number of rows and columns can be varied depending on the screen size.

3.5 Hybrid Schemes

Two or three graphical passwords are a mix of hybrid systems. These systems are implemented to address the limits of a single programme, including the issue of hotspots, shoulder surfing, guess passwords and spyware. Many single schemes are addressed and some mixed schemes merged for recognition-based and recall-based systems. Based on colour, templates for users containing many troubles are provided in this scheme.

First, the user picks an icon and then taps on the image location then selects the template position, and saves the password. The user then selects the template location. When logged in, the users must select the correct prototype, put it to the correct position on the image, and enter the characters seen from top to bottom through the holes. The passwords in this pattern are more memorable than password-based text since this system allows users just to recall where the picture template stands.

4. CONCLUSION

This paper proposes a new graphical password Authentication which attempts to fulfill simultaneously the requirements of usability and protection. The scheme has a wide room for passwords, and the user can easily generate a password and even save it with the basic implementation. That is also because of the convenient and conveniently retrievable use of the graphical password. The graphical login technology is safer than traditional passwords. It is precise and trusted rather than passwords in text. Various algorithms include visual password verification systems based on recognition based, pure recall based, recall-based and hybrid are tested. In this article, we identify various benefits of authenticating a graphical password. It can also be argued that breaking visual passwords is more complex than breaking alphanumeric passwords.

5. REFERENCES

[1] "A Graphical Password Authentication System", Ahmad Almulhem.

[2] "The Security Analysis of Graphical Passwords", Wei Hu, Guoheng Wei and Xiaoping Wu, November2010.

[3] "A Different Graphical Password Authentication Techniques", Dhanashree Kadu, Shanthi Therese and Anil Chaturvedi.

[4] "A Secure Graphical Password Authentication System", Ms. Sreya Prakash, Mrs. Sreelakshmy M K.

[5] "Enhancement of password authentication system using graphical images", vaibhav desale, Amol Bhand, and Swati Shirke.

[6] "A New Hybrid Visual User Authentication Technique based on Drag and Drop Method", Salim Istyaq and Khalid Saifullah.

[7] "Survey on Graphical Password Authentication Techniques", Aishwarya N. Sonar1a nnd Purva D. Suryavanshi.

[8] "Graphical Password Authentication: Methods and Schemes", Geeta M. Rane.