Graphical Passwords: Behind the Attainment of Goals

Vikas Nandwana[1], Pranit Nehete[2], Ashutosh Patil[3]

Abstract: ***Users who enter their credentials in a public location risk having their passwords stolen by intruders. An attacker can steal a password by watching the individual's authentication session or recording it. Shoulder-surfing is a well-known risk, and it's especially dangerous while authenticating in public. Until recently, the user's awareness was the sole barrier against shoulder-surfing. Shoulder surfing resistant password authentication ensures that the user's authentication is not compromised by shoulder surfing. Because the user is never required to click directly on password symbols, it allows users to authenticate by inputting their password in a graphical manner in vulnerable areas. This mechanism's usability testing revealed that inexperienced users were able to correctly input and remember their graphical password.***

Keyword: Image Selection, Extraction, Machine learning

1. Introduction

The shoulder surfing attack is an assault in which the adversary watches over the user's shoulder while he inputs his password in order to steal the password. Sobrado and Birget presented three shoulder surfing resistant graphical password methods since traditional password schemes are prone to shoulder surfing. Most modern graphical password methods, on the other hand, are subject to shoulder-surfing, a recognised vulnerability in which an attacker can acquire a password by watching or recording the authentication session. Shoulder-surfing is worsened with graphical passwords because of the visual interface. For most individuals, remembering a graphical password is simpler than remembering a text-based password. Assume you need an 8-character password to obtain access to a certain computer network. Strong passwords that are resistant to guessing and dictionary attacks can be created. Key loggers, shoulder-surfing, and social engineering are all examples of cyber crime. Mobile phones, ATM machines, and E-transactions have all employed graphical passwords for authentication.

2. Motivation

We're putting the system in place because The graphical capabilities of portable devices was restricted in the early days; the colour and pixel it could display was limited. Users may use their personal accounts to send private work emails, upload images to cloud albums, or remit money from their e-bank account at any time and from any location, thanks to the growing number of mobile devices and web services. They may accidentally reveal their passwords to unexpected individuals while logging onto these services in public. As a result, it is dangerous for users to enter their credentials in public areas.

3. Problem Definition

The suggested technology in this project is PassMatrix, a secure graphical authentication framework that uses one-time login indications to prevent users from becoming victims of shoulder surfing assaults while typing passwords in the open. For each pass-picture, a login indicator is generated at random and is rendered useless after the session has ended. Because users utilise a dynamic pointer to point out the position of their credentials rather than clicking on the password object directly, the login indicator provides superior protection against shoulder surfing assaults.

4. Literature Survey

Ankitha Vaddeti1 Deepthi Vidiyala1 Vineetha Puritipati1 Raveendra Babu Ponnuru1 Ji Sun Shin2 Goutham Reddy Alavalapati1, et. al [1] Over the last few decades, graphical authentication methods have evolved as a viable alternative to traditional authentication methods. Recognition-based authentication is one of the most common forms of graphical authentication systems, in which the user authenticates by tapping on pass pictures from one or more challenge sets of images. A review of existing graphical authentication solutions reveals that some of them undermine security while simplifying the approach, potentially allowing for attacks such as guessing, hidden camera, smudging, shoulder surfing, and others. Furthermore, a number of them make performance sacrifices in the sake of security. However, this work provides a novel technique that effectively resists the aforementioned threats.

Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin, et. al [2] An attacker can capture a password by directly seeing or recording the authentication session, which is known as shoulder-surfing. This difficulty has been worsened with graphical passwords due to the visual interface. Some graphical schemes have shown to be resistant or immune to shoulder-surfing, but they come with substantial usability costs, most notably in the time and effort required to log in. In this study, we present and analyse a novel shoulder-surfing-resistant strategy with good PDA usability. For sequence retrieval, we were inspired by DAS's drawing input approach and Story's association mnemonics. Instead than clicking straight on their password pictures, users must now draw an ordered curve through them. The drawing input technique, in combination with other precautions such as deleting the drawing trace, showing degraded images, and starting and terminating with randomly determined images, provides strong shouldersurfing resistance. Users were able to type their passwords reliably and remember them over time, according to a preliminary user research.

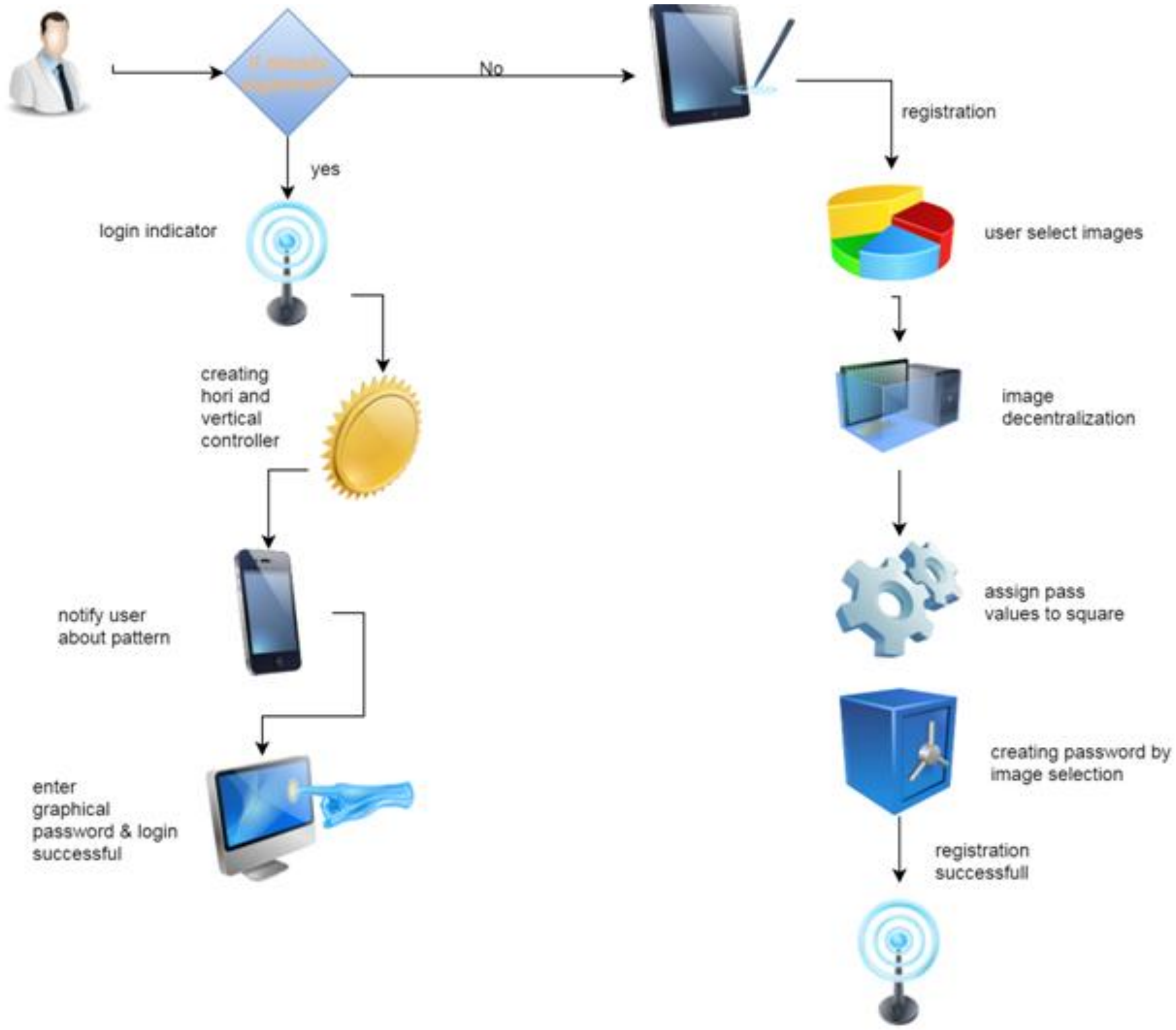
Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng et. al. [3]-Password-based authentication is commonly used in computer security and privacy applications. Human activities, on the other hand, are viewed as "the weakest link" in the authentication chain, such as picking incorrect passwords and entering passwords insecurely. Users prefer short or meaningful passwords over random alphanumeric sequences because they are easier to remember. People may now access online and mobile applications from a variety of devices at any time and from any location. This development is beneficial, but it also raises the risk of credentials being exposed to shoulder surfing assaults. In order to gather users' credentials, attackers can either view them directly or employ external recording equipment. We presented PassMatrix, a unique authentication method based on graphical passwords that can withstand shoulder surfing assaults, to solve this problem. PassMatrix gives no suggestion for attackers to figure out or narrow down the password, even if they execute several camera-based assaults, with a one-time valid login indicator and circulative horizontal and vertical bars encompassing the whole scope of pass-images. We also built a PassMatrix prototype for Android and tested it with real users to see how well it remembered and used. The suggested approach delivers higher resistance against shoulder surfing attacks while preserving usability, according to the testing results.

ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, et. al. [4]Graphical passwords are an alternative to alphabetic passwords since remembering alphanumeric passwords is a very time-consuming procedure. It is much easier to access and utilise any programme with user-friendly authentication. According to psychological research, visuals are easier to recall than alphabets or figures, which is one of the main reasons for using this strategy. We are utilising graphical passwords to represent cloud authentication in this study. We suggested a cloud with graphical security using an image password. One of the methods we provide is based on choosing a username and using photos as a password. We want to provide a set of graphics based on the alphabet series with this article.

Gi-Chul Yang. [5]Graphical passwords employing graphics have emerged to tackle the challenge of text-based password authentication. Authentication using graphical passwords is done by selecting particular spots on a screen picture. If the relevant spots on the screen cannot be picked in the same order, these traditional graphical password schemes will fail to recognise the user. To address this issue, PassPositions, a new graphical password method, was developed. PassPositions was created with universal design in mind, making it accessible to people of all abilities. PassPositions does, however, have certain flaws in some situations. This paper will identify a PassPositions problem and provide ways to enhance them.

5. System Architecture

PassMatrix is a shoulder surfing-resistant authentication method based on graphical passwords. Users may point out the position of their pass-square without physically clicking or touching it, which is prone to shoulder surfing assaults, by using a one-time login indication per picture. Because the horizontal and vertical bars that cover the full pass-image are designed in such a way that attackers have no way of narrowing down the password space, even if they have several login records for that account. For a series of n pictures, a password in PassMatrix consists of only one passsquare per pass-image. The number of pictures (n) is set by the user. Instead of n squares in one image, like in the PassPoints system, users pick one square every image for a succession of n photos in PassMatrix. The authentication process in PassMatrix is divided into two phases: registration and authentication. The user establishes an account with a username and password at this point. For a sequence of n photos, the password contains just one pass-square per image. The user selects the number of photos (i. e., n) after weighing the system's security and usefulness. The user logs into PassMatrix at this point with his or her username, password, and login indications. Please provide feedback.



6. Advantages, Disadvantages and Application

6.1 Advantages

Graphical Passwords provide a larger password field and are not restricted to alpha-numeric combinations. The problem of keystroke logging is addressed with the Graphical Password.

6.2 Limitation

Text-based passwords take up a lot more storage space. The procedure of creating a password and logging in takes far too long. Shoulder Surfing: As the name suggests, shoulder surfing involves keeping an eye on people's shoulders as they digest information.

6.3 Application

Require a lot more storage space than text-based passwords. The password registration and log-in processes take much too long. Shoulder Surfing: While the term indicates, shoulder surfing involves peering over people's shoulders as they absorb information.

7. Conclusion and Future Work

PassMatrix is a proposed shoulder surfing-resistant authentication system based on graphical passwords. Users may point out the position of their pass-square without physically clicking or touching it, which is prone to shoulder surfing assaults, by using a one-time login indication per picture. Because to the design of the horizontal and vertical bars that cover the full pass-image, attackers have no way of narrowing the password space, even if they have many login records for that account. In addition, we developed an Android PassMatrix prototype and conducted user tests to assess memorability and usability. Users can enter into the system with an average of 1: 64 tries (Median=1), and the Total Accuracy of all login trials is 93: 33 even two weeks after registration, according to the testing data. With an average of 3: 2 pass-images, the whole time necessary to enter into PassMatrix is between 31: 31 and 37: 11 seconds, which is deemed acceptable by 83: 33 of our user survey participants. PassMatrix is a novel and easy-to-use graphical password authentication system that may successfully prevent shoulder-surfing assaults, according to testing findings and survey data. PassMatrix may also be used in any authentication scenario and on any device with basic input and output capabilities. PassMatrix is also beneficial in the real world, according on the poll findings from the user study.

References

[1] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin" A New Graphical Password Scheme Resistant to Shoulder-Surfing"

[2] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng. " A Shoulder Surfing Resistant Graphical Authentication System".

[3] Ankitha Vaddeti1 Deepthi Vidiyala1 Vineetha Puritipati1 Raveendra Babu Ponnuru1 Ji Sun Shin2 Goutham, Reddy Alavala pati1, " Graphical passwords: Behind the attainment of goals".

[4] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochar" Graphical Password Authentication".

[5] Gi-Chul Yang, " PassPositions: A Secure and User-Friendly Graphical Password Scheme"