International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 12, Number 2 (2016), pp. 197-201

http://www.ripublication.com

A Secure Graphical Password Authentication System

Ms. Sreya Prakash

M-Tech, Dept. of CSE, Malabar Institute of Technology, Anjarakandy, India.

E-mail: sreyaprakash0@gmail.com

Mrs. Sreelakshmy M K

Asst. Professor, Dept. of CSE, Malabar Institute Technology, Anjarakandy, India.

E-mail: mksreelakshmy@gmail.com

Abstract

Nowadays most popular method for User Authentication is using Textual Password. This method has several significant drawbacks like dictionary attack, brute force attack etc. A secure text based password must be formed using a combination of uppercase, lowercase, and special characters. Users have a tendency to select weak text-based passwords, which are short and easy to remember. To overcome the limitations of text-based passwords, several picture-based passwords have been proposed. Picture based password systems suffer from several problems, one of them is the shoulder surfing attack, ie, images that users select as password are both easy for an attacker to watch by snooping over shoulders or by using a camera to record input and also relatively predictable. An authentication system called PassMatrix is used to overcome the shoulder surfing attack. User has to select pictures as their password during the registration phase and choose a pass-square per image. A one-time login indicator and horizontal and vertical bars are used.To secure the pass-images from the attackers, Generic Visible

Watermark Embedding technique is used to blend a cover image and a pass-image. PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing .This method can be extended to secure web applications by using QR code.

Keywords: Graphical password, shoulder surfing, watermarking, QR Code.

1. INTRODUCTION

Authentication based on passwords is used in many applications for computer security and privacy. Comprised of numbers and upper- and lowercase letters, textual passwords are considered strong enough to resist against brute force attacks. They are very easy to implement. Alphanumeric passwords are required to satisfy two contradictory requirements. They should be easy to memorize and also at the same time they should be hard to guess. Various graphical password authentication schemes were developed to overcome the problems and weaknesses associated with textual passwords. Humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. However, most of these image based passwords are vulnerable to shoulder surfing attacks.

A secure graphical authentication system named PassMatrix [1]is used that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public by the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session ends. The login indicator provides better security against shoulder surfing attacks because users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly. If a passimage is faintly printed on a cover image, the legitimate user who is near to the monitor screen can see the pass-image but someone who is away from the screen cannot recognize the pass-image. Generic Visible Watermark Embedding technique is used to blend a cover image and a pass-image. Moreover, because images with less independent objects usually suffer more on the hot-spot problem, carefully selecting images with rich objects can alleviate the hot-spot based random guess attacks. This method can also be extended to secure login of web applications in computers by using QR code.

II. RELATED WORK

Syed Shabih et al. [2]proposed a operation code authentication scheme technique which provides more security to a user in typing his password, in a public place, and in case that user is in critical position, of accessing his computer system. At the time of sing up, the user will be asked to submit two things which he can remember besides the username. Passcode is any numeric number of 3 to 6 digits which can be easily remembered. Four letter word is a four letter word like Iran, Iraq, iram etc, which represents the 4 arithmetic operators i.e. division, multiplication, addition, and subtraction. This four letter word will be used to perform the arithmetic operations. At the time of signing in, the user will have to enter his username, system will give user a formula which he has to solve.

Tsung-Yuan et al. [10] proposed a novel method for generic visible watermarking with a capability of lossless image recovery is proposed. The method is based on the use of deterministic one-to-one compound mappings of image pixel values for overlaying a variety of visible watermarks of arbitrary sizes on cover images. The compound mappings are proved to be reversible, which allows for lossless recovery of original images from watermarked images. The mappings may be adjusted to yield pixel values close to those of desired visible watermarks. Different types of visible watermarks, including opaque monochrome and translucent full color ones, are embedded as applications of the proposed generic approach. A two-fold monotonically increasing compound mapping is created and proved to yield more distinctive visible watermarks in the watermarked image.

Sarosh Umar et al. [11]proposed a a novel recognition-based image authentication system called Select-to- Spawn which is secure, robust and convenient to use. This system allows the user to create a graphical password by first selecting an initial image from a collection of available pictures. The selected image will be opened in a new window in which the picture is further divided into 4x4 grid or 16 rectangular parts. The grid lines can be highlighted if one desires to facilitate ease of selection but as a default case they are rendered invisible. The user can then click on any one of the grid cell. This further spawns into a new image with invisible grid ines dividing it into 16 cells. Selecting any cell of the image spawns yet another picture with invisible grid lines. This process of selection may progress depending upon the user and each image selected by the user becomes the part of the password.

EXISTING SYSTEM

In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. A login indicator is randomly generated for each pass-image and will be useless

after the session terminates. To protect against shoulder surfing, the indicator is not shown until the hand touches the screen and will vanish immediately when the hand leaves the screen. There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. Users can fling either bar using their finger to shift one alphanumeric at a time. They are used to align the one-time indicator with the pass-square in each passimage during the authentication phase. In order to obfuscate and thus hide the alignment patterns from observers, randomly shuffled the elements on both bars in each pass-image and let users shift them to the right position.

PROBLEM DEFINITION

Most of the graphical passwords are vulnerable to shoulder surfing. In Passmatrix, the pass-image is displayed on the screen and the user can easily identify the pass image. PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing. This method is only implemented in mobile devices for screen locking.

PROPOSED SYSTEM

Proposed system allows the user to create a graphical password by first selecting an image from a collection of available pictures . In the selected image user has to select one grid as the password. The selected image is watermarked with a cover image using Generic Visible Watermark Embedding technique. The method is based on the use of deterministic one-to-one compound mappings of image pixel values for overlaying a variety of visible watermarks of arbitrary sizes on cover images. During login, after entering the user details a QR Code is generated in the computer. User has to scan the QR code using his mobile phone. After scanning, a collection of images will be appeared in the screen of the phone. User has to select the image. After choosing correct image, the watermarked image will be appeared on the screen. User has to choose the correct grid position that he has already registered in the watermarked image.

CONCLUSION

Graphical passwords are an authentication method that uses pictures as passwords instead of using alphanumeric characters. They are attractive since humans normally remember pictures better than words. In this project a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public. User has to choose their pass image from a collection of available pictures. To hide the pass-image from the attackers Generic

Visible Watermark Embedding technique is used to blend a cover image and a pass-image. It is easy for legitimate users to recognize the pass-image in the blended image. On the other hand, this task is di_cult for attackers. This method is extended to secure web applications by using QR

REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, and Chia-Yun Cheng. A shoulder surfing resistant graphical authentication system.

[2] Tsung-Yuan Liu and Wen-Hsiang Tsai. Generic lossless visible watermarkinga new approach. IEEE transactions on image processing, 19(5):1224–1235, 2010.

[3] Mohammad Sarosh Umar and Mohammad Qasim Rafiq. Selectto- spawn: A novel recognition-based graphical user authentication scheme. In Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on, pages1–5.IEEE