International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

A PASSMATRIX AUTHENTICATION SCHEME FOR SHOULDER SPOOFING RESISTANT

R.Aravindhan

M.Tech(CSE),II Year

PRIST UNIVERSITY, Thanjavur

Abstract - Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users’ credentials. To overcome this problem, a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks is proposed. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

Keywords: Shoulder surfing, Graphical password, Key logger, Sector base, Authentication

1. INTRODUCTION

One of the major functions of any security system is the control of people in or out of protected areas. Authentication is the process of determining that the person requesting a resource is the one who he claims to be. Most of the authentication system these days uses a combination of username and password for authentication. Shoulder surfing is a technique of gathering information such as usernames and passwords by watching over a person‟s shoulder while he/she logs into the system, thereby helping attacker to gain access to the system. Keylogging is the practice of noting the keys struck on a keyboard , typically in a manner so that person using the keyboard is unaware that such action is monitored. There are two types of keyloggers viz. software keylogger and hardware keylogger. Software keylogger are installed on the computer systems which usually are located between the OS and the keyboard hardware, and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

every keystroke is recorded. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and saves every keystroke into the file or In the memory of the hardware device.Many authentication systems are invented to avoid problem of shoulder surfing and keyloggers for e.g. biometric systems. But these systems are costly and each and every individual user cannot afford to purchase biometric system.As conventional password system is vulnerable to shoulder surfing and keyloggers.

2. LITERATURE SURVEY

1. "SECURE USER AUTHENTICATION IN INTERNET BANKING,"

- Applied in online banking environments . The banking industry as well as way people interact with financial institution and one another financially.

- **METHOD**

  - Virtual Keyboard

DRAWBACKS

- Screenshot Capturing
- Shoulder Spoofing

2. "ON USER CHOICE IN GRAPHICAL PASSWORD SCHEME,"

Permitting user selection of passwords in two graphical password schemes, one based directly on an existing commercial product, can yield passwords with entropy far below the theoretical optimum and, in some cases, that are highly correlated with the race or gender of the user.

METHOD

Two graphical schemes

- Face scheme
- Story scheme

DRAWBACKS

- No requirement for users to change their passwords
- Recovery of password is a difficult process

3."REDUCING SHOULDER SURFING BY USING GAZE BASED PASSWORD ENTRY,"

Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome.

METHOD

- Eye-Password

DRAWBACKS

- When compared to password-entry time with the keyboard the gaze based approaches are about five times slower
- Trigger-based mechanism had considerably higher error rates due to eye-hand coordination

4., "SECURE AUTHENTICATION USING DYNAMIC VIRTUAL KEYBOARD LAYOUT,".

- Virtual Keyboard authentication has helped users to protect their username and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

passwords from being captured by key loggers, spyware and malicious bots. However Virtual Keyboard still suffers from numerous other fallacies that an attacker.

METHOD

- click based screenshot capturing, over the shoulder spoofing and co-ordinate position noting.
- virtual keyboard that is generated dynamically each time the user access the web site. Also after each click event of the user the arrangement of the keys of the virtual keyboard are shuffled.

DRAWBACKS

- The time taken to type the password is slightly more than traditional virtual keyboard.

3. PROBLEM STATEMENT:

The graphical password and virtual keyboard has been proposed as an alternative to alphanumeric password scheme as it is vulnerable to shoulder-surfing, hidden camera and spyware attacks. the graphical password scheme achieves memorability and security to certain extent but it is captured by direct observation or by recording login session called shouldersurfing attack.

4. EXISTING SYSTEM

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts.

Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies .As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically.

Drawbacks of Existing System

- The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain
- Most of the image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

Proposed System

In this paper, a secure graphical authentication system named PassMatrix is presented that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

Advantages of Proposed System

The login indicator for each pass-image varies so that each pass-image is an independent case. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes

PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped

5. IMPLEMENTATION

Image Discretization Module

At this stage, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if Pass-Matrix is applied to authentication .The user has to choose images from a provided list as pass-image. Then the user will pick a pass-square or each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.This module divides each image into squares, from which users would choose one as the pass-square.An image is divided into a 7 _ 11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations. Hence, in this implementation, a division was set at 60-pixel intervals in both horizontal and vertical directions, since 60 pixels is the best size to accurately select specific objects .

Login Indicator Generator Module

This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In this implementation, characters A to G and 1 to 11 for a 7 _ 11 grid is used. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually.

Horizontal and Vertical Axis Control Module

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag function for users to control both bars. Users can drag either bar to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the user's pass-square.

Dynamic Virtual Keyboard Layout Generation:

In this module a virtual keyboard layout is generated. A virtual keyboard is a software component that allows a user to enter characters. A virtual keyboard can usually be operated with input devices, which may include an actual Computer keyboard and a computer mouse.the keys are hidden when the user clicks a particular key.After the release of mouse click, the keys are visible. Since the keys are hidden after user presses the hide keys button, even if the screen shot is recorded it would make no sense to the attacker. For example for the same password "abdg" the screen capture would record the following things. This makes no sense to attacker and user password is thus secure. we shuffle the keyboard after every click. As a result if a person is standing behind to spoof the password over the shoulder, he cannot remember the password since the layout and arrangements of alphabet change after every click. Also noting the coordinates would be of no help since even if the position is noted, the next click would again reshuffle the keyboard. Thus if "v" was currently at position (3, 1), the next click would have some other alphabet at the same position (3, 1).

Database

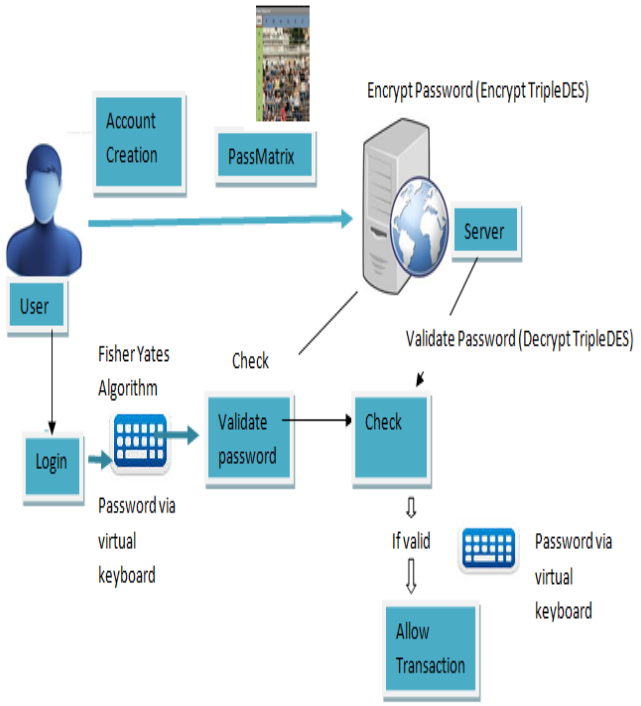
The database server contains several tables that store user accounts, passwords (ID numbers of pass-images and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase.

PassMatrix _Authentication Algorthim

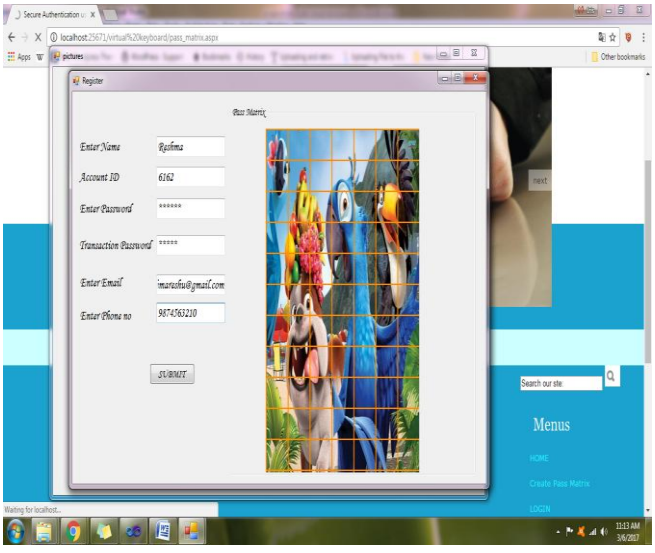
1. when user inputs username & password
2. if valid(username & password)
3. then
4. login Indicator Generation
5. if verifying the shifting of horizontal & vertical bar matches the login indicator
6. then Login Success
7. else
8. print invalid login
9. end if
10. else
11. print invalid username or password
12. end if

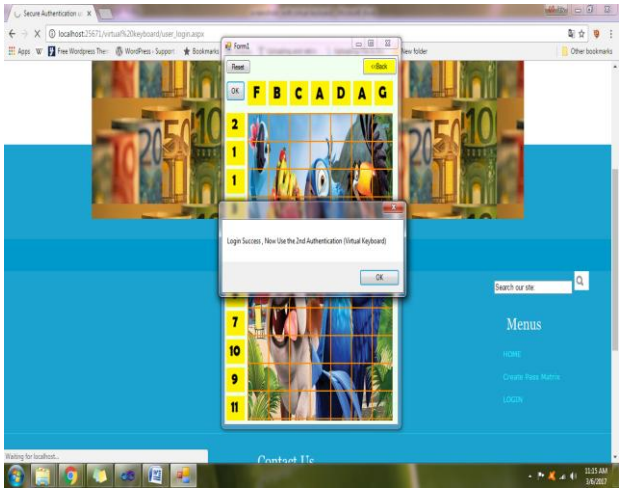
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

7. SYSTEM MODEL



Screenshots:





8. CONCLUSION AND FUTURE WORK

Shoulder surfing and key logger resistant textbased graphical password scheme is proposed. In this system user can easily login into system without worrying about shoulder surfing and key logger attack. User just have to remember pass sector and alphanumeric password. This scheme is simple and efficient. Unlike other graphical password schemeuser can easily log into the system without remembering graphical sequences.Thissystem do not need use of physical or on-screen keyboard.

9. REFERENCES:

1] Xiaoyuan Suo, Ying Zhu G. Scott. Owen, 2005, 'Graphical passwords: a survey', 21st Annual Computer Security Applications Conference.

[2] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 2005, 'An Association-Based Graphical Password Design Resistant to ShoulderSurfing

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 28, 2017 ISSN: 2348-6600
Reference ID: IJCS-292 PAGE NO: 1927-1933

Attack', IEEE International Conference on Multimedia and Expo (ICME).

[3] Julie Thrope, P. C. van Oorschot, Anil Somayaji, 2005, 'Passthoughts: authenticating with our minds', Proceedings of the 2005 workshop on New security paradigms, ACM.

[4] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean-Camille Birget, 2006, 'Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme',Proceedings of Advanced Visual Interfaces (AVI2006).

[5] Furkan, Tari, A. Ant Ozok, Stephen H. Holden, 2006, 'A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords', Proceedings of the second symposium on Usable privacy and security, ACM.

[6] Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan, 2007, 'Graphical passwords & qualitative spatial relations',Proceedings of the 3rd symposium on Usable privacy and security, ACM.

[7] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, 2007, 'Reducing shoulder-surfing by using gaze-based password entry',Proceedings of the 3rd symposium on Usable privacy and security, ACM.