ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Survey on an Authentication Scheme for a Better Security against a Peeping Attack by a Video Camera

Dr.R.SeethaLakshmi[1], Lakshmi.A[2], Anusha.R[3], Sangeethavani.R[4]
Professor[1], Department of Computer Science and Engineering,
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering, College, Avadi, Tamilnadu
UG scholar[2, 3, 4,] Department of Computer Science and Engineering,
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering, College, Avadi, Tamilnadu
drseethalakshmi@velhightech.com[1], lakshmiannand@gmail.com[2], anooyadhav@gmail.com[3],
sangeetharaj2295@gmail.com[4]

Abstract- ***Peeping attack in the real world is one of threats to a user authentication. What is worse is that an emerging attack method such as video capturing makes traditional measures against peeping attack insufficient. In this paper, I propose a unique user authentication scheme named "fake Pointer" for a solution to a peeping attack by video capturing. It makes hard for attackers to get a secret even if he/she captures an authentication scene using a video camera.***

1 .Introduction

Textual passwords have been the most widely used authentication method for decades. Comprised of num-bers 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 [1]. 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 [2]. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in 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 period-ically. However, most of these 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. In this paper, we present a secure graphical authentica-tion system named PassMatrix that protects users from be-coming 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.

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

2. Related work

In several decades, a research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems.. Many other schemes such as those in may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc.In the early days, the of handheld devices graphical capability was weak; the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) technique was proposed by Jermyn et al. in 1999 In 2005, Susan Wiedenbeck et al. introduced a graphical authentication scheme PassPoints and at that time, handheld devices could already show high resolution color pictures. Christo Ananth et al. [3] proposed a system, this system has concentrated on finding a fast and interactive segmentation method for liver and tumor segmentation. In the pre-processing stage, Mean shift filter is applied to CT image process and statistical thresholding method is applied for reducing processing area with improving detections rate. In the Second stage, the liver region has been segmented using the algorithm of the proposed method. Next, the tumor region has been segmented using Geodesic Graph cut method. Results show that the proposed method is less prone to shortcutting than typical graph cut methods while being less sensitive to seed placement and better at edge localization than geodesic methods. This leads to increased segmentation accuracy and reduced effort on the part of the user. Finally Segmented Liver and Tumor Regions were shown from the abdominal Computed Tomographic image. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

In order to defend the shoulder surfing attacks with video capturing, FakePointer was introduced in 2008 by T. Takada. In addition to the PIN number, the user will get a new ”answer indicator” each time for the authentication process at a bank ATM. In other words, the user has two secrets for authentication: a PIN as a fixed secret and an answer indicator as adisposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. At each login session, the FakePointer interface will present the user an image of a numeric keypad with 10 numbers (similar to the numeric keypad for phones), with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow key. This operation is repeated until all the PIN digits are entered and confirmed. This approach is quite robust even when the attacker captures the whole authen-tication process.

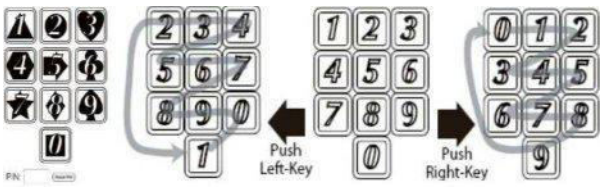

Fig. 1. FakePointer

2.1 Problem Statement

The following lists the research problems we would like to address in this study:
The problem of how to perform authentication in public so that shoulder surfing attacks can be allevi-ated.

- The problem of how to increase password space than that of the traditional PIN.
- The problem of how to efficiently search exact pass-word objects during the authentication phase.
- The problem of requiring users to memorize extra information or to perform extra computation during authentication.
- The problem of limited usability of authentication schemes that can be applied to some devices only.

2.2Attack Model

In this paper, based on the means the attackers use, we categorize shoulder-surfing attacks into three types as below:

Type-I: Naked eyes.

Type-II: Video captures the entire authentication process only once.

Type-III: Video captures the entire authentication process more than once.

2.3Assumptions

In this paper, we do not discuss the habitual movements and the preference of users that the attacker may take advantage of to figure out the potential passwords. In addition, we have four assumptions in this study:

Any communication between the client device and the server is protected by SSL so that packets or information will not be eavesdropped or intercepted by attackers during transmission. The server and the client devices in our authentica-tion system are trustworthy. The keyboard and the entire screen of mobile de-vices are difficult to protect, but a small area (around 1:5 cm^2) is easy to be protected from malicious people who might shoulder surf passwords. Users are able to register an account in a place that is safe from observers with bad intention or surveillance cameras that are not under proper man-agement.

3.Implementation:

Although the Pass Matrix prototype was implemented on an Android system which has a small screen, it is not limited to the applications on a small screen device, for example screen locking. In fact, it could be applied to a wide range of authentication scenarios. For instance, user account login on web browser, and

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

application login/unlick OS.

The PassMatrix prototype was built with Android SDK 2.3.3 since it was the mainstream version of the distribution in 2012.After connecting to the Internet, users can register an account, log in a few times in practice mode, and then log in for the experiment with a client's device (see Figure 3(a)). In the client side of our prototype, we used XML to build the user interface and used JAVA and Android API to implement functions, including username checking, pass-images listing, image discretization, pass-squares selection, login indicator delivery, and the horizontal and vertical bars circulation. In the server side of our implementation, we used PHP and MySQL to store and fetch registered accounts to/from the database to handle the password verification.Although in our proposed system we mentioned that users can import their own images, we used alist of 24 fixed test images in ourexperiment.

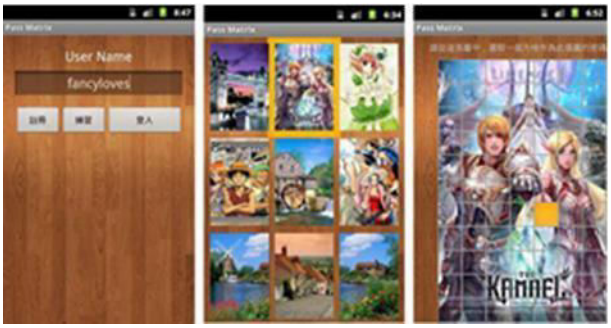

Fig. 3. (a) The Main page of PassMatrix, users can register an account, practice or start to log in for experiment. (b) Users can choose from a list of 24 images as their pass-images. (c) There are 7 11 squares in each image, from which users choose one as the pass-square.

Each imageis displayed in a size of 420 660 pixels and is discretized into 60 60 pixel squares. Thus, users have 7 11 squares to select in each image (see Figure 3(c)). After a user selects three to five images with one pass-square per image, the password will be stored as a list of coordinates in a database table (i.e., the locations of those selected pass-squares in the 7 11 grid). The password space depends on the number of images set by users. For instance, if a user creates an account with four images, the password space is (7 11)4.

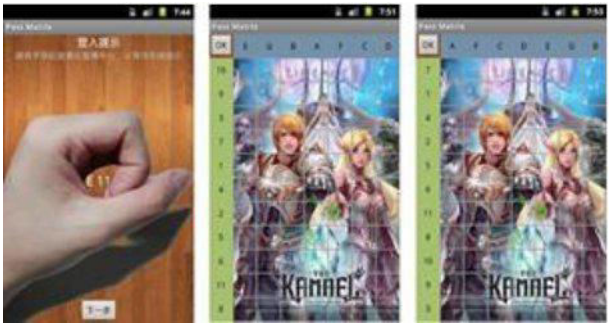

Fig. 3(a) A visual way for users to obtain a one-time valid login indicator. (b) The permutations of alpha-numeric in horizontal and vertical bars are randomly generated for each image. (c) Users can shift the bars to the correct position sothat the login indicator aligns with the pass-square.

In our implementation, we adopted the simplestway: grasping the hand with a little space left in the center and then touching the screen of smart phones (see Figure 3(a)). 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.

In our implementation, we adopted the simplest way: grasping the hand with a little space left in the center and then touching the screen of smart phones (see Figure 3(a)). 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.

The number of elements on both the horizontal and vertical bars depends on the discretization degree of the images. In our implementation, there are 7 letters (from A to G) and 11 numbers (from 1 to 11) on the horizontal bar and on the vertical bar, respectively. They are used to align the one-time indicator with the pass-square in each pass-image during the authentication phase. In order to obfuscate and thus hide the alignment patterns from observers, we randomly shuffled the elements on both bars in each pass-image and let users shift them to the right position (see Figure 3(b) and (c)). We implemented two bar-shifting functions: dragging and flinging. Since the entire bar is shiftable and can be circulated on either side (i.e., bi-directional and circulative), users do not need to place their finger on a specific element in order to move it.

4.Future Enchancement:

The shoulder surfing has done with the enhancement of,Proposed model provide the user friendly and the interactive environment for the user. The efficient and the innovative banking service provided for the authentication system.The forget password module is designed with an innovative idea. Based on idea of framing forget password questions on the users handheld device.Blocking the user account if wrong password injected to the server frequently and intimate the user through Email and user's alternative mobile number via SMS about current location of the mobile.

5.Results:

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed sys-tem. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the suc-cessful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase. The results of these two analyses strongly suggested that PassMatrix is practical to use. At the end of this section, we also presented the statistics of the survey data from participants about their personal background and user experience on smart phones and Pass Matrix.

6. Conclusion:

In this paper I proposed a novel user authentication scheme named fake pointer. This is a unique user authentication scheme that makes peeping attack with the video camera hard. Peeping at a in the real world is on of the threat to a present user authentication and uses has been exposed to a risk of this attack

7.References:

[1] DOI10.1109/TDSC.2016.2539942,IEEE Transactions on depandable and secure 2016.

[2] S.Gurav,L.Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] Christo Ananth, D.L.Roshni Bai , K.Renuka, C.Savithra, A.Vidhya, "Interactive Automatic Hepatic Tumor CT Image Segmentation", International Journal of Emerging Research in Management &Technology (IJERMT), Volume-3, Issue-1, January 2014,pp 16-20

[4] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nichol-son, and P. Olivier, "Multi-touch authentication on tabletops," inProceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.].

[5] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "Pas: predicate-based authentication services against powerful passive adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical pass-word authentication using cued click points," Computer Security– ESORICS 2007, pp. 359–374, 2007.

[7] L. Cranor and S. Garfinkel, Security and Usability. O'Reilly Media, Inc., 2005.

[8] De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "Vip: a visual approach to user authentication," inProceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.