# An authentication scheme for a better security Against a peeping attack by a video camera

**R. Seetha Lakshmi*, Lakshmi A, Anusha R, Sangeethavani R**
Department of Computer Science and Engineering, Vel Tech High Tech DrRangarajanDrSakunthala Engineering College, Avadi, Tamilnadu
***Corresponding author: E-Mail: drseethalakshmi@velhightech.com**

**ABSTRACT**

Shoulder peeping attack is one of threats to a user for authentication. The attack method such as video capturing against peeping attack insufficient. In this paper, I propose a alternate 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.

**KEY WORDS:** Security, authentication, attack, privacy.

## 1. INTRODUCTION

Textual passwords have been used long days which Comprises of numbers and upper- and lower-case letters, however, a strong textual password is hard to memorize and recollect. Mostly, user prefer to use short alphanumeric strings as their passwords. Even worse, it is not a rare case that users may use only one username and password for multiple accounts (Gurav, 2014). According to an article in Computer world, a security team at a company hacked network password cracker and surprisingly hacked approximately 80% of the employees' passwords within 30 seconds (Know, 2014). Textual passwords are often insecure due to the difficulty of maintaining strong ones. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. 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 way of authenticating our passwords that cannot be viewed through camera or peeped by anyone. TO avoid been seen by others we provide a login indicator. This login indicator provides an authentication that the password can be viewed by the user only.

**Related Work:** In several decades, a research on password authentication has been done in the literature... 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. of handheld devices graphical capability was weak; the color and pixel it could show was limited. Using the Pass Point scheme, the user clicks on a set of pre-defined pixels .In addition to graphical authentication schemes, there was some research on the extension of conventional personal PIN entry authentication systems. In 2004, Roth et al introduced PIN entry against shoulder surfing attacks by increasing the noise to observers. The PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN number the user intended to enter by intersecting the user's choices...In order to defend the shoulder surfing attacks with video capturing, Fake Pointer 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 a disposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. 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 authentication process.


**Figure.1. Fake pointer**

The problem of how to perform authentication in public so that shoulder surfing attacks can be

- 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.

**Attack 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.
**Assumptions:** 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 authentication 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.
**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 instance, user account login on web browser, and application login/unlick OS. The Pass Matrix 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 inourexperiment.

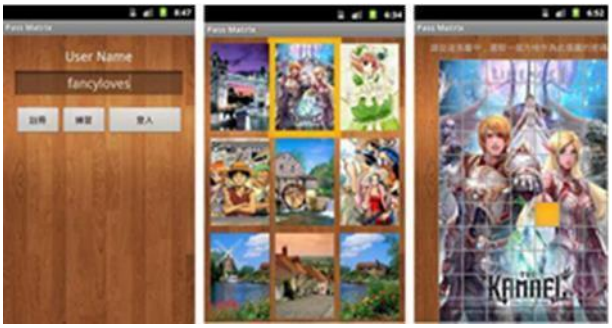


**Figure.2. Main page of pass matrix**

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

Each image is 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. 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.

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. 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. 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. 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. We implemented two bar-shifting functions: dragging and flinging. Since the entire bar is shift able 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.
**Future Enhancement:** 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.

## 2. RESULTS

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed sys-tem. The usability perspective is measured by the amount of time users spent in each Pass Matrix phase. The results of these two analyses strongly suggested that Pass Matrix 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.

Successful attempts

Total Accuracy = Total attempts

## 3. CONCLUSION

In this paper I proposed a user authentication scheme known as fake pointer. Peeping at a in the real world is one of the threat to a present user authentication and uses has been exposed to a risk of this attack.

## REFERENNCES

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

Chiasson S, Van Oorschot P and Biddle R, Graphical pass-word authentication using cued click points, Computer Security– ESORICS, 2007, 359–374.

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

De Angeli A, Coutts M, Coventry L, Johnson G, Cameron D and Fischer M, Vip: a visual approach to user authentication, in Proceedings of the Working Conference on Advanced Visual Interfaces, ACM, 2002, 316–323.

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

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

Kwon T, Shin S and Na S, Covert attentional shoulder surfing: Human adversaries are more powerful than expected, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44 (6), 2014, 716–727.