13 - 14 Dec 2010, Putrajaya, Malaysia

Anywhere On-Keyboard Password Technique

Dalia Abdul Hadi Abdul Ameer, Ahmed Abdulhakim AL-Absi, Abu Obaydah Mohammed, Adib M. Monzer Habbal,

, Suhaidi Hassan SMIEEE

InterNetWorks Research Group, UUM College of Arts and Sciences,

University Utara Malaysia, 06010 UUM, Sintok, MALAYSIA

{ s800053,s806145, s801763}@ student.uum.edu.my, adib@uum.edu.my, suhaidi@uum.edu.my

***Abstract* - Traditional authentication technique generally requires an id and password to verify the identity of user. By nature, user is looking for a password that is easy to remember and secured from any attack. However, remembering many complicated passwords, especially when user has different accounts, is not an easy task. Moreover, Traditional technique is still vulnerable to attack such as hidden camera. To overcome these drawbacks, we propose a new password authentication technique called "Anywhere On-Keyboard Password (AOKP)". The experiment results show that 40% of the spies succeed to catch the password shape but all of them fail to detect the number of the strokes. Therefore, the proposed technique provides more secure and memorable authentication method through changing password from text to mix shape and number of strokes. In addition, it has high level of scalability and simplicity though the freedom of writing the password anywhere on keyboard, password length and language independent.**

Keywords - Security, Authentication , Anywhere On-Keyboard Password (AOKP).

I. INTRODUCTION

Nowadays, Computer security and authentication have become an issue for computer users to protect their important data from the impostors and intruders. Moreover, most of the access applications are depending on the general password authentication as security although this general approach has a lot of problems such as forgetting the password especially over the Web, where there are a lot of sites that provide the general password authentication for its all services and there are millions of people from everywhere who are accessing these sites, in this case people are facing difficulties on keep remembering all their passwords [1]. Since users frequently use a password to access their computers, emails, bank account, etc. these passwords must be known only to its real user to be effective. By nature, user is looking for a password that is easy to remember and secured from any attack. However, remembering many complicated passwords, especially when the user has many different accounts, is not an easy task. Moreover, Traditional technique is still vulnerable to attack such as hidden camera and shoulder-surfing. To overcome these drawbacks, we propose a novel alternative password authentication technique called "Anywhere On-Keyboard Password".

In this technique, the password is about any connected shape drawn using keyboard's keys mixed with the number of strokes on each key accordingly. To recall this password, it is required to map the same password anywhere on the keyboard using the same number of strokes on each key. This technique is proposed to improve the security of user authentication through changing password from text to mix shape and number of strokes. In addition, Anywhere On-Keyboard Password has high level of scalability and simplicity though the freedom of writing the password at any location on keyboard, password's length and its ASCII independent.

To prove this technique's features usability evaluation have been done through a laboratory experiment design. In addition, a system has been developed to help users to enter their password and apply the technique concept through the keyboard device.

The paper is organized as follows: section II is about the related work which summarizes previous researches on the authentication techniques. Moreover section III provides more information about the technique concept. Section IV describes the system design implementation. Then the laboratory experiment and the result analysis are depicted in section V and the last one, section VI presents the conclusions and future work.

II. RELATED WORKS

Several of password authentications techniques have been proposed, each has its own features. Recently, Zheng et al. [2] proposed a hybrid password authentication scheme that is based on shape and text. This technique involves from users to shape and stroke their password on a grid with text using a traditional input device. However, the technique requires users to be familiar with the use of this scheme. Furthermore, the users is required to enter the same shape and strokes at the signup which is vulnerable to any attack, another drawback is

it has a long login process where users have to enter their original shape password carefully [2].

Another password authentication technique is Passfaces [3], the authentication process is done via identifying previously chosen person face as password from a larger set of pictures whereas users must recognized one of their pre-selected pictures from several pictures.

An alternative authentication mechanism is Locimetric systems which require the users to recognize and select a sequence of regions on an image via any pointing device. The same sequence of regions has to be selected later [4].

PassShapes approach [5], this technique is depends on geometric shapes with stokes rather than PINs numbers. The user has to repeat his PassShape either using a touch pad or any pointing device. The strokes of a PassShape should be drawn in same order, in addition user need not to redraw a PassShape exactly the same size or position, because only the strokes and their order are evaluated.

Jermyn, et al. [6] proposed a technique that is based on user to draw a password on a two dimension grid called "Draw a Secret (DAS)".in this technique user must touch the same grid on the same sequence to get authenticated.

III. ANYWHERE ON-KEYBOARD PASSWORD CONCEPT

Anywhere On-Keyboard Password is a proposed technique for computer applications authentication; it is based on the password's shape and key strokes number regardless to the sequence of the inputted keyboard keys and their locations. The basic idea of this technique is to map a password on keyboard as a connected shape, users have a freedom to press and specify the number of strokes for a particular key or even all keys for purpose of increasing the security of the password. This shape map will support user's memory by just remembering the shape and the number of strokes at each key to made it more secure, after that users can shape it anywhere on the keyboard.

So, by comparing the Anywhere On-Keyboard Password technique to other existing techniques, Anywhere On-Keyboard Password technique which presented in the next section is conceptually similar to the Hybrid Password Authentication Scheme which is based on shape and text. However we consider our technique to overcome some limitations of Hybrid Password Authentication Scheme. First, no grid is needed to use anywhere on-keyboard password technique. So the users do not have to recall a specific starting point and do not have to take care of touching the grid while drawing. It's worth mentioning that the technique is done by entering the password wherein keyboard irrespective to the keys locations and has a short login process. The technique help to resolve two of the issues related to password authentication: the insufficient secured authentication and the possibility of forgetting the passwords due to using multi-passwords.

The process of the technique requires two stages: password creation or sign up stage and password verification or login stacge. Fig. 1. Shows process of a user entering his password by shaping the password on keyboard.

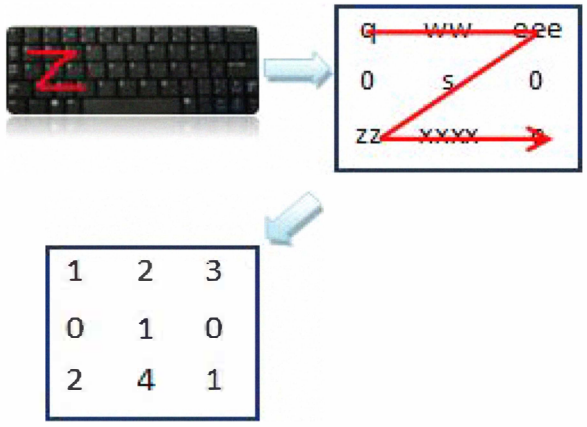

Fig. 1. Shaping a password on keyboard.

In fact the user enters his password as keys from the keyboard while the system considers the password as numbers depending on the number of strokes. From Fig. 1. We can see how the system omitted the sequence of the entered password. This technique gives the password a power because when the user press more strokes on pressed keys the password becomes longer and this is better to save it from any attack. This led us to formulate the following equation (1) to count the length of the entered password:

$$pwlength = \sum_{i=0}^{m} \sum_{j=0}^{n} k\,(i,j)\ , where \qquad (1)$$

$pwlength$: is the length of the entered password

k: is the array of entered keys from keyboard and the number of strokes

i, j: represent the indices of array k

n : the number of rows of k

m : the number of columns of k

So, from equation (1) and the demonstrated example in Fig. 1. the $pwlength = 14$, which means the password length is too much for user to memorize it but through our technique this process become easy and more secured from any attack as well.

For the second stage, login stage the user maps his password at any location on the keyboard and the system will verify it, as clarified on Fig. 2 the user enter the same shape and number of strokes that he saved it on signup stage, but this time at another location of the keyboard.

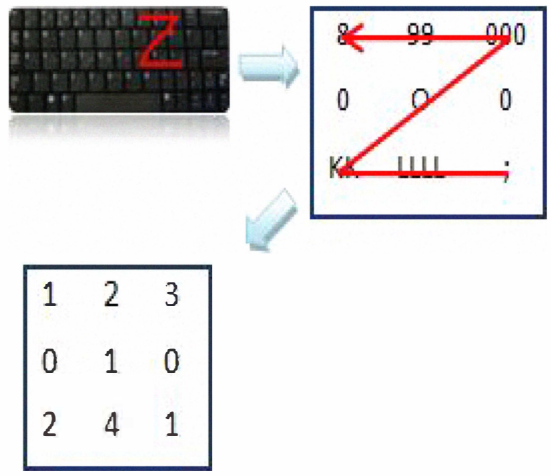

Fig. 2. Entering the same shape and strokes number but at another location.

The worth of this technique is on mentioning that the system has ability to accept any password regardless to language, ASCII and the location at the keyboard.

IV. SYSTEM IMPLEMENTATION

A system was implemented for our technique using Java programming language. From the name of the technique it is obvious that user has the ability to enter his password anywhere on the keyboard via keyboard without any concern to the keyboard keys locations and input sequence. For purpose of implementing the concept of the technique, the system consisted of three forms, the signup form, login form, and the welcome form. The first form is for the user to register the password whereas user could confirm the password at another location of the keyboard to check the idea of the independency of the keyboard keys location. While in the login form, user has also the freedom to login by entering the password at a new location on the keyboard other than the signup keyboard keys location. User requires to signup first with their username and password, in this case user should enter password based on shape that is easier for him to recall via keyboard. For example at the first login, user could shape his password on the upper right side of the keyboard while at the next login he could shape the password on the down left side of the keyboard to prove the concept of our technique.

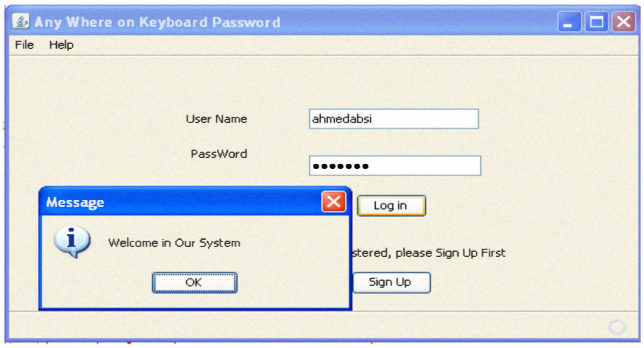

Fig. 3. Anywhere On-Keyboard Password main interface

Fig. 4. Represent the stages of password at sign up stage and the password verification login stage.

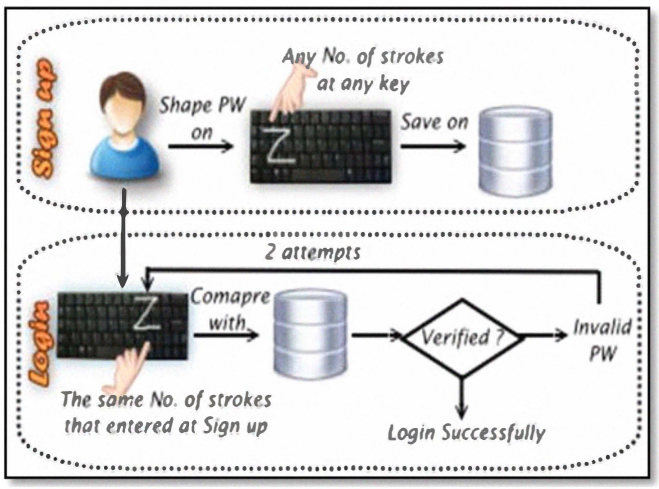

Fig. 4. The two stages of the password process.

V. EVALUATION

A. *laboratory experiment*

In the evaluation of Anywhere On-Keyboard password technique, we have chosen a laboratory experiment design as a usability evaluation of this technique. We have focused on two features: the easiness of understanding the concept of the technique from the participants, the other one knows the ability of the spies on observing and identifying the victims' password. We installed our prototype software on ten systems and we asked the participants to use the prototype for purpose of creating their password.

The participants were of total twenty (13 males and 7 females from computer science and non-computer science

undergraduate and postgraduate students of University Utara Malaysia; half of the participants played role of a spies by trying to know and guess passwords of the other participants who were in role of the victims.

Age of the participants ranged from 20 to 34 years old, with an average age of 25.05. Typing proficiency of the participants was normal however there were users who are two-finger typists.

For purpose of knowing the potential of the spies' participants to reveal the victims' participants password before and after the experiment, we have decided to undergo the evaluation process into two main stages: the first stage was by teaching only the victims participants about the concept of the technique and how it works and ignoring the spies' participants. The second stage was by teaching the spies participants about the concept of the technique.

So in the first stage, only victims' participants have been trained to the concept of the Anywhere On-Keyboard password technique by shaping their password on the keyboard regardless of the keyboard keys location. The spies' participants have no idea about the feature of the technique that it does not depend on the locations of the keyboard keys, the spies have got the freedom to move from one side to the other side trying to get the victim's password. The spies provided a notebook and pen for purpose of allowing them writing down notes at time of observing the victims entering their passwords.

In the second stage, Since our technique is dependent not on the keyboard keys location, the victims' participants have been instructed to login using different keyboard's keys location than what they have used on the first stage.

After the participants finished from the task that been given to them, we gave the participants a post-experiment questionnaire to provide more information based on their thoughts about the authentication vulnerability, and their satisfaction in the Anywhere On-keyboard Password, furthermore, participants been asked to rate our new authentication technique.

The results of this laboratory experiment have been analyzed and presented in the next section.

B. Results

The main focused point of the experiment evaluation was to know how many spies will be able to reveal the victims password that were following our technique in entering their password. And as we said earlier in the experiment evaluation, the spies have no idea about the concept of our technique in the first stage; the result of this stage was that among the ten spies, no one (%0) from the spies' participants could reveal the password of the victims' participants, which was expected. On the second stage since we taught the spies the concept of anywhere on keyboard password technique and how it is depending on shaping passwords and on the number of strokes as well, the result of this stage was four (40%) spies out of ten who succeeded only on knowing the shape of the password but they failed on revealing the number of the strokes. Lastly after finishing the second stage we have distributed a post-experiment questionnaire for all the twenty participants.

Questions of the post-experiment questionnaire were about the authentication vulnerability and their understanding and satisfaction to the concept of the Anywhere On-keyboard Password technique. The participants answer to the questionnaire reveals that almost 90% of the participants reported they liked the idea of the technique and they understand the concept of the technique very easily.

When asked if they would like to use this technique in their authentication, 90% of participants said they really satisfied to use it since they can run the password anywhere and remember only a shape as their password instead of memorizing a lot of passwords, Fig. 5 shows the statistics of experiment result graphically and Fig. 6 represents the participants satisfaction on the technique.

From this study we could indicate that Anywhere On-Keyboard password is definitely a secured authentication technique against shoulder-surfing and hidden cameras and easy to be used.

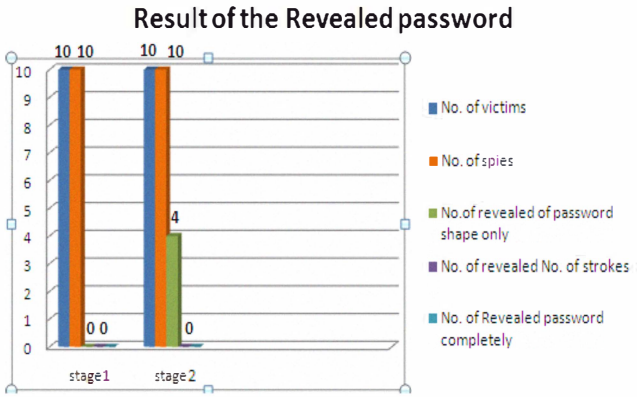

Fig. 5. Result of the number of the revealed the password.

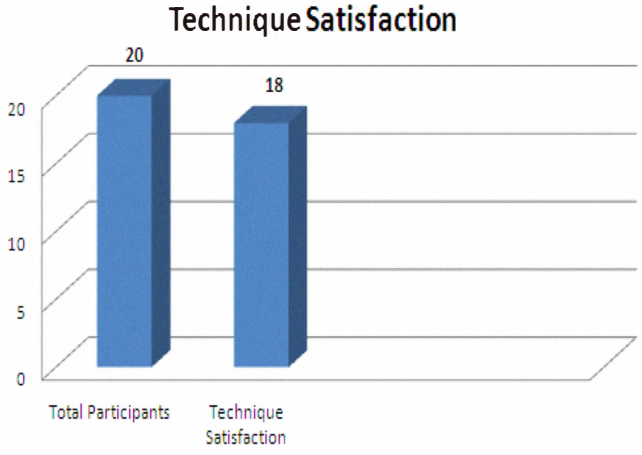

Fig. 6. The result of the participants satisfaction on the AOKP technique.

VI. CONCLUSION AND FUTURE WORK

As the related works shown in this paper, there are many authentication techniques for particular aspects of password authentication is available, user is looking for a flexible technique that could potentially encompass features of easy to use, recall and more secure at same time.

The main contribution of this paper is on proposing a new authentication technique called Anywhere On-Keyboard Password. In addition, we built a prototype that can help users to enter their password and apply the AOKP technique concept, aiming at providing more security wherein entering passwords anywhere in the keyboard irrespective to the keys location. The evaluation showed that the technique is resistant to shoulder-surfing and hidden cameras; furthermore, the technique provides more security and memorable authentication method because the number of strokes increases the workload for attackers and helps user maintain many accounts with shaping passwords. Another aspect of this technique is its more memorable and usable by helping a user maintain many accounts with different passwords.

For future work, In spite of the satisfactory results, we have gotten in the laboratory experiment. Our future work includes testing of this schema in scenarios with a hidden camera. Moreover, we will also check the viability of using Neural Network technique for proper shape detection.

ACKNOWLEDGMENT

We would like to thank Mr. Ahmed Talib for his helpful discussions.

We would like to thank also to the participants of University Utara Malaysia students who contributed to our research.

REFERENCES

[1] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," *ACM Transactions on Information and System Security*, vol. 5, No. 4, Pages 367–397, November 2002.

[2] Z. Zheng, X. Liu, L. Yin, And Z. Liu, "A hybrid password authentication scheme based on shape and text, "in *Journal of computers* , vol. 5, NO. 5, MAY 2010.

[3] F. Tari, A. Ozok, and S. Holden," A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical Passwords, " in *Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, USA July, 2006.

[4] G. E. Blonder, "Graphical passwords," in United States Patent, vol. 5559961, 1996.

[5] R. Weiss, and A. Luca, " PassShapes - utilizing stroke based authentication to increase password memorability, "in Proceedings *NordiCHI* , Lund, Sweden October,2008.

[6] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proceedings *of the 8th USENIX Security Symposium,* 1999.