Identifying the Reusability of the Triangle and Intersection Schemes on Mobile Devices

Lim Kah Seng (Corresponding author)
Department of Computer System and Communication
Faculty of Computer Science & Information System
Universiti Teknologi Malaysia, Malaysia

Norafida Ithnin
Department of Computer System and Communication
Faculty of Computer Science & Information System
Universiti Teknologi Malaysia, Malaysia

Hazinah Kutty Mammi
Department of Computer System and Communication
Faculty of Computer Science & Information System
Universiti Teknologi Malaysia, Malaysia

Received: March 21, 2011 Accepted: April 21, 2011 doi:10.5539/cis.v4n4p109

Abstract

Graphical passwords are vulnerable to shoulder-surfing attacks as the images are easier to remember than text. Therefore, existing graphical password schemes incorporate anti-shoulder-surfing mechanisms to ensure that the graphical password is safe against such attacks. Unfortunately, according to the literature review, most graphical password schemes with anti-shoulder-surfing mechanisms are for general devices, not mobile devices. Therefore, in this experiment, two general device graphical password anti-shoulder-surfing mechanisms, which are the Triangle and Intersection schemes, are reconstructed on a mobile device to test if general device graphical password anti-shoulder-surfing mechanisms can be reused in mobile devices.

Keywords: Graphical password, Mobile device, General device, Shoulder-surfing

1. Introduction

Nowadays, the most widely used knowledge-based authentication method is done via textual passwords. Unfortunately, textual passwords are insecure and prone to most computer attacks. Moreover, textual passwords are difficult to recall (Thorpe, 2004; Bandyopadhyay, 2008). Hence, a graphical password, another form of knowledge-based authentication method is introduced as an alternative to textual passwords.

A graphical password is an authentication method whereby users create their passwords by selecting or producing pictures (Thorpe, 2004; Ejetlawi, 2008a; Ejectlawi, 2008b). A graphical password is proposed based on the principle that pictures are easier to remember than words. However, due to this reason, graphical passwords are vulnerable against shoulder-surfing attacks. To overcome this issue, an anti-shoulder-surfing mechanism has to be integrated into the said graphical passwords. A shoulder-surfing attack is a type of attack during which the shoulder-surfer steals his victim's passwords by peeping over the victim's shoulder (Shi, 2009).

In this day and age, graphical passwords are not only categorized as recognition-based and recall-based. They also can be classified as graphical password with and without anti-shoulder-surfing mechanisms, and those that are for both general and mobile devices as what is shown in Figure 1.

The difference between recall-based and recognition-based graphical passwords is that recall-based graphical password requires the users to recall and reproduce their previously registered picture password, while the recognition-based graphical password requires that the users recognize and choose their previously registered

pictures (Ejetlawi 2008; Ahmet, 2007). Apart from this, a general device graphical password refers to graphical password that operates in devices such as servers, workstations, desktop computers, or laptops. On the other hand, mobile device graphical passwords are graphical passwords that work specifically on mobile-based frameworks, such as that of cell phones, smart phones, feature phones and even personal digital assistants (PDAs).

2. Existing Graphical Password Schemes

In this paper, the reviewed graphical password schemes included are the S3PAS (Huanyu, 2007), Triangle Scheme (Sabrado, 2002), Intersection Scheme (Sabrado, 2002), Moveable Frame (Sabrado, 2002), YAGP (HaiChang, 2008), ColorLogin (HaiChang, 2009), RGGPW (Lin Phen-Lan, 2008), CTZ (Kumar V., 2009), Use Your Illusion (Eiji Hayashi, 2008), Association-based Graphical Password Scheme (Zhi Li, 2005), Blonder's Graphical Password Scheme (G. Blonder, 1996), PassPoint (S. Weidenbeck, 2005), Pass-Go (H. Tao, 2008), Passfaces (realuser.com), V-Go (Passlogix, 2007), Random Art (R. Dhamija, 2000), 3D (Alsulaiman F.A., 2006), Hasegawa et al. Algorithm (Hasegawa, 2009), An Interaction and Secure User Authentication Scheme (Qibin Sun, 2008), User Authentication for Mobile Device through Image Selection Scheme (Sarwar M.I, 2008), SFR Password (http://www.sfr-software.de/cms/EN/pocketpc/sfr-password/index.html, 2009), Jansen et al. Algorithm (W. Jansen, 2004), Recall-A-Story (Yves Maetx, 2009), Awase-E (Tetsuji Takada, 2008), Stroke-based Graphical Password Scheme (ZiranZheng, 2009), and DAS (Jermyn I., 1999).

Among these graphical password schemes, a few of them are for general devices while some of them are for mobile devices. Additionally, some of these reviewed graphical password schemes have anti-shoulder-surfing mechanisms while some do not. In Table 1, examples of general device graphical password schemes that utilize anti-shoulder-surfing mechanisms are shown.

Table 1 has shown that there are eleven of the reviewed graphical password schemes which are for general devices, and that which anti-shoulder-surfing mechanisms. Unfortunately, the same cannot be said of mobile device graphical password schemes. In Table 2, mobile device graphical password schemes having anti-shoulder-surfing mechanisms are shown.

Table 2 has shown that only two out those reviewed graphical password schemes are mobile device graphical password schemes that incorporate anti-shoulder-surfing mechanisms.

3. Usability

Usability refers to the ease of using a particular computer application for achieving a particular goal (Eljetlawi, 2008). According to (Samaneh Farmand, 2010), a usable computer application should have a user friendly graphical user interface, is portable, fun to use, and does not need any on-going or continuous training. In Table 3, the usability of some existing graphical password schemes is shown.

Table 3 describes that, usable graphical password schemes comprise of general device graphical password schemes, and not that of mobile device graphical password schemes.

4. Motivation and Selected General Device Graphical Password Schemes having Anti-Shoulder-surfing Mechanisms

Based on the previous study, most usable existing graphical password schemes having some kind of anti-shoulder-surfing mechanism are general device schemes. Although there are mobile device graphical password schemes which are usable and have anti-shoulder-surfing mechanisms, such as An Interactive and Secure User Authentication Scheme for Mobile Device, these are comparatively fewer than that of general devices. Therefore, in this paper, we have decided to conduct an experiment to indicate whether the existing general device graphical password anti-shoulder-surfing mechanisms can be reused in mobile devices.

In this experiment, two general device graphical password anti-shoulder-surfing mechanisms are chosen for this experiment. These two general device graphical password anti-shoulder surfing mechanisms are the Triangle and Intersection schemes.

Originally, Sabrado and Birget (Sabrado, 2002) had proposed three anti-shoulder-surfing mechanisms for the prevention against shoulder-surfing attacks. They are the Triangle Scheme, Moveable Frame, and Intersection Scheme. However, in this experiment, we only chose the Triangle (convex-hull shoulder-surfing resistant) and Intersection scheme (special geometric configuration) because these two schemes have been widely discussed by many authors. In the Triangle Scheme, users need to first register their graphical password by selecting a number of pictures. During the authentication phase, he or she has to form the pass-triangle by using three previously registered pictures. An example of a pass-triangle of the Triangle Scheme is shown in Figure 2 below.

After the users have formed the pass-triangle, they will be required to click on any picture that is located inside the pass-triangle. For the Intersection Scheme, the registration is similar to that of the Triangle scheme. The only difference is that for the Intersection Scheme, the users have to form a cross-path (Figure 3) using four previously registered pictures instead of a pass-triangle.

After the users have formed a cross-path using the four previously registered pictures, users are require to select a picture, which is located near or at the top of the intersection point.

5. Experiment Methodology

To test whether the general device graphical password anti-shoulder-surfing mechanism is suitable for reuse in mobile devices, the Triangle and Intersection schemes are tested using the four elements shown below.

a. Security of the Triangle and Intersection schemes against shoulder-surfing attacks on mobile devices.
b. Usability of the Triangle and Intersection schemes on mobile devices.
c. Drawback of the Triangle and Intersection schemes on mobile devices.
d. Adaptability of the Triangle and Intersection schemes on mobile devices.

Based on the experiment result on different aspects (Table 4) of these four elements, it will determine whether or not general device graphical password anti-shoulder-surfing mechanisms can be reused in mobile devices. We have successfully persuaded 14 respondents to participate in this experiment. All respondents are student at Universiti Teknologi Malaysia. As shown in Table 4, the respondents are divided into two groups. They are:

Group One: Consists of eight respondents. Their responsibility is to identify the usability of the Triangle and Intersection scheme, its drawbacks, as well as its adaptability for use in mobile devices.

Group Two: Consists of six respondents. Their responsibility is to determine whether the Triangle and Intersection schemes are secure against shoulder-surfing attacks.

6. Experiment Result

In this section, the usability, security against the shoulder-surfing attacks, drawback, as well as adaptability of the mobile device Triangle and Intersection schemes are analyzed and discussed.

6.1 Analysis of the Triangle Scheme and Intersection Scheme's security and usability in mobile devices

To verify the usability of the mobile device Intersection and Triangle schemes, the ease of logging in and registration of the schemes are evaluated. In Figure 4, the usability of these two schemes is shown.

Figure 4 above has shown that the mobile device Triangle Scheme is easy to log into and register. However, the result has also shown that the mobile device Intersection Scheme is easier to register but logging in is more difficult. Hence, in terms of usability, the mobile device Triangle Scheme is more usable than the mobile device Intersection scheme. Given that the percentage of positive responses as described in the chart above is not too low, we can safely deduce that the mobile device Intersection Scheme is still considered somewhat usable in this experiment. Overall, the Triangle and Intersection schemes are still usable in mobile devices.

In order to test the mobile device Triangle Scheme and mobile device Intersection Scheme, security against the shoulder-surfing attacks, the simulated attacks are conducted by the respondents. In Table 5, the number of successful attempts made by the respondents is illustrated.

The result in Table 5 shows that half of the shoulder surfers were able to attack the mobile device Triangle and Intersection schemes successfully via shoulder-surfing attacks in their first attempt. The result also shows that 100% of the shoulder surfers were able to penetrate the schemes' defenses against shoulder-surfing attacks within five attempts. From this we can deduce that both the Triangle and Intersection schemes have lost their ability to prevent shoulder-surfing attacks when they are reused in mobile devices. In our further study, we discovered that the main reason for the Triangle Scheme and Intersection Scheme being vulnerable to shoulder-surfing attacks is that the number of pictures in the schemes is insufficient. In Figure 5, the reason why the Triangle Scheme and Intersection Scheme are vulnerable for the shoulder-surfing attack is shown.

According to the shoulder surfers in this experiment, the main reason why they were able to steal the passwords with little effort is because there were too few images used in the schemes. They could easily log-in successfully simply by guessing or randomly clicking the images, on top of performing a shoulder-surfing attack on the

schemes. Additionally, the result has shown that the size of the pictures is not an influencing factor for both the mobile device Triangle and Intersection schemes.

6.2 Drawbacks of the mobile device Triangle Scheme Intersection Schemes

After identifying the usability and security of the mobile device Triangle and Intersection schemes against shoulder-surfing attacks, the next step is to identify their drawbacks. In Figure 6, the schemes' drawbacks are illustrated.

The result of Figure 6 has shown that the drawbacks for both schemes are similar, which are small picture size, slow login rate, and the low number of pictures. This is due to the display screen size being fairly small. What we did not come to expect were the respondents' complaints about the log-in rate. Because of the limited screen-size of the mobile device, the respondents were expected to better remember all the pictures displayed on the screen. But, in the real experiment, it showed that most of the respondents took too long to log into the system. One hypothesis that can be drawn here is that the processor speed for mobile devices is lower than that of general devices. Therefore, the users waited longer for the schemes to respond to their input. However, this is just an assumption at this point. The exact answer for this question is still subject to research.

6.3 Adaptability of the Triangle Scheme and Intersection Scheme in mobile device

The last element that is tested here is the adaptability of the Triangle Scheme and Intersection Scheme for mobile devices. In Figure 7, the adaptability of these schemes for mobile devices is shown.

The bar graph in Figure 7 shows that the Triangle Scheme and Intersection Scheme are adapting well in the mobile device, especially the Intersection Scheme. This is because of the Intersection Scheme being more secure against shoulder-surfing attacks than the Triangle Scheme, in the mobile devices. In terms of usability, these two schemes are almost as usable as the other. Hence, it is of course the Intersection scheme that is more suitable for reuse in the mobile devices than the Triangle Scheme.

7. Discussion

In our pre-experiment study, it showed that most mobile device graphical password schemes do not include any anti-shoulder-surfing mechanism, but, it does for general device graphical password schemes. Hence, an experiment is conducted for identifying whether general device graphical password anti-shoulder-surfing mechanisms can be reused in mobile devices. To test the re-usability of general device graphical password anti-shoulder-surfing mechanisms on a mobile device, two general device graphical password anti-shoulder-surfing mechanism, the Triangle Scheme's as well as the Intersection Scheme's usability, security against shoulder-surfing attacks, drawbacks, and adaptability for mobile devices, are tested. Through this experiment, the results have shown that the mobile device Triangle Scheme and Intersection Scheme have lost their functionality in preventing some shoulder-surfing attacks, although they remain somewhat usable. Moreover, these two schemes do also have some drawbacks like small picture size and slow login rate. Although the schemes are found to work fairly well on mobile devices, the Triangle Scheme and Intersection Scheme are not suitable for reuse in mobile devices.

According to what Sabrado and Birget did in their experiment (Sabrado, 2002), the security of the Triangle Scheme and Intersection Scheme is proportional to the number of pictures that are displayed on the screen. They even suggested having at least 1000 pictures at the same time for increasing the schemes' security. Unfortunately, this is almost impossible on mobile devices as the screens are usually quite small. This reaffirms that there are some differences in characteristic between general and mobile devices. Because of these differences, general device graphical password anti-shoulder-surfing mechanisms perform best on general devices only.

8. Conclusion and Future Work

This paper is focuses on exploring the possibility of reusing general device graphical password anti-shoulder-surfing mechanisms in mobile devices. Through this experiment, the results have shown that it is not a good idea to reuse general device graphical passwords anti-shoulder-surfing mechanisms in mobile device. This has motivated us to develop a secure and usable graphical password anti-shoulder-surfing mechanism that special for use in mobile devices only. However, before proposing this mobile device graphical password anti shoulder-surfing mechanism, we are more interested to know the features that are best suited to mobile device graphical password anti-shoulder-surfing mechanisms. Thus, in the next activity, we plan to conduct a user affinity of choices survey to better understand and determine the features that best suit the said anti shoulder-surfing mechanism.

References

Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget. (2007). Modeling user choice in the PassPoints graphical password scheme. *SOUPS '07 Proceedings of the 3rd symposium on Usable privacy and security*, doi: 10.1145/1280680.1280684, http://dx.doi.org/10.1145/1280680.1280684.

Alsulaiman, F.A., Saddik, A.E. (2006). A Novel 3D Graphical Password Schema. *Proceedings of IEEE International Conference of Virtual Environments, Human-Computer Interfaces and Measurement Systems*, pp. 125-128, doi: 10.1109/VECIMS.2006.250805, http://dx.doi.org/10.1109/VECIMS.2006.250805.

Bandyopadhyay, S.K., Bhattacharyya, D., Das, P. (2008). User authentication by Secured Graphical Password Implementation. *Information and Telecommunication Technologies, 2008, APSITT, 7th Asia-Pacific Symposium*, pp. 7-12, doi: 10.1109/APSITT.2008.4653531, http://dx.doi.org/10.1109/APSITT.2008.4653531.

Eiji Hayashi et al. (2008). Use Your Illusion: secure authentication usable anywhere. *SOUPS '08 Proceedings of the 4th symposium on Usable privacy and security*, doi: 10.1145/1408664.1408670, http://dx.doi.org/10.1145/1408664.1408670.

Eljetlawi, A.M. Ithnin, N. (2008a). Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods. *ICCIT '08, Third International Conference of Convergence and Hybrid Information Technology*, Vol. 2, pp. 1137, doi: 10.1109/ICCIT.2008.20, http://dx.doi.org/10.1109/ICCIT.2008.20.

Eljetlawi, A.M. Ithnin, N. (2008b). Graphical Password: Prototype Usability Survey. *Advanced Computer Theory and Engineering, ICACTE, International Conference*, pp. 351, doi: 10.1109/ICACTE.2008.34, http://dx.doi.org/10.1109/ICACTE.2008.34.

Farmand, S. Bin Zakaria, O. (2010). Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4). *Information Management and Engineering (ICIME), 2nd IEEE International Conference*, pp. 644, doi: 10.1109/ICIME.2010.5478017, http://dx.doi.org/10.1109/ICIME.2010.5478017.

G. Blonder (1996), "Graphical Passwords". United States Patent 5559961.

Haichang Gao et al. (2008). YAGP: Yet Another Graphical Password Strategy. *Computer Security Applications Conference, ACSAC*, 1063-9527, pp. 121-129, doi: 10.1109/ACSAC.2008.19, http://dx.doi.org/10.1109/ACSAC.2008.19.

Haichang Gao et al. (2009). Analysis and Evaluation of the ColorLogin Graphical Password Scheme. *Image and Graphics, ICIG, Fifth International Conference*, pp. 722, doi: 10.1109/ICIG.2009.62, http://dx.doi.org/10.1109/ICIG.2009.62.

Hasegawa, M. Tanaka, Y. Kato, S. (2009). A study on an image synthesis method for graphical passwords. *International Symposium of Intelligent Signal Processing and Communication Systems, ISPACS*, pp. 643, doi: 10.1109/ISPACS.2009.5383758, http://dx.doi.org/10.1109/ISPACS.2009.5383758.

Hai Tao , Carlisle Adams. (2006). Pass-Go: A Proposal to Improve the Usability of Graphical Passwords, *International Journal of Network Security*, 7(2), 273-292.

Huanyu Zhao, Xiaolin Li. (2007). S3PAS: A Scalable Shoulder-surfing Resistant Textual Password Authentication Scheme. *AINAW '07 Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, 0-7695-2847-3, doi: 10.1109/AINAW.2007.317, http://dx.doi.org/10.1109/AINAW.2007.317.

Ian Jermyn et al. (1999). The design and analysis of graphical passwords. *SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium.*

Kumar, V. et al. (2009). Click to Zoom-Inside Graphical Authentication. *International Conference of Digital Image Processing*, pp. 238 - 242, doi: 10.1109/ICDIP.2009.65, http://dx.doi.org/10.1109/ICDIP.2009.65.

Leonardo Sobrado & Jean-Camille Birget. Graphical passwords. [Online] http:http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (November 26, 2009).

Nazir, I. Zubair, I. Islam, M.H. (2009). User authentication for mobile device through image selection. *Networked Digital Technologies, NDT '09, First International Conference*, pp. 518, doi: 10.1109/NDT.2009.5272104, http:dx.doi.org/10.1109/NDT.2009.5272104.

passfaces, Passfaces: Two Factor Authentication for the Enterprise. [Online] Available: http://www.realuser.com/ (December 24, 2009).

Peipei Shi Bo Zhu Youssef, A. (2009). A PIN Entry Scheme Resistant to Recording-Based Shoulder-Surfing. *Emerging Security Information, Systems and Technologies, SECURWARE '09, Third International Conference*, pp. 237, doi: 10.1109/SECURWARE.2009.43, http://dx.doi.org/10.1109/SECURWARE.2009.43.

Phen-Lan Lin, Li-Tung Weng, Po-Whei Huang. (2008). Graphical Passwords Using Images with Random Tracks of Geometric Shapes. *CISP '08 Proceedings of the 2008 Congress on Image and Signal Processing*, 978-0-7695-3119-9, pp. 27-31, doi: 10.1109/CISP.2008.603, http://dx.doi.org/10.1109/CISP.2008.603.

passlogix, Security -- Passlogix v-Go. [Online] http://www.passlogix.com (February 2007).

Qibin Sun et al. (2008). An interactive and secure user authentication scheme for mobile devices. *ISCAS, IEEE International Symposium of Circuits and Systems*, pp. 2973 - 2976, doi: 10.1109/ISCAS.2008.4542082, http://dx.doi.org/10.1109/ISCAS.2008.4542082.

Rachna Dhamija, Adrian Perrig. (2000). Déjà vu: A user study using images for authentication. *SSYM'00 Proceedings of the 9th conference on USENIX Security Symposium*, vol. 9.

SFR Software GMBH, SFR Password. [Online] Available: http://www.sfr-software.de/cms/EN/pocketpc/sfr-password/index.html (December 09, 2009)

S. Weidenbeck et al. (2005).Using graphical password basic results. *International conference of Human computer interaction.*

Thorpe, J. van Oorschot, P.C. (2005). Towards secure design choices for implementing graphical passwords. *Computer Security Applications Conference, 20th Annual*, 1063-9527, pp. 50, doi: 10.1109/CSAC.2004.44, http://dx.doi.org/10.1109/CSAC.2004.44.

Tetsuji Takada & Hideki Koike. (2003). Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images. L. Chittaro (Ed.). *Human-Computer Interaction with Mobile Devices and Services* (pp. 347-351). Springer-Verlag Berlin Heidelberg.

Yves Maetz, Stéphane Onno, Olivier Heen. (2009). Recall-a-story, a story-telling graphical password system. *Proceedings of the 5th Symposium on Usable Privacy and Security*, 978-1-60558-736-3, doi: 10.1145/1572532.1572566, http://dx.doi.org/10.1145/1572532.1572566.

W. Jansen. (2004). Authentication Mobile Device Users through Image Selection. *Information and Communication Technologies*, 1743-3517, Vol. 30, pp. 336, doi: 10.2495/NL040191, http://dx.doi.org/10.2495/NL040191.

Zhi Li et al. (2005). An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack. *Multimedia and Expo, ICME, IEEE International Conference*, pp.245 - 248, doi:10.1109/ICME.2005.1521406, http://dx.doi.org/10.1109/ICME.2005.1521406.

Ziran Zheng et al. (2009). A Stroke-Based Textual Password Authentication Scheme. *Education Technology and Computer Science, ETCS, First International Workshop*, pp. 90, doi: 10.1109/ETCS.2009.544, http://dx.doi.org/10.1109/ETCS.2009.544.

Notes

Note 1. The usability of the elaborated graphical password schemes are the reference from (Farmand, 2010).

Table 1. General device graphical password schemes use anti-shoulder-surfing mechanisms

No.	Graphical password schemes' name
1.	Triangle Scheme
2.	Intersection Scheme
3.	Moveable Frame
4.	S3PAS
5.	YAGP
6.	RGGPW
7.	ColorLogin
8.	Hasegawa et al. Algorithm
9.	CTZ
10.	Association-based graphical password scheme
11.	Stroke-based graphical password scheme.

Table 2. Mobile device graphical password schemes having anti-shoulder-surfing mechanisms

No.	Graphical password schemes' name
1.	User authentication for mobile device through image selection
2.	An interactive and secure user authentication for mobile device

Table 3. Usability of some existing graphical password schemes

Graphical Password Scheme	**Usability (Note 1)**	**Device Type**
Universal	The password is hard to remember	General device
A remote user authentication based on Draw-A-Secret	Good usability	General device
Random geometric graphical password (RRGPW)	Fast login rate, password easy to remember	General device
An interactive and secure user authentication scheme for mobile device	Easy to use, password easy to remember	Mobile device
Association-based graphical password	Password easy to remember	General device
Jetafida	Good usability	General device
3D	Good usability	General device
Stroke-based textual password authentication scheme	Good usability	General device
Convex-hull	Good usability	General device
Challenge response identification	Password hard to remember	General device
Cognitive trapdoor game	Password easy to remember but not usable	General device

Table 4. The details of the experiment elements

Usability		Security		Drawback		Adaptability to mobile device	
Group one	Group two	Group one	Group two	Group one	Group two	Group one	Group two
Ease of logging-in	(not deployed)	(not deployed)	Effect of Image's size for schemes' security	Drawback of Triangle Scheme and Intersection Scheme in mobile devices	(not deployed)	Adaptability of the Triangle Scheme and Intersection Scheme on mobile devices	(not deployed)
Ease of registration			Effect of Image's number for schemes' security				
			Security against shoulder-surfing attack				

Table 5. Number of Attempts taken for attacking the schemes successfully via shoulder-surfing attack

No. of attempt	Mobile device Triangle scheme	Mobile device Intersection Scheme
1	50%	50%
2	16.67%	16.67%
3	33.33%	16.67%
4	0%	0%
5	0%	16.67%

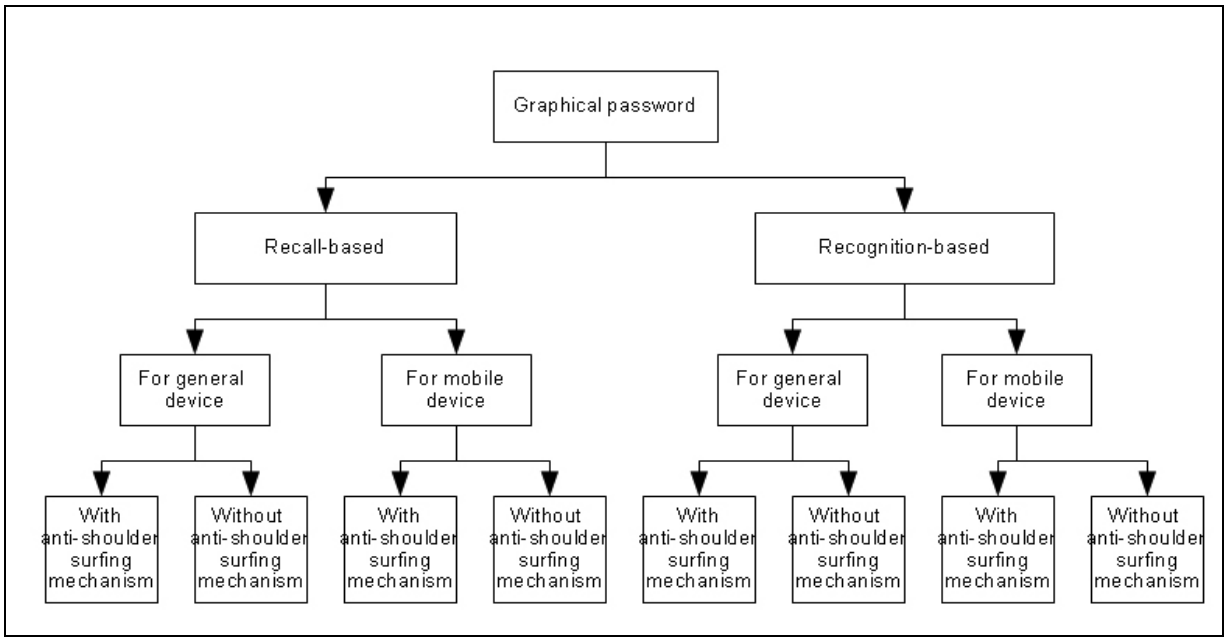

Figure 1. Different types of graphical password

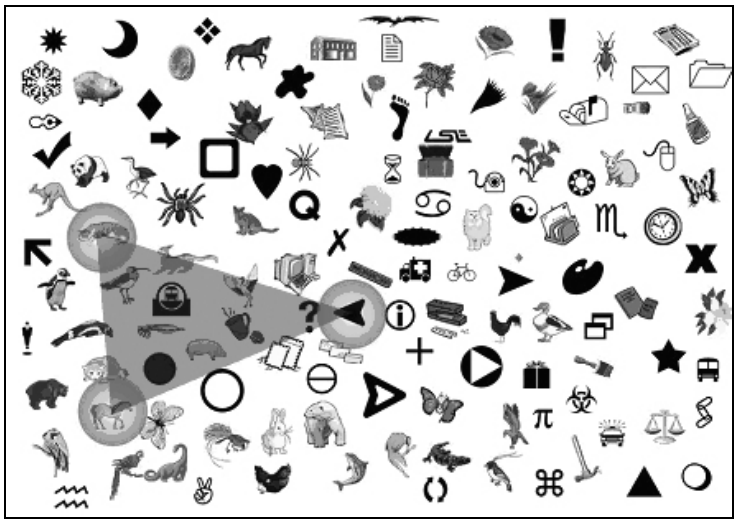

Figure 2. Pass-triangle of Triangle Scheme

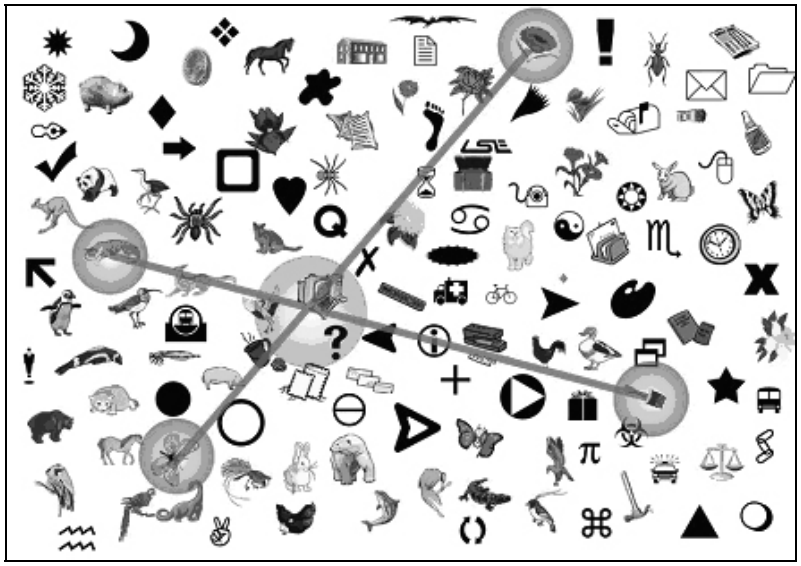

Figure 3. Cross-path of Intersection Scheme

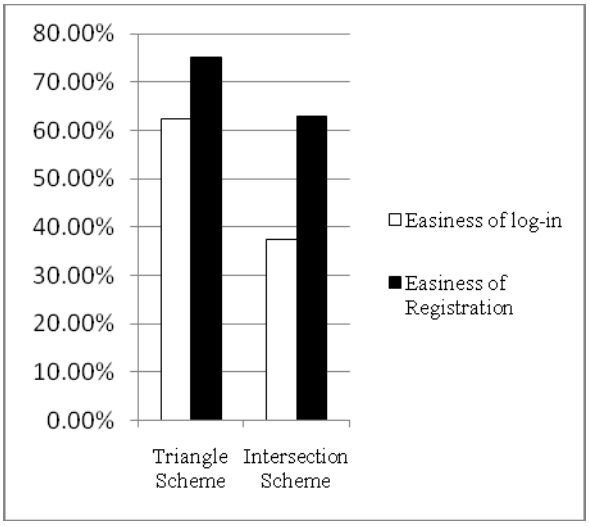

Figure 4. Usability of the Triangle Scheme and Intersection Scheme in mobile devices

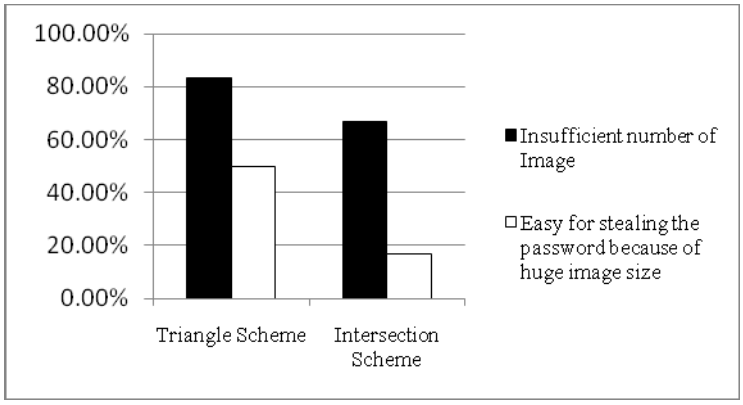

Figure 5. The reason why the mobile device Triangle Scheme Intersection Scheme is vulnerable to shoulder-surfing attack

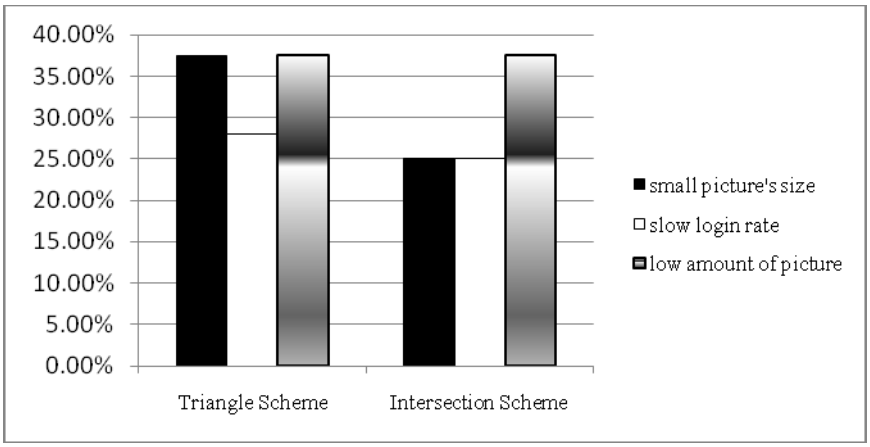

Figure 6. Drawbacks of the Triangle Scheme and Intersection Scheme in mobile device

ISSN 1913-8989 E-ISSN 1913-8997

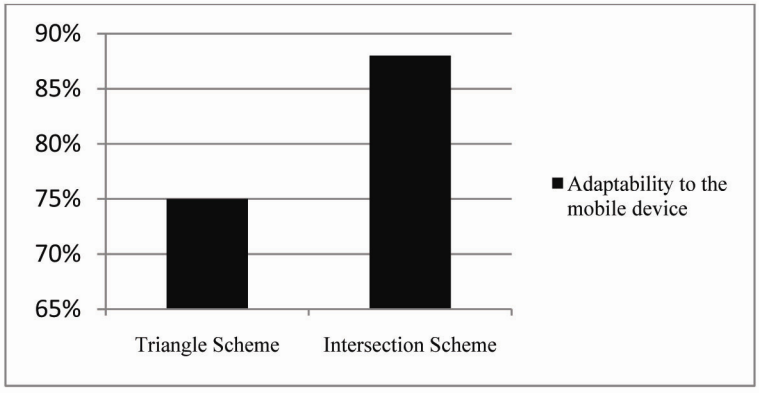

Figure 7. Adaptability of the Triangle Scheme and Intersection Scheme in mobile devices