Science World Journal Vol 13(No 1) 2018
www.scienceworldjournal.org
ISSN 1597-6343

AN IMPROVED MAP BASED GRAPHICAL ANDROID AUTHENTICATION SYSTEM

Safiyanu Ahmad (ahmadsafiyanu100@gmail.com)[1]; Souley Boukari (bsouley2001@yahoo.com)[2]; Samson Henry Dogo (dogojankasa@gmail.com)[1] and Aishat Mohammed (aishamohammed28@gmail.com)[1]

[1]Department of Mathematical Sciences, Kaduna State University, Kaduna- Nigeria
[2] Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi-Nigeria

ABSTRACT

Currently, graphical password methods are available for android and other devices, but the major problem is vulnerability issue. A map graphical-based authentication system (Dheeraj et al, 2013) was designed on mobile android devices, but it did not provide a large choice or multiple sequence to user for selecting password which made it vulnerable to brute-force attack, and there is no randomization which made it prone to shoulder-surfing attack. This proposed system seeks to improve the map graphical-based password authentication system android application devices. The system adds the password space size, rule and randomization during registration and login stage. This will improve the system and make it more secured against brute force and shoulder surfing attacks. The experimental results revealed that 910 trials instead of 730 using two countries selection, 5760 trials instead of 5050 for the existing system are available on the map using 3 countries, 352807 trials instead of 30250 for the existing system are available on the map using 4 countries and 181440 trials instead of 151210 for the existing system are available on the map using 5 countries. Thus, very larger number of trials has to be done for detection to succeed using brute force technique.

Keywords: Authentication, Graphical Passwords, Randomization, Password Space Size.

1. INTRODUCTION

There are increasing threats to networked computers and mobile device systems, and thus there is need for security innovations and improvements. Security practitioners and researchers have made strides in protecting systems and mobile device. However, the problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Users interact with secured technologies either passively or actively. For active use people need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction. Today there is an increasing recognition that security issues are also fundamentally human-computer interaction issues (Ahmad et al, 2010). When a user uses services in their mobile devices; networked systems, servers and mobile devices have the ability to authenticate the user's identity. Otherwise, anyone can easily impersonate like a legal user to login to the server or mobile device. For personal computers and phones, passwords consist of letters, numbers, and special characters on a standard keyboard. This is called text-based (alphanumeric-based) password authentication. The most common knowledge based authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. The problems of this method are how attacker can guess and the difficulty of remembering passwords (Xiaoyuan, 2006).

However, mobile devices do not have standard keyboard to conveniently enter text-based alphanumeric passwords, and therefore alternative graphical password were introduced. Graphical passwords are type of knowledge-based authentication that attempts to leverage the human memory for visual information (Iranna, 2013). Graphical password requires authentication through images or objects, and thus have the advantage of been less vulnerable to attacks. A number of algorithms for graphical authentication systems have been proposed, see for example, (Blonder, 1996), (Alia et al, 2012), (Iranna et al, 2013), (Daniel et al, 2013), (Dheeraj et al 2013), (Lashkari et al 2014), however two major problems with all these methods are that they are vulnerable to attacks and do not provide a large choice to user for selecting password (Ahmed et al, 2014). The common attacks to graphical authentication systems include shoulder surfing which is looking over someone's shoulder, possibly using binoculars or close-circuit television, in order to obtain information such as password (Wiedenbeck et al, 2005), brute force Brute force attacks, where the attacker tries all the available trials to get the the correct password, are the simplest attack form for an authentication scheme(Wei et al, 2010), dictionary A dictionary attack is a type of brute force attack where the attacker uses a dictionary of common text or graphical passwords (Masrom, 2011), guessing attack where the attacker tries possible passwords related to the user (Nali et al, 2004) and spyware attacks where Spyware collects information entered by the user (Sarious et al, 2004) & (Wang et al 2010). In this paper, we propose a new graphical-based password system for mobile devices based on graphical based algorithm. The advantages of this method is that it allows for randomization, provides a larger choice to user for selecting password and order of selection which makes it less vulnerable and hard to crack.

The rest of the paper is organized as follows. In Section 2, we review the related works. We present the new methodology in Section 3. In Section 4, we present the results and discussion. Section 5 is the summary and conclusion.

1.1. Related Work

Memorability and security of passwords are key human factor. Graphical User Authentication systems require a user to select an image that is memorable and more secured. By selecting memorable and meaningful images it helps the user to remember his/her clicked areas and the sequence of the clicks. Blonder is the first person to introduced graphical password system

As introduced by blonder (Mohammed et al, 2012), in his algorithm, user points to one or more predetermined positions on an image that is presented to the user in a predetermined order as a way of pointing out his/her password to be allowed access to a resource. However, the security is not strong because it has only one phase of verification. This is illustrated in Figure 1.

401
400
1
401
3
2
401

Figure 1: Blonder System Interface (source: Mohammed et al, 2012)

Lashkari et al (2014) proposed a new graphical user authentication scheme called Tri-Pass in 2014. The system based on the two techniques mentioned earlier, PassPoint and Triangle algorithms. To create a password user has to choose one image from the library of pictures and then select any three points by clicking on the image (password point). To login user has to merge an invisible triangle around the area of the first “password point” and click on any three points that will form a triangle. User will do the same for the second and third “password point”. The disadvantage of this approach is the user has only one stage of authentication, therefore vulnerable for shoulder-surfing attack.

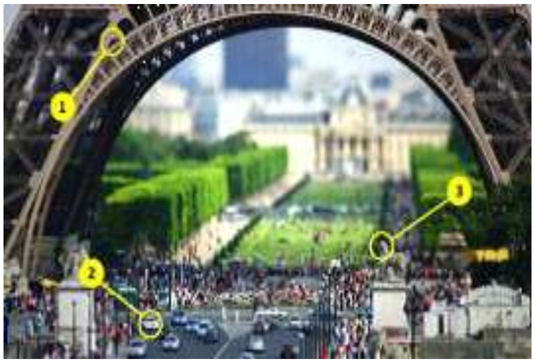


Figure 2: An example of Tri-Pass Interface (Source: Lashkariet al, 2014)

Dheeraj et al (2013) proposed a new graphical authentication scheme which is based on the map. In registration phase, the user will be presented with the map of the world covering countries and each country has it cities. User will select any part of the map that contains clear and visible point that represent the cities in it and connect the different cities in the sequence manner. The sequence of path of the different cities connected to each other is the password. To login the user simply point and connect the selected cities in the sequence manner as he/she did during registration. However this method is vulnerable to brute-force and shoulder-surfing attacks.

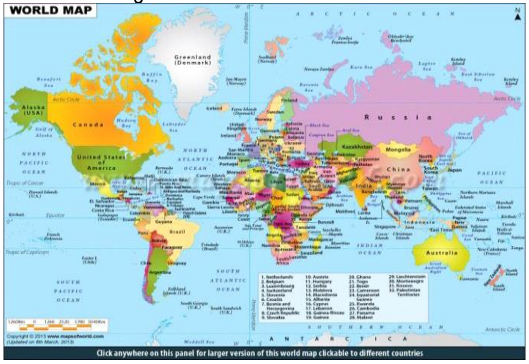

WORLD MAP
Greenland (Denmark)
Canada
United States of America
Russia
China
India
Australia
Click anywhere on this panel for larger version of this world map clickable to different countries

Figure 3: Map based authentication scheme interface (Dheeraj et al 2013)

The drawback in Dheeraj et al, (2013) method is that the user can guess an image containing the cities and with few trials and errors the pattern can easily be drawn. This work seeks to address this above problem.

2.0 Materials and Methods

This section reviews the existing system, identifies area of improvement and presents the new proposed improved system. The algorithm used is pseudo random number algorithm.

2.0 Existing system

Before presenting the proposed system algorithm we first describe Dheeraj et al. (2013) method in which the proposed method is derived. In this method, the map of the world is initially downloaded or prepared and cities on the map are pointed and assigned one unique number or the serial number. A user chooses some cities on the map such that it is easy to decode the city to correspond with unique number mapping. Then select the portion of the map, which contains the clear visible point that represents the cities. Now user will connect the different cities in a sequential manner. So the password is the sequences of path of the different cities connected to each other on the map. The number of cities included in the password is completely user dependent, and the more the number of cities used in creating the password the more secured and complicated to break. Figure 4 is the flow chart of Dheeraj et al. (2013) method.

However, the method as discussed in Section 1 is prone to brute force attack in the sense that if an attacker luckily touches the right area containing the country he would be only left with the last stage of pattern of the states to be drawn to gain access. Also it is prone to Shoulder Surfing attack in the sense that if an attacker sees what the user chooses and as the pattern, he can easily memorize it as it is static and the method has no rule and complications to confuse the attacker.

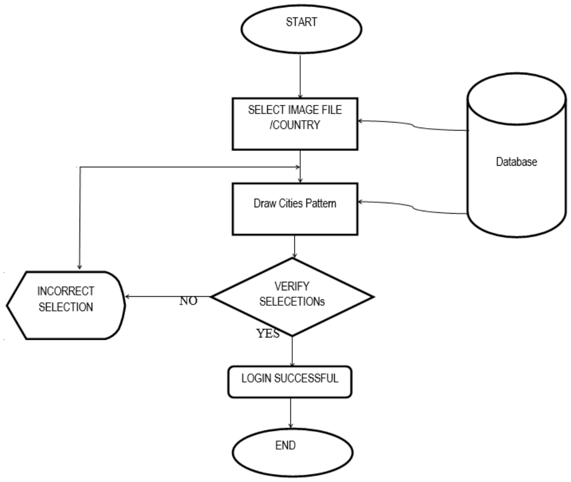


Figure 4: Existing System Flow Chart

2.2 Proposed system algorithm

As in Dheeraj et al. (2013) method the proposed system is based on the use of map of the world. The map containing all the countries in the world is captured in the program. Each country serves as a button which contains its cities beneath. A user begins the registration process by identifying his/her authentication procedure credentials, for example, the countries and states he chooses to use in his password. Secondly, he enters the chosen countries in a sequential order, which must be followed in the same manner during the login phase; for each country entered one or more cities beneath it must equally be entered. Lastly, only one of the selected countries map will appear at random during login phase for selection before the user finally gain access.

The proposed system is more secured because the user has to select two or more countries and in the order he selected during registration on the map before selecting the states under them, this improved the system against brute-force technique attack. In the 2nd level authentication, any of the selected country map could appear (appears at random) which makes it more secured and complicated to break. This also improved the system against shoulder –surfing technique attack.

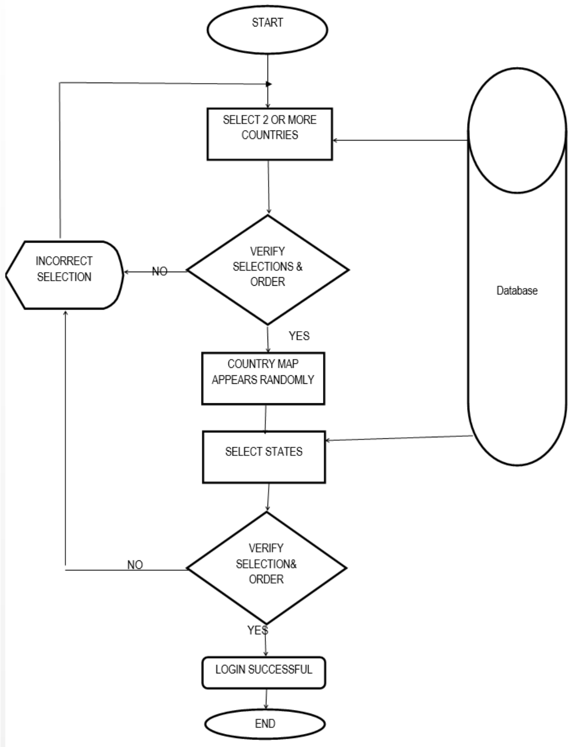


Figure 5: Proposed System Flow Chart

2.2.1. Program Testing Procedure

False Accept Rate (FAR) and False Reject Rate (FRR) are the error rates used to express matching trust ability (Ikuomola et al, 2015). False Accept Rate is the probability that a wrong selection is accepted as valid for a selection during verification. False Reject Rate is the probability that the system fails to match a valid selection. True Acceptance occur when a selection matches with the selection of same country or state, while True Reject occur when the system rejects a wrong selection in the process of verifying country or state. The probabilities of FAR and FRR were obtained by

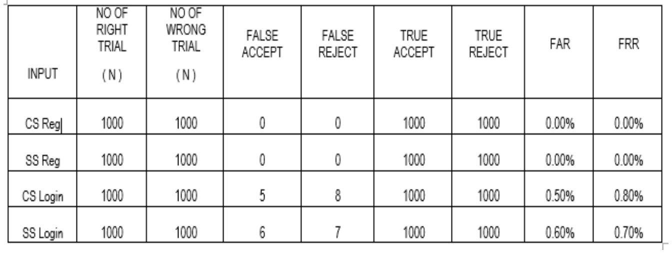
$$FAR = {}^{FA}/_{N} \times 100 \qquad (1)$$

$$FRR = {}^{FR}/_{N} \times 100 \qquad (2)$$

whereFA is the number of False Accepts, FR is the number of False Rejects and N is the number of verifications (Ikuomola et al, 2015) .

In order to evaluate the effectiveness of the proposed system program 1000 number of verification were made and each case we record the values of false accept (FA) and false reject (FR), which we then used to calculate FAR and FRR. Table 1 shows a summary of the result, where we obtained the probabilities of false accept and false reject as, Login Country Selection False Accept Rate (FAR) = 0.05, Login Country Selection False Reject Rate (FRR) = 0.08,
Login State Selection False Accept Rate (FAR) = 0.06, Login State Selection False Reject Rate (FRR) = 0.07.

Table 1: Inputs test verification for the system



INPUT	NO OF RIGHT TRIAL (N)	NO OF WRONG TRIAL (N)	FALSE ACCEPT	FALSE REJECT	TRUE ACCEPT	TRUE REJECT	FAR	FRR
CS Reg	1000	1000	0	0	1000	1000	0.00%	0.00%
SS Reg	1000	1000	0	0	1000	1000	0.00%	0.00%
CS Login	1000	1000	5	8	1000	1000	0.50%	0.80%
SS Login	1000	1000	6	7	1000	1000	0.60%	0.70%

Comparing this result with (Ikuomola et al, 2015) where the probabilities of false accept (FA) and false reject(FR) are all 0, it appears better. However, the maximum number of trials and verifications in (Ikuomola et al, 2015) is 55 which are too small to be used as test measurement for a program, and is a program with a single stage of thumb prints authentication process of student. Unlike in our own system as shown in table 1 above, 1000 verifications trials were used with two stages of authentication process. Therefore, our result is more reliable for program testing.

3.0 RESULT AND DISCUSSION

3.1. Simulation Parameter Evaluation

21

Let's assume we have an option of 20 countries on our map, out of which the user can choose any number of countries he/she desires as his/her first level password. We also assume the country that appears has 10 states on the map. The user will make selection of 1 country in existing system and 2/3 countries in improved system and then route/selection of 3&5 cities/states of the country as second stage password.

3.1.1. Brute force Attack

3.1.1.1. Test Case 1

In the existing system the password is the selection of a country and path route between the cities. The possible selection of a country is 10 and total number of paths possible between first and last city chosen by the user on the map assuming 3 route/selection is 10 * 9 * 8 = 720. So total 720 paths are available on the map when we connect 5 cities on the map, therefore 720 + 10 = 730 is the total possible selection/route require to break the system using brute-force attack technique.

In the improved system, the password is the selection of countries and selection of the states on the map of the country selected. Assuming 2 country selections, the possible selection of these countries in map of the world is 10 * 9 = 190 and total number of selections possible between first and last city chosen by the user on the map assuming 3 route/ selection is 10 * 9 * 8 = 720. So total 720 paths are available on the map when we connect 5 cities on the map, therefore 720+ 190 =910 is the total possible selection/route require to break the system. Therefore, 910 > 730 making the new system an improved secured system in brute-force attack

3.1.1.2. Test Case 2

In the existing system the password is the selection of a country and path route between the cities. The possible selection of a country is 10 and total number of paths possible between first and last city chosen by the user on the map assuming 4 route/selection is 10 * 9 * 8 * 7 = 5040. So total 5040 paths are available on the map when we connect 4 cities on the map, therefore 5040 + 10 =5050 is the total possible selection/route require to break the system using brute-force attack technique.

In the improved system, the password is the selection of countries and selection of the states on the map of the country selected. Assuming 3 country selections, the possible selection of these countries in map of the world is 10 *9 *8 = 720 and total number of selections possible between first and last city chosen by the user on the map assuming 4 selections is 10 * 9 * 8 * 7 = 5040. So total 5040 paths are available on the map when we connect 4 cities on the map, therefore 5040+ 720 =5760 is the total possible selection/route require to break the system. Therefore, 5760 > 5050 making the new system an improved secured system in brute-force attack

3.1.1.3. Test Case 3

In the existing system the password is the selection of a country and path route between the cities. The possible selection of a country is 10 and total number of paths possible between first and last city chosen by the user on the map assuming 5 route/selection is 10 * 9 * 8 * 7 * 6 = 30240. So total 30240 paths are available on the map when we connect 5 cities on the map, therefore 30240 + 10 =30250 is the total possible selection/route require to break the system using brute-force attack technique.

In the improved system, the password is the selection of countries and selection of the states on the map of the country selected. Assuming 4 country selections, the possible selection of these countries in map of the world is 10 * 9 * 8 * 7 = 5040 and total number of selections possible between first and last city chosen by the user on the map assuming 5 selections is 10 * 9 * 8 * 7 * 6 = 30240. So total 30240 paths are available on the map when we connect5 cities on the map, therefore 5040+ 30240 =35280 is the total possible selection/route require to break the system. Therefore, 35280 > 30250 making the new system an improved secured system in brute-force attack.

3.1.1.4. Test Case 4

In the existing system the password is the selection of a country and path route between the cities. The possible selection of a country is 10 and total number of paths possible between first and last city chosen by the user on the map assuming 6 route/selection is 10 * 9 * 8 * 7 * 6 * 5 = 151200. So total 151200 paths are available on the map when we connect 6 cities on the map, therefore 151200 + 10 =151210 is the total possible selection/route require to break the system using brute-force attack technique.

In the improved system, the password is the selection of countries and selection of the states on the map of the country selected. Assuming 5 country selections, the possible selection of these countries in map of the world is 10 * 9 * 8 * 7 * 6 = 30240 and total number of selections possible between first and last city chosen by the user on the map assuming 6 selections is 10 * 9 * 8 * 7 * 6 * 5= 151200. So total 151200 paths are available on the map when we connect 6 cities on the map, therefore 30240 + 151200 =181440 is the total possible selection/route require to break the system. Therefore, 181440 > 151210 making the new system an improved secured system in brute-force attack

Thus, very large number of trials has to be done for detection, to succeed using brute force technique. Complexity of breaking the password increases with number of the cities chosen in the password increase and further by hiding the information that which region is selected for the password.

3.1.2. Defense against Shoulder Surfing Attack

With the existing system, the attacker might sight the sequence assigned to the country to get him access to the last level of authentication. But with the improved system, the attacker has to know the 2 or 3 countries to select and also the cities' sequence. More so, any of the countries can appear at RANDOM making the hacker more confused in dealing with this complicated system.

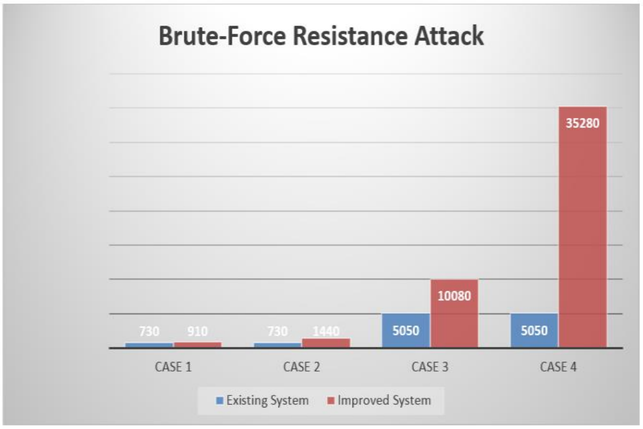


Figure 6: Comparison of Brute-Force Resistance between Existing and Improved System

It can be seen from the above graph that in both case 1, 2, 3and 4 that the improved system has higher resistance to brute-force attack than the existing system, also from the graph it can be concluded that no matter the number of selections set for the systems brute-force resistance value of the improved system will always be higher.

It can also be seen that the higher the number of country selected the higher the strength of the security, however the higher the complexity of the system. This gives a user clear options on how he wants his system in terms of complexity.

4.0 SUMMARY AND CONCLUSION

In this paper, we proposed a new graphical-based password system for mobile android devices. The advantage of this algorithm is that it allows for randomization and order of selection which makes it less vulnerable to brute-force and shoulder surfing attacks. This algorithm improved the map graphical-based password authentication system for mobile android application devices proposed by Dheeraj at al (2013). Therefore, improved the system and made it more secured.

This method is suitable for mobile app lock. The time and all security features are obtained when user enters his or her graphical password so this system does not cause any extra burden on users. In this system also, a user is able to login to the system when he or she can successfully authenticate via the graphical password.

However, the proposed improved system needs to be checked how efficient could be when deployed in other operating systems or working places. More research can be carried out and focus on exploring more feasibility, usability features and improve the system for better attack technique resistance.

REFERENCES

Ahmad A.Z, Arash. H.L, (2014). Pass-Coob a New Graphical Password Based on Colors and Objects. Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology – IPCT. Pg 2-14

Alia.M.A, Hnaif.A.A, Al-Anie. H. K., Tamim. A. A, (2012). Graphical Password Based On Standard Shapes: Science Series Data Report Vol. 4, No. 2, Feb 2012 p. 1-69.

Daniel. R, Micheal. W, Micheal. W and Marcel.W (2013).Multitouch Image-Based Authentication on Smartphones. CHI'13 Extended Abstracts on Human Factors in Computing Systems. Pg 787-792

Dheeraj. D, Viral. P and Vipul. K.D, (2013). Map Based Graphical Authentication. Institute of Computer Technology &Applications,Vol 4 (6),1005-1009 IJCTA.Pg 1-20

Ikuomola.A.J, (2015).Fingerprint-Based Authentication System for Time and Attendance Management.British Journal of mathematics and Computer Science 5(6), 735. Pg 6-18

Iranna A M, Pankaja. P, (2013). Graphical Password AuthenticationUsing Persuasive Cued Click Point. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.Vol. 2, Issue 7,pp 262-2966

Lashkari.A, Elmira. Y, Kanat. Y, Mustafa M. A, Mohammad. S, (2014). Tri-Pass: A new graphical user authentication scheme. Pg 1-9

Masrom.M, Towhidi .F, and Habibi.L, (2009).Pure and Cued Recall-Based Graphical User Authentication, in Application of Information and Communication Technologies (AICT).ieeexplore.ieee.org Pg1-20

Mohammad. H, Norafida. I and Rezvan.P, (2012). Multi Touch Graphical Password Asian Journal of Applied Sciences, 5, pp 20-32.

Nali .D and Thorpe .J, (2004).Analyzing User Choice in Graphical Passwords.School of Computer Science, Carleton University, Tech. Rep. TR-04-01.Pg 4-10

Susan.W, Jim. W, (2010).Authentication Using Graphical Passwords. College of IST.pg 4-8

Saroiu .S, Gribble.S and Levy.H .M, (2004). Measurement and Analysis of Spyware in a University Environment in Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation. (NSDI), pp. 141–153

Wang. L, Chang. X, Ren. Z, Gao. H, Liu. X and Aickelin.U, (2010).Against Spyware Using CAPTCHA in Graphical Password Scheme. 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 760–767.

Wiedenbeck. S, Waters. J, Birget. A and Memon.N, (2005) PassPoints Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, vol. 63, no. 1–2, (2005) July, pp. 102–127.

Wei H, Wu. X and Wei.G, (2010).The Security Analysis of Graphical Passwords. International Conference on Communications and Intelligence Information Security, pp. 200–203.

Xiaoyuan.S, (2006).A Design and Analysis of Graphical Password, Computer Science Thesis.Paper 2.Pg 5-18