A Simple Method for Improving the Security of Internet Banking

[1]Ehsan Sharifi, [2]Mostafa Khadem Almelleh
Taali Higher Education Institute of Information Technology
Qom, Iran

[3]Mahboubeh Shamsi
School of Electrical & Computer Engineering,
Industrial University of Qom
Qom, Iran

Abstract— ***At present information technology takes the task of supporting and raising service efficiency in banking industry and expanding bank service opportunities to its customers. That's why all the big banks looking to enter the electronic transactions and banking more quickly and more serious and want supply banking services through the Internet to their customers. Besides the numerous benefits that go along with e-banking and e-commerce, the providers of these services must be more responsive towards security requirements. One method of increasing security, is the One Time Passwords that enhances security compared to the usual password systems but have many weaknesses against certain kind of attacks, particularly the Phishing attacks. In this paper we proposed a new method for generating One Time Passwords based on the spatial relationship between icons for enhancing security of internet banking.***

Keywords-component; Internet Banking; Information Security; One Time Passwords (OTP); Usability of Internet Banking.

I. INTRODUCTION

E-Banking is the new kind of banking industry that supply banking services on electronic environments. These types of banking, pandemic since 1991, when the Internet become prevalent in the world and is known that if e-banking become prevalent in the community, so we also hope to boost e-commerce, such as e-banking is prerequisite for entering to the e-commerce. Despite that electronic banking was formed several years ago by ATM (Automatic Teller Machine) and telephone banking, but this type of banking has attracted the attention of customers via internet and mobile banking in recent years.

Many services of banking provided via electronic banking, such bank statements services, funds, transfer and bills pay, apply for loans and credit cards, foreign exchange transactions, new accounts inauguration and insurance services. This type of banking tries to reduce customer's bank visiting by the use of communication channels and thus increase their comfort and satisfaction. Internet as one of the most important and most widely used of these channels, eliminates the constraints of time and place by a computer, and everywhere and in all places, has established a customer relationship with the bank.

Communication between the client computer and the bank's central computer by the browser that installed on the client computer, will form the basis of this type of banking. Nowadays All banking services other than cash transactions supported by internet banking and addition to these advantages, bank fees reduce by reducing paper consumption, reducing the number of staff and no need to fixed and large office, are the main factors of bank's trend to Internet banking [1].

One of the biggest obstacles that impede the development of online banking is the security and of financial transactions on the Internet [2].Trust and confidence in e-commerce, enhanced over the years with the advancement of technology related to security, but it is normal that with start of using modern communications and the Internet, threats of attackers that try to menace the information security always existed. In recent years we have witnessed a variety of attacks on internet banking, which in some cases has caused heavy losses [3]. That's why banks continue to boost the customer' confidence with trying to increase the security of their internet based services to attract customers to utilize internet banking.

On the other hand however very strong and complex security methods can increase security of internet banking, but reduces the usability of this service [4]. So we had to think about strategies that while support security of financial transactions, don't involve users with technical issues. Because Constant use of greater security technologies enhances the level of secure banking contradictorily affecting the usability of the services.

In this paper we proposed a new cipher method to increasing the security of Internet banking. In the proposed system, icons rather than alphanumeric characters, forms user's key and the spatial relationship between these icons are used to generate One Time Password (OTP) for entering into the user's account.

In section 2, the OTP systems will be reviewed and examples of the OTP generating systems that are currently used in Internet banking will be mentioned. The new method will be presented in Section 3 and in Section 4 the security of this new method will be evaluated and finally, results will be summarized in Section 5.

II. One Time Passwords

A. *Normal OTP*

One Time Password, is the password that is valid for only one entry or transaction that covers many weaknesses of the old password systems. The most important flaw that compensated by OTP is vulnerability against an attack's repeat [5]. By using this method, an adversary who access to the password that used for a service or transaction, will not be able to take advantage of it, because the password has expired. Difficult remembering them by humans is the main The OTP's disadvantage, thus often benefiting from assistive technology is mandatory. OTP often produced by using mathematical algorithms (Hash) and Time-synchronized systems.

In Hash method The OTP system works by starting with an initial seed S, then generating passwords f (s), f (f (s)), f (f (f (s))), ... Each password is then dispensed in reverse, with f (f (... f (s)) ...) first, to f (s). If an indefinite series of passwords is wanted, a new seed value can be chosen after the set for S is exhausted. In this method due to one-way function f (), All generated keys will be unique and exclusive. In Time-synchronized method users use an OTP security token which is a hardware device capable of generating one-time passwords. Some of these devices are PIN-protected, offering an additional level of security. The user enters the one-time password with other identity credentials (typically user name and password) and the bank server validates the login request.

Apparently due to generating a separate password for each session of the relationship between bank and customer in the above methods, the security level is very high, but because some of the characteristics of Internet banking, there are several weaknesses against some attacks, including Phishing attack.

Phishing attack refers to a person or a group of cyber-criminals who create an imitation or copy of an existing Web page to fraud users into providing sensitive personal information [6]. Usually a Phishing attack is done in combination with email spam. Spamming is simply to send millions of emails. The spammer doesn't know his victim, so the emails sent out are general, impersonal, and often focused on the big popular banks with a large customer base. Then the customer also assumes that entered into the bank's website and enters a username and password to log in without any hesitation. Then adversaries enter into the Bank's main site by using the obtained information, and doing their tricks.

Because in Time-synchronized method Password must be entered into the system in Real Time, the security of this method is higher than the Hash method. But if an adversary can enter the password into the bank system very quickly, even using the Time-synchronized method is not effective against attacks [7].

B. *spatial relationship based OTP*

Spatial relationship based OTP can be used for improving the security of system against attacks. In this method, instead of entering characters that formed user's password to the system for logging, the spatial distance between the user's password character values are entered into the system. Therefore adversary can't achieve user's main password. Fig. 1 shows an example of this method.

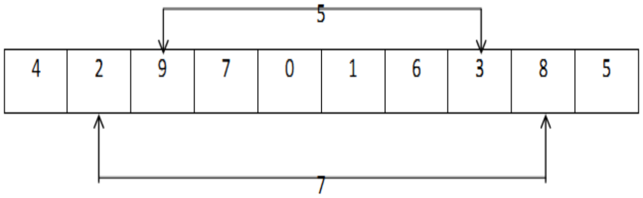

Figure 1. example for spatial relationship between numbers.

The Fig. 1 shows OT-password generating by using spatial relationships between users' main password's first and second character and distance between third and quarter character. In with assumes that the Customer's main password has been 2893, The distance between the password‘s first character (2) with The second character (8) is 7 (9-2). Likewise, the distance between the password's third characters (9) and the fourth character (3) is 5. Therefore the generated OTP value will be 75. As we will see in this method user doesn't enter his/her main password into the system and only enters spatial relationships between main password's characters.

For this reason the attack planner even if the customer is deceived and adversary led him/her to a fake website, only obtained information about the spatial relationships between the main password's characters. Adversary need answer of several questions about spatial relationships between password's characters to achieve customer's main password with analyzes of these answers. As noted in following, the method that proposed in this paper is more secure against attacks compared to the normal spatial relationship based OTP method.

III. Proposed Method

Main feature of the new method compared to the existing OTP generating methods is the ability to use more than 10 icons to generate a spatial relationship based OTP. In this method, security level enhanced with increasing of the number of the icons. In this paper, for example, 15 icons considered as the question's table icons number. Two main advantages of the new method compared to the current methods are the security improvement by using 15 icons instead of 10 numeric characters (0 to 9) and also ease of remembering icons by human than by numbers [8].

In the new method, the customer visits the bank and specifies the username and 4 (for example) icons as her/his main password. Thus when the customer is trying to use internet banking services, the first step is to logging by account number into the bank system. In second step bank's system request the customer enters her/his user name and then shows a table with 1 row and 15 columns that contain 15 different icons and asked the customer to answer two questions about the table. These two questions are about the spatial relationship between the 4 icons that selected by costumer as main password. Each of these two questions about the distance between the two icons of the 4 main icons that were randomly selected by the system between 6 possible questions about 4 icons. An example is given below for better understanding of the system's operation.

Assume that the costumer select ball, bus, cows and PC as a password. Bank system shows Fig. 2 to him and asked him to answer the following two questions:

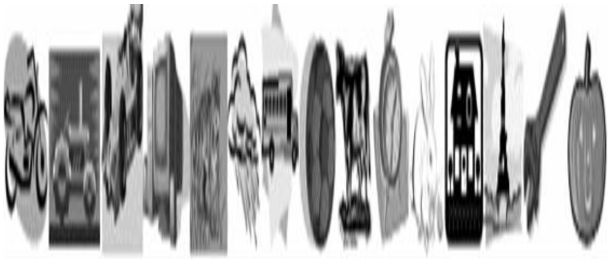

Figure 2. Table.1 that presented by the Bank.

1 - How much is the distance between the second and third icons of your password in Figure?
2 - How much is the distance between the first and fourth icons of your password in Figure?

Customer calculates distance between bus icon in seventh place (from left to right) and cow icon in ninth place $(9-7\ =2)$ and number 2 will be entered into the system for the first question. Similarly, for second question number 4 will be entered into the system. Therefore 24 will be calculated as OTP and costumer will log in to the system.

As noted, due to the spatial relationship characteristics, the answers that are given to the questions involved many pairs of icons, because it adversary cannot achieve main password by OTP. So in this case, one Phishing attack is not sufficient to achieve the costumer's password and designer of attack must get many answers of different questions about spatial relationships between icons to analyze them and guesses main password.

IV. Security Analysis

As the main feature of the proposed method, bank's system can has a database containing a large number of icons and related to the costumer's username that entered into the first stage, bank's system can blend consumer's password's icons with other icons and present as a question table. Therefor if the user doesn't see one of her password's icons in the table that presented by the bank, simply notice that the site is fake and designed by adversary. While normal numerical methods for this type of cipher system contains 10 characters and therefore bank's question involve all numeric characters and costumer not able to detect attacks. That's why it can be regarded as a special feature and most important advantage of this method compared to other methods. In the following, more detailed study of the performance of these systems against Brute Force, Phishing and key logger attacks be noted.

A. *key logger attack*

a) Key logger is software or hardware that can store keystrokes on the keyboard and an attacker can steal user typed information. These attacks can target internet banking customers and obtain their password and do criminal actions [9]. In the proposed system, due to user does not enter the main password to the bank's system, thus the system is safe against key logger attack and this attack is not a threat for the system's security.

B. *Brute Force Attack*

Brute-force attack that also known as a dictionary attack is a type of attack that all possible solutions is checked to reach an answer [10]. Examine all possible scenarios are used as a method for finding the password for target internet banking customers. If an attacker gets consumer username by social engineering like methods, probability of Brute Force attack's success in the proposed system will have an inverse relationship with the number of keys that can be created in the system. In other words, if the range of key's that generated by the systems is reduced, the likelihood of Brute Force attack's success will be increased. For example, if consider the range of the OTP as A, the probability of password finding by Brute Force attack will be . In this paper we assume that the system generates the 2-digit OTP and range of any digits can be any number from 1 to 9. The total number of OTPs that can be generated by the system is .Therefore the probability of achieving password by Brute Force attacking will be . However, unlike classical password systems that by 81 times test in a row, attacker certainly can be entered into the system, because in the proposed system bank's system changes the table and questions each time that the password entered wrongly, probability of password finding will be for each duplicate try.

On the other hand, with the restriction on the number of wrong password entering times by the bank's system, indeed Brute Force attack cannot be successful in proposed method. Of course It should be kept in mind that 4 icons for consumer main password, 15 icons in the form of questions and two questions about table, considered only to review to the superiority and advantages of the proposed system compared to current systems, otherwise security system designer can increase the number of customer's password's icons and the number of icons in the questions table also number of questions for improving system's security.

C. *Phishing attack*

Phishing attack is one of the most common attacks on banks and financial institutions and also more common in recent years. In this type of attack, attack planner design a similar website to bank website and induce the customer to answer to the question about the relationship between the constituent icons of the main password, in best term acquires an OTP. Then, with analyzing this OTP guess customer's main password and try to enter into the bank website.

In conventional systems, the password that attacker obtains is the costumer's main password. But in the proposed method, the attacker obtains an OTP. More possible and candidate passwords derived from this this OTP means more robustness of systems against attacks. In the new method, the number of candidate passwords that derived from the OTP has a direct correlation with the number of icon pairs that acceptable for OTP. The greater distance between two icons is reduced the number of acceptable icon pairs. For this reason, we consider 9 as the maximum acceptable distance between icons.

When the OTP's both constituent digits are 9 is the weakest condition in the proposed system against Phishing attack. The security analysis of this case investigated in following with an example.

Assume that consumer select house, scale, rabbit and car as a password. Bank's systems present the Fig. 3 table to consumer and asked two questions.

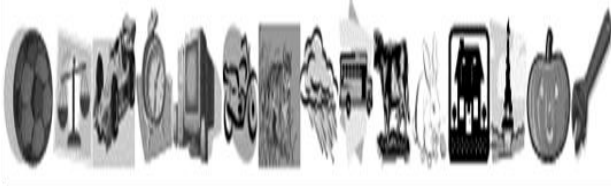

Figure 3. . example for spatial relationship between numbers.

1 - How much is the distance between your password's second and third icon in the table?

2 - How much is the distance between your password's first and fourth icon in the table?

Therefore 99 will be produced as OTP and as noted is the weakest condition in the proposed system. There are 6 candidate icon pair for 9 value. For the first 9 digit, the attacker will guess the consumer's password's two icons with probability. Also the attacker needs to try twice for finding the exact location of this two icon between the password's icons. For second 9 digit there are 5 candidate icon pair of 6 icon pairs. Like the first 9 digits, twice trying is needed to finding the exact location of the two icons. So in the weakest condition of the system, the number of possible and candidate password will be and Phishing attack planner Even if gain customer's entered OTP, will be obliged to try 120 times. It is again noted that assume 4 icons for costumer's password, 15 icons in the question table and two questions for the session, considered for test the proposed method and increase of each of these factors will lead to increased system security.

V. Summary and Conclusions

With the increasing financial transactions on the Internet, security improvement of these transactions has become one of the most important issues. However, research has shown that sophisticated security methods to deal with the attackers, however, increases the level of security in Internet banking, but decreases usability. So banks have to achieve simple and safe methods. in this paper, for reducing internet banking security weaknesses that is the main reason for most people that are not interested in for using this service, propose a new method for password generating that can improve security of internet banking. Using icons in the proposed method, has two principal advantage for new method.

First, easier recall of the icons compared with alphanumeric for human mind and other is using more icon than 10 digit by bank's system in the form of questions table that would increase the level of security in system. Security analyze of the proposed method system against Phishing and Brute Force attack indicated improvement of system's security and resistances.

References

[1] L. V. Casalo, C. Flavián, and M. Guinalíu, "The role of security, privacy, usability and reputation in the development of online banking," Online Information Review, vol. 31, pp. 583-603, 2007.

[2] C. K. Dimitriadis and C. CISA, "Analyzing the security of Internet banking authentication mechanisms," Information systems control journal, vol. 3, p. 34, 2007.

[3] A. R. A. Grégio, D. S. Fernandes, V. M. Afonso, P. L. de Geus, V. F. Martins, and M. Jino, "An empirical analysis of malicious internet banking software behavior," in Proceedings of the 28th Annual ACM Symposium on Applied Computing, 2013, pp. 1830-1835.

[4] D. K. Smetters, "Cyber Security Technology Usability and Management," Wiley Handbook of Science and Technology for Homeland Security, 2014.

[5] P. Hanacek, K. Malinka, and J. Schafer, "e-banking security-A comparative study," Aerospace and Electronic Systems Magazine, IEEE, vol. 25, pp. 29-34, 2010.

[6] Y. Peng, W. Chen, J. M. Chang, and Y. Guan, "Secure online banking on untrusted computers," in Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 720-722.

[7] L. Peotta, M. D. Holtz, B. M. David, F. G. Deus, and R. de Sousa, "A Formal Classification of Internet Banking Attacks and Vulnerabilities," International Journal of Computer Science & Information Technology, vol. 3, pp. 186-197, 2011.

[8] M. Polasik and T. P. Wisniewski, "Empirical analysis of internet banking adoption in Poland," International Journal of Bank Marketing, vol. 27, pp. 32-52, 2009.

[9] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of verbal Learning and verbal Behavior, vol. 6, pp. 156-163, 1967.

K. Apostol, "Brute-force Attack," 2012