# Authentication and Security, issues of modern banking services in Iranian banking sector

Ali AghaeiRad, Bernardete Ribeiro

CISUC, Department of Informatics Engineering, University of Coimbra, Portugal
{ali, bribeiro}@dei.uc.pt

**Abstract:** Interbank Network "SHETAB" has been working for several years in Iran, and provides banking services such as withdrawals from ATM machines, buying from the POS machines, and also recently the online shopping service for the clients of the member banks. In another paper we have shown that the interbank network in the present form can jeopardize users' privacy. In this paper, we show that users are not aware of security issues in modern banking services by using a statistical study, and they usually do not consider such issues. Therefore, we conclude that the methods used by interbank network "SHETAB" are not safe. Finally, for solving the mentioned problems, a banking system based on the collaboration between the banks is offered, that will eliminate problems facing the current system. The presented method is based on short-term passwords, which in author's opinion, is one of the best available methods. Based on the information of field research, it is concluded that so few people, who use the new bank services, are aware of security issues; among these few people, so few consider these issues. Therefore, in the presented solution, we tried to design the system in a way to be intrinsically secure, and to be independent from user behavior regarding security issues consideration, as far as possible. Moreover, besides security and privacy of the system, another issue, which shall be considered for acceptability of a system, is its simplicity. Therefore, we tried to design the presented system as simple as possible for users.

[Ali AghaeiRad, Bernardete Ribeiro. **Authentication and Security, issues of modern banking services in Iranian banking sector.** *Life Sci J* 2014;11(11):956-960]. (ISSN:1097-8135). http://www.lifesciencesite.com. 169

**Keywords:** E-banking, Security, Authentication mechanisms, Collaborative banking.

## 1. Introduction

Banking services are an integral part of everyday life of people in today's world. At any time of day, people can withdraw cash from ATM machines or transfer funds to other accounts. They can purchase from most stores and even supermarkets, without carrying cash. They can also manage their accounts or transfer money from anywhere in the world via the Internet. New strategies for managing accounts using mobile phones as SMS - Banking and Mobile Banking have also recently been launched. And in Iran, these services are being launched by some banks. The modern banking services have become a vital part of people's lives and businesses.

Traditionally, the financial information relating to financial institutions and credit transfer between institutions and their clients, have been very important. Therefore, many banks are trying to keep this information safe. Privacy is of special importance in the modern banking. One part of privacy, which is the inference of private information, from those information that are not alone classified as confidential, is being reviewed in another article [1] . However in this paper, we concern the problem of unauthorized access to account information.

Currently, most Iranian banks that offer ATM services use fixed password for authentication of clients. The user can use the ATM card and a fixed password to purchase from POS devices. He can transfer money from ATM machines, or choose to withdraw cash. Users can also use the specifications listed on the card and a password to do online shopping. While this method is only able to provide security, when appropriate length and non-guessable passwords are used, the password should be modified regularly, and authentication data should not be saved on devices that are completely unsafe, such as personal computers [2] ▯ . Bank customers rarely consider all these cases.

Fixed password authentication is almost one of the most insecure authentication methods [2] ▯ , and is vulnerable against all the attacks such as card copying, card theft, offline information stealing or online channel breaking. And in any case, the authentication information get in the hands of another person, so user account can be easily accessible.

In this paper according to data collected through the questionnaire, it is explained that the majority of people have very little information about security issues when using modern banking systems. As a result, the likelihood of becoming a victim of financial fraud is very high. Consequently, it is proposed that the system must be designed in a way to be intrinsically safe. In addition, banks need to increase people's knowledge about security issues. In the next part of this article, we review the history of authentication methods in banking. The third section presents the tested hypotheses. The fourth section presents the results of the questionnaire analysis. In the fifth section suggested solutions to solve the problem are explained, and finally, in the sixth section, conclusions are presented.

## 2. Literature Review

By the expansion of the Internet and web, bank transactions have entered a new space of technology in which organizations are able to cooperate in financial calculations and transactions within a common space. Always between these transactions, amounts of private banking information are also transferred. Numerous studies have been carried out to increase the security of authentication protocol. Many people introverted from internet banking because of the security threats. Users worry about the fraudulent bank transactions that pop up every now and then. This problem should be solved by banking sectors using a proper security technology in protecting their websites [3].

For a first time user, navigating through a website of an internet bank may be hard and may take some time. Due to numerous personal details queried the potential customer felt inconvenience in opening an account and this made the customer discouraged of using of internet banking service. Friendly environment, tutorials and live customer support can be provided to help users performing their required tasks in dynamic environment [4].

The more a bank relies on Internet banking; the more the bank may gain an impersonal feel. Both of these problems may discourage clients from choosing a bank that relies on internet banking, regardless of how convenient internet banking may be. E-banking increases convenience, but it also opens a bank to security issues. A criminal might hack into the bank’s server in order to acquire bank account data, or a software malfunction might cause the bank to unintentionally distribute personal data to the wrong person. Banks that use Internet banking have to constantly update their software and hardware to make sure that compatibility issues and increased knowledge of security systems do not increase their security risks [5].

## 3. Assumptions

This study is investigated by using survey techniques and quantitative research methods. The quantitative method provides a possibility to test hypotheses. And these hypotheses are tested using a questionnaire. Then, proposed hypotheses are described, which include six hypotheses. In this study, the method of probabilistic sampling is used. This means that all members of the population will be able to get into the samples. So the generalized results are available to the entire population.

Population includes customers of banks in Tehran, who use multiple ATM cards. Among these, 100 individuals were randomly selected as sample. Research hypothesis that are put into three test grouped categories are as follows.

First Part: Security Assumptions

- Most customers are not aware of the security issues associated with modern banking systems.
- Most customers that are familiar with security issues do not consider these issues.

Second Part: Simplicity of Use

- Lack of knowledge about using electronic banking will result in less use of electronic banking.
- Inadequate and ambiguous interface design will have a negative impact on taking use of e-banking.

Third Part: Privacy Assumptions

- Most people are not familiar with the violation of privacy in the electronic banking system.
- People with a high average account balance are more sensitive to disclosure of their private information.

To test these hypotheses, a questionnaire with 33 questions was designed, and after the pilot interviews, the numbers of questions were reduced to 20. Six of these questions are general questions which are asked to classify people to social and economic classes. Four questions evaluate the interviewee's general knowledge of computer and Internet; eight questions evaluate the interviewee's knowledge of the security assessment of electronic banking. And other questions evaluate the role of simple and intuitive user interface in electronic banking, the tendency of people to use e-banking tools, and importance of privacy in e-banking, and finally a question about the respondent's view on the token in the Internet Banking.

## 4. Results

The data show that most participants are men between the ages of 20 and 50 and eighty percent of them have an income level between 5 million to 20 million Rials per months.

In the Figure 1, the knowledge of the respondents regarding security is plotted. As it is clear from the figure, the first five questions from the left are questions that most people are familiar with them, but people are less familiar with the last four questions. Although more than fifty percent of respondents have considered at least 3 of the 5 cases of security issues, they were informed about. But this ratio is very low. On the other hand, as it is clear from the figure, the more difficult has been consideration of security issue, the less percent of people has followed it. For example, avoiding the use of meaningful passwords and choosing different passwords for each account which are perhaps the most difficult ones, took place by less than ten percent of respondents. But, avoiding storing the password on an insecure device is followed by many more of them.

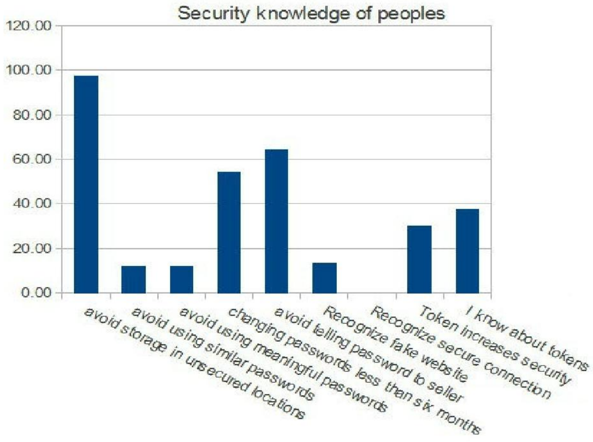

***Figure 1*** *Security knowledge of peoples*

Questions related to the security and taking use of token in internet banking has been answered by a few of respondents. And it expresses the fact that the extent of public knowledge of security issues especially in Internet banking is very low. Especially in the current situation, while banks are pushing more customers to use the new tools such as mobile banking, these findings justify the need for more public informing programs on security issues.

The last two columns of the chart explain the situation regarding the use of tokens to increase security. Diagram expresses the fact that a significant number of the population, more than 60%, do not know about tokens or have no idea about its impact on security.

In the Figure 2, the views of people about simplicity of using the ATM and the Internet to conduct banking transactions is shown. As you can see, over ninety percent of respondents find the ATM usage simple, while more than thirty percent of those who use computer and internet regularly find the Internet banking difficult to use, or generally do not use it. Of course, this could be due to a longer age of ATM systems than Internet banking in Iran. In any case, the need for advocacy programs to use Internet Banking is fully felt.

Also, a survey conducted shows that about ten percent of people, due to inconveniences caused by the use of the Internet or ATM, have revised in taking use of these tools, and use them more carefully. And a total of about thirty-five percent of people still prefer to go to bank branches for their banking matters.

*Although, nearly all people were not aware of possibility of collecting and verifying information about their account transactions by the bank, more than eighty-seven percent of the respondents found this fact important. Thus it is clear that banks should present more and clearer information about their practice in this field. And also should speak clearly about their policy in regard to storage of transaction histories. Of course, customers must agree on the ways that these information are going to be used.*

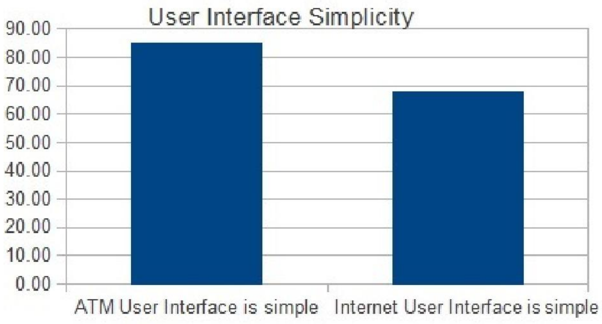

***Figure 2*** *Perceived simplicity of modern banking tools*

At the end the six hypotheses have been put to the test in this study, it was concluded that, awareness about security issues of modern banking services are not uniform, and knowledge about security issues relating to the ATM systems are much more than internet banking. But in any case the amount of considering security issues is very low. Unfamiliarity with the Internet banking has led to use of these services by very small number of people. Even though the user interface design of many ATM machines is not clear, people prefer to use them rather than wasting their time in the bank branches. Finally, although almost all the interviewees were unaware about the possibility of getting private information through their banking transactions, many of them, regardless of the account balance were sensitive to the use of this information.

Notable among interviewees was that, while 51 percent of them have high school diploma or below, over 70% of them regularly use computers and Internet. And yet, only 47% of people have used the internet banking. This means that, almost 33% of regular users of computers and Internet have not used Internet banking.

## 5. Problem Definition

Interbank Network "SHETAB" has been worked for several years in Iran, and provides banking services such as withdrawals from ATM machines, and purchasing from the POS machines, and recently the online shopping service, to the clients of the member banks.

Currently, most Iranian banks that offer ATM services, Use fixed password for authentication of clients. The user can use the ATM card and a fixed password to purchase from POS devices. He can transfer money from ATM machines, or choose to withdraw cash. Users can also use the specifications listed on the card and a password to do online shopping.

Based on the information of field research, it is concluded that so few people, who use the new bank services, are aware of security issues; among these few people, so few consider these issues.

In the other hand, as we have shown in another paper [1], the interbank network in the present form can jeopardize users' privacy. And by using transaction data, information about clients may be inferred that they are not willing to disclose it.

So the next purpose of this paper is to design an interbank network that, while provides the current facilities and services of "SHETAB" interbank network, it is inherently safe, protects users' privacy and security, and just requires minimum knowledge of security issues by users, and finally, it is simple to use for users. In the next section, an approach is presented to solve the above problems, and to create a safe interbank network.

## 6. Proposed Solution

In this section, the solution which is based on Onetime-Short time Passwords is proposed to upgrade the banking system in Iran, and to remove security and privacy problems in the current system as far as possible.

One of the notable conditions which is considered, is the lack of a PKI infrastructure at the current time in the country, on the other hand, because many ATMs and POS machines are working across the country, the new system is designed so that there is no need to change existing hardware. Also, in the design of new system, simplicity of use is taken into consideration. And hardware operation has changed very little, so users do not get confused. Moreover, as explained in another article [1], the system prevents intermediate banks access to the financial information of clients, and also minimizes the inference probability, and identification of clients through financial transactions by intermediate banks.

### 6.1 Collaborative Inter banking System

Based on the above considerations, the proposed system is as follows:

1. Actual client profile information (client identity) is kept in the Central Bank, and Central Bank assigns a unique identification number (Bank-ID) to each Dual pair (bank - client).

2. Central Bank gives every client a onetime password token (OTP), and by receiving the password generated by the token, and identification number (Bank-ID) of the Dual pair (bank-client) from the Bank, confirms the identity of the client. Central Bank approves an identification number (Bank-ID) only for the bank, which is part of the Dual pair (bank-client).

3. In every bank, a client has a unique account number, for each account. Thus, a bank client can have separate accounts with a single Bank-ID. Only through Internet website and ATMs of the reference bank it is possible to get account report or account balance.

To perform banking operations via ports of the bank, client gives password generated by the token along his account number to the bank. Bank sends Bank-ID associated to client's Account-Number along the password received from the client, to the central bank. And finally, after receiving the customer authentication from Central Bank, will allow the client to perform banking operations.

For banking through ATM, POS Machines and Internet portals of other banks, Intermediary bank receives account number and password from the user and sends it to the reference bank. Then reference Bank announces the result of the authentication process to the intermediary bank.

Tokens can be equipped with a USB port, so when the required hardware is present (e.g. online banking), users do not need to type the generated password. A PIN code will be placed on the token,

So if the token is lost, it is not abuse.

### 6.2 Discussion

In using the proposed banking system, each person is given a token from the central bank, and the person's authentication token can be used with various banks. And thus the use of multiple accounts with a single token will be very simple.

Clients of each member banks of the network can receive banking services from any other bank.

On the other hand, token produces one-time and short-time password, which is robust against offline data theft and many online attacks as well.

In case of physical token theft, token requires a PIN code to be activated otherwise it will not work. Also, the thief must have the account number to generate correct password, which also makes it even harder for the burglar to use the token.

Thus, except from the central bank and the reference bank, a customer's true identity assigned to a Bank-ID is not revealed to other banks or agents. And if a customer has two bank accounts in different banks, one bank will not be able to identify the client's identity through the Bank-ID in another bank.

Therefore, the system proposed here, in addition to maintaining the functionality of the SHETAB interbank network system which is currently on use; will increase security of transactions to the great extent, will prevent the disclosure of client's financial transactions to intermediate banks, and also it will be easier to be used by users.

## 7. Conclusion

In the first parts of this paper, it was shown how the banking system in present form is insecure, and how individual authentication information can be stolen and abused. Field research also demonstrated the extent to which users are unaware of security issues especially in the area of Internet banking. Then, an alternative for this matter is introduced with maximum usage of current hardware and minimum change in software User Interface. As a result of using short term onetime passwords, the method is robust considering numerous offline data thefts. Furthermore, in comparison to the current vulnerable state of banking transaction security, this method can provide highly improved security in banking services. Also from privacy point of view, transactions data does not jeopardize privacy.

On the other hand, in regards to users with little knowledge in the context of low security, and, non-compliance with the difficult security issues, using this system will cause consideration of a lot of security issues without requiring the user's knowledge.

Method proposed in this article would be very easy for bank customers, and they do not need to remember passwords for their various accounts or separate passwords for Internet banking. Also, users do not need to carry ATM cards and tokens of various banks. If they know their account numbers, they will need only a one-time password token to access their accounts at different banks from the nearest port.

## References

1. A.AghaeiRad, B.Fathi-Vajargah, M.Afzali, "Security and privacy issues of modern banking services in Iranian banks," Advances in Computer Science and its Applications (ACSA) Vol. 2, No. 2, 2012.
2. A. Hiltgen, T. Kramp, and T. Weigold, "Secure Internet Banking Authentication," *IEEE Security & Privacy*, 2005.
3. Uppal, R.K. Rimpi Kaur, "Internet Banking in India – Challenges and Opportunities", ISBN: 8177081373, 2007.
4. Ms Megha Jain, Ms Rashmi Tiwari, Ms Namrata Jain, (2011), "Internet Banking in India: Problems and Prospects", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, May-June 2011.
5. Wanda Thibodeaux (2011), "Challenges of Electronic Banking", eHow Contributor, accessed 11 August 2011.

8/16/2014