Indian Streams Research Journal
Vol - I , ISSUE - V [June 2011] **ISSN:-2230-7850**

INTERNET BANKING AND ITS SECURITY MEASURES

Mr. Santosh T. Jagtap
Prof. Ramkrishna More ACS College, Akurdi, Pune
E-mail: st.jagtap@gmail.com

ABSTRACT

Online banking is fastest, efficient way of Banking. It is very easy and simple way of Banking compared to traditional methods. Security issue of online transaction is subject of deep concerns for the banks.

In this research paper we have provided new security measures for safe and secure online transactions, along with the suggestive measures to customers using online transactions.

Keywords: login password, transaction password, encryption key, SL1 password

INTRODUCTION:-

Online banking frauds are one of the reasons for the people or potential customers tend to avoid online banking, as they perceive it is being at risk to fraud. Banks try their level best to provide security measures for online transactions .But sometimes it may lead to unsafe and insecure.

We have gathered data from 40 customers of Axis Bank and Bank of Baroda.

Scenario 1

Bank of Baroda: - It is nationalized bank. It was started in 1908 and has been a long and eventful journey of almost a century across 26 countries.

There are two passwords for making transaction. One is Login password and second is transaction password.

Problems:-

1) It may lead to risk in the following situation
   - 1.1) when customer uses other computer or cyber café.
   - 1.2) when password is lost.
   - 1.3) when internet and network data is hacked.
   - 1.4) when customers respond to phishing mail.
2) The current method of using only one factor of authentication definitely has its weaknesses.
3) The fact that a wrong click can cause monetary losses may be a deterrent.

4) One of the measure and unnoticed drawback of online banking is if one is asking for help on internet baking to customer care and if official customer care executive asks for password and provide it to fraudulent. Then one's money at risk without his/her mistake.
5) The internet is supposed to make things faster but there can be unnecessary delay due to technical difficulties.

Scenario 2

Axis Bank: Axis bank is first of all private banks to have begun operations in 1994, after the Government of India allowed new private banks to be established.

There are three passwords necessary for transaction. One password is for login. Second one is transaction password and third password for net secured purpose is sent via SMSor email.

Problems:-

1) If there is problem of network coverage for SMS, then customer have difficulty to make transaction at that time.
2) It is expensive for bank to send SMS.

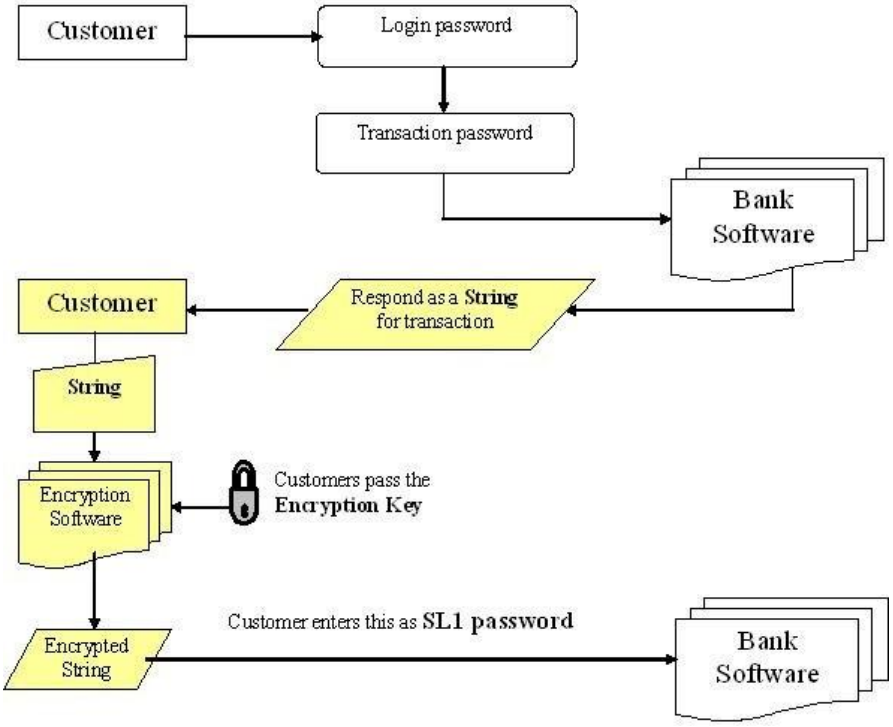
Methods:-

To fix the errors or loopholes of existing scenario we have proposed two methods forsecurity.

Security Level 1:-

1. There are three passwords i.e. Login, transaction and SL1
2. Login and transaction password both are provided by bank and SL1 is usergenerated password.
3. Initially user login to his Bank account by using Login password.
4. For transaction user provides second or transaction password.
5. After successful authentication of these passwords bank software will replay with normal string to user.
6. User possesses encryption software along with encryption key provided by Bank(provided required encryption software is installed on user machine/mobile.)It is also available on bank's website.
7. User will enter that string in encryption software and pass encryption key.
8. User will get encrypted string from that software and this encrypted string is SL1 password which is generated by user.
9. After authentication of SL1 password transaction will proceed.
10. An encrypted string will be different for different users depending on the encryption key provide to that particular user, so one software generate dissimilar output.

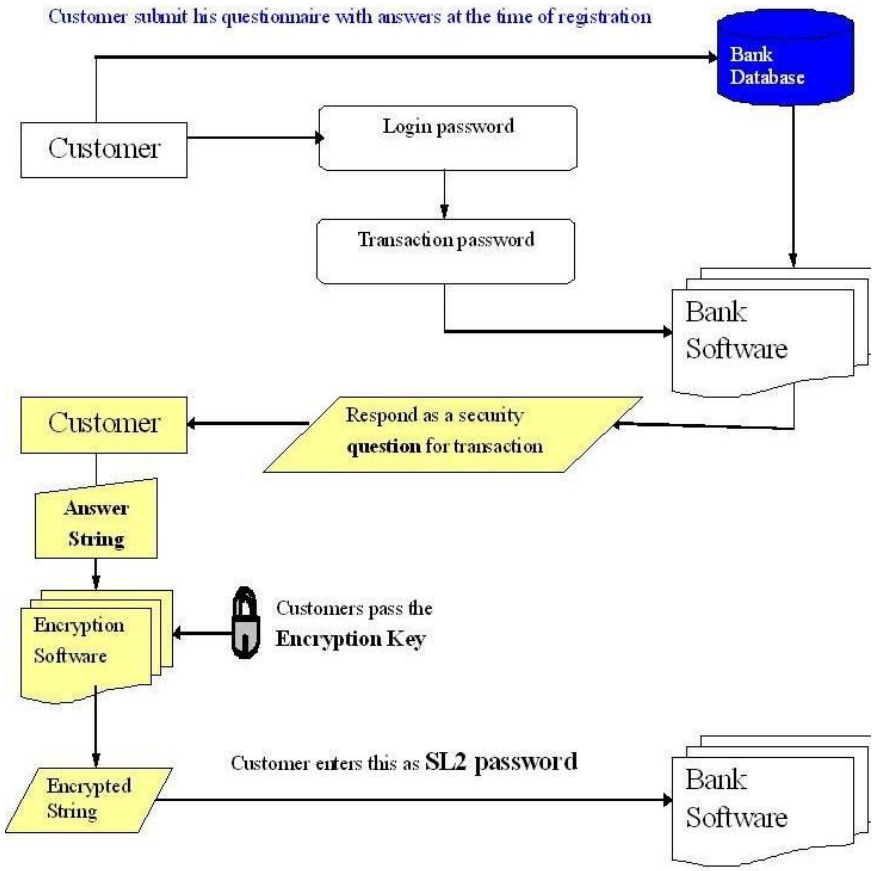
Security Level 1:



Security Level 2:-

1. There is list of questions with their answers such as birth date, vehicle no, phone no, pin code, anniversary date, fax no, PAN no etc which is provided by user atthe time of account opening.
2. There are three passwords i.e Login, transaction and SL2
3. Login and transaction password both are provided by bank and SL2 is usergenerated password.
4. Initially user login to his Bank account by using Login password.
5. For transaction user provides transaction password.
6. After successful authentication of these passwords bank software will replay with **one question** to user and answers to these questions already with the bank (bank software will replay with randomly selected question from list of question mentioned above to user.)
7. User possesses encryption software along with encryption key provided by Bank (provided required encryption software is installed on user machine/mobile.)It is also available on bank's website.
8. User will enter that answer to encryption software and also pass encryption key.
9. User will get encrypted string from that software and this encrypted string is SL2 password which is generated by user.
10. After authentication of SL2 password transaction will proceed.
11. An encrypted string will be different for different users depending on the encryption key provide to that particular user, so one software generate dissimilar output.

Security Level 2:-



Suggestive Measures

Customers

1) The most important thing for customers "To do the right things in the right way at the right time"

   Customers can also follow some simple precautionary measures as suggested below.

   1. Install anti-virus, firewall, and anti-spyware programs on your computer andkeep them up to date.
   2. Regularly check your online account balance for unauthorized activity.
   3. Avoid situations where personal information can be intercepted, retrieved, or viewed by unauthorized individuals.
   4. If you receive email correspondence about a financial account, verify its authenticity by contacting your bank or financial institution.
   5. Before setting up any online bill payment, check the privacy policy of the company or service you will be sending payment to.
   6. If you have disclosed financial information to a fraudulent web site, file reports with cyber crime branch of police

2) Customer can get stuck due to connectivity, congestion in the computer and telephone network and technical difficulties. On the other hand, in normal banking, you can simply converse with the bank officials to sort out any problem.

3) Most of the customers don't know how to use internet banking. They prefer personal interactions rather than internet banking.

Banks:-

1) Use multiple password that's increased security threads with also encryption and decryption software
2) Registration and enable online account process should be fast.
3) Web server speed should be fast.

Conclusion

Online banking involves certain risks. It is important to educate yourself about these risks, how unauthorized access to your financial information occurs, and the preventive measures one can take to protect your financial information. Learning about your liberties and tasks as an online banking consumer can make a difference to your financial needs sothat every customer can say online banking is easy to use and keep your money safe by saving time.

Reference

1. Network Security and Management –Brijendra Singh, PHI learning Pvt. Ltd.
2. Bobibanking.com:-https://www.bobibanking.com/
3. http://www.axisbank.com/24x7banking/internetbanking/Internet-Banking.asp