One Time Password Security through Cryptography
For Mobile Banking

Dr. D.S. Rao, Gurleen Kour, Divya Jyoti
MM University
Mullana, Ambala, -133203, India
Dr.dsrao1@gmail.com

Introduction

Electronic banking- which provides the economic services through internet- changed the business trade of banks drastically, also decreasing the cost and improving the ease for the user. Highly usage of phones in which internet is enabled makes the change of banking operations to mobile phones from desktop computers - a reasonable growth of electronic banking. This newly formed banking which a division of electronic banking is called mobile banking. The mobile banking is explained as: “the execution of financial services inside an electronic procedure- where the customer utilizes the mobile statement methods in combination with mobile devices” (Key & Martin 2004). Mobile banking allows the user to access services give by banks without any constraint on location and time- access the services at anytime and anywhere. Security is the main problem in mobile banking, because it uses simple authentication mechanisms which are easily accessed by hackers. Another problem is when customer enters into new location it is difficult for the user to find location of nearest banks or cash machines.

Background

Since the last decade the number of users using the internet banking increased rapidly, so this makes the developers to create to develop more suitable methods to perform baking transactions remotely. Mobile banking is the new convenient scheme for the customers to access all the services offered by banks. The foundation for mobile computing is the security. As mobile banking services grow, the defenceless handsets and associated platforms will become the targets for the hackers or criminals who were try to attack. Mobile devices present many of the same risks as Internet banking (Jin and Xianling 2008).

2: Literature Review

Electronic commerce (EC) electronic banking is the one of the most successful business to consumer applications. Satisfying the customer needs using EC reduces the spatial and temporal limitations. Banks uses e-banking because this not only satisfy the customer needs but also it reduces they had more economic advantage replacing the highly paid bank clerks with central web server which costs less. At the same time internet enabled mobile devices and PDAs becoming the most popular. Since people consider that cellular phone is a personal dependable tool and it becoming the essential thing of their lives, and almost all the devices are capable of using internet,
the usual conclusion was the alteration of banking operations to the cellular phones was the subsequent move in the development of electronic banking (Key & Martin 2004).

Mobile banking (M-banking) has more advantages than the electronic banking: these devices can be accessed at anytime and anywhere, mobile devices provides more security than personal computers, the high infiltration of mobile phones achieves all levels, and the income and loss account is moreover favourable: for instance bank transaction via clerk costs 2 US $ where as transaction using mobile banking application costs only 15 cents (Key & Martin 2004).

2.2. Operation of Mobile banking

The mobile banking system includes data processing centre and mobile banking unit; the data processing unit may be a mainframe for storing the data and processing the transactions. The mobile banking includes different terminals like ATM machines, number of wireless connections from handsets/PDA’s and so forth. A typical architecture of mobile banking is shown below.

Figure 3: Mobile Banking Operation System. [Jin and Xianling, 2008].

In this operation customer send the request or perform some action in application which installed in Handset or PDA. The request is then transmitted to Mobile Operator which provides the mobile services to the customer using wireless transmission protocols. The request is then transmitted to the Banking system using internet from Mobile Operator. Similarly the response for the request is transmitted to Mobile Operator from banking system. From the Mobile Operator the response is transmitted to customer of the bank (Jin and Xianling, 2008).

Mobile banking offers good basis for providing customer - oriented and personalized financial services with new model, which comprises more channels to provide wireless communication.

2.3. Security zones in Mobile banking

In mobile banking the financial services which were performed using wireless transmission have been targeted by many attackers since its emerging. The following figure shows the security zones of Mobile Banking.

Figure 4: Security zones of Mobile Banking. [Jin and Xianling, 2008]
Mobile Banking has two security zones as shown in above figure. The first security zone is called Mobile security zone which is lies between mobile devices and mobile operator. The second security zone called Banking security zone and it is lies between mobile operator and banking system. The security issues related to information were happened in these zones only for example virus attacks, hackers and so forth (Jin and Xianling, 2008).

Developing a Mobile banking application to provide secured banking services.

3.1. Objectives:

Analyse and research the existing services provided by the banks like account information, account transactions, transaction history and so forth. Understand different authentication mechanisms provided by the banks. Create as well as plan a set of models for the practical implementation of the system. Importance need to be given for building a software application model for performing high security mobile banking application.

3.2. Future Work:

As an enhancement to this application, it can be possible to provide more security by identifying whether customer who is using the application is registered with the same mobile during the customer registration. This enhancement provide to check whether the application used by authenticated user or not. One more enhancement is to this application is – using the GPS (Global Positioning System) to provide location based service. This enhancement makes the customer to easily navigate to the location using route maps.

4.1. Intellectual Challenge

The important challenge for this proposal is to construct proposed system which is a mobile banking application.

- In existing m-banking applications, for authentication they used simple login mechanisms containing user id and password, which are easily accessed by hackers. Therefore the application should develop in such a way that it allows the user to enter some memorable information which is provided by the user during the registration.

In existing system, while performing the transaction it consumes much time to complete it. Therefore the application should reduce the time required to perform the transaction.

In the existing system, location based services are offered using SMS alerting system but not providing any GUI to track the location of the nearest bank and cash machine locations.

4.2. Project Research Methodology

Gathering the information about different services provided by bank for customers. This involves: Analysing the existing mobile banking applications and collecting the information from the customers and employees of the banks to know their views on these applications.
The received knowledge can be applied while implementing the Mobile banking application.

Collecting the information about different authentication mechanisms provided by the banks using the bank websites. Developing mechanisms to track location of the banks and cash machines. Developing secure login (Authentication) mechanism, which uses memorable information as key to entering into the application. Developing the application which include above mentioned services as well as general banking services like knowing account information, performing transactions, checking the transaction history and so forth.

5: IMPLEMENTATION

Implementation of One Time Password:

The Main Security implementation of our project is the concept of One Time Password i.e. every time a new password is generated and sent to the user on his mobile phone. One Time Password is a Random 6 Digit Number that changes every time, when ever user logs on to the system and performs some transaction. The Concept has been implemented in a such a way that it adds high level of security to our banking Application.

The Implementation of concept is as follows:

The user when he logs on the Online Banking Website from his Mobile of Computer gets a screen that just prompts him to enter his username. Once he enters the username the user is redirected to another screen where along with his Password is prompted to enter the One Time Password. The OTP meanwhile has been delivered on to the users registered mobile number that user had provided at the time of opening the account with the bank. The OTP is valid only time every next time user logs in he needs to provide an new OTP that the user would have received at that particular moment of time. Now when a user is performing an transaction such as Fund Transfer, again an OTP is sent on to his mobile that he needs to complete the fund transfer.

Thus this OTP becomes the most secure way to implement security in Net and Mobile banking applications as even if the password of a customer is compromised but using this OTP he is secure in the sense that the other password that he/she need to log in or perform a transaction will only be sent on to his mobile phone.

Business Logic behind OTP:

When ever user logs on to Mobile Banking or Net Banking Website and enters his users name a function is called that generates a Random Six Digit Number and passes the Number on to another function that first queries that database for the mobile number, thats associated with the particular username after getting the Six Digits Code and the Mobile No. the Function calls Push SMS API that provides our application connectivity to the Mobile Network and
Sends the Six Digit Code to the Mobile Number of the customer.

Now in the Mean time the customer has been transferred to new page where he need to enter his banking password along with this OTP that he has received on to his mobile phone. The user enters the Password and OTP on the screen and after that the password and OTP are encrypted using SHA1 cryptography technique so that they are not traced by any TCP/IP packet sniffing application and at the server end this Password and OTP are compared to the Password that is stored in the Database and OTP that was generated by the application respectively. Once both are authenticated then only user is allowed to proceed further. The Main Classes that we are using for this Module are:

1. System.Net.Cryptography: This Class a core class from Microsoft.Net SDK provides us access to Encryption Mechanisms
2. SMS Send Class: This Class is a Part of SMS API we have been Provided by the Push SMS Service Provider. This Class provides methods for Sending SMS’s on GSM as well as CDMA network.

6: CONCLUSION

This application is only a model to show how security in mobile banking can be improved and more work is needed after running and launching attacks on the system in a real time environment. This application is a working model that can be developed to become an important tool for banking customers. To increase the security of the system by being cost-effective, the design architecture can be optimized by identifying the various types of attacks and providing protection against such attacks. A certain level indication of security in the system has been provided by trying a reasonable set of test cases. Further tuning and testing of the application is necessary before the system can be implemented in real-time for meaningful purposes. The application testing in this scenario has been carried out under true operating conditions. In implementing this application most time consumed when developing location tracking system. This is because a separate mechanism is developed to provide this future to customers of the bank.

References.

