Enhancement of Security in Mobile Banking Applications

Mr. Mayur Waghmare[1] Ms. Priya Golekar[2] Mr. Akshay Hatwar[3] Ms. Rushali Parimal[4] Ms. Akanksha Hiware[5]
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]RTMN University, India

Abstract— Mobile Banking is an option which gives user the possibility to perform various banking operations such as account transaction and other basic services available daily in banks through a mobile device such as smartphone or tablet. The security and privacy of sensitive financial data is one of the main concerns in acceptance of these systems all over the world. It is specifically important to secure the transmission of the financial data between the financial institutions' server and the mobile device used by consumers, as their communications are via unsecured networks (Internet). In this paper, a trust negotiation approach is proposed to address these security concerns. Trust negotiation is combined with the Transport Layer Security (TLS) as the underlying protocol. This combination of technology aims to maximize the existing security of m-banking applications. It results in significant improvements in security compared to the traditional identity-based only access control techniques. The proposed approach is implemented as a mobile application.

Key words: Security, Mobile Computing, Mobile Banking, Ubiquitous Access

I. INTRODUCTION

Nowadays, Mobile phones are not only used for communication purposes i.e. making and receiving phone calls or sending text messages, but are also used for variety of day to day works such as an information distribution platform. The growing use of smartphones have replaced the computer-dependent transaction applications with the mobile transaction applications. Mobile cellular subscriptions reached approximately 6 billion worldwide in 2011 [1]. Mobile banking (or M-banking) is the most popular medium for carrying out mobile transactions. Mobile banking is the service that allows a user to freely access his/her bank account through his mobile device. The main reason for why mobile banking is preferred over e-banking is its convenience, ease of use, portability and reliability. The availability of access and no place restriction, are among the main factors that help in saving customer time and reducing their expenses. However, given that mobile devices may be vulnerable to threats, attack and loss, so the security and privacy of sensitive financial data is one of the main concern for acceptance of these system globally by many customers. Other aspects also need to be considered, such as content display, memory limitations and the ability to incorporate security features, which adds more complexity to the issue of adaptation. We propose a security approach for M-banking and a prototype solution which aims to secure the transmission and access to financial data over wireless networks through mobile devices [2]. This approach secures the communication channel and authenticates the user and the device in use.

II. MOBILE BANKING

Mobile banking (m-banking) is considered to be one of the most important mobile commerce applications currently available [2]. The ubiquitous access to data with no place restrictions helps to promote this technology. The security and privacy of sensitive financial data is one of the main concerns in acceptance of these systems in the world. It is specifically important to secure the transmission of the financial data between the financial institutions' server and the mobile device used by consumers, as their communications are via unsecured networks such as the Internet. In this paper, a trust negotiation approach is proposed to address these security concerns. Trust Negotiation is combined with the Transport Layer Security (TLS) as the underlying protocol. This combination of technology aims to maximize the existing security of m-banking applications. It results in significant improvements in security compared to the traditional identity-based only access control techniques. The proposed approach is implemented as a mobile application. It demonstrates that the developed application is easy to use and deploy in typical mobile environments.

Smartphones and other mobile computing devices are being widely adopted globally. The increasing popularity of smart devices has led users to perform all their day to day activities using these devices. Hence, M-banking has become more convenient, effective and reliable. It is extremely necessary to provide the security services including; confidentiality, integrity, and authentication between the financial institutions‟ servers and the mobile device used by the customer, as their communications are through unsecured networks such as the Internet. User's confidential information may be at risk due to fixed values-based security schemes, one level authentication, separate hard token-based authentication, hardware stealing, and Android-Based attacks. This paper specifies a comprehensive sought of how M-banking schemes can be assessed. Also it introduces a solution to mitigate most of these risks.

III. THE SECURE MOBILE BANKING APPROACH

The existing security approach for mobile banking includes only the identity-based only access control techniques such as username and password which are less secured and can compromise with the security of the financial data. Also the financial transactions through mobile devices are made through unsecured networks such as internet [3]. Through this unsecured connection the parameters used in the identity-based technique can be easily hacked by the attackers which will allow them to gain unauthorized access to user's data. Because of this reason most of the users are not comfortable in using their mobile devices for making financial transactions. Rather than this people prefer to visit the banks manually for carrying out their transactions. The ease of accessing the user's financial data from any mobile device other than the user's device is a limitation of the current system. With this, attackers can gain access to user's data by simply knowing the username and password of the user's account and then can easily have access to the account from other device.

The secure mobile banking operation starts by creating a secure session between the client's mobile device and the bank's server. The bank server is where the client's financial data is stored. This secure session is established using the TLS handshake mechanism. The TLS ensures that the data exchanged between the user and the bank server is encrypted which helps in protection against intruders. After establishing the secure session, the next phase is the authentication phase. In the first level of authentication the requester (client or user) is authenticated using a username and password, to the bank's server. Then in the second level of authentication, the user's mobile device is authenticated through IMEI and SIM serial number. The IMEI and the SIM serial number are field in the background without user interference. This all credentials i.e. username, password, IMEI and SIM serial number are combined into array and sent to the server side. The parameters in this array are then checked one by one by the server. If all the parameters are correct then the user is granted access to his/her financial account, otherwise he/she will be asked to enter the username and password again.

IV. DEVELOPMENT OF MOBILE BANKING APPLICATION

Our system consist of client and server application in which database management plays an important role description of our system is as follow.

- The first part is a client side application which has a graphical user interface which allows users to enter their credentials and request access to their accounts.
- The second part is the server side application which holds the user's financial data in a database. This database is responsible for generating the server's responses to the requests from the client side.

This application uses the TLS version 1.0 protocol for securing the communication between its browser and the web server (Apache). After establishing secure session, the client side application collect the username and password, from the clients, using the interface. It also collects the user's mobile device's IMEI and the SIM card serial number using the Telephony Service class and store them into variables as shown below,

```
StringSerial = ((TelephonyManager)getSystemService
(Context.TELEPHONY_SERVICE)).getSimSerialNumber()
;
StringIMEI = ((TelephonyManager)getSystemService
(Context.TELEPHONY_SERVICE)).getDeviceID();
```

This credentials collected from the mobile device, are added to the array along with the username and password previously collected. This array is then sent as a parameter with the string request, to the server side. The server proceeds with the verification process as described in fig.3

The server side application mainly consists of the class login.php which compares the received credentials with those stored in the database.

```
require_once('dbConnect.php');
If ($_SERVER ['REQUEST_METHOD']
=='POST')
```

Next the values extracted from the array are stored in PHP variables, as shown in the code below,

```
$username = $_POST ['username'];
$password = $_POST ['password'];
$serial = $_POST ['serial'];
```

Then the server proceeds with the verification process by verifying the client's username and password stored in the "$username" and "$password" PHP variables. The queries used for verification process is as shown in the following statements,

```
$sql = "SELECT * FROM volley WHERE
username = '$username' AND password = md5 ('$password')
AND serial = '$serial'";
$result = mysqli_query ($con,$sql);
$check = mysqli_fetch_array ($result);
```

If the server failed to verify the username and password, it generates an unauthorized message using the following statement,

```
If (isset ($check)) {echo 'success';}
Else {echo 'failure';}
```

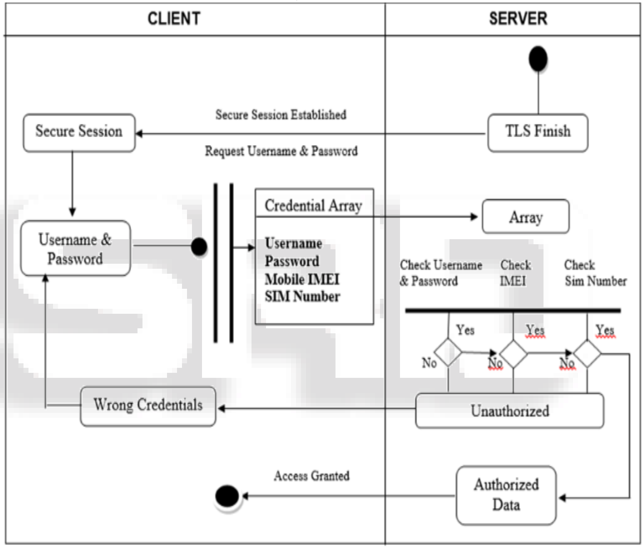

Fig. 3: Activity Diagram

V. CONCLUSION

In our work we provide financial clients with a mobile application through which they can access their personal or business accounts anywhere and at any time in a secure way. The proposed approach verifies the user and its device. It provides users an opportunity of registering their mobile devices and also gives the financial institutions a possible way to verify the users device. As we have provided two-levels of authentication, this clearly enhances the security of the existing m-banking systems by adding extra protection features to the authentication mechanism. It also enhances the user experience by minimizing the users' inputs. Although the mobile device emulator which is used for testing the application mimics all the hardware and software features of a physical mobile device, some possible problems might arise when a real mobile is used. This and others issues such as, performance and delays are among the limitations that need to be considered. Our future work will address these issues and other issues as well.

REFERENCES

[1] "The World in 2011 – ICT Facts and Figures", International Telecommunication Union (ITU) 2011.

[2] Tzong, et al. , "Adoption of mobile Location Based Services with Zaltman Metaphor Elicitation Techniques," Int. j. Mol. Commun. , vol. 7, pp. 117-132, 2009

[3] Mahmoud Elkhodr, Seyed Shahrestani, Khaled Kourouche, "A Proposal to Improve The Security Of Mobile Banking Applications", pp 3,2, IEEE 2012.

[4] Hisham Sarhan, Ahmed A. Hafez, Ahmed Safwat, A.A. Hegazy, "Secured-Android –based Mobile Banking Scheme", IJCA 2015.

[5] N. Mallat, M. Rossi, and V. K. Tuunainen, "Mobile banking services," Commun. ACM, vol.47, pp. 42-46, 2004