An Efficient Authentication and Payment Method for M-Commerce

Sukhjit Kaur
Post Graduate,RIMT Institutes
Mandi Gobindgarh (PB) –147301

Anuj Kumar Gupta
Associate Professor,RIMT Institute of Engg. & Technology
Mandi Gobindgarh (PB) - 147301

Abstract

Technological advances in mobile phones (e.g. Smartphones) have also made it possible to carry out e-commerce via mobile phones (m-commerce). M-commerce involves the use of mobile devices such as mobile phones and PDA's in carrying out electronic transactions.Just like e-commerce, the security of m-commerce applications is critical, especially when it involves applications that deal with user sensitive data such as credit cards details, medical details etc. Authentication and secure payment is a major security issue when it comes to carrying out mobile financial transactions remotely.However, the security issues that arise with the growth in this field cannot be neglected. For example, how does one ensure that participants in an m-commerce transaction are who they claim to be (authentication)? Also, how does one support secure financial transactions in m-commerce businesses? **Credit card fraud** *is identity theft in its most simple form. It can happen when your pre-approved credit card offers fall into the wrong hands. Acc to survey,The Federal Trade Commission estimates that 10 million people are victimized by credit card theft each year.The objective of this research work is to propose a secure platform-independent authentication and payment method for m-commerce applications free from Simishing attacks , Dictionary attacks etc. It is necessary to prevent Simishing and since its occurrence may affect the image and the potential customer base of a company.So security enhancement of mobile payment system is done and as well as modification of current authentication system. Apart from these proper SMS alerts will be given whether to proceed with the transaction or not with suitable timing constraints. The objective of research is to enhance existing authentication and mobile payment method to prevent from credit card fraud attack.*

1. Introduction

Applications in Mobile commerce domain range from normal information consumption to high security financial electronic transactions. Just like e-commerce, the security of m-commerce applications is critical, especially when it involves applications that deal with user sensitive data such as credit cards details, medical details etc. The technique of using PIN for authentication has been shown to have memorability problems. Users adopt non-secure behaviours to circumvent those problems. To improve the usability and the security of authentication, alternative techniques have been suggested. PIN authentication remains as the primary login technique across many (or possibly all) implementations of mobile banking. However, the security issues that arise with the growth in this field cannot be neglected. For example, how does one ensure that participants in an m-commerce transaction are who they claim to be (authentication)? Also, how does one support secure financial transactions in m-commerce businesses?

Figure 1.Frequent Usability of credit card

2. Literature survey

2.1 Introduction

It involved researching previous studies that were conducted in the area of authentication, as well as re-viewing what underlining techniques current existing authenticating systems use. To achieve this, the following research questions were looked into:

What are the security threats that are currently faced by m-commerce systems? What are the necessary security requirements that must be met by a platform-independent authentication and payment system? What are the current authentication methods/solutions available? What are the current payment methods/solutions available?

2.2 Types of Security threats

Security threats of authentication systems can be classified into two categories: malicious and non-malicious. Malicious security threat is a state when a system or a user deficiency is being exploited by illegitimate users with an intention to do harms. Phishing (or smishing6) attacks, for example, are a malicious activity made by attackers to trick legitimate users to give out their login passwords or personal information. The obtained information can be used to gain access into the user's accounts. Other common forms of malicious attacks against password systems are dictionary attacks, keystroke logging, and shoulder-surfing. Dictionary attack is a type of password attack that uses words from dictionaries to crack a user's password. Users tend to choose weak passwords ; therefore this attack is most efficient against authentication systems that allow users to choose personalized passwords without policy restrictions. A more exhaustive version of dictionary attack is brute force attack; it attacks a password by trying all possible combinations of password elements .

Figure 2. Example of Simishing Attack

3. Objective

The objective of this work is to propose a secure platform-independent authentication and payment method for m-commerce applications free from **Simishing attacks , Dictionary attacks etc. Credit card fraud** is identity theft in its most simple and common form. The objective is to enhance existing

authentication and mobile payment method to prevent from credit card fraud attack. Dictionary attack is a type of password attack that uses words from dictionaries to crack a user's password. Users tend to choose weak password, therefore this attack is most efficient against authentication systems that allow users to choose personalized passwords without policy restrictions.

4. Facilities required for Research Work

The authentication and payment method tested through Android emulator**.** Coding done in Java through Eclipse Software.

Figure 7. Android Emulator

5. Results/Conclusions of Research Work

The current mobile banking login method is PIN authentication. For a client to use mobile banking, the bank requires the client to register for the service. During registration, the client receives (or provides) a four or five digit Personal Identification Number (PIN) as a password. To access the service, the client is required to enter the correct combination of his/her identification (usually the account number or the mobile number) and the registered PIN to authenticate. Yet, this mechanism is unsatisfactory. The use of a text-based password requires a trade-off between security and memorability; the trade-off arises from the

limitation of human memory, and, as a result, passwords are easily forgotten. System security is often considered to be a technical issue. Before conducting a transaction, a client is required to login with a PIN (some systems may also require their users to input a valid identification), and only a valid PIN code will grant the client access to the service.   In public key encryption and other authentication methods , proper authentication of user is missing. So security enhancement of mobile payment system is done in this work and as well as modification of current authentication system is done .

Results

Step1.Username and password will be provided for login. 2. User will enter the registered PIN to authenticate.3. To prevent simishing , dictionary attacks from attacker , an SMS alerts (For example within one minute a user has to reply with yes or no to enable transaction to execute.)will be given whether to proceed with the transaction or not with suitable timing constraints(1 minute). (Reply in Y or N).4. User has to reply with Y or N to enable transaction to execute.5. SMS will be generated to genuine user to his/her registered mobile number (regarding attacker's location or phone no. credit card no. etc).6. If the attacker is going to do M-Commerce transaction then transaction will not execute.
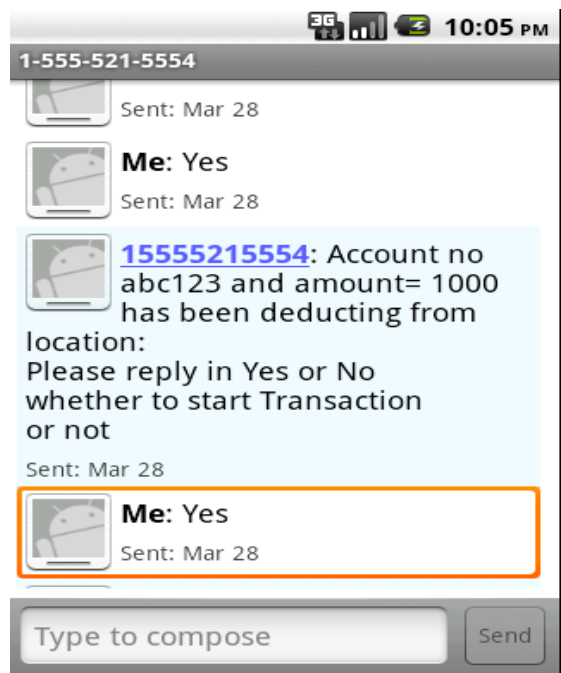

Figure 5. Time given for confirmation(1minute)
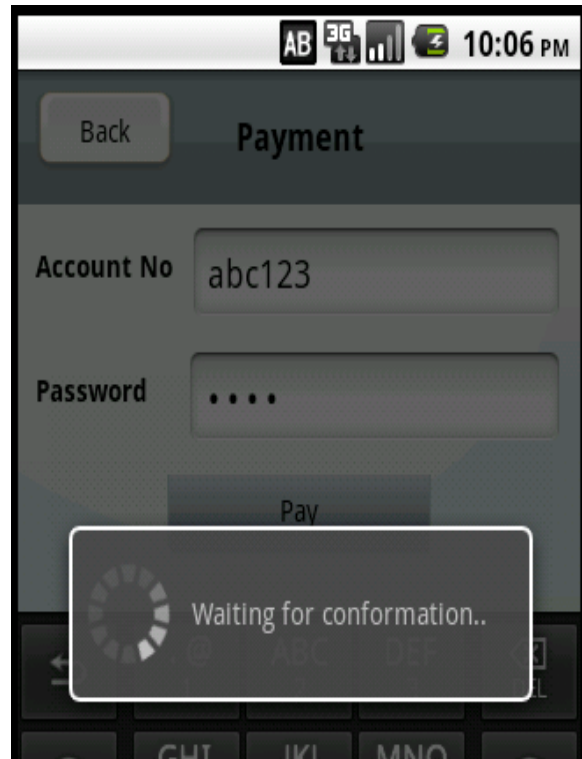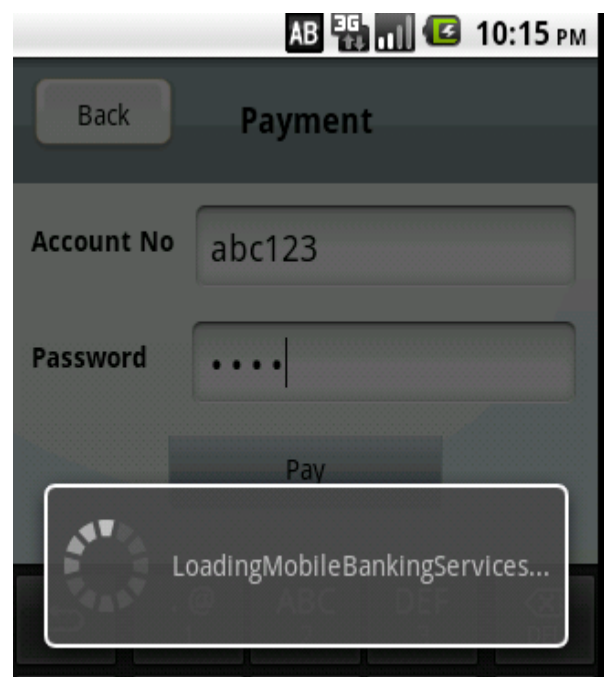

Figure 6.Successful Execution Starts

   Figure 4.Based on user reply 'Yes'via SMS

6. References

[1]http://www.android.com/

[2 http://www.androiddeveloper.com/

[3]http://developer.android.com/guide/topics/location/obtaining-user-location.html

[4]http://developer.android.com/guide/developing/tools/emulator.html

[5]http://developer.android.com/resources/tutorials/hello-world.html

[6]http://mobiforge.com/developing/story/sms-messaging-android

[7]http://mobileprogramming.com/

[8]http://www.youtube.com/watch?v=EfTkDg9cC0c