GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

A MULTIFACTOR SECURITY PROTOCOL FOR WIRELESS PAYMENT-SECURE WEB AUTHENTICATION USING BIOMETRIC CHARACTERISTICS AND SMS

Pawandeep Singh Aujla & Harneet Arora
Dept. of Computer Science & Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab

Abstract

In this we uses a Biometric property of user for authentication and SMS (short message service) to enforce an extra security level along with the traditional Login / password system. Biometric properties are needed when a user wants a transaction then the user gives their fingerprint information. This method keeps the biometric properties as a secret code. A user creates the biometric properties on their Mobile device with the help of fingerprint scanners. Then the pre-installed application creates an image of the fingerprint. This technique is not a one-time password technique, it can be used as more as user wants. This code is used to initiate secure web transaction using cell phones. In this we use SMS service as a third authentication i.e, the user give their cell no. to the bank , which further receives message and that message gives the pin code no. which will be used for completing the transaction. Finally we extend the system for two way authentication which authenticates both parties (user and e- service provider).

Keywords— *Protocol for Wireless Payment, SMS (short message service), and Fingerprint Scanner*.

1. Introduction

Set is secure electronic transaction. It design to protect credit card transaction through internet it provide the security and authentication by registration. Set protocol permit user or customer who wants to make credit card payment to any of the web based services. It is a useful protocol for message exchanging between three parties: cardholder, merchant, payment gateway.

Some pseudo –code is used in this protocol-

C---------M: initiate request
M---------C: initiate response
C---------M: purchase request
M-------MB: Authorization and capture request
MB------CB: Authorization request
CB------MB: Authorization response
MB-------M: Payment Ack.
M---------C: purchase response

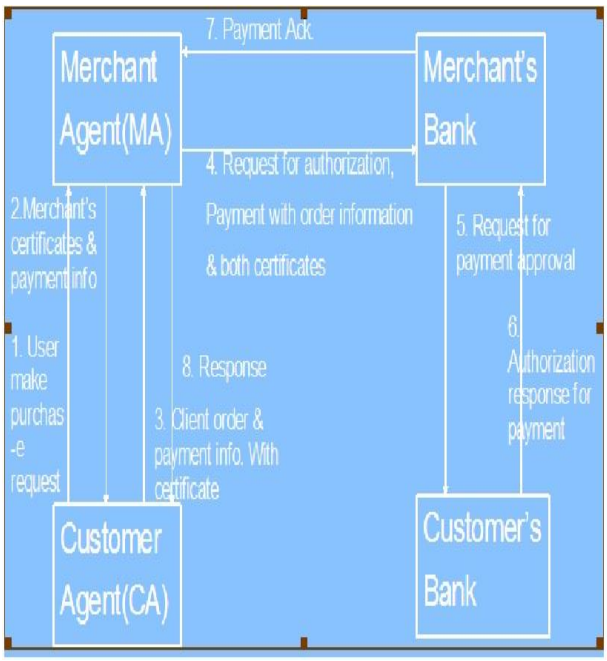

Fig.1. Transaction flow in SET

A brief description of the SET protocol, as depicted Figure 1, is described below:

1. The customers visit the merchant's web site to select various goods for purchasing and get the total cost of all the selected goods, including taxes and shipping costs.
2. The system asks for payment method and the consumer chooses to pay through a credit card using SET.
3. Special software on the consumer's PC, called Digital Wallet, is invoked and it give choices to customer to select one credit card from the list of credit cards issued to customer.
4. The consumer selects the card to make payment, and the electronic transaction take place based on SET protocol.
5. After getting details of customer payment the merchant contacts the merchant's Bank for customer authorization and payment.
6. Merchant Bank will contact the customer's Bank for the same and get approval of payment.
7. Merchant will notify, if transaction is successful.
8. A few seconds later, there is a confirmation to the customer that this order has been processed.

Some disadvantage of set protocol is:-

1) Set is only design for wired network. It not support fully wireless network.
2) Set is end to end security mechanism which means it requiring traditional flow between customer and merchant.
3) All the transaction is flow from the customer to merchant so that it increases the risk of middle attacker. So that at the middle all information can be copied.
4) No one notification received from the customer bank to the customer after successful transaction.
5) Set protocol is only for card based not support account based payment system. So that we use a two way authentication protocol.

2. Related Work

2.1 Multifactor Authentication

Single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. To provide secure web transactions using cell phones multi factor authentication techniques have to be used. In our system we are using multi factor authentication using two different modes. The implementation is performed using Biometric Properties and SMS. While SMS has been used in previous approaches to the problem, we are introducing the new concept of Biometric Properties as a novel method of authenticating a transaction and the user.

2.2 Biometric Authentication:

Biometric Authentication is the technique which is used to identify both the user and the ongoing transaction. It certifies that the current transaction has been initiated by the right person and it is a valid user who is trying to access his/her account.

Biometric Identification is:-

* Image of finger-print is created by user itself.
* Image is generated with the help of inbuilt finger-print scanners on the devices which are used by users.
* This image is encrypted using public key cryptography before send through the wireless media.

The Bank or Financial institution will keep a record of users finger-print and match the same during the online web transaction.

2.3 SMS Authentication:

Another method to validate user transaction is an SMS confirmation. The Bank or financial institution stores user cell phone number to provide multifactor authentication. We believe that users will carry their cell phone and can receive and send the short message. As a result, only valid users who have account will receive confirmation SMS from the authentication server. After getting an SMS with secret code then the user can acknowledge the choices. When authentication server receives right secret code, it knows that the user is valid and the user has approved their initiated transaction. On the other hand, if the user sends a wrong secret code or the user does not send any response within a specified time period then the transaction will be rolled back and terminated.[1]

2.4 Secure Web Authentication Protocol

This shows the Protocol for secure web authentication using Mobile devices. This protocol starts with the action of money transfer decided by user. Here we assume that the user information is available at server which includes user's cell phone number. A separate authentication server is recommended to maintain strong security to authenticate users and their transactions with regular web and database servers of user information.

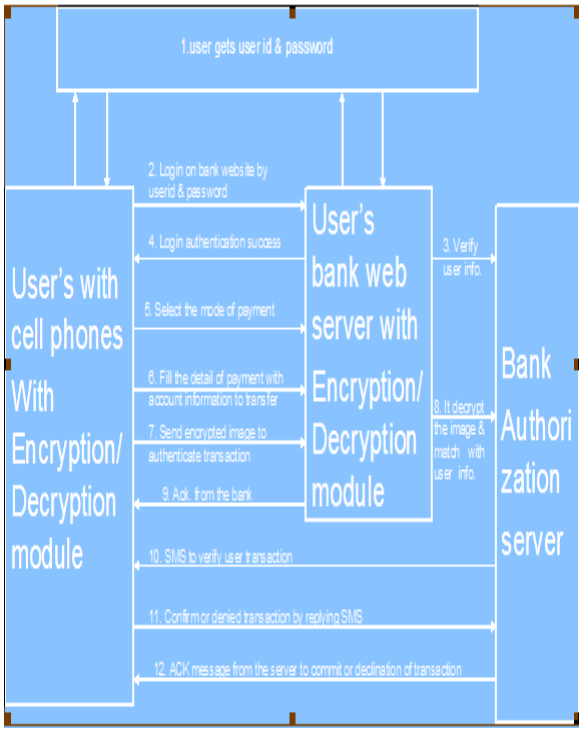

Fig.2. Multifactor secure Web authentication protocol using mobile

Below we describe each step of the above protocol.

1. User gets username & password from the Bank. Each user has only one username/password to their account.
2. A Web-based username/password basic authentication is used to identify the user to the Web server.
3. The username and password will be verified by the Bank Authentication Server. After user recognition the user will get option screen to proceed further.
4. The user will get a notification of a successful logging with welcome message.
5. The user will select mode of payment. We have considered two modes of payment: Credit Card based system & Account based Electronic transfer. It is straightforward to add other modes to our system.
6. User will insert the details of payment by filling in a simple form with details such as merchant's bank and branch code information, invoice number and account number to which an amount has to be transferred.
7. The user generate a image of finger-print using finger-print scanners which is inbuilt in the mobile device. All details of the transaction, with attached image, will be submitted to the bank web server. The bank web server would pass it on to the authentication server where it would be matched with the finger-print image which is stored in the users information on server side.
8. The bank authorization server received the message. It then verifies the image received from the user by comparing it with the stored image in the user account information at server database. If both images match then it goes to the next step. If no image matched with those in database then the authentication server will deny the user transaction and display appropriate error message to the user.
9. Bank server generates an acknowledgement to the user, which makes user free to logout from the web portal and wait for a confirmation SMS or to initiate another financial web transaction.[1]
10. After completing the database updation with respect to the ongoing transaction, the authentication server will send an SMS to the user's cell phone to verify the initiated web transaction. The cell phone number of the user is available on authentication server.
11. The user would confirm their initiated transaction by giving right secret code or deny it by wrong secret code by replying confirmation SMS.
12. The server will notify the user by a Message to acknowledge the successful completion of transaction or declination of the transaction.

4. Factors of authentication

Online banking fraud- The Internet is a medium which allows large number of people or organizations to communicate with each others in a few seconds, without much efforts and charges.

Now online fraud is very popular all over the world, it has become a major source of revenue for criminals. The banks or financial institutions are very attentive in detecting and preventing online frauds.

4.1 Key types of online fraud:-

The Online fraud has been categorized broadly into two categories as mentioned in User identity theft:-

 Phishing attacks which trick the user into providing access information. Key-loggers and "spyware" which clearly capture access information.

User Session Hijacking:-

Attacker gets control over the active user session and monitors all user activities.
- Local malware session hijacking attack performs host file redirection.
- Remote malware session hijacking attacks performs.

Authentication Methodologies :-
Existing authentication methodologies have basic three “factors
- Know: The user knows (password, PIN);
- Has: The user has (ATM card, smart card); and
- Is: The user is (biometric characteristic such as a fingerprint).[2]

5. Security Requirements Met by the Proposed Protocol

Multiple Authentications: In our research work we use three authentications which will guarantee to increase the security level.
Party authentication: As we use multiple authentication system, only those users are authenticated which are authorized, so the receivers ensure that the right user is authenticated.
Transaction privacy: All the transactions are going through authentications, hence the privacy is guaranteed.

6. Comparison of our Technique and Older Techniques

Authentication Comparison	Single Authentication	Double Security System	Our Authentication Technique
User name/password	✓	✓	✓
Biometric	✗	✗	✓
SMS	✗	✗ only confirmation	✓

So in the previous page we are comparing the three different general techniques of authentication in which we discuss single authentication, double security system and our technique of authentication, so in the single authentication technique which we are using generally now a days that we use user name/password for authenticating the valid user. So as there is only one privacy gate this is no more secure.

So to provide a security some researchers gave double security system technique, so in this the older user name/password technique is there but a addition of SMS confirmation which gives the confirmation message to the user , so this technique is also not secure because message received by user after the completion of work so there are some drawbacks . So to remove the drawbacks of above technique we develop the idea of triple authentication technique. In this we use older user name/password, fingerprint authentication and SMS authentication. In this message received by user which gives secret code with the help of this code user can authenticate.

7. Conclusion

In online payment security is a major part. There are many internet threats that affect the security system of internet. single factor authentication increases risk in communication because it require only username and password so that any attacker hank this information and treat as a valid user, that’s way use the multifactor authentication like a two way authentication technique is used for this purpose so that it reduce fraud and provide strong security application for online transaction. The implementation of this protocol will not increase expenses of users significantly. This protocol can be easily implemented and executed on the current expenses charged by financial institution from the users to perform online payments or with very less addition to the current charge of online payment. Basically, the cost model of the proposed protocol depends mostly on the policies that financial institutions adopt for implementing this protocol.

8. Future Work

Future work will focus on developing a new and efficient way of using biometrics characteristics using cell phones/PDA. Finger-print scanning is efficient on the user’s device with the help of appropriate scanner so that user send correct information to the bank or financial institution. Another future work is that to make fast and efficient matching algorithm to match the fingerprint image fastly and efficiently. Server side maintenance, management mechanism and distribution to satisfy the demand from a large number of users are also part of future work.

References

1) Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Sugata Sanyal and Knapskog, "A Multifactor Security Protocol For Wireless Payment-Secure Web Authentication using Mobile Devices", IADIS International Conference, Applied Computing 2007, Salamanca, Spain, pp. 160- 167, February 2007.
2) Lawton G., "Moving Java into Mobile Phones", IEEE Computer, Volume 35 Issue 6, pp.17- 20, June 2002.
3) Jablon David P., Integrity, Sciences, Inc. Westboro, MA, ACM SIGCOMM, "Strong Password –Only Authenticated Keyexchange",Computer Communication Review, Vol. 26, pp. 5 - 26, September 2005.
4) Pointcheval D. and Zimmer S., "Multi-Factor Authenticated Key Exchange," in Proceedings of Applied Cryptography and NetworkSecurity, pp.277