Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 2; January-March, 2015, pp. 112-116

http://www.krishisanskriti.org/jbaer.html

A Three Tier Novel Approach for Secure user Authentication and Online Payments

Ankit Dhamija[1] and Deepika Dhamija[2]

[1]Amity Business School Amity University Haryana
[2]Amity College of Commerce Amity University Haryana
E-mail: [1]adhamija@ggn.amity.edu, [1]dhamija.ankit@gmail.com,
[2]aghi.deepika@gmail.com, [2]ddhamija@ggn.amity.edu

Abstract—*The growth of the Internet continues to have a tremendous influence on businesses. Companies and organizations of all types and sizes are rethinking their strategies and how they run their operations. The sudden rise in so many e-business ventures is the proof that e-commerce is here to stay and will be the first choice of shopping as people have no time left to visit stores by burning fuel, stand in queues for billing and come back totally exhausted. Thus, rise in e-commerce has made shopping easier for users but at the same time, it calls for safe and secure techniques for making payments online. Today, users are finding it difficult to remember multiple username-password combinations, hassle of entering the debit/credit card numbers and pins each time they want to shop.*
This paper proposes the concept of a third party Authentication Service Provider (ASP) which will develop a biometric fingerprinting device, a one touch device for making payments. In this scheme, the authentication and payment methodology proceeds through a three way secure process which combines the traditional username password combination with the biometric fingerprinting and one time password (OTP) scheme that makes the payment transaction safe and secure. The biometric fingerprinting device work as a standard device for all user requirements and making their payments for shopping, paying bills, buying tickets etc and all other similar purposes. Thus, the user doesn't need to remember multiple passwords, pins, card numbers etc for making payments. Also, the proposed scheme defies the possibility of phishing and brute force attacks where the intruders try to guess the pins/passwords entered by the user through key pressing.
The paper also demonstrates the four way relationship of interaction and interdependence between the ASP, client organizations, banks and the users.

Keywords: *Authentication, payment, ecommerce, security, intruders, password, biometric*

1. INTRODUCTION

The tremendous rise in the number of internet users, with so many services and applications on offer becomes the base for the growth of ecommerce vendors on the internet. Apart from convenience and speediness to shop, it's the trend that people are following as they are realizing the importance of time that gets wasted in moving out for shopping. However, this convenience comes with a price in the form of security threats, pain of remembering multiple username-password combinations, tiredness of entering debit/credit card numbers each time and so on. The two most important points where ecommerce gets vulnerable are the user authentication and the mode of payments

Authenticating users and establishing their identity becomes the core of security in any online interface. So, it becomes necessary that only authorized user can access the stored data and access further features on offer [1]. The server in a traditional password authentication scheme, allow or deny any remote user based on identity and password. In general, textual password schemes are the most widely used, but they have many weaknesses. These drawbacks denotes that the user find it difficult in memorizing long or complex passwords, and the security risks can be obtained by depending short simple passwords [2].

Passwords are prone to attacks such as dictionary or brute-force attacks because passwords are only a combination of the symbols that are present on keyboards. As a result, an intruder or malicious person may attempt all possible combinations until detecting a correct password; such type of attacks is called brute-force attack. Additionally, most customers tend to pick something such as phone number, favorite game, and name to use as a password as these things are easily to remember. Consequently, intruders can build a table of significant words to hack the system, which is named dictionary attack. Furthermore, by using the password based authentication, the users are still vulnerable from the malicious attacks such as on/off-line attack, replay attack, *Man-in-the-Middle* (MITM) attack [3].

The second most important aspect that affects the ecommerce growth is the mode of payment. The statistics in [4] show that India ranks second in the world among all online shopping users with 31 % and China topping the chart with flipkart, irctc, myntra, snapdeal and jabong being the most preferred sites for shopping[5]. However, the credit card frauds have

posed a bigger threat to the chances of expansion and adoption by the users and have exposed the security weaknesses in traditional credit card processing system. Because customers repetitively use the same card numbers on the web portal, it gets easy for attackers to steal them. It involves Packet intercepting where an attacker sniffs e-commerce packets during on-line credit card payment. In some cases, the attacker does not need to break down the possibly encrypted on-line payment packets (e.g., over Secure Socket Layer), but fools the customer into thinking that he/she is visiting an intended site but actually the attacker's spoofing site. It also includes Database stealing where to encourage easier purchasing; many merchants (who provide services to customers) choose to store credit card numbers in online databases [6]. A statistics reported that attackers broke into merchants' sites and stole databases of millions of credit card numbers [7]. The credit card fraud not only causes money loss but it also adds worry about online transactions and makes them hesitant in proceeding towards it.

This paper proposes the concept of a third party Authentication Service Provider (ASP) which will develop a biometric fingerprinting device, a one touch device for making payments. In this scheme, the authentication and payment methodology proceeds through a three way secure process which combines the traditional username password combination with the biometric fingerprinting and one time password (OTP) scheme that makes the payment transaction safe and secure. The biometric fingerprinting device will work as a standard device for all user requirements and making their payments for shopping, paying bills, buying tickets etc and all other similar purposes. Thus, the user doesn't need to remember multiple passwords, pins, card numbers etc for making payments. Also, the proposed scheme defies the possibility of phishing and brute force attacks where the intruders try to guess the pins/passwords entered by the user through key pressing.

The paper also demonstrates the four way relationship of interaction and interdependence between the ASP, client organizations, banks and the users.

The rest of this paper is organized as follows. The literature study and existing work exist in section II. The proposed scheme and its working are explained in detail in section III. The benefits of the proposed scheme are covered in Section IV. Finally, the Conclusion is presented in section V.

2. LITERATURE STUDY AND RELATED WORK

Viet et al. [8] proposed the first anonymous password authentication scheme that aggregates a password scheme with the *Private Information Retrieval* (PIR) scheme. The limitations of this scheme are that it requires the server to be passed a whole database to detect user and it cannot resist on-line guessing attacks.

Florencio and Herley [9] proposed a proxy web service that allows customers to arrive at web sites by employing a MITM proxy. The password customer is pre-encrypted and implemented as one-time passwords' list. Thus, the proxy cannot contain the passwords, but more correctly the keys with which the customers' passwords have been encrypted previously. This, however, is classified within a single-factor scheme. Moreover, there is a drawback to an adversary who misappropriates one-time password.

Y Li and X Zhang [10] proposed the concept of using One Time Transaction numbers to enhance the security in credit card payment by the use of hash function. However, this technique proved to be heavy in terms of server load due to extra computation of hash values.

J Liu *et al* [11] introduced a semi-trusted third party (S-TTP) to provide a fair commerce environment. S-TTP takes part in the protocol online and is not leaked any secure information about the business. The limitation of this approach is that they don't allow the user account to be created and thus the user can't get the required information if they want.

Rubin and Wright [12], augmented a credit card transaction with an additional connection between a customer and a card issuer. The customer card issuer communication must be secured, typically by SSL (otherwise CCTs can be learned by someone in the middle before their use). With a large number of customers connecting to a card issuer (or its server) with SSL simultaneously, the performance of the server will become a bottleneck: customers may have to wait long time for CCTs before or during purchase. Such a centralized solution with SSL does not fit the scalability of credit card service. In general, a server with pure function of collecting credit card numbers from customers is dangerous because it is vulnerable to single point failure, web site spoof, and DNS redirection.

3. PROPOSED SCHEME

In this section, we present our scheme which aims to provide a secure authentication mechanism as well as a secure payment method for the users. The purpose of the scheme is to give the users a simple, secure and a standard way of making online payments. The scheme involves the use of following entities:

AuSP: It stands for Authentication Service Provider. It can be any organization that provides a biometric fingerprinting device to the user for secure payments. It has tie-ups with the financial institutions like banks and merchants.

Merchant: Merchants are the companies where the user usually shops.

FI: Financial institutions like banks, which authorize payments and verify the bank account details as entered by the users.

Users: Finally, the users are the customers who will use the biometric device provided by AuSP, for making payments, on the web portal of the merchant

The AuSP is the most important entity in the whole scenario because he is acting as a mediator between the merchants, users and the financial institutions like banks. Each of these entities is dependent on or connected with the AuSP in some sense. At first, we propose a simple block diagram of our scheme which depicts the flow of the things and functionality in a very summarized and brief manner.

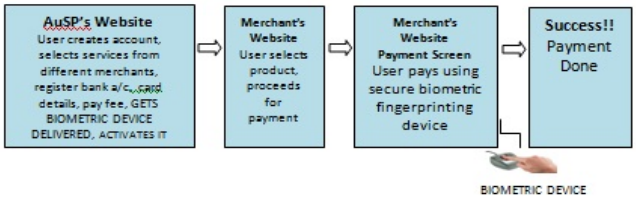

Fig. 1: Block Diagram

The Fig. 1 depicts the block diagram of the proposed scheme.

It consists of the following steps:

STEP 1: User needs to register at the AuSP's website by filling his details on the prescribed form which includes basic details including the bank account details and the fee for the biometric fingerprinting device. The user also selects the various services from various merchants listed with AuSP. The user pays the required fee through normal online payment. A username and password is allotted to him. On receiving the biometric device, the user log in to his account at AuSP's website and registers his device and fingerprints by inserting the device.

STEP 2: Now the user goes to the merchant's website where he wants to shop. The user selects product and proceeds towards payment.

STEP 3: On the payment screen at the merchant's website, along with all the normal debit/credit card or net banking options, the user also see a "pay using XYZ biometric device" option. The user selects that option "pay using XYZ biometric device"

STEP 4: User is asked to insert biometric device on the PC and give the thumb impression. The impression gets verified and the payment is successful.

In the whole process stated above, the user is not asked to enter any pin or password through the keyboard while making payments, which are prone to brute force attacks by intruders and malicious users. Instead, the user just has to insert the biometric fingerprinting device given to him by the Cloud Service provider and give the thumb impression on that device. With that, the user's identity gets established and it matches with the AuSP's database and the payment gets completed successfully.

In this next part, we present a more detailed explanation of our scheme which is categorized in two different segments: Biometric Device Activation & registration part and the usage part. In the first segment, we show the device activation and registration process of the user at the AuSP and we depict the use of biometric device. Finally, in the second part, after the user has been successfully registered with the AuSP, we'll show the process of making payment using biometric device when the user is at the merchant's payment page.

Biometric Device Activation & registration

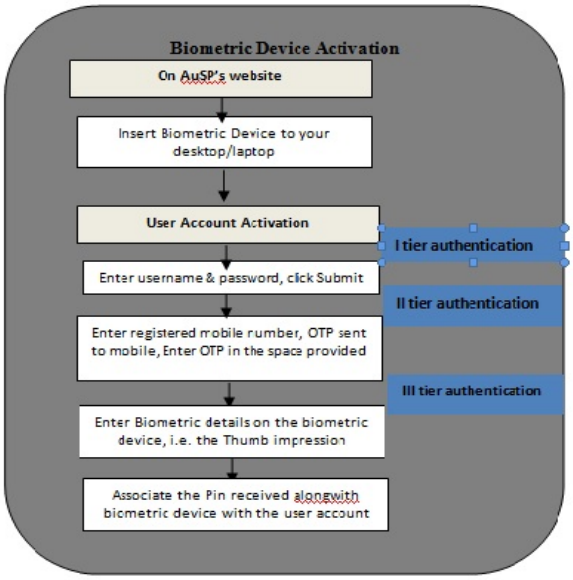

Fig. 2: Biometric Device Activation & Registration

Fig. 2 Describes the processof device activation and registration. It includes the following sequential steps:

STEP 1: After the user had received his biometric device kit, now is the time to activate that device. For this, the user goes to ASP's website and connects the biometric device with desktop USB port.

STEP 2: On the AuSP website, the user performs first tier authentication by providing his valid login id/username and password. On correct entry of the combination, the user is redirected to the next page.

STEP 3: On this page, the user performs the second tier authentication by providing the registered mobile number(RMN), an OTP is sent on this RMN and the user enters this OTP in the space provided. This the user's mobile

gets registered with the AuSP. The user is again redirected to the next page.

STEP 4: On this page, the user performs third tier authentication by entering biometric device details and by providing his thumb/finger impression. This thumb/finger impression is matched with the stored thumb/finger impression in the AuSP's database and on a correct match, it gets verified. Also, the pin is associated with the biometric account of the user.

Thus, all the three tier authentication steps took place during the Biometric device activation.

Now, after the device has been activated, the user can use it for doing shopping, booking tickets, paying bills, and so on. The user can do all such activities on those merchant websites which have tie-ups with the AuSp. It means that while creating the user account on the AuSP website, the user had chosen some merchants and the services provided by them. So now, the user can use this biometric device as a payment option on these merchant websites. In this way, the security of user transactions is strengthed because, the user will now give his thumb/finger impression and he is not required to enter all the passwords, card number and other details time and again. This saves users from phishing and brute force attacks. Fig. 3 shows this process of using the Biometric Device on the merchant's website.

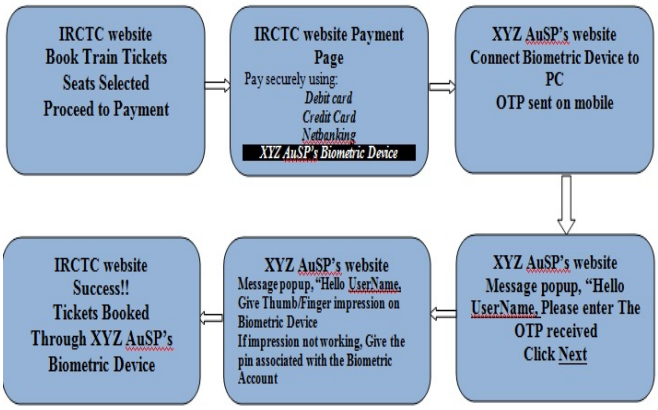

Fig. 3: Using the Biometric Device for payment

Using the Biometric Device for payment

It includes the following steps:
STEP 1: Imagining that the user is on a merchant website that is registered with the AuSP and try to book tickets. User selects the seats and proceeds towards payment.

STEP 2: Because the merchant is registered with the AuSP and the user, while making the account with AuSP had selected this merchant in its preferred list of merchants, the payment page of merchant website asks the user to proceed towards payment using several traditional options like debit/credit cards, netbanking. The user also sees a "Pay using Biometric Device" option. User selects this option.

STEP 3: The user is now redirected to the AuSP's website and is asked to insert his biometric device. The user connects the biometric device.

STEP 4: The user is asked to enter his registered mobile number (RMN). On this number, an OTP is sent by the payment server of AuSP. The user enters the OTP in the space provided and click "Next" button.

STEP 5: Now, the payment gateway asks the user to give his finger/thumb impression on the connected biometric device. The user gives his impression. If matched, the user is preceded further. If match fails due to some reason, the user is asked to enter the pin associated with the biometric device that is already registered with the AuSP in its database.

STEP 6: After all these checks and verification, the payment is made, the amount is deducted from the user's account and the user is redirected to the merchant's website with a message of successfully completed transaction and other related details.

Thus we saw from Fig. 3, the detailed functionality of the processes and Fig. 4 below depicts the relationships of all the parties involved in the whole process. All the involved parties are taking inputs, giving outputs and are dependent on each other.

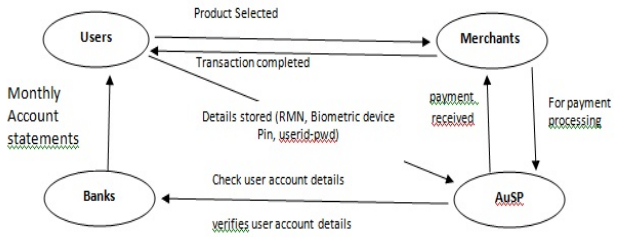

Fig. 4: Relationship of the entities involved

4. BENEFITS OF THE APPROACH

As we have seen the working of the proposed scheme, the benefits can be figured out from the working. First, the proposed scheme prevents phishing attacks from the intruders, i.e. the user is not required to enter pin/passcode in the textbox at the web portal, instead, they just needs to give an impression on the biometric device and they can login without typing. Second, it denies all the brute force attacks. Third, the scheme is much better than the costlier biometric schemes that are based on iris scan, face recognition techniques etc. Fourth, the complexity involved is much less than the other biometric based schemes. Fifth, it is an improvement over the hardware based OTP schemes as every second organization is using the

OTP based hardware scheme and it is much easier to crack but this scheme avoids all such possibilities. Sixth, the user is not required to remember so many passwords.

5. CONCLUSION & FUTURE WORK

In this paper we proposed a three tier biometric and OTP based authentication and payment scheme using biometric fingerprinting device where at the first level the user gets authenticated by using username password method and at the second level, the OTP is used to verify the user's identity and at the third level the user has to insert a biometric device for him to get authenticated and access the things and for making payments. We presented a detailed working of the proposed scheme in two steps- the REGISTRATION and the WORKING of the scheme process was explained in detail and we figured out a few benefits of the proposed scheme like it defies phishing attacks, brute force attacks, less costlier than other biometric methods and less complex than other hardware based methods like OTP. As for future work, the proposed line of research includes designing architecture for the mobile platform and devices.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol.34, No.1, Jan. 2011, pp.1-11.

[2] M. Zhou, Z. Rong, W. Xie, W. Qian, and A. Zhou , "Security and Privacy in Cloud Computing: A Survey", Proc. of the Sixth International Conference Semantics Knowledge and Grid (SKG'10), Beijing, China,Nov. 2010, pp.105-112.

[3] S. Shin, K. Kobara, and H. Imai, "A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange", IEICE Transactions on Fundamentals, Vol.E91-A, No.11, 2008, pp.3312-3323.

[4] http://www.statista.com/chart/1846/b2c-ecommerce-sales-growth/

[5] http://inc42.com/resources/online-commerce india%E2%80%8A-%E2%80%8Akey-stats/

[6] Yingjiu Li and Xinwen Zhang, "A security-enhanced one-time payment scheme for credit card", 14th International Workshop on Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings, Print ISBN: 0-7695-2095-2, Page(s): 40 – 47, 28-29 March 2004

[7] Editorial. Security is in the smart cards. In eWeek, page 30, March 3, 2003

[8] D. Q. Viet, A. Yamamura, and T. Hidema, "Anonymous Password-Based Authenticated Key Exchange", Proc. of 6th International Conference on Cryptology in India (Indocryp'05), Bangalore, India, Dec. 2005, pp.233- 257.

[9] D. Florencio and C. Herley, "One-Time Password Access to Any Server Without Changing the Server", Proc. of the International Supercomputing Conference(ISC'08), Taipei, Taiwan, 2008, pp.401-420.

[10] Yingjiu Li and Xinwen Zhang, "A security-enhanced one-time payment scheme for credit card", 14th International Workshop on Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings, Print ISBN: 0-7695-2095-2, Page(s): 40 – 47, 28-29 March 2004

[11] J Liu et al, "A practical electronic payment scheme", 9th International Symposium on Communications and Information Technology, 2009. ISCIT 2009, E-ISBN : 978-1-4244-4522-6 Print ISBN: 978-1-4244-4521-9, Page(s): 805 - 808

[12] A. D. Rubin and R. N. Wright. Off-line generation of limiteduse credit card numbers. In Proceedings of Financial Cryptography, pages 196–209, 2001