American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-10, pp-62-70
www.ajer.org
Research Paper Open Access

Securing Online Banking Services in an Insecure Environment

*Sarjiyus[1], O, Manga[2], I.
Department of Computer Science Adamawa state university, Mubi PMB 25 Mubi Adamawa state, Nigeria.
Corresponding Author: Sarjiyus

Abstract: *This research, Securing Online Banking Services in an Insecure Environment sought to address security problems resulting from account credentials theft and all other forms of malicious activities surrounding online banking transactions. A new system implemented using JavaScript for securing online banking transaction has been provided in this research with the aim of increasing security over the existing models. The new system enables the customers and banks to authenticate each other and sign processed transactions online. From the results, the new framework also solves the issues of authentication, confidentiality, integrity and non-repudiation, using an integrated three-tier, trusted and secure channel. In addition to the creation of a secure channel between client's computers and the bank's server, a secure algorithm, challenge-Respond security algorithm that would be suitable for clients' side security (web browser) was implemented. Thus, the secure three-tier transaction model was recommended for banking services as it was found to be suitable for building client trusts.*

Keywords*: Security, Trust, Models, transaction, Environment.*

Date of Submission: 19-09-2017 Date of acceptance: 10-10-2017

I. INTRODUCTION

In recent times, internet banking has passed through different implementation, developmental and architectural stages; and consequently, there has been a wide acceptance of this service by both customers and banks due to its tremendous advantages. As the service evolves, new functions and features continue to be added to it. This has reduced the time and financial resources spent in conducting transactions, as one can simply log into the internet banking website or system make huge transactions worth several millions in just a matter of seconds, without physically visiting a bank branch. Today, long queues in banking halls have either disappeared or reduced drastically in most countries.

Bank branches have either been shut down or completely erased and subsequently, resulting to savings made from reduced staff remuneration and branch office maintenance budgets [17].

The advancement of Internet banking and its associated services have not been without an increased probability of attacks and serious threats. [18] reports that the trend of growth of online banking has brought so many security issues and increasing cost of implementing higher security system for both online banking users and the banks. According to [20], the wide use and application of information technology in the banking industry has also led to emerging threats and attacks, basically in the form of computer crimes/cybercrime and fraud. Also [19] writes that the adoption of electronic banking (e-banking) has brought some major challenges to the banking industry in terms of risk exposure. This leaves customers with the choice of enjoying the ease, the service it gives, with the resultant vulnerabilities that accompany it, or continuing with the traditional banking procedure which is often tedious and less user friendly while hoping that no one gains unauthorized access to their account and savings.

As more and more people become exposed to the information superhighway, privacy of information and the security that goes hand in hand with this information is crucial to the growth of electronic transactions [21]. Consequently, there is need to develop a more secure system that can handle most of the security needs and flaws that have been identified in the current Internet banking systems. One of such flaws is the threat posed by the "man-in-the-middle" attack, where an attacker hijacks an existing session after the genuine party to that session has been authenticated by the server and logged in. When this happens, the attacker can then carry out their attacks with ease. This raises strong arguments about the effectiveness of systems that rely on trusting the client's computers, rather than using a secure device to create a trusted path from the client to the internet banking server. For customers to use Internet banking facilities comfortably, they must have confidence that their online services are trustworthy and secure. Similarly, for banks to provide Internet banking services, they need confidence in the security of online transactions. Internet security is well known and many security models and protocols have been developed for it. Secure Socket Layer/Transport Layer Security (SSL/TLS) is known to be the de facto Internet banking standard to offer trust and secure transactions [5].

The greatest snag on internet banking security implementation is that security system developers tend to be reactive instead of being proactive.

According to [22], most of the defenses on Internet banking attacks have been reactive. [23] Posits that the current

Internet banking models are focused on fraud identification instead of fraud prevention, which means that actions are taken only after fraud has occurred instead of performing a series of preventive procedures that would stop fraud from occurring in the first instance. Again, most researches tend to focus on network and server side security for banks at the expense of the client browser side.

The overall motivation of this research is to propose and model a system that solves most of the security problems and threats existing against Internet banking systems considering also, the client side security by employing tools that seem to capture the basic functionalities needed to develop the new system. Essentially, this research tends to address this leakages and flaws by strengthening the existing SSL layer with two other layers namely, Internet Protocol Security (IPSec) and Application Layer Security (ALS) to establish a three-tier model framework.

I.I MOTIVATION FOR THE RESEARCH

The rise in cyber attacks has caused a decline in the use of online banking and has negatively affected consumer confidence in the ability of financial institutions to protect them. Consumers are questioning the safety of their transactions and are looking up to banks to fix the problem.

II. CONCEPTUAL FRAMEWORK

The increase use and rapid developments of information technology enabled fundamental changes in how companies including banks interact with customers [2]; [6], [1]. Whether banking organizations are newly established or fully mature, they maintain their vitality by innovating, changing, and learning from their experiences [4]: [9].

Insecure environment in the context of internet banking is an e-platform that is not secure and trustworthy enough to guarantee smooth online banking transactions. Such e-platform environments are characterized by different types of threats resulting from phishing and pharming – server bugs, super user exploit, Trojans, denial of service attacks, password cracking, packet sniffers, social engineering, port scanners etc.

Essentially, an insecure environment is an e-platform that is exposed to all risk associated with online activities[24]. . As pointed above, most of these threats are brought about by the activities of hackers and widespread phishing websites and all these have projected the perceived unsafe, insecure Internet banking transactions.

II.I EXISTING MODELS FOR INTERNET BANKING

Internet-based (electronic) banking schemes rely on the existence of an Internet connection over which a customer can access bank services. Customers can use existing “browser” software such as Mozilla Firefox or Microsoft Internet Explorer as the client interface to the bank system. In this model, the bank’s server provides HTML forms-based interface through which customers can make requests and conduct transactions, communication security is provided by the SSL protocol which is built into the browser or else, customers can download Java applets from the bank-server’s web site.

The downloaded applet provides the interface through which customer transactions can take place. In this case, communication security is provided by the applet in addition to the security provided by SSL.

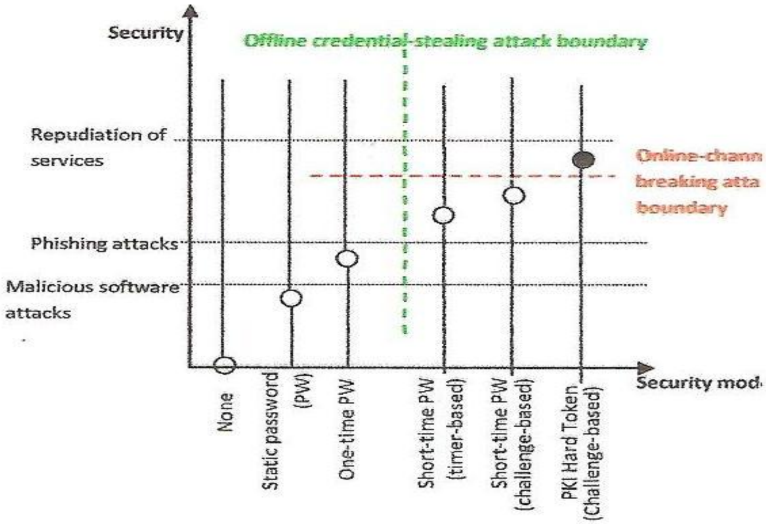


Fig.1: Comparison of existing models based on authentication mechanism, using SSL tunneling

II.II WEAKNESSES OF SINGLE-LAYER BASED SECURITY MODELS USING SSL/TLS PROTOCOL

The existing environment (SSL trusted channel) has proved to have some weaknesses, since the level of security also depends on the authentication mechanisms used. This research seeks to examine why high security provided by SSL is being weakened, and then tries to build a secure environment, taking into cognizance, these weaknesses.

As the de-facto Internet security standard; SSL provides authentication, confidentiality, integrity and non-repudiation of messages transmitted over Internet between the web browser and the web server only [12]. However, this protocol operates below the Application layer in TCP/IP networks and does not provide way to ensure whether a user is, in fact, who he or she claims to be by asking for direct or indirect proof of the knowledge about some sort of secrecy or credential. It is a common mistake for some users to believe that their online banking sessions are perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window or the URL start with *"https"* rather than "http" [7]. The following facts explain why SSL does not guarantee the safety and security of transaction over the Internet:

SSL is designed to serve as a secure tunnel from the end user computer's browser to the server's web server of the bank, and does not in any way protect the end points such as client's computer. A Trojan exploits this security hole. In addition to that, SSL is beyond providing end-user authentication services [13]; [14].
The security offered by SSL is based on the use of digital certificates of financial entities' web servers and in which case, many Internet users are not able to discern the validity of a certificate, and may pay only little or no attention to it [14].

Different browser versions will offer different levels of security as some are restricted to the use of strong cry- ptography. For instance, some previous versions of Netscape and Internet Explorer will even be restricted to offering only weak encryption, unless they are connecting to servers using Server-Gated Cryptography enabled SSL certificate. So, depending on the browser's vender and version some are only capable of encrypting at 40 or 56-bit encryption, while the latest and more recent browser versions are capable of 128 and even 256-bit encryption key [7].

III. METHODOLOGY

The framework employed for this prototype consists of a complete range of robust high performance client and server platforms with integrated enterprise application and data extendable to banking customers in real-time.The client system includes personal computer (PC). The servers are used to maintain connectivity to enterprise resources for the online banking solution that includes the customer's service, standing order and payment of bills.

Also an offline card reader was used to generate customer's RESPONSE; as PKI- tamper resistant smartcard is entered, the customer ID_C and the CHALLENGE using cryptographic mechanisms, are encrypted to generate the appropriate RESPONSE string. In general the CHALLENGE-RESPONSE security model was built upon a three-tier security model which is made up of the SSL (layer 2) tunnel and two other tunnels given one at the IP layer (IPsec) (layer l)and another, the application layer of TCP/IP networks (ALS) (layer 3) as shown in Fig.2(a) and 2(b) below.

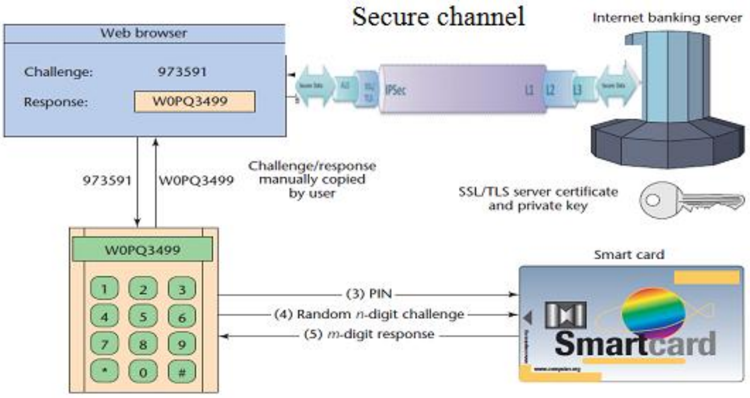


Fig. 2(a): Challenge - Response Security Model

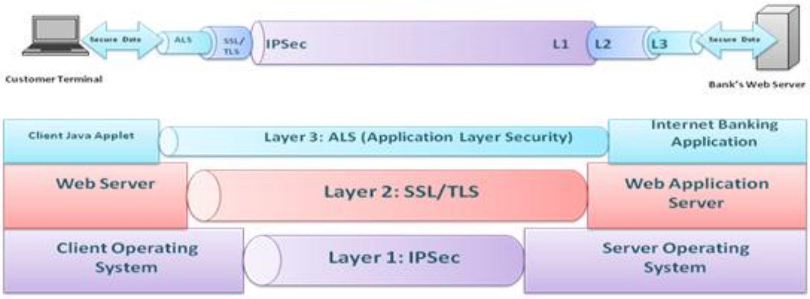


Fig. 2(b): Three-tier Security Model for Internet Banking

III.I ALGORITHM FOR THE PROPOSED MODEL.

```
Step 1:  Connect web browser to sever.
Step 2:  Enter account number
         If account number exist in database
         Then, Server supplies CHALLENGE#
         Else, the message, INVALID account number is prompted
Step 3:  Insert smart card into card reader.
Step 4:  Enter PIN# to authenticate smart card.
         If PIN# is correct
         Then a welcome message is prompted
         Else the message incorrect PIN# is displayed
Step 5:  Enter CHALLENGE# into smart card.
Step 6:  Enter encoded "RESPONSE"
         If "RESPONSE" match CHALLENGE#
         Then customer is authenticated.
         Else GOTO step 2.
```

III. II SYSTEM PSEUDOCODE

```
BEGIN:
         SYSTEM PROMPT "Welcome to Secure Online Banking";
//Customer supplies password, username
SERVER AUTHENTICATE A CUSTOMER;
//Customer supplies account number
SERVER AUTHENTICATE A CUSTOMER ACCOUNT NUMBER;
         WHILE NOT EOF DO
             SERVER request enquiry from customer;
         CUSTOMER supplies enquiry;
         IF enquiry is in database THEN
             SERVER supplies CHALLENGE from database;
         ELSE
             SERVER process enquiry
```

```
                SERVER send notification to
                CUSTOMER;
            ENDIF
        ENDDO
//Customer inserts smart card into CARDREADER
      Smartcard AUTHENTICATES customer using PIN from customer
      CUSTOMER enters CHALLENGE# into smartcard
     //CARDREADER displays RESPONSE on screen.
     CUSTOMER enters encoded RESPONSE;
     SERVER checks DATABASE to decrypt RESPONSE;

    WHILE NOT EOF DO
    SERVER request enquiry from customer;
    CUSTOMER supplies enquiry;
             IF RESPONSE match CHALLENGE# IN DATABASE THEN
     SERVER authenticate CUSTOMER
            ELSE
            SERVER process enquiry;
            SERVER send a notification to
            CUSTOMER;
            ENDIF
     ENDDO
END
```

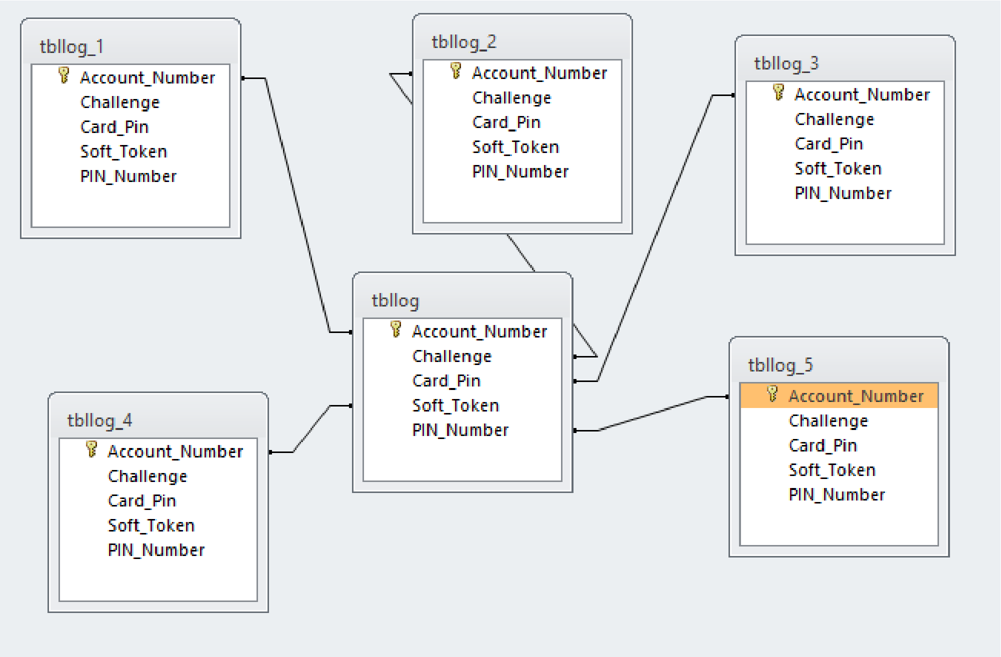


Fig. 3a: Entity Relationship Model (E-R Model) of the New System

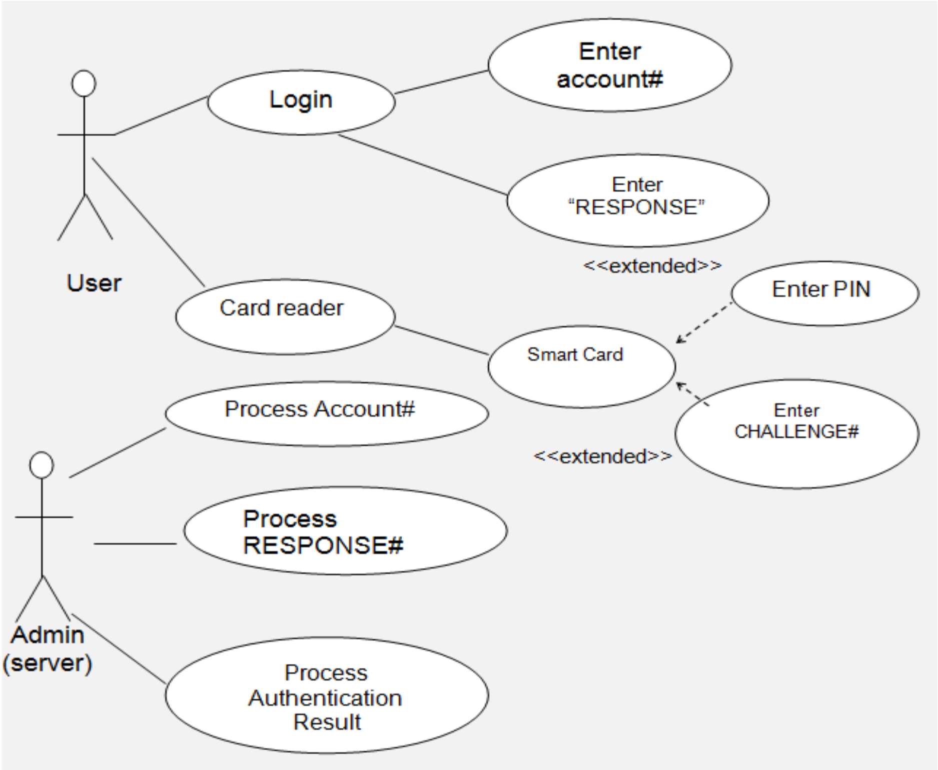
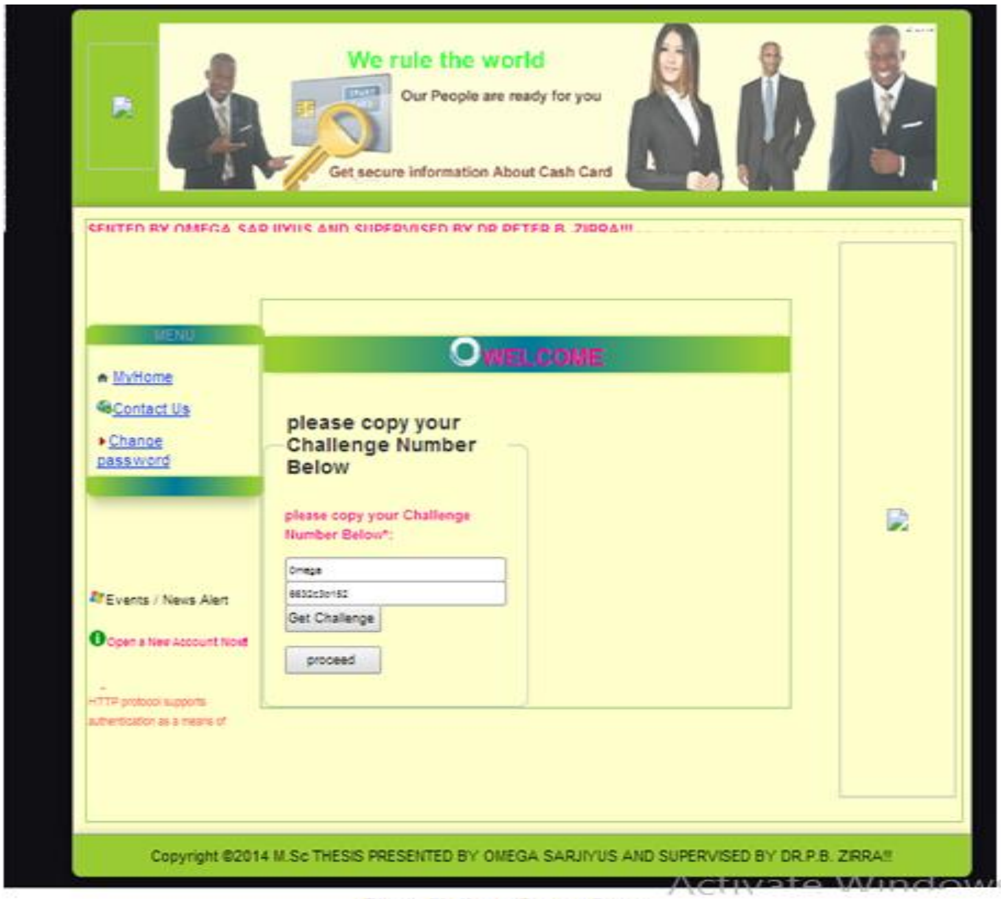


Fig. 3b: The Use Case UML diagram for Challenge-Response security system.

IV. RESEULTS


We rule the world
Our People are ready for you
Get secure information About Cash Card
SENTED BY OMEGA SARJIYUS AND SUPERVISED BY DR PETER B. ZIRRA!!!
MENU
MyHome
Contact Us
Change password
WELCOME
Events / News Alert
Open a New Account Now!

please copy your Challenge Number Below

please copy your Challenge Number Below*:

Omega

8632c3c152

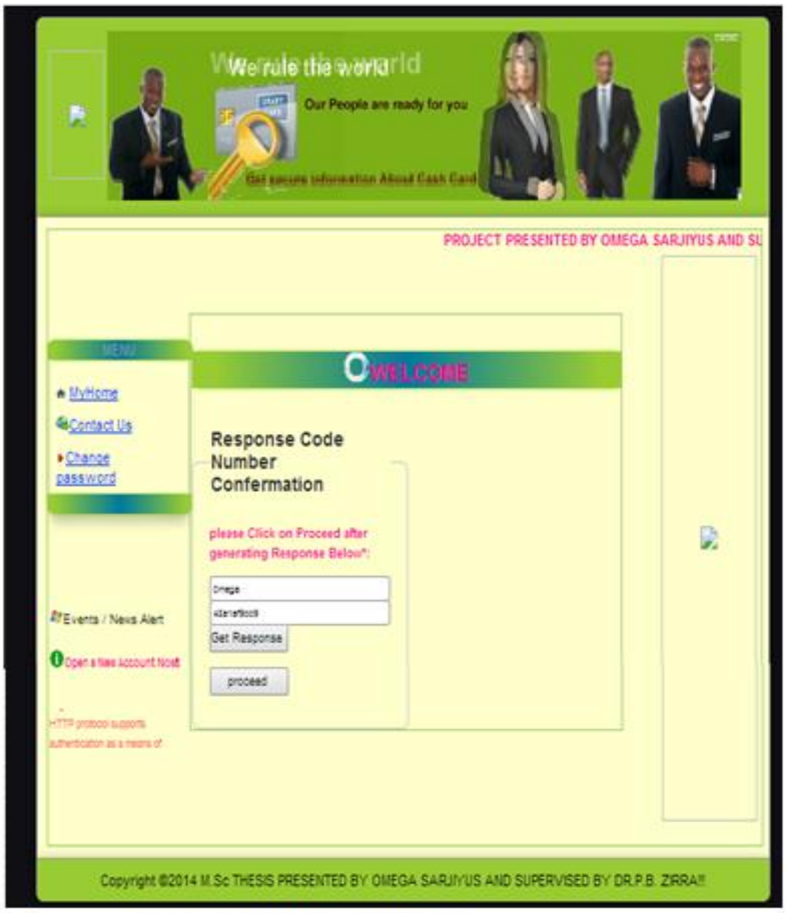
Get Challenge

proceed

HTTP protocol supports authentication as a means of

Copyright ©2014 M.Sc THESIS PRESENTED BY OMEGA SARJIYUS AND SUPERVISED BY DR.P.B. ZIRRA!!

Fig.4: Challenge Prompt Page.



PROJECT PRESENTED BY OMEGA SARJIYUS AND SU

Response Code Number Confermation

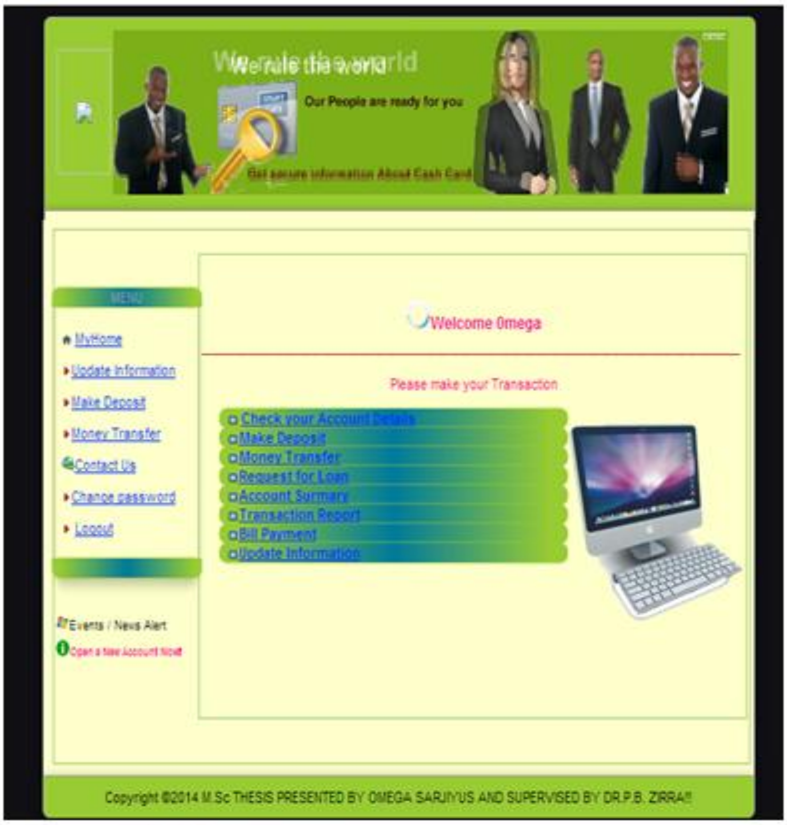
please Click on Proceed after generating Response Below*:

Omega

HTTP protocol supports authentication as a means of

Copyright ©2014 M.Sc THESIS PRESENTED BY OMEGA SARJIYUS AND SUPERVISED BY DR.P.B. ZIRRA!!

Fig. 5: Response String Confirmation Page

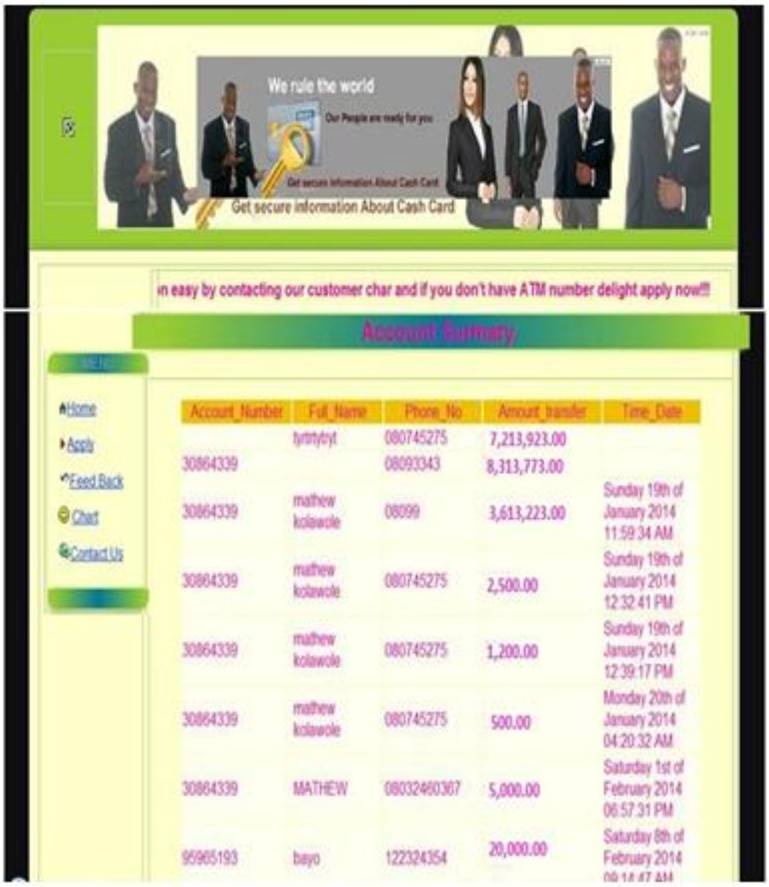


Welcome 0mega

Please make your Transaction

Copyright ©2014 M.Sc THESIS PRESENTED BY OMEGA SARJIYUS AND SUPERVISED BY DR.P.B. ZIRRA!!

Fig. 6: Transaction Page


We rule the world
Our People are ready for you
Get secure information About Cash Card
Get secure information About Cash Card
Home
Apply
Feed Back
Chat
Contact Us

n easy by contacting our customer char and if you don't have ATM number delight apply now!!

Account Summary

Account_Number	Full_Name	Phone_No	Amount_transfer	Time_Date
	tyrtrtytyt	080745275	7,213,923.00	
30864339		08093343	8,313,773.00	
30864339	mathew kolawole	08099	3,613,223.00	Sunday 19th of January 2014 11:59:34 AM
30864339	mathew kolawole	080745275	2,500.00	Sunday 19th of January 2014 12:32:41 PM
30864339	mathew kolawole	080745275	1,200.00	Sunday 19th of January 2014 12:39:17 PM
30864339	mathew kolawole	080745275	500.00	Monday 20th of January 2014 04:20:32 AM
30864339	MATHEW	08032460367	5,000.00	Saturday 1st of February 2014 06:57:31 PM
95965193	bayo	122324354	20,000.00	Saturday 8th of February 2014 09:14:47 AM

Fig.7: Account Summary

V. DISCUSSION

Fig.4 shows the challenge prompt page, was obtained by successfully entering the customer account number in the account confirmation page. After a successful login, the bank server gets the account number and then checks to ascertain its validity in the database, if it is a valid account number the server supplies CHALLENGE (N) which is bound to the account number it received, otherwise an error message is prompted.

The RESPONSE string confirmation page as shown in Fig.5 was obtained by inserting the CHALLENGE (N) obtained, into the offline smartcard and encrypting it with the customer identity (IDc). The RESPONSE string could only come from that specific customer device and could only be based on the use of that specific bank-issued smartcard. This encrypted message (RESPONSE string) is sent to the web server via web browser and upon receipt, the bank authentication servers finds the customer's record on its data base, decrypt the CHALLENGE using the shared secret key and compares the result with what the customer has sent. If they match, the customer is authenticated into Transaction page, which is in conformity with the assertion of [15] who stated that building a trusted and secured environment entails creating a Challenge-Response scheme that authenticates both the customer and the bank.

Consider Fig. 6, which is the Transaction page was obtained as a result of the successful decryption of the initial account-bound CHALLENGE by bank's server to match the one in the encrypted RESPONSE.

Clearly, it can however be deduced from Fig.6 that all the steps taken (from entering customer account number to RESPONSE string generation) aimed at making customers data at the transaction page secured. At the transaction page therefore, a high level of authenticity, confidentiality, integrity and non repudiation is thus maintained in accordance with assertion of [5] who stated that any Internet banking system must provide authentication, confidentiality integrity and non repudiation.

Furthermore, Fig.7 which is the Account summary table, was obtained by selecting and clicking the account summary option in the transaction page menu. The account summary displays the result of transaction (for instance money transfer) carried out by the customer. It displays the account number, name of the customer, phone number, amount transferred, the day and date of such transfer including the time the transaction was carried out. The result in Fig.7 is in accordance with the assertion of [15] who stated that every transaction made in a secure environment is traceable and verifiable.

In conclusion, and in addition to authentication and non repudiation, confidentiality and integrity have been built up in the research. The environment has thus been shown to counter all forms of credential-stealing and Channel-breaking attacks.

VI. CONCLUSION

Implementing the three-tier security model of Online Banking serves to offer safe Internet banking environment where transactions are secured from all sorts of malicious attacks. Hence, customers are certain that they are sending their personal information and banking credentials to legitimate banks' servers and not impostors, and that the privacy(confidentiality) of such transactions and credentials is ensured before and during the transmission over the network.

The research also demonstrated how banks and their customers will receive signed transactions that either party cannot later refute.

The use of IPSec strengthens trust since only the customers' PCs can be used online to access customers' related accounts.

Moreover, the use of hard token Public Key Infrastructure (PKI) online smartcard readers to provide mutual authentication, ensures that only qualified people can access banking accounts.

Hence, the level of customer trust has increased proportionally to the increase in the level of security.

REFERENCES

[1]. H. H., Bauer, M, Falk T Hammershmidt . Measuring the quality of e-banking portals. Int. J. Bank Mark., 23(2), 2005, 153-175.

[2]. P. Dabholkar, & R Bagozzi,. . An attitudinal model of technology based self-service: moderating effects of consumers traits and situational factors. J. Acad. Mark. Sci., 30(3), 2002,184-201.

[3]. O., Danhash, P. L., Dung, & B. Srinivasan. Security Analysis for Internet Banking Models, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence Networking and Parallel/Distributed Computing 3, 2007, 1141-1146

[4]. D. Hellriegel, S. E. Jackson, & J. W. Slocum.. Management: A Competency Based Approach. (Ohio,South Western, 2005).

[5]. A., Hiltgen, T. K. Zurich, & , T. Weigold Secure Internet Banking Authentication. IEEE Journal of Security & Privacy. 4 (2), 2006, 21 – 29.

[6]. A. Parasuraman &, G. M. Zinkhan Marketing to and serving customers through the Internet: an overview and research agenda. J. Acad. Mark. Sci., 30(4), 2002, 286-295.

[7]. Thawte. The value of authentication. 2009, http://www.thawte.com

[8]. V., Zeithaml, A. Parasuraman, & A. Malhotra. Service quality delivery through websites: a critica review of extant knowledge. Acad. Mark. Sci. J., 30(4), 2002, 362-375.

[9]. J. W., Slocum, Jackson, S .E & D. Hellriegel. (2008) Management: A competency Based Approach . (Ohio, South Western,2008).

[10]. X., Zhang, . & R.P. Victor. " A Consumer Perspective of E- Service Quality" . IEEE transactions on Engineering Management. 52(4), 2005,461-477.

[11]. K. E., Lee, K .N Kwon, & D. W .Schumann.. Segmenting the non adopter category in the diffusion of Internet banking. International Journal of Rank Marketing. 23(5), 2005,414-437.

[12]. W., Stallings. Cryptography and Network Security Principles and Practices (4th Ed.),(Upper Saddle River, New Jersey, Prentice Hall,2006) ,483-562.

[13]. C., Wueest Threats to Online Banking Symantic Security Response Dublin. 2006.

[14]. A. S., Martino & X. Perramon. Defending e-banking Services: An antiphishing approach services, IEEE Congress on Services (1), 2008, 251-254.

[15]. Y., Lasheng & P. Mukwande. Three-tier Security Model for e-business. Proceedings of the second Symposium International Computer Science and Computational Technology (ISCSCT). 2009,114-119.

[16]. I.U. Cletus, Y.Ibrahim, & P. D. Bala. Banking reform and National Development in Nigeria, Global Journal of Human Social Science. 2 (1), 2015, 2-5.

[17]. N. E Reginald."Internet banking implementation in Nigeria; security issues analysis and solutions," unpublished.

[18]. M. Hole and T.Jostheim. ."An analysis of the online banking security issues," Department of Computer Science, University of Auckland ,2013.

[19]. Z. Abaenewe, O. Ogbulu., and M. Ndugbu. Electronic banking and bank performance in Nigeria," West African Journal of Industrial & Academic Research .6 (1),2013.

[20]. F. Wada., O.,Longe. and P. Danquah . "Action speaks louder than words – understanding cyber criminal behavior using criminological theories," Journal of internet banking and commerce,17, (1), 2012.

[21]. Y.Yang, "The security of electronic banking," 2010.

[22]. M.Johnson . and S. Moore. A new approach to e-banking," In U´ lfar Erlingsson and Andrei Sabelfeld, editors, Proc. 12th Nordic Workshop on Secure IT Systems (NORDSEC 2007), 2007,127–138.

[23]. L. Peotta, D.Marcelo .H. Bernardo .,M. David., F. G. Deus and R. Timóteo de Sousa Jr. A formal classification of internet banking attacks and vulnerabilities,International Journal of Computer Science & Information Technology (IJCSIT), 3, (1). 2011.

[24]. K.M. Nor and J.M. Pearson. The Influence of Trust on Internet Bankimg Acceptance. Journal of Internet Banking and Commerce.12,(2),2017.

Sarjiyus. "Securing Online Banking Services in an Insecure Environment." American Journal of Engineering Research (AJER), vol. 6, no. 10, 2017, pp. 62–70.