Identification of Cloned Payment Page in Ecommerce Transaction

Maureen Akazue and Aghaulor Augusta
Mathematics and Computer Science Department, Delta State University
Abraka, Delta State, Nigeria
akazuem@gmail.com

[Abstract] Electronic commerce is the application of information and communications technology from the point of customer's login to the point of customer's receiving the goods along electronically with manually processing system. The Internet potential for electronic commerce was expected to boom with the spread of the Internet but, the lack of consumer confidence in electronic payments as regards security of payment mechanisms explained the slow growth of online purchase. Thus, in this paper, a centralized merchant registration retrieval (CMRR) component of e-commerce model is used to serve as an advisory tool that identify cloned payment page in e-commerce transaction. An online evaluation of the use of CMRR in identifying cloned payment page and acting as an advisory to customer were carried out through the use of questionnaire. Data analysis of generated questionnaire showed that CMRR can enhance customer's confidence and trust in the purchase of online goods and services via identifying cloned payment page.

[Keywords] Cloned payment page, Central Merchant Registration Retrieval, Advisory tool, customer's trust, Electronic commerce

Introduction

Electronic commerce is the application of information and communications technology from the point of customer's login to the point of customer's receiving the goods along electronically with manually processing system (Wigand, 1997). In other words, payment-related problems and sellers unknown were reasons for consumers disinterest in e-commerce. Therefore, building trust became necessary since consumer perceived risks are high in buying goods and services online (Zhongwei, 2006; Suh & Han, 2003). That is why (Gefen, 2002) redefined customer's trust as depending on the components of the e-commerce transaction environment. The environment refers to the activities of the components of e-commerce transaction website and the CMRR is an essential component in e-commerce transaction (Akazue, 2015). Thus, in this paper, a CMRR component of e-commerce model is used to serve as an advisory tool that identify cloned payment page in e-commerce transaction. The process that the CMRR uses to distinguish cloned payment page from legitimate payment page in e-commerce transaction was highlighted.

Related Works

Characteristics of the Online System

Online system relies on the Internet and thus, the unpredictability and the doubt associated with the Internet is a key challenge faced by e-commerce. These Internet characteristics have introduced issues related to consumer and merchant trust, as well as opinions of risk and security (Claessens, Dem, Cock, Preneel & Vandewalle, 2002). Thus, (Radwan & Mumtaz, 2010) proposed the use of a model to test the capability and limitation of e-commerce sites using design and content among others. Akazue (2015) surveyed existing fraud prevention models that can check merchant integrity within the transaction system in ecommerce models. Analysis of the findings showed that merchant integrity is not verified within e-commerce model to the awareness of the customer. Thus, a CMRR component, which consistently checks the merchants that upload goods and services, was introduced as an additional component to existing e-commerce model (Akazue, Aghaulor & Ajenaghughrure, 2015).

Building Customer and Merchant Online Trust

There is need to establish trust around the environment in which e-commerce transactions is operating to attract people to explore the medium for their transaction. This is due to factors such as distance between customers and merchants, identifying genuine customers and merchants, protection of customer's privacy and financial details, protection of transaction process to prevent hijacking, and the like. Some online activities could be for positive motives or for negative motives. Thus, there is need for clear distinction between these two motives in other to ascertain trust in e-commerce environment.

Different types of models have being designed to enhance customer and merchant trust from cloning of website or payment page to ensuring the authenticity of the credit card used (Jithendra, 2006). According to Claessens et al. (2002), online activities are available to customers and merchants through mediums such as the websites and ATM. The features of each environment (website and ATM) are based on several factors such as the users and types of transaction, as well as the transaction medium. Rehab et al. (2010) compared the characteristics of electronic payment system and address verification system (AVS) technique in preventing online fraud in "card not present" (CNP) transactions. The findings showed that electronic payment system provides protection in lost/stolen card fraud, credit card validation, skimming fraud, assumed identity/counterfeit cards fraud, IP tracking and email notification.

According to Dejan (2005), the Capabilities and limitations of some security protocols such as Secure Electronic Transaction (SET), Secure Sockets Layer (SSL), 3D SET, Visa's 3D Secure and MasterCard's Secure Payment Application (SPA) showed that the 3D SET is better in mitigating fraudulent activities. Akazue, Aghaulor & Ajenaghughrure, (2015) used the CMRR component of e-commerce model to check the genuineness of the online stores in e-commerce transactions. According to Suh & Han (2003), the security of the Internet is defined by the weakness and the protective advantages of mechanism used over the Internet.

Web Page Cloning

Cloning is the process of replication or alteration of a block of codes. Dedicated hackers and criminals always seek new ways to commit fraud. Two of such ways are webpage cloning and use of fake virtual stores (Lacohee, Crane & Phippen, 2011; Dejan, 2005). When a cloned credit card /webpage is properly done, it is difficult to detect (Giuseppe, Massimiliano & Fasolino, 2002).

Formulation of Problem

The security of e-commerce is a continuing process that requires the acceptance of strong security policies and the use of proven security software. Thus the use of CMRR component will add to the existing knowledgebase of Information technology. Furthermore, the huge problem of credit card fraud is being mitigated but a more severe problem is credit card cloning and web page cloning (Arcot, 2012). Thus, a CMRR is shown and proven to identify cloned payment page in ecommerce transaction and prompt customers not to send credit card details.

Research Framework

Analysis of the Existing System

It is difficult to find e-commerce components with CMRR component built into it. Most times, the existing e-commerce web sites comprises of the Retail component, Shipping component, Switching component, Reporting component, Merchant component, and List component (Akazue, 2015). Thus, customer ignorantly sends the credit card details to supposed correct URL address while the merchant endlessly wait for the payment of his goods and services. Problem arises as the customer and merchant are defrauded.

The Work of CMRR Component

Authentication techniques such as One-Time Password Tokens, IP Geo-location, Device Identification, Browser Cookie, Personal Assurance Message and so on, are predefined checks that are used to make Man-in-the-Middle and cloned web page(s) ineffective. But, protecting customer from cloned websites and Webpages requires more than authentication techniques. Based on the analysis of the existing authentication techniques, there is need to use a token in the MAE-commerce system (Akazue, 2015). The token is used to perform pre-verification and post-verification of the merchant and URL of the payment page. In other words, the use of merchant token generated by centralized merchant registration retrieval (CMRR) system and product token were applied in authentication of merchant and payment web page.

Clone Web Page Detection Process (CMRR Activity)

The system detects a clone web page by the detailed activity of the CMRRS. In the MAE model, the payment page is wrapped in the order page. By this act, the CMRRS token is generated by the CMRRS at the point of filling the shopping cart. At the order form view where credit card details are to be entered, the generated tokens will automatically appear on the order form view. The token is verified and pops up a warning signal for inconsistency. The abstract description of the behavior of the token based e-commerce security is shown in Figure 1. Each state diagram represents objects of a single class and tracks the different states of its objects through the system. The behavior of the model is represented in series of events that occur in the sixteen possible states.

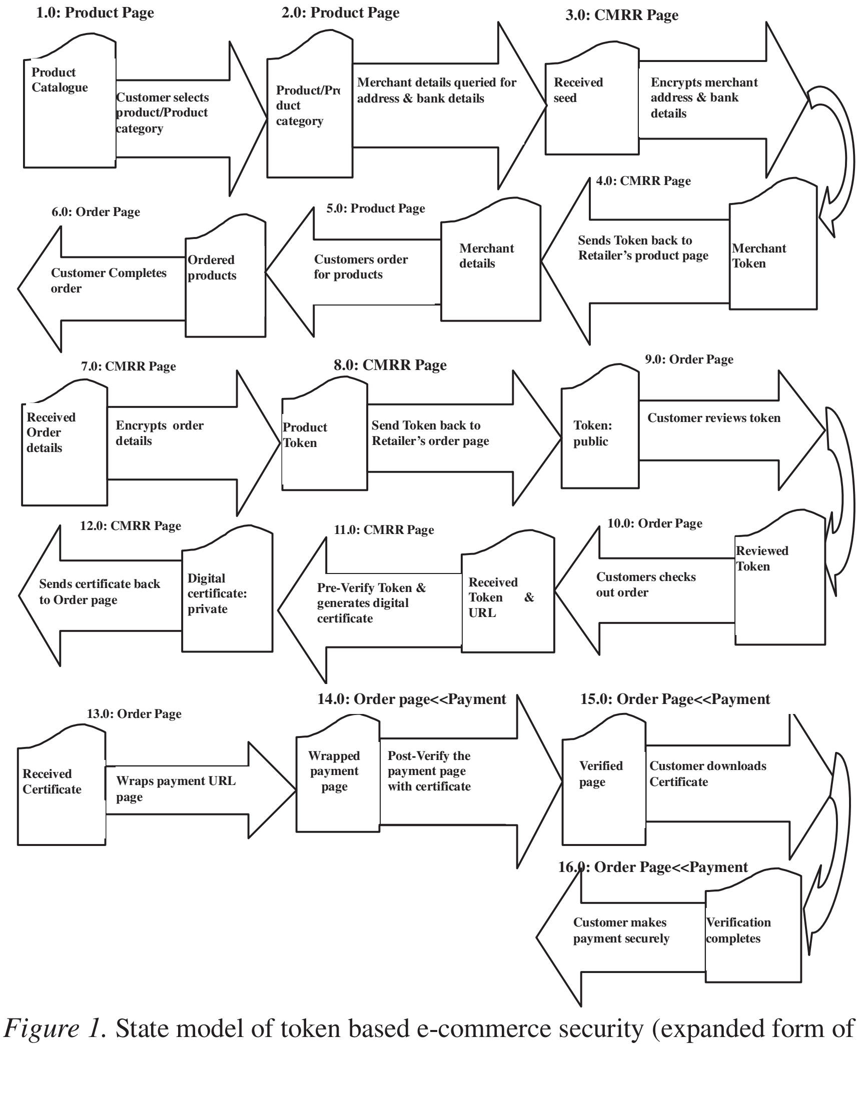
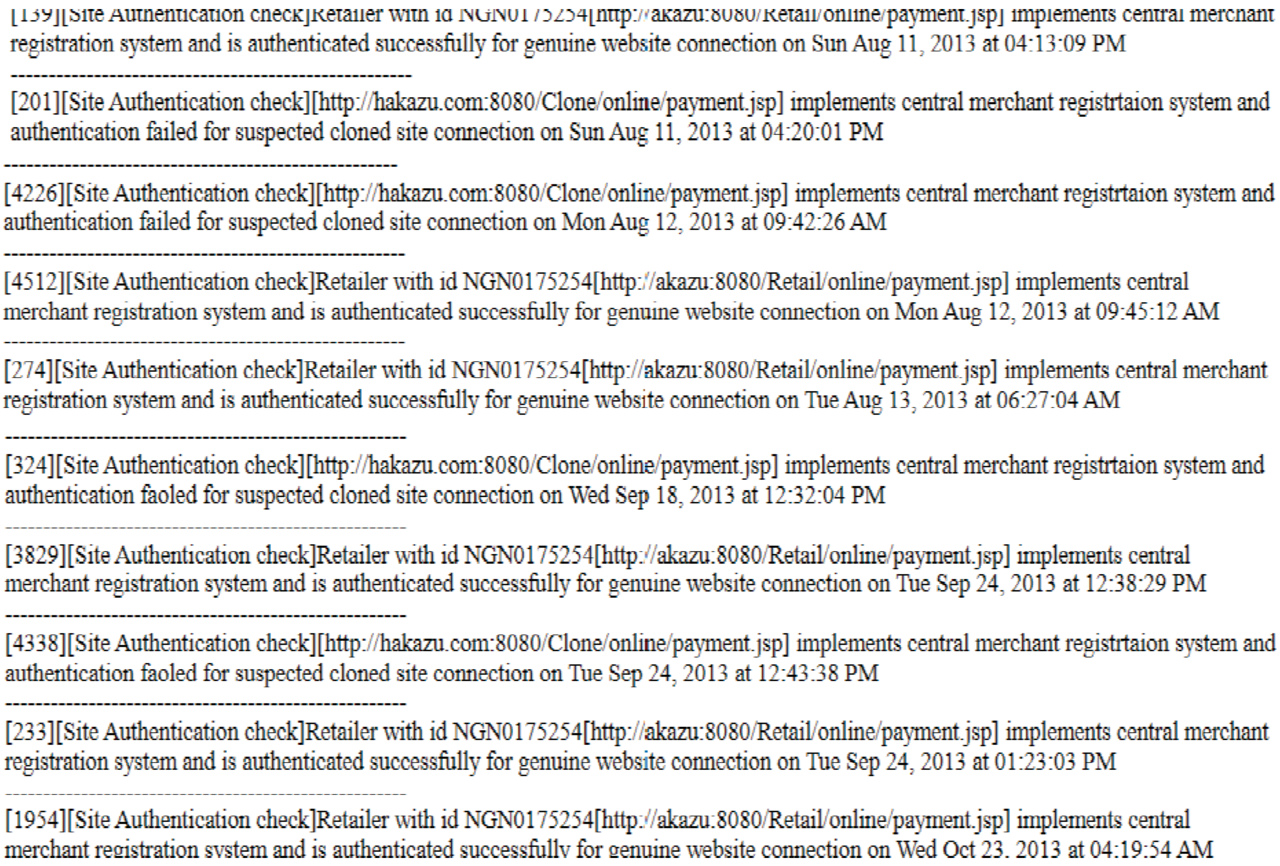

1.0: Product Page
Product Catalogue
Customer selects product/Product category
2.0: Product Page
Product/Product category
Merchant details queried for address & bank details
3.0: CMRR Page
Received seed
Encrypts merchant address & bank details
4.0: CMRR Page
Sends Token back to Retailer's product page
Merchant Token
5.0: Product Page
Merchant details
Customers order for products
6.0: Order Page
Ordered products
Customer Completes order
7.0: CMRR Page
Received Order details
Encrypts order details
8.0: CMRR Page
Product Token
Send Token back to Retailer's order page
9.0: Order Page
Token: public
Customer reviews token
10.0: Order Page
Reviewed Token
Customers checks out order
11.0: CMRR Page
Received Token & URL
Pre-Verify Token & generates digital certificate
12.0: CMRR Page
Digital certificate: private
Sends certificate back to Order page
13.0: Order Page
Received Certificate
Wraps payment URL page
14.0: Order page<<Payment
Wrapped payment page
Post-Verify the payment page with certificate
15.0: Order Page<<Payment
Verified page
Customer downloads Certificate
16.0: Order Page<<Payment
Verification completes
Customer makes payment securely

Figure 1. State model of token based e-commerce security (expanded form of CMRR activities)

Implementation and Testing of the CMRR Component

When a webpage is hijacked or cloned, the CMRR checker checks the site and stores the details in the transaction log shown in Figure 2.



```
[139][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central merchant
registration system and is authenticated successfully for genuine website connection on Sun Aug 11, 2013 at 04:13:09 PM
-----------------------------------------------------
[201][Site Authentication check][http://hakazu.com:8080/Clone/online/payment.jsp] implements central merchant registrtaion system and
authentication failed for suspected cloned site connection on Sun Aug 11, 2013 at 04:20:01 PM
-----------------------------------------------------
[4226][Site Authentication check][http://hakazu.com:8080/Clone/online/payment.jsp] implements central merchant registrtaion system and
authentication failed for suspected cloned site connection on Mon Aug 12, 2013 at 09:42:26 AM
-----------------------------------------------------
[4512][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central
merchant registration system and is authenticated successfully for genuine website connection on Mon Aug 12, 2013 at 09:45:12 AM
-----------------------------------------------------
[274][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central merchant
registration system and is authenticated successfully for genuine website connection on Tue Aug 13, 2013 at 06:27:04 AM
-----------------------------------------------------
[324][Site Authentication check][http://hakazu.com:8080/Clone/online/payment.jsp] implements central merchant registrtaion system and
authentication faoled for suspected cloned site connection on Wed Sep 18, 2013 at 12:32:04 PM
-----------------------------------------------------
[3829][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central
merchant registration system and is authenticated successfully for genuine website connection on Tue Sep 24, 2013 at 12:38:29 PM
-----------------------------------------------------
[4338][Site Authentication check][http://hakazu.com:8080/Clone/online/payment.jsp] implements central merchant registrtaion system and
authentication faoled for suspected cloned site connection on Tue Sep 24, 2013 at 12:43:38 PM
-----------------------------------------------------
[233][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central merchant
registration system and is authenticated successfully for genuine website connection on Tue Sep 24, 2013 at 01:23:03 PM
-----------------------------------------------------
[1954][Site Authentication check]Retailer with id NGN0175254[http://akazu:8080/Retail/online/payment.jsp] implements central
merchant registration system and is authenticated successfully for genuine website connection on Wed Oct 23, 2013 at 04:19:54 AM
```

Figure 2. Log details of checking site authentication based on URL address from Thu Jun 20, 2013 at 08:44:42PM to Wed Oct 23, 2013 at 04:23:17AM

Evaluation of the Use of CMRR to Identify Cloned Payment Page

The evaluation of the use of CMRR component in identifying cloned payment page in e-commerce transaction was carried out using SPSS to analyze administered questionnaires. The findings are shown in Table 1. It was observed that CMRR has the capability to identify cloned payment page by comparing the URL of the payment page at the time of customer check out with the URL address of the merchant entered during local merchant registration (Akazue, 2015). Thus, the CMRR sends advisory message to the customer and a transaction log to the retailer alerting both parties of URL mismatch. Therefore, the CMRR ensures that the customer's account details are not sent to fraudulent payment page. This is another attribute of CMRR that makes the component distinctive and essential in e-commerce model.

Table 1.
A comparative study of CMRR in identifying cloned payment page

Characteristics	Jumia	CMRR
I believe that the payment page is not hijacked /cloned and so can be trusted to fill credit card details	No	Yes
I believe that the payment page is not compromised and so the website is trusted	No	Yes
Capable of advising customer on URL mismatch	Customer is unaware	Yes
confirmation of the authenticity of the payment page is seen and so the site is trusted	Customer is unaware	Yes
Seeing the authenticity of the payment page enhances customer confidence in online business	Customer is unaware	Yes

The average mean values of the respondents are shown in Figure 3. The mean values were computed from the average score of each respondents answer to each question. The increase in mean values is an evident of the good quality of the tested tool. Thus, the third and fourth characteristics of the CMRR have the highest average mean value.

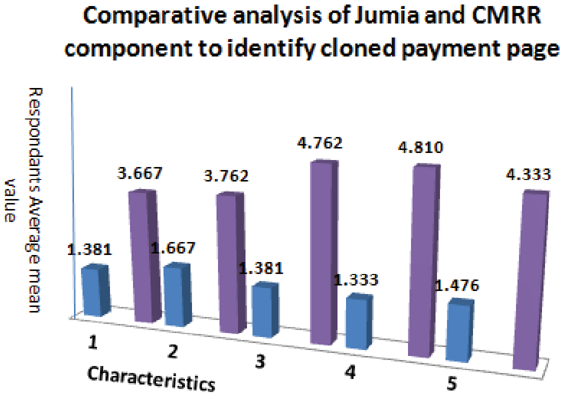


Figure 3. Comparative analysis of Jumia and CMRR component to identify cloned payment page

The responses of the Jumia e-commerce model are blue and that of CMRR are purple color. The capability of the CMRR component in e-commerce model can further be elaborated using line diagram in Figure 4.

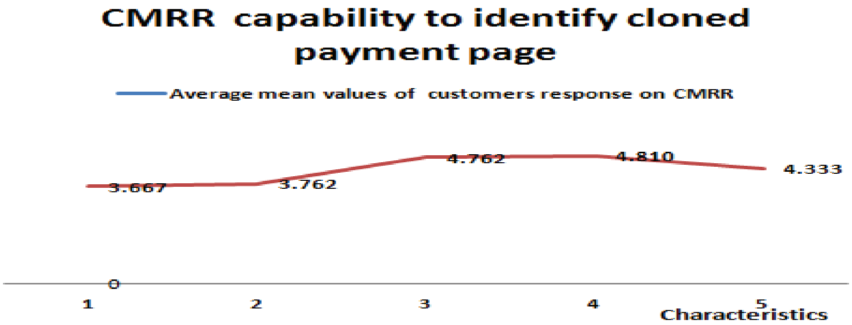


Figure 4. CMRR Capability to Identify Cloned Payment Page

Discussion and Conclusion

The CMRR component has the ability to identify cloned payment page. This is accomplished through the use of URL verification filter to consistently check that the payment URL address received at the time of customers check out matches the URL address in the database of the CMRR. Also, CMRR advise customers on such mismatch by prompting a dialog box alert. CMRR uses token based technique to further help customers to identify cloned payment page and prevent customers from sending their bank details to fraudulent site as well as protect merchant from financial loss. The effectiveness and usefulness of the CMRR in enhancing customer's confidence and trust has being demonstrated in this work. The CMRR component has several capabilities and its inclusion in the existing e-commerce models cannot be over emphasized. Further research work can be carried out based on the findings in this paper.

Acknowledgment

This paper is an extended version of preliminary manuscripts that have already been published in the *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government, published in 2015.* (EEE'15: ISBN: 1-60132-413-8 - part of WORLDCOMP Congress); Editors: Hamid R. Arabnia, Azita Bahrami, Leonidas Deligiannidis, and Fernando G. Tinetti with Associate Co-Editors: George Jandieri and Ashu M. G. Solo.

References

Akazue, M. I. (2015). A survey of ecommerce transaction fraud prevention models. *The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications,* Dubai, UAE.

Akazue, M . I., Aghaulor, A., & Ajenaghughrure, B. I. (2015). Customer's protection in ecommerce transaction through identifying fake online stores. *The Proceedings of the 2015 World Congress in Computer Science, Computer Engineering, and Applied Computing*, July 27th – 30th July, Nevada, USA.

Arcot. (2008). Protecting Online Customers from Man-in-the-Middle Attacks. Retrieved from www.arcot.com

Claessens, J., Dem, V., Cock, D. D., Preneel, B. & Vandewalle, J. (2002). On the security of today's online electronic banking systems, *Computers and Security, 21(3),* 257-269.

Dejan, S. (2005). Reducing fraud in electronic payment systems*, The 7th Balkan Conference on Operational Research, BACOR 05 Constanta*, Romania,1-11. Retrieved from http://users.sch.gr/baloukas/papers/BACOR_2005.pdf.

Gefen, D. (2002). Customer loyalty in e-commerce. *Journal of the Association for Information Systems, 3* (1), 2.

Giuseppe, A. D. L., Massimiliano, D.P., & Fasolino, A. R. (2002). An approach to identify duplicated web page, *In Proceedings of the 26th International Computer Software and Applications Conference (COMPSAC'02)*, 481486.

Jithendra, D. (2006). Credit card security and e-payment, enquiry into credit card fraud in e-payment. (Masters project), Luleå University of Technology. Retrieved from http://epubl.ltu.se/1653-0187/2006/23/LTU-PB-EX-0623-SE.pdf.

Lacohee, H., Crane, A., & Phippen, A. (2011). *Trustguide final report online*. Retrieved from http://www.trustguide.org.uk . 2006. Accessed January 2011.

Radwan, M. A., & Mumtaz, A. K. (2010). Business-to-consumer e-commerce Web Sites: Vulnerabilities, Threats and quality evaluation model. *International Conference on Electronics, Communications, and Computers – CONIELECOMP.*

Rehab, A., Shiraz, B., Malik, S., Hayat, K., Aihab, K., & Memoona, K. (2010). Online credit card fraud prevention system for developing countries. *International Journal of Reviews in Computing*, 62-70.

Suh, B., & Han, L. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce 7(3)*,135-161.

Wigand, R. (1997). Electronic commerce: Definition, theory, and context. *The Information Society: An International Journal, 13(1),* 1-17.

Zhongwei, Z. (2006). Improving efficiency and scalability of service network graph. *IEEE Transactions on Image Processing, 15(5),* 1300-1312.