

BOOK CHAPTER | E-Transaction Security

E-Transaction Security Approaches: Vulnerabilities, Challenges, Opportunities and Risk Mitigation Strategies

¹Arinze, U.C., ²Eneh, A.H. & ³Longe, O.B.

^{1&2} Department Computer Science, University of Nigeria, Nsukka, Nigeria

³Computational Sciences & informatics Academic City University College, Accra, Ghana

Email: ¹arinzeuchukwu@gmail.com , ²agozie.eneh@unn.edu.ng,

³olumide.longe@aun.edu.ng

Tel: +2348066532557, +2348076756975, +233595479930

Abstract

The emergence of information and communication technology has not only transformed the way businesses are conducted by moving it to the virtual domain, but has spurred innovative financial products and services. One of these financial products is electronic payment services (EPS) or e-payment. However, security mechanisms deployed to safeguard this payment innovation is grossly inadequate. This necessitates the implementation of novel security technologies. In this paper, we highlighted the motivation for e-transaction, problem statement, identified technological gaps in the existing electronic transaction security authentication protocols and proffer solutions to the vulnerabilities with a view to mitigating the risks associated with e-transaction in order to boost customer confidence and promote financial inclusion.

Keywords: E-transaction, Cybersecurity, network security, financial inclusion.

Introduction

In addition, there is the possibility of aggregation of demand by several individual buyers, leading to better negotiation of prices on behalf of these buyers and search engines and rating sites providing aggregated information to the buyer about the different sellers of a particular goods or service are some of the features of e-transactions [2]. It is widely accepted that all of these changes have enabled efficiencies and the creation of wealth. Today, the internet has been able to facilitate research, e-mail, facsimile, e-bulletin boards, databases, file transfer, e-learning and e-commerce just to mention a few [3]. The emergence of information and communication technology has not only transformed the way businesses are conducted by moving it to the virtual domain, but has spurred innovative financial products and services. One of these financial products is electronic payment services (EPS) or e-payment. Payments effected to offset transactions done online or offline through virtual means are known as e-transactions and for e-commerce to be very successful, an efficient, effective, safe and secure e-payment system is imperative. E-commerce refers to the buying and selling of goods and services via computer mediated networks. Also, the use of formal payment systems enhances the ability to execute and manage monetary and fiscal policies, which is very essential for a country's financial and economic stability.

E-transaction payment models can either be in the form of digital cash, credit card, debit card, micropayment, money orders or electronic funds transfer (EFT). Each electronic transaction system has its own procedures and protocols, hence the availability of country and product-specific systems. The standardization of electronic transaction systems and networks has enabled them to grow at global scale. Examples of payment systems that have become globally available are credit cards, debit cards, point-of-sale (POS) terminals and automated teller machine (ATM) networks as shown in Figure 1 below.

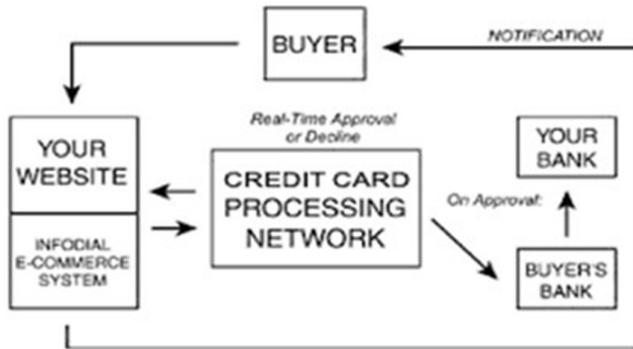


Figure 1: Architecture of e-commerce business model (Source: google.com)

Specific forms of payment systems are also used to settle financial transactions for products in the equity markets, bond markets, currency markets, futures markets, derivatives, option markets and to transfer fund between financial institutions both domestically using clearing and Real Time Gross Settlement (RTGS) Systems and internationally using the SWIFT network [4]. Electronic Payment Systems (EPS) apart from their convenience and safety also have a significant number of economic benefits which include mobilising savings and ensuring most of the cash available in the country are with banks. This will make funds available to borrowers both businesses and individuals. This information is also useful to the government when making decisions. EPS also have the ability to reduce cash handling and printing costs. According to Moody's Analytics [5] real global GDP grew an extra 0.2% per year on average beyond what it would have without card usage [4].

The payment system is the infrastructure consisting of institutions, instruments, rules, procedures, standards and technical means established to effect the transfer of monetary value between parties discharging mutual obligations [4, 6]. Its technical efficiency determines the efficiency with which transaction money is used in the economy and risk associated with its use [4, 6]. Nigeria is predominantly a cash-based economy with a lot of cash in circulation. Analysts opined that the cash-based nature of payments in the country is responsible for the abysmally low level of participation in e-Commerce where the acceptable medium of settling transactions is e-Payment [7]. Prior to the ICT revolution, over eighty percent of Nigerians rely on physical cash rather than electronic payment methods in their daily business transactions for both positive and negative reasons. It is positive because of its instant convertibility to other forms of value without intermediation of any financial institution and negative because of its anonymity and untraceability.

Problem Statement

Several factors militating against the widespread acceptance and adoption of electronic transaction and payment by the banking populace around the globe and threatens the financial inclusion agenda of the Central Bank of Nigeria include: Integrity; Non-repudiation; Confidentiality; Reliability; Authorization; Platform security and privacy respectively. Several scams have made Nigeria infamous such as Advance Fee Fraud (419) and individuals are concerned about fraud risks from e-transaction.

Vulnerabilities from the platform, hackers and virus attacks have led to many fraudulent incidents originating through e-transaction channels such as: US\$ 10 Million loss by Citibank of New York, U.S in 1995 and 20 Nigerians arrested in U.S for involvement in Multi-million dollar credit card fraud on April 7, 2013 are notable examples. This paper will critically evaluate the existing authentication protocols on e-transaction platforms in Nigeria so as to identify technological gaps and proffer a robust multi-factor authentication approach to address the limitations in existing authentication protocols.

Aim and Objectives

This research work aim at identifying technological gaps in the existing electronic transaction security authentication protocols and proffering solutions. The following research objectives will be explored so as to achieve the stated aim viz:

- a) Examine authentication services development in Nigeria financial system
- b) Investigate E-payment systems in Nigeria
- c) Identify key authentication services for e-transactions
- d) Evaluate various E-transaction security authentication protocols on the electronic transaction platforms of various banks in Nigeria

Motivation

The Central Bank of Nigeria (CBN) as the financial services regulatory body in Nigeria established by CBN Act of 1958 has been concerned with the high rate of e-banking frauds especially with the ATM being the commonest. In a bid to curb the alarming crime rate, the CBN had issued a circular to all banks in Nigeria to enforce migration from Magnetic stripe type of debit card to chip and PIN type of debit card (also known as Euro Master Visa - EMC or Verve cards). Fraudsters were able to clone debit cards as was the case before the migration and according to the CBN governor's statement in July 2013, "statistics showed that ATM fraud has been reduced by 90% in Nigeria", this has boosted customers' confidence in the use of ATM cards.

Moreover, consolidating on this achievement, the CBN is presently driving cash-less policy in order to strengthen the payment system in Nigeria and biometric authentication is being considered for point of sales (POS) and automated teller machine (ATM) e-banking services. Several breaches of e-transaction platforms as highlighted above have questioned the reliability and security of this novel and smart technology. This paper is motivated by these reasons and will investigate e-payment in Nigeria, evaluate existing e-transaction authentication protocols and authentication services development in e-transaction in Nigeria with a view to proffering solutions using multi factor authentication approach respectively.

Conceptual Framework and Review Of Related Works

The current inclination of Nigeria's Central Bank which is the predominant regulator in the sector appears to be to shape policy towards a Portuguese model in the mould of SIBS (Sociedade Interbancaria de Servicos-Interbank Services Company). SIBS was founded in 1983 and provides secure payment solutions including fully integrated cards, ATM and POS multi-system management (Visa, American Express, Mastercard etc), multi-vendor, multi-application processing and security management to support ATM, POS, On-line and mobile transactions. The Nigerian vehicle envisaged by the CBN to play this role is evidently Nigerian Inter-Bank Settlements System (NIBSS) owned by the banks, discount houses and central bank, with its board chaired by a CBN Deputy Governor. NIBSS Plc was set up in 1993 and commenced operations in June 1994.

NIBSS has put in place infrastructures for handling inter-bank payments, inter-bank funds transfer and settlements and operates the Nigeria Automated Clearing System (NACS) electronic funds transfer, Automated Direct Credits and Automated Direct Debits. NIBSS has acquired technologies for the operation of the Nigeria Central Switch (NCS). The other recent policy initiative from the CBN is the cancellation of the N100 charge levied by banks on ATM usage by customers of other banks with the objective of reducing cost of alternatives to cash.

While these initiatives may be attractive from the user/cost perspective (since NIBSS has a shared services, rather than profit objective), one consequence may be to discourage private, entrepreneurial initiatives [8]. A conceptual framework of e-transaction system is shown below in Figure 2.

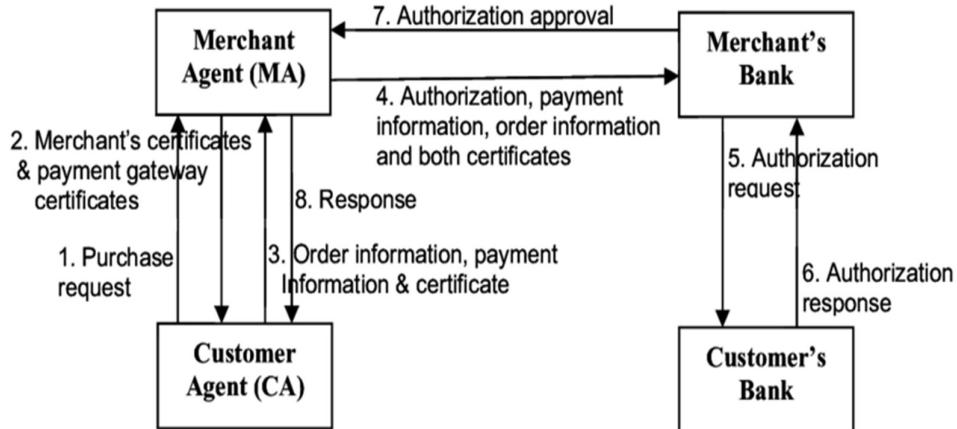


Figure 2: Transaction-flow-in-Secure-Electronic-Transaction

Source: https://www.researchgate.net/figure/Transaction-flow-in-Secure-Electronic-Transaction-SET_fig1_51953690

Important Security Requirements For Secure E-Transaction

For information to be secured, it needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability) [9]. Taxonomy of these three security goals is shown below in Figure 3:

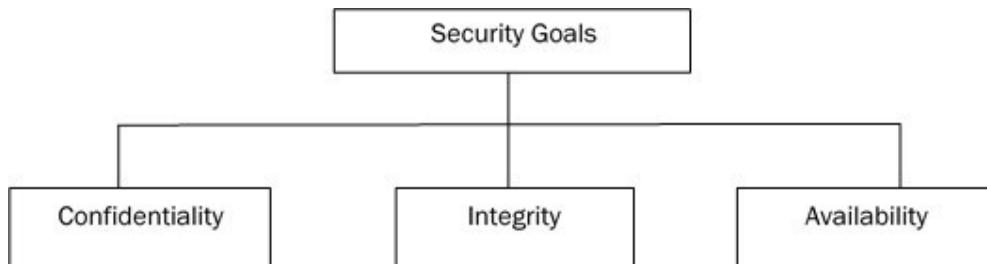


Figure 3: Taxonomy of network security goals [9]

Although the literature uses different approaches to categorizing network attacks, I will classify them into three (3) groups related to network security goals as shown in Figure 4 below.

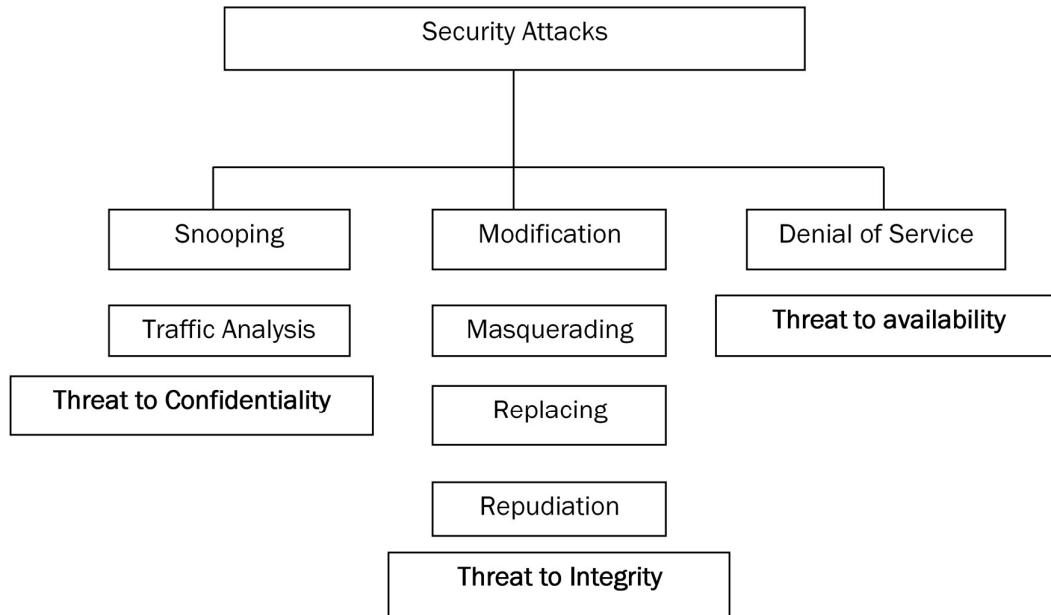


Figure 4: Taxonomy of computer security attacks with relation to security goals
Source: Forouzan, B. (2003), p.733 [9].

Recommendations for Secure E-Transactions

What follows are a set of recommendations

- 1) **Governance:** Payment Service Providers (PSPs) should implement and regularly review a formal internet payment services security policy.
- 2) **Risk Management:** PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services.
- 3) **Monitoring and Reporting:** PSPs should ensure the central monitoring, handling and follow-up of security incidents, including security-related customer complaints.
- 4) **Risk Control and Mitigation:** PSPs should implement security measures in line with their internet payment services security policy in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence-in-depth").
- 5) **Traceability:** PSPs should have processes in place ensuring that all transactions can be appropriately traced.

Conclusion

In work we highlighted the motivation for e-transaction, problem statement, identified technological gaps in the existing electronic transaction security authentication protocols and proffer solutions to the vulnerabilities with a view to mitigating the risks associated with e-transaction in order to boost customer confidence and promote financial inclusion.

References

- [1] Berners-Lee, T., Caillau, R., Luotonen, A., Nielsen, H., & Secret, A. (1994). The World-Wide Web. Communications of the ACM, 37(8), pp.76-82.
- [2] Arinze, U.C., Eneh, H.A., & Ezugwu, A.O. 2017. E-Commerce and Electronic Taxation in Nigeria, Nigerian Journal of Taxation Studies (NJTS).
- [3] Inyiamama, H.C. (2006): Computer and Information Technology Literacy, Positive Point Venture Publishers, pp. 181-187.
- [4] Okifo, J., & Richard, Igbunu. (2015). Electronic Payment System in Nigeria: Its Economic Benefits and Challenges, Journal of Education and Practice [Online], Vol.6, No.16, 2015. Available at: www.iiste.org [Accessed: 25/2/2017].
- [5] Moody's Analytics (2010). The impact of electronic payments on economic growth.
- [6] Massimo, C. & Gracia, J.A. (2008). Measuring Payment System Development. The World Bank.
- [7] Ayo, C.K. & Ukpere, W. I. (2010). Design of a secure unified e-payment system in Nigeria: A Case Study. African Journal of Business Management, Available online at <http://www.academicjournals.org/AJBM>, 4(9), pp. 1753-1760.
- [8] Agbaje, O. et al. (2013). Electronic Payments and economic growth in Nigeria, a report by RTC Advisory Services Limited.
- [9] Forouzan, B.A. (2008). Cryptography and Network Security, McGraw-Hill International Edition, pp. 1-10.