Mara International Journal of Scientific & Research Publications
Vol. 1, No. 1, June 2017, Pages 9 – 17

Understanding Security Status of an Online Banking Infrastructure

Makupi Daniel
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: dmakupi@kabarak.ac.ke

Received: June 19, 2017
Published: June 26, 2017

Abstract

In the present world of high-speed Internet connectivity, millions of transactions occur every minute. For these transactions, data need to be readily available for the genuine people who want to have access, and it must be kept secure from imposters. As the number of clients using online banking increases, online banking systems are becoming more desirable targets for attackers. To maintain the clients trust and confidence, security of their online banking services need to be assured; financial institutions must identify how attackers compromise accounts and develop methods to protect them. Towards this purpose, we propose a framework for assessing security status of an online banking infrastructure. Therefore, the said framework will take into consideration banking threats, infrastructure investment and defense in-depth strategies adopted by the financial institutions. The cumulative factors contributed from risk domains can then be used for computation of online status of a banking facility.

Keywords: Online, Banking, Security, Infrastructure

1. INTRODUCTION

Online banking is the facility of transacting or doing banking service over the public network (the Internet), through which customers can use different kinds of banking services ranging from the mobile transactions such as “Lipa na Mpesa” and pay bill facility provisioned by Safaricom (Garrett, P., & Regen, P., 2017). In advanced nations, online banking has been almost fully integrated to provision services, while the developing countries are just beginning to embrace these services. And to be realized as a fact it’s not so long ago, banks have embraced information and communication technology in the delivery of their products and services. With the proliferation of Internet, many of these banks are offering Internet banking services to their customers, in a bid to provide convenience, and to remain competitive. In an attempt to improve the quality of service delivery and customer experience, some banks have deployed Internet banking services to their customers, to enable them perform basic financial transactions such as balance enquiry and funds transfer. According to Clemes et al., (2012), the advent of the Internet has a significant impact on banking service that is traditionally offered by the branches to the customers. Internet banking can be defined as performing financial transactions over the Internet through a bank’s website.

It should be noted that a good number of banks in Kenya operate virtual banks. According to (Mueller, S. D. 2008), notes that Kenya faces unprecedented macroeconomic challenges with huge deficits expected to impact on the Kenyan economy for a significant period of time. The foreseeable economic challenges of two years ago as actuated and double up, and fueled government debt and inflation. These in effect, have translated to sharp depreciation of the local currency, and a weaker pace of economic growth. The situation as actually continued to be a Macroeconomic challenge. These issues have weighted negatively on

economic growth. The adding pertinent factors in the economy include the rising wage bill, high and rising interest rate, and continued upward trajectory of net international reserves. Aside from the negative impacts, banks play significant role in the Kenyan economy. It can be noted that commercial banks have continued to achieve impressive growth in terms of assets while providing the Kenyan economy with the necessary banking services. Indeed and especially with the advent of Internet and communication technology (ICT), which has significantly revolutionized the way business and service delivery is carried out by companies and businesses across the globe. The internet is seen as the nervous system of the 21st century and organizations recently are reaping the benefits of the internet's neural network; and, the banking sector is no exception (Qomi, M. A., et al 2014). The Internet also has continued to spread into banking technologies and now provides an important platform to keep customers engaged and remain competitive.

Also, the use of Internet in banking has become a useful channel of banking adopted by most banks to enable their valuable products and services to be availed to its customers. Contrary to the ideas by Njuguna et al., (2012) in which he observed that the use of network banking as a platform for carrying out banking services has continued to rise globally, and most banks particularly, in developing economies such as Kenya have recorded very low Internet banking users over the years. The unavailability of infrastructure support and also proper industry regulations will in long run impact negatively on the use of the Internet banking services offered by banks in Kenya. According to (Ameme, B. K., 2015), Kenya has had full Internet connectivity since 1993. The penetration rate during this period was 88%, since then, mobile data figures recorded an increase – today Kenya's mobile market has continued to grow steadily, supported by a mobile subscriber base of about 39 8 million by early 2017. Despite this impressive and rapid growth of mobile Internet usage, with the significant increase recorded in the use of mobile phones for financial services. This trend in comparison with developed countries is today among the highest. This is in negation to a study by Maria (2011) indicating that an increase in the use of electronic financial services is due to increase in internet penetration among the population, in contrast to Kenya, where for example, mobile leveraged the financial services by the majority of the population. The difference in these assertions is likely due to the fact that other factors besides Internet penetration rate lead to ICT powered financial adoption. Some attractive features of Internet banking service is the ability of customers to access their bank accounts at anytime, from anywhere and to perform such transactions as balance enquiry, statement of accounts request, cheque book request, electronic funds transfer among others. Despite these convenient features offered by online banking facilities, most banking customers prefer to use other channels of banking in, particularly the traditional method of electronic funds transfer.

Therefore, the secure handling of network banking services is very vital, it's critical especially in convenience offered by anywhere, anytime facility which is not provisioned in traditional banking. These necessitates financial institutions the need to ensure that these innovative technological services are supported by measures that maintain high and total customer experience with a sense of guarantee of service without interruption. Banking users need to be supported as soon as they experience challenges in using online services. This is supported by the fact that financial institutions do not fully understand the way customers experience banking websites, as customers generally do not have a platform on which to express their frustrations with online services and left to the chance of locating the physical branch, in the end, this does frustrate customers who intends to use online banking facility (Redlinghuis & Rensleigh, 2010). It is also very vital to ensure that these online services are much secured in order for users to develop confidence in these online banking infrastructures. As the numbers of customers increasingly rely on the internet for routine financials and investment, the threat of online fraud becomes a risk (Oghenerukeybe, 2008).

Banking customer need to be educated, in the how of using Internet banking, because it's critical to the adoption of Internet banking as some customers need to be aware of the benefits of these services and how to use them. Despite the fact that Internet banking provides a fast and convenient way to perform banking

transactions, customers are still reluctant to adopt and make use of these online services. All this advancement negates assertions that online banking is a disruptive innovation in banking industry, some of the bank customers in developing countries are hesitant to adopt this innovation, and are still keeping to the old paradigm of brick and motor branch banking (Clemes et al., 2012). Therefore, in order to grow consumer Internet banking adoption, banks must make key improvements that address consumer concerns (Kazi, 2013). Banks also need to understand and target customer groups and categories differently, in order to obtain significant efficiencies in their operations in online banking (Nerme, 2013). Therefore the relative success of internet banking can be gauged by identifying the current and anticipated users of internet (Munusamy, 2013). It is, therefore, crucial to investigate this phenomenon and to make recommendations that benefit both the banks and the customers.

1.1 Statement of the research problem

The lack of a framework for assessing the security status of an online banking facility has proved difficult to gauge the awareness and status level of risk factor exposure of a financial institution. Therefore, the method in place has been occasioned by operation of financial institutions in a silo, situation unaware of its risk factor level, because of being unaware of its status. Often when online attacks and fraud do happen that's the time a financial institution gets to understand they had vulnerability. The aftermath of fraud, the financial institution ends-up spending heavily on forensic investigators. In addition, there has not been a mechanism in form of a model to cumulatively come up with the threshold inform of status level as a result of risk exposure by financial institutions, therefore, this research will serve to inform the status level of risk tendency.

1.2 Objective of the study

Our main focus is to come up with a framework that would aid baking institutions to measure the security status of their online banking infrastructure by commutatively considering banking facilities, investments and defense in-depth strategies (SSOB).The status will serve to appropriately inform the security posture of the banking institution.

2. SURVEY OF LITERATURE

Transactions through online banking may include obtaining account balances and lists of latest transactions, electronic bill payments, and funds transfers between customers or their accounts (Schmidt, C., 2004). Therefore, some apps also enable copies of statements to be downloaded and sometimes printed at the customer's premises; while some banks charge a fee for mailing hardcopies of bank statements.

To access a financial institution's online banking facility, a customer with internet access would need to register with the institution for the service, and set up a password and other credentials for customer authentication. The credentials for online banking are normally secured against adversaries. Financial institutions now routinely allocate customers numbers, whether or not customers have indicated an intention to access their online banking facility. Customer numbers are normally not the same as account numbers, because a number of customer accounts can be linked to the one customer number. Technically, the customer number can be linked to any account with the financial institution that the customer controls, though the financial institution may limit the range of accounts that may be accessed to, say, cheque, savings, loan, credit card and similar accounts.

From the bank's perspective, online banking reduces the cost of transacting by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions. Online banking does not handle transactions involving cash, and a customer needs to visit an ATM or bank branch for cash

withdrawals or deposits of money. Many apps now have a remote deposit option; using the device's camera to digitally transmit cheques to their financial institution (Owens et al, 2006).

The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up. The types of financial transactions which a customer may transact through online banking are determined by the financial institution. Today, many banks are Internet-only institutions. These "virtual banks" have lower overhead costs than their brick-and-mortar counterparts. In Kenya, for example, the online banking as shifted to economic core of operation without which the Kenyan economy would be in crisis without an MPesa facility provided by Safaricom limited for mobile money transfer and also banking.

2.1.1 Security issues in online banking

The online banking facility is a powerful tool for increasing the accessibility of remote anytime anywhere banking, but it also provides potential openings for fraudulent activity committed against customer accounts online. Online thieves are continuously devising new means of gaining access to online banking facilities through online banking. Although banking sector is continually struggling to stay ahead of these adversaries, they have not been able to completely remove attacks occurring through customer devices or their adversaries.

The existence of banking as an industry is to guarantee the security of a customer's financial information without which the banking sector would be of less impact to the economy and, therefore, online banking. Similarly, the reputational risks to the banks themselves are important (Tiwari et al., 2006). Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted.

The use of a secure website has been almost universally being embraced such as single password authentication which still in use, it is by itself is not secure enough for online banking in some countries especially developing world also admitted by (Peterson, J., 2017).

The online attacks normally are of two main types; Attacks on online banking based on deceiving the user to steal login data and valid TANs through *phishing* and *pharming, Cross-site scripting* and *key logger/Trojan horses* are being used to steal login information (Ziegler, S., & Horváth, P., 2014). The other method are attacks on the *signature by manipulating* software being used in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

A 2008 U.S. Federal Deposit Insurance Corporation Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

In 2015, the British insurance company Lloyd's estimated that cyber-attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more (Morgan, 2016). Furthermore, from 2013 to 2015 the cybercrime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015 (Morgan, 2016).

The other kind of attacks are the so-called *man-in-the-browser attack*, a variation of the man-in-the-middle attack where a Trojan horse permits a remote attacker to secretly modify the destination account number and also the amount in the web browser.

As a reaction to advanced security processes allowing the user to cross-check the transaction data on a secure device there are also combined *attacks using malware* and *social engineering* to persuade the user himself to transfer money to the fraudsters on the ground of false claims (like the claim the bank would require a "test transfer" or the claim a company had falsely transferred money to the user's account and he should "send it back"). Among these are the attacks that are mostly being perpetrated in Kenya with financial institutions sometimes being unaware or lack the technical infrastructure to deter these attacks. And, in most cases, do not want to admit of the occurrence of breaches to protect their reputation.

3. PROPOSED FRAMEWORK

The framework that will aid in the implementation of the model to compute the online status of a banking infrastructure is as shown in Fig 1.

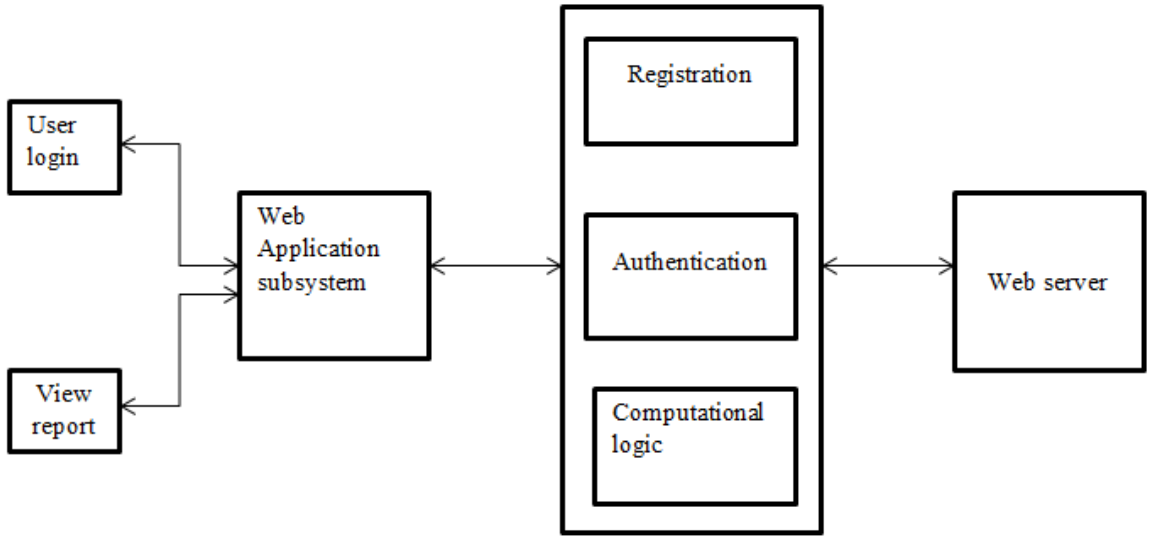

Fig 1: Web based Framework for computing online status (source: Author)

The operation of the framework is such that it will enable the users to be registered and consequently login to access the system. Once the user accesses the system depending on the need of the user as such could be a financial institution who may want to compute the online status of their online banking infrastructure then they would be able to do so by entering the attacks they have or considering their infrastructural investment and also their in-depth strategy.

3.1. Framework Operation

The online status of an online banking infrastructure will be derived from (OWASP) Open Web Application Security Project. The individual threshold of vulnerabilities will be taken into consideration based on its ranking from the security project. The percentage value of the attack will contribute to the online status of a banking infrastructure. The expert list of OWASP attack index of 2013 (Gao, J. B. 2013) is as shown Table 1.

Table 1: The expert list of OWASP attack index of 2013

Attack ranking	Type of attack
A1	Injection
A2	Broken Authentication and session mangemnt
A3	Cross-site scripting (XSS)
A4	Insecure Direct Object Refrence
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Insecure Cryptographic Storage
A8	Crossite-Scripting Request Forgery (CSRF)
A9	Using components with known vulnerabilities
A10	Unvalidated redirects and forwards

From Table 1 above, the attack vectors of an online based infrastructure ranking we can then be able to compute the status of an online baking infrastructure as follows:

Security Status of online Banking Infrustructure (SSOB) = Attack Vectors × Percentage Value Of Attack

Therefore, Security Status Of An Online Banking Infrustructure (SSOB) will be computed using the formula;

$$SSOB = F\ (A_1I_1 + A_2I_2 + A_3I_3 + \ldots\ldots\ldots\ldots\ldots\ldots\ A_nI_n)$$

Where: $A_1, A_2, A_3 \ldots A_n$ respectively are the weights that can be determined through focus groups.

While; $I_1, I_2, I_3 \ldots\ldots I_n$ respectively are the specific attack vectors that can be managed when the SSOB is computed.

The model works in the premise that an assigned threshold warrants a status. Attack will then be assigned weights depending on their ranking.

Therefore, once an agreed threshold is arrived at, it will serve to inform the type of attack such as the banking insecurity intensity and in this regard will be able to inform appropriately on the security status of an online banking infrastructure

4. DISCUSSION

The proposed system can present a number of advantages towards assessing online status of a banking infrastructure, these are:

- *Capture of user detail*: these details will be captured once, used many times and can be shared to other incidental utilizations.
- *Availability of user detail*: the financial institutions and customers will be enable to capture details of an attack vectors and, therefore, compute the online status of a banking infrastructure that would ordinarily not be impossible without considering the wide range of online vulnerabilities..
- *A system that's easy*: the utilization of the Web based model for computation of online status of a banking infrastructure will make it very easy to use.

- *Operation affordability*: the use of the Web based model will be relatively low cost because multiple users will connect to a common system.
- *Generation of report:* in implementing the framework it will make it possible to produce summary reports of security status of online infrastructure. This information is often not availably and accurate in the present setup that relies on manual records.

4.1 Challenges

The main concern that will be of a challenge especially to the financial providers will be provisioning the facility online. Some financial institutions might not be willing to fully welcome the idea of allowing members of public or account holders to know their security status.

5. CONCLUSIONS

This concept, therefore, envisions this approach of using a framework that automatically upon considering banking threats, infrastructure investment and defense in-depth strategies adopted by a financial institution, thus it automatically computes the security status. In its working the system will go hand in hand in appropriately informing the financial institution appropriately on their status.

6. AREAS FOR FURTHER STUDY

The proposed framework can also be utilized by government and other interested players in considering fraud exposure indexes of banks and also advising appropriately by coming with relevant laws to ensure banking institutions are up-to-date on their baking infrastructure security.

7. REFERENCES

Ameme, B. K. (2015). The impact of customer demographic variables on the adoption and use of internet banking in developing economies. *Journal of Internet Banking and Commerce*, *20*(2), 1.

Ayrga, A. (2011). Is Mauritius ready to e-bank? From a customer and banking perspective. *Journal of Internet Banking and Commerce*, *16*(1), 1.

Clemes, M. D., Gan, C., & Du, J. (2012). The factors impacting on customers' decisions to adopt Internet banking. *Banks and bank systems*, *7*(3), 33-50.

Detzer, D., Dodig, N., Evans, T., Hein, E., Herr, H., & Prante, F. J. (2017). The Institutional Structure of the German Financial System. In *The German Financial System and the Financial and Economic Crisis* (pp. 55-70). Springer International Publishing.

Gao, J. B., Zhang, B. W., Chen, X. H., & Luo, Z. (2013). Ontology-based model of network and computer attacks for security assessment. *Journal of Shanghai Jiaotong University (Science)*, *18*(5), 554-562.

Garrett, P., & Regen, P. (2017). *U.S. Patent No. 9,536,238*. Washington, DC: U.S. Patent and Trademark Office.

Kazi, A. K. (2013). An empirical study of factors influencing adoption of Internet banking among students of higher education: Evidence from Pakistan. *International Journal of Finance & Banking Studies*, *2*(2), 87.

Kregel, J. A. (2008). Changes in the US financial system and the subprime crisis.

Kumari, J. P. A Study of Online Banking Usage among University Academics. *Social Sciences*, *18*(18.75), 32.

Lallmahamood M (2007)Anexamination of individual's perceived security and privacy of the internet in malaysia and the influence of this on their intention to use E-commerce: Using An Extension of the Technology Acceptance Model. Journal of Internet Banking and Commerce12: 1.

Maria RA (2011) Adoption of E-banking in Romania–An Exploratory Study. Annals of Faculty of Economics1: 785-790.

Morgan, S. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019 https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3abb66f43a91

Mueller, S. D. (2008). The political economy of Kenya's crisis. *Journal of Eastern African Studies*, *2*(2), 185-210.

Munusamy J, De Run EC, Chelliah S, Annamalah S (2012) Adoption of retail internet banking: A Study of Demographic Factors. Journal of Internet Banking and Commerce17: 1-14.

Nerme P, Stenström C, Darefelt N (2013) Usage of Internet Banking Among Different Segments as an Example of Innovation–Trust and Information Needs. Journal of Internet Banking and Commerce18: 1-7.

Njuguna PK, Ritho C, Olweny T, Wanderi PM (2012) Internet banking adoption in Kenya: The case of Nairobi County. International Journal of Business and Social Science 3: 246-252.

Oghenerukeybe EA (2008) Customers Perception of Security Indicators in Online Banking Sites in Nigeria. Journal of Internet Banking and Commerce13: 1-15.

Owens, J., & Bantug-Herrera, A. (2006). Catching the technology wave: mobile phone banking and text-a-payment in the philippines. *Washington, DC: Chemonics International, Inc*.

Oyewole, O. S., Abba, M., & El-maude, J. G. (2013). E-banking and bank performance: Evidence from Nigeria. *International Journal of Scientific Engineering and Technology (IJSET)*, *2*(8), 766-771.

Peterson, J. (Ed.). (2017). *Institutions of the European Union*. Oxford University Press.

Qomi, M. A., Krakowiak, K. J., Bauchy, M., Stewart, K. L., Shahsavari, R., Jagannathan, D., ... & Ulm, F. J. (2014). Combinatorial molecular optimization of cement hydrates. *Nature communications*, *5*.

Redlinghuis A, Rensleigh C (2010) Customer perceptions on Internet banking information protection: original research. South African Journal of Information Management12: 1-6.

Schmidt, C. (2004). *Entwicklung eines neuen Datenakquisitionssystems für das CB-ELSA-Experiment* (Doctoral dissertation, PhD thesis, Bonn).

Thiemann, C. (2008). *Rechtsprobleme der Marke Sparkasse* (Vol. 60). W. Kohlhammer Verlag.

Tiwari, R., Buse, S., & Herstatt, C. (2006). *Mobile banking as business strategy: Impact of mobile technologies on customer behaviour and its implications for banks* (Vol. 4, pp. 1935-1946). IEEE.

Tiwari, R., Buse, S., & Herstatt, C. (2006). *Mobile banking as business strategy: Impact of mobile technologies on customer behaviour and its implications for banks* (Vol. 4, pp. 1935-1946). IEEE.

Tiwari, R., Buse, S., & Herstatt, C. (2007). Mobile services in banking sector: the role of innovative business solutions in generating competitive advantage.

Trommler, P. (2015). A FORMALLY VERIFIED DIGITAL SIGNATURE DEVICE FOR SMARTPHONES. *IADIS International Journal on Computer Science & Information Systems*, *10*(2).

Vaidya, S. R. (2011). Emerging trends on functional utilization of mobile banking in developed markets in next 3-4 Years. *International Review of Business Research Papers*, *7*(1), 301-312.

Ziegler, S., & Horváth, P. (2014). Auswirkungen von Basel III auf das Geschäftsmodell und auf die Steuerung einer Sparkasse. *Controlling*, *26*(11), 662-665.

Cite this article:

Makupi, D. (2017). Understanding Security Status of an Online Banking Infrastructure. MIJSRP. Vol. 1, No. 1, Pages 9 - 17