A Robust And Scalable Four Factor Authentication Architecture To Enhance Security For Mobile Online Transaction

Elliot Mbunge, Talent Rugube

Abstract This paper was focusing on the designing of a robust and scalable four factor authentication architecture to enhance security for electronic transactions. Mobile device are vulnerable to several security threats especially when purchasing good and services online. Currently, some banking institutions and e-commerce websites use two factor authentication to verify and validate customers when making online payments. Two factor authentication is regarded as the weakest authentication method. Mobile devices users are vulnerable to online mobile fraudulent activities due to several factors. The researchers designed a four factor security architecture to mitigate security threats because security is vital when making online transactions.

Index Terms: Authorization, multifactor authentication, online transaction

1 INTRODUCTION

SECURITY is of paramount importance when performing mobile online transactions in the modern world. Due to globalization, people buy and sell goods or services online. Statista (2017) stated that, "an estimated 1.61 billion people worldwide purchase goods online in 2016." This reflects the tremendous increase and magnitude of online shopping and E-commerce worldwide. Currently, customers are increasing using mobile devices to perform different online shopping activities such as booking, ordering mobile money transfer ,and also to make payments. Customers usually make online payments through mobile phones and smartphones. In United States of America , 125 million customers own smartphones and 62% of purchases were done through mobile devices in 2017 (Justin, 2018) . According to Rani (2018), 54% of online transactions are done through mobile phones and tablets , surpassing desktop computers. However , online mobile transactions are vulnerable to passive attacks (Usman & Akintoye, 2014) and active attacks (Ashish et al., 2013). These threats violate goals of security namely; avalilability , intergrity, non-repudiation, and confidentiality. Passive attacks are security threats that monitor, eavesdrop the network with the aim of gaining unauthorised access of information. Examples of passive attacks are ; traffic analysis, eavesdropping and monitoring . Active attacks are security threats that attempt to break the security system. Examples of active attacks include; Denial of Service (DoS), spoofing, modification, fabrication and wormhole (Mohan & Anuradha, 2015).

- *Elliot Mbunge is currently pursuing Doctoral studies program in Information Technology in South Africa. E-mail: mbungeelliot@gmail.com*
- *Talent Rugube is currently pursuing Doctoral studies program in Information Technology and Systems in South Africa. E-mail: ttrugube@gmail.com*

To counter these security threats , the researchers are proposing to design and develop a four (4FA) authentication to enhance security for online mobile transactions. Four factor authentication is the process of authenticating and authorising system user by using four factors; knowledge, possession, inherence and location factor (Asif et al., 2017).Kowledge is what the user know, possession is what the user have , imherence is what the user is, and location is the current physical location of the system user. Single factor , two factor and three factor authentication have security loopholes when making online payment. The traditional username and password have been prone to hacking , shared amongst system users and also exploited by illegitimate system users.

The objectives of this research are to:

- Determine online mobile transaction security threats.
- Design a robust and multifactor authentication architecture to enhance security for online mobile transactions.

This research intends to address the following research questions;

a) What are security threats being faced by customers when performing online mobile transactions.
b) How to design a robust and scalable multifactor authentication architecture to enhance security for online mobile transactions.

2 LITERATURE REVIEW

Most mobile users continue to protect the physical mobile handsets rather than data, yet not knowing that data is far more valuable than the handset itself. Mobile phone users and corporates should put in place strong security measures to ensure that data and network infrastructure are secured from unauthorized access.

2.1 Security in mobile devices

2.1.1 PINs/Passwords & Patterns

Currently, mobile devices are using Personal Identification Number (PIN) /Passwords and patterns to secure the device and data. PINs are usually an n-digit (where n may vary) code that users enter into their mobile device to unlock it. Other mobile devices use passwords which differs from a PIN in that it allows the use of alphanumeric letters and special

characters.

2.1.2 Mobile Operating System and mobile data

Mobile applications are installed on mobile operating system. Hackers exploit mobile operating systems to get unauthorized access to mobile applications programs, cache memory, and internal memory to manipulate data and the device.

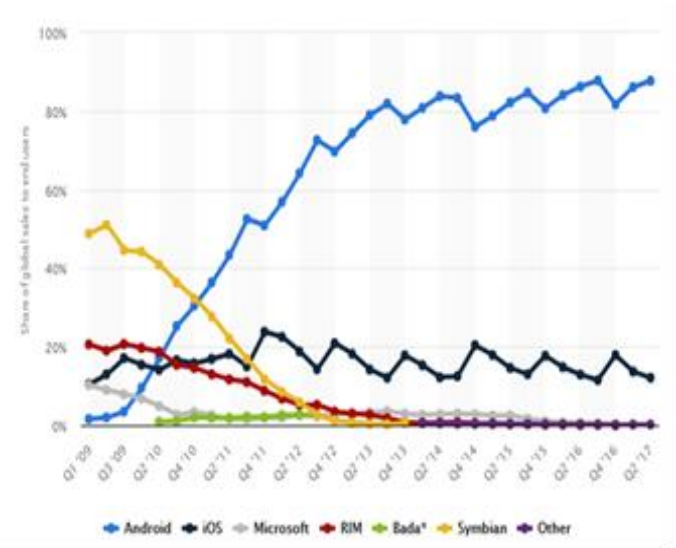

Fig 1. *Mobile Operating Systems, (Statista, 2018)*

According to Statista(2018), 87.7% of mobile phones, tablets and personal digital assistant (PDA) run on Android operating system followed with 12.1% of these devices execute instruction on iOS platform.All these mobile operating systems have their security flaws. For instance, Android operating systems allows Android applications to access system, user, device information and mobile device's external resources through permission-based model (Karthick & Sumitra, 2017). In most cases, Android users' grand permission to Android application programs to install from unknown and unreliable sources which makes online shopping (E-commerce) applications vulnerable. Once the application is installed, it has the privilege to access system (mobile) resources and user information anytime. It is rare but iOS were exploited by a malware called Pegasus in 2016, with the intention to have unauthorized access to private messages, calls, and electronic mails (Lucas, 2017). Once there is unauthorized access of information, customers are susceptible to different online and offline security threats. Mobile online transaction are increasing affected by vulnerability of mobile data at various levels such as application level , system level , device memory , and user's security knowledge also contributes. Factors impacting the vulnerability of mobile data are: lost or stolen mobile device with saved or cached PIN /passwords which enables online payment, malicious programs downloaded and installed on mobile device, unsecured internet connection, insecure web browsing, unavailability of security patch from both service provider and manufacturer, lack of customer security awareness programs (campaign) to educate customers on what to do when purchasing goods or services online.

2.2 Online mobile transactions security threats

2.2.1 Eavesdropping

It is an illegal interception of information in transit between the sender and receiver on real-time basis (Federico et al., 2016). Customer banking details such as bank card number, account number and card verification Value (CVV) can be tapped and later used for fraudulent activities (Elliot et al., 2017) by hackers. So to ensure that information in transit is safe and secure, modern unknown encryption algorithms must be used to communication link must be encrypted by using. In addition to that, customers must be encouraged to use secured online shopping websites (https). Secured Online shopping websites use Secure Socket Layer (SSL) protocol to ensure that information being transferred between web browser and the web server is not modified or tampered with by unauthorized people (Deepak & Nivesh, 2016).

2.2.2 Transaction Management

Real-time online transaction management is very difficult if the bank and payment gateway is not well synchronized. Time taken to reverse intermitted transaction usually affects other services.

2.2.3 Mobile Malware

Hackers can use mobile malware to carry out targeted attacks (spoon) to mobile device users. Malware usually operates in the background and reroute sensitive customer details with the aim of carrying out malicious transactions.

3 METHODOLOGY

Researchers considered four elements to authenticate online transaction. Such elements are: something the user has, something the user knows, Biometric feature and token. In Figure 1.2, customer starts to navigate e-commerce websites secured with Secure Socket Layer (https protocol). HTTPS protocol ensures that data being sent between e-commerce website and web browser is secured. Customer can add products to his /her shopping cart before logging in. When done, customer can checkout to process payment. At this point, customer has to login with traditional username and password authentication. The username might be PayPal customer's username and or customers' online banking username. During this phase, authentication process is done using two factor authentications – username and password. However, the challenge of using username and password is that it can be shared (Russell, 2017), and one can easily falsify the system pretending to be the legitimate user. In Figure 2, if login credentials are correct, and then customer is allowed to proceed with checkout process. A token is generated with session. Secure Socket Layer with https protocol secures (Joel, 2005) session id, username, password and other customer details when send from one

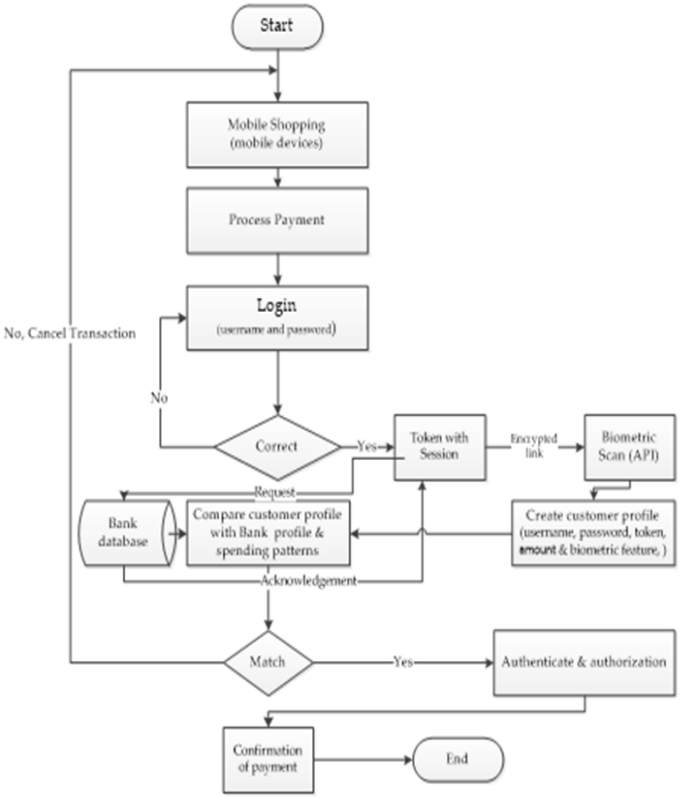

Fig 2, *Multifactor authentication architecture*

page to the other as well as from website to the web browser. A customer has to scan his/ her finger or any biometric element that was captured by the bank. Biometric feature is unique and not shareable because of its intrinsic physical traits. Biometric technologies include, fingerprint technology (Anil et al., 2010), iris technology (Vanaja & Laxman, 2014), face recognition (Renu, 2013), handy geometry technology, retina technology (Vaclav & Zdenek, n.d.), and voice recognition technology. Biometric features can be used as a verification and or authentication tool (Debnath et al., 2009). In this research, biometric feature is used as a verification tool after user logged in order to temporary customer profile. The temporary customer profile is made up of username, password, and token, amount to be paid and biometric feature. Temporary customer profile is compared with customer profile stored in the bank database to calculate the degree of similarity. If the degree of similarity is greater than or equal to threshold value, then it is regarded as a match, otherwise the transaction is called and labelled as suspicious transaction. A research conducted by Elliot et al.,(2017), customers spending patterns and login trials, customer mobile location could be used to create customer profile, and to classify e-transaction as either suspicious transaction or normal transaction. A token is a digit number (Manav & Shashikala, 2012) generated by the token generator module residing on the bank server side. It has a session time which means once its life span expires it becomes inactive. It is shared between mobile bank client application server and bank server side. Client
application server sends token generated to the customer's mobile phone / email. A token is used to create temporary

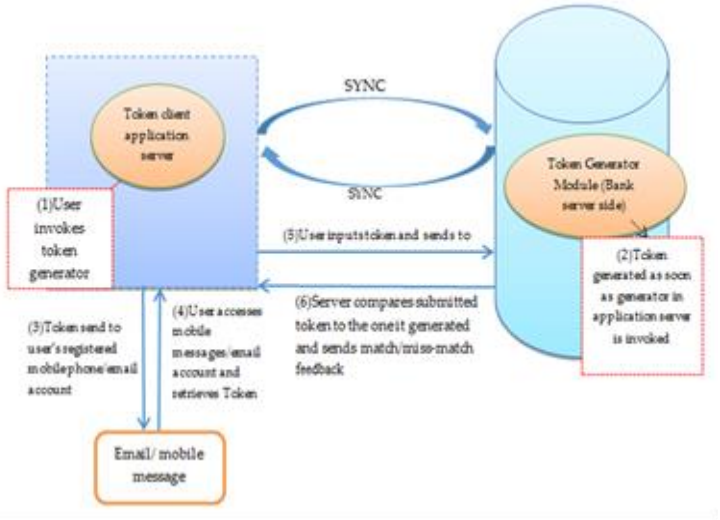

Fig 2, *Token generating module*

customer profile. Once the session lapses, then customer must login to get an active token to process e-transaction. The design in Fig 3 implements token generating module on the bank server side and the client application server only requests a token form the server side and then send it to the bank client's email address and mobile number submitted by the account holder during the sign up phase (bank account application phase). Both the server side and the mobile client application server must be synchronized to avoid too much time delays since the token is generated using session.

Token generation algorithm

The algorithm shows the steps that have to be followed when generating a session token:

i) Retrieve International Mobile Equipment Identity of mobile device.
ii) Retrieve International Mobile Subscriber Identity which is found in Subscriber Identity module in the mobile phone and it is unique.
iii) Retrieve current time (hour, minute and second) from the bank server side and client application server and then synchronize time. Each element should have its own variable.
iv) Record year, month and day of the month.
v) Bank client's username.
vi) Password/ Personal Identification number of the bank account holder (customer).

All these elements are concatenated and encrypted using SHA-1 hashing technique (Marc et al., 2017) and generate a six-character hashed string as a result. The encrypted concatenated outcome is send and decrypted with client application server

4 Conclusion

The purpose of this was to design robust design robust and scalable multifactor authentication architecture to enhance security for online mobile transactions. The size of a token is subjective from one banking institution to another. Some might adopt automatic authentication of the token from client application server. Some might choose to enter a token (digits) manually. The drawback of such technique is that some

customer may enter incorrect digits and then redirected to login again. This consume more time as compared to automatic verification of token between the client application server and bank server side. Future research may focus on design of a robust and scalable four factor authentication (4FA) on Automated Teller Machines (ATM) in banking institutions.

References

[1] Anil, J., Jianjiang, F. & Karthik, N., 2010. FINGERPRINT Matching. [Online] Available at: HYPERLINK "http://biometrics.cse.msu.edu/Publications/Fingerprint/JainFpMatching_IEEEComp10.pdf" http://biometrics.cse.msu.edu/Publications/Fingerprint/JainFpMatching_IEEEComp10.pdf [Accessed 20 February 2018].

[2] Ashish, W., Rugved, M. & Ashlesha, G., 2013. Mobile Commerce and Related Mobile Security Issues. International Journal of Engineering Trends and Technology (IJETT), 4(4).

[3] Asif, A., Israr, u.H. & Monisa, N., 2017. TWO FACTOR AUTHENTICATION. International Journal of Computer Science and Mobile Computing, 6(7), pp.5-8.

[4] Debnath, B., Rahul, R., Farkhod, A. & Minkyu, C., 2009. Biometric Authentication: A Review. nternational Journal of u- and e- Service, Science and Technology , 2(3).

[5] Deepak, K. & Nivesh, G., 2016. Security Issues in M-Commerce for Online Transaction. ieeexplore.ieee, pp.2-5.

[6] Deepak, K. & Nivesh, G., 2016. Security Issues in M-Commerce for Online Transaction. [Online] Available at: HYPERLINK "http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7784990" http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7784990 [Accessed 07 February 2018].

[7] Dimensional Research , 2013. THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS. [Online] Available at: HYPERLINK "https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf" https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf [Accessed 07 February 2017].

[8] Elliot, M., Ralph, M., Nation, C. & Antony, C., 2017. Fraud Detection in E-Transactions using Deep Neural Networks - A Case of Financial Institutions in Zimbabwe. International Journal of Science and Research (IJSR), 6(9), pp.1036 - 1041.

[9] Fadi, A., Syed, Z. & Wassim, E.-H., 2009. Multi Factor Authentication Using Mobile Phones. International Journal of Applied Mathematics and Computer Science , pp.65–80.

[10] Federico, M., Simone, G. & Giacomo, B., 2016. A Fast Eavesdropping Attack Against Touchscreens. [Online] Available at: HYPERLINK "http://www.syssec-project.eu/m/page-media/3/iclearshot-ias11.pdf" http://www.syssec-project.eu/m/page-media/3/iclearshot-ias11.pdf [Accessed 07 February 2018].

[11] Joel, D., 2005. How to secure session tokens. [Online] Available at: HYPERLINK "http://searchsecurity.techtarget.com/tip/How-to-secure-session-tokens" http://searchsecurity.techtarget.com/tip/How-to-secure-session-tokens [Accessed 20 February 2018].

[12] Justin, S., 2018. Mobile eCommerce Stats in 2018 and the Future Trends of mCommerce. [Online] Available at: HYPERLINK "https://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics" https://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics [Accessed 06 February 2018].

[13] Karthick & Sumitra, B., 2017. Android security issues and solutions. IEEE Xplore.

[14] Lucas, M., 2017. Android vs iOS security: Which is better? [Online] Available at: HYPERLINK "https://www.computerworld.com/article/3213388/mobile-wireless/android-vs-ios-security-which-is-better.html" https://www.computerworld.com/article/3213388/mobile-wireless/android-vs-ios-security-which-is-better.html [Accessed 07 February 2018].

[15] Manav, S. & Shashikala, T., 2012. Software Tokens Based Two Factor Authentication Scheme. International Journal of Information and Electronics Engineering, 2(3).

[16] Marc, S. et al., 2017. The first collision for full SHA-1. [Online] Available at: HYPERLINK "https://shattered.io/static/shattered.pdf" https://shattered.io/static/shattered.pdf [Accessed 21 February 2018].

[17] Mohan, P. & Anuradha, 2015. Network Security and Types of Attacks in Network. In International Conference on Intelligent Computing, Communication & Convergence. India, 2015. ScienceDirect.

[18] Rani, M., 2018. For the first time, more people will do their holiday shopping on mobile than on desktop. [Online] Available at: HYPERLINK "https://www.recode.net/2017/11/2/16582034/holiday-shopping-mobile-desktop-online-revenue-retail" https://www.recode.net/2017/11/2/16582034/holiday-shopping-mobile-desktop-online-revenue-retail [Accessed 06 February 2018].

[19] Renu, B., 2013. Biometrics and Face Recognition Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.93-99.

[20] Russell, B., 2017. TWO-FACTOR AUTHENTICATION IS

A MESS. [Online] Available at: HYPERLINK "https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess" https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess [Accessed 20 February 2018].

[21] Statista, 2017. E-commerce worldwide. [Online] Available at: HYPERLINK "https://www.statista.com/topics/871/online-shopping/" https://www.statista.com/topics/871/online-shopping/ .

[22] Statista, 2018. Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2017. [Online] Available at: HYPERLINK "https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/" https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/ [Accessed 07 February 2018].

[23] Tim, G., 2016. Startup touts four-factor authentication for VIP-level access. [Online] Available at: HYPERLINK "https://www.networkworld.com/article/3036293/security/startup-touts-four-factor-authentication-for-vip-level-access.html" https://www.networkworld.com/article/3036293/security/startup-touts-four-factor-authentication-for-vip-level-access.html [Accessed 06 February 2018].

[24] Usman, J.W. & Akintoye, O.O., 2014. MOBILE COMMERCE AND SECURITY ISSUES. International Journal of Scientific Research Engineering & Technology, 3(4), pp.1-6.

[25] Vaclav, M.J. & Zdenek, R., n.d. Biometric Authentication Systems. [Online] Available at: HYPERLINK "http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.3840&rep=rep1&type=pdf" http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.3840&rep=rep1&type=pdf [Accessed 20 February 2018].

[26] Vanaja, R. & Laxman, W., 2014. Iris Biometric Authentication used for Security Systems. Image, Graphics and Signal Processing, 9, pp.54-60.

[27] YoHan, P. et al., 2017. Security analysis and enhancements of an improved multi-factor biometric authentication scheme. International Journal of Distributed Sensor Networks, 13(8).