International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 9 Issue 3 Series. I || Mar.2020 || PP 16-21

Standalone Two Factor Authentication System Using Push to Approve

Jovworie Tanshi[1], Nkolika O. Nwazor[2]
[1,2]*Centre for Information and Telecommunications Engineering, University of Port Harcourt, Choba, Rivers State Nigeria*

Abstract:*The Push to Approve (PTA) application is proposed in this work with the purpose of authenticating a transaction on a banking application. This can be used to demonstrate the concept of two factor authentication that is more secure than One-Time Password sent over email service and Short Message Service (SMS) because of the higher vulnerability of email accounts and Short Message Service Centers (SMSC) of public telephone service carriers. The back end of the online banking system and the PTA application was built with hypertext preprocessor (PHP) while the front end was built with hypertext markup language (HTML), cascading style sheet (CSS), for the online banking platform and Java for the android application. The PTA application will require the user to provide a username and a password mapped to a particular time of the day in other to access and accept/decline an authentication request (valid for 59 seconds) for a transaction conducted on the banking platform.*

Keywords–*Cybercrime,Cyber Security, Encryption, Intrusion, Two FactorAuthentication*

Date of Submission: 28-02-2020 Date of Acceptance: 08-03-2020

I. INTRODUCTION

Cyber Security is not just a question of infrastructure but a question of awareness. This means that security concerns are not just about the technologies available but rather the way users and developers interact with them.

The internet was conceived around 1960's. Its usage was restricted to couple of researchers, specialists and defense as it were. Web client base have advanced exponentially. At first the PC wrongdoing was just kept to making a physical harm to the PC and related framework. Around 1980's the pattern changed from causing the physical harming to PCs to making a computer glitch utilizing a vindictive code called virus. Till then the impact was not all that far reaching since web was just bound to guard arrangements, enormous global organizations and research networks. In 1996, when web was propelled for commercial use, it quickly wound up prevalent among the majority and they gradually ended up reliant on it to a degree that it have changed their way of life. The GUIs were composed so well that the client don't need to bother how the web works. They need to just make few snap over the hyperlinks or type the ideal data at the ideal spot without wondering where this information is put away and how it is sent over the web or whether the information can gotten to by someone else who is associated with the web or whether the information parcel sent over the web can be ridiculed and tempered. The focal point of the computer crime moved from harming the computer or obliterating or controlling information for individual advantage to budgetary violations. These cybercrimes are expanding at a fast pace. Consistently around twenty five computers moved toward becoming unfortunate casualty to cybercrime and around 800 million people are influenced by it till 2013[1].

In the early stages of the design and development of the internet, security was not part of the concerns raised because the goal at that time was just for researchers to share and exchange knowledge. As the technology started expanding and gaining wide acceptance in the civil sector, fraudulent organizations and individuals in the Information Technology (IT) ecosystem started exploring the loopholes within the network to intercept, modify and even obstruct data transmission. The high growth of cybercrime brought about the emergence of the profession called Cyber Security. The sole purpose is to contain and minimize the crime rate (known as Cyber Crime) on the internet.

According to the work in [2], the worldwide expense of cybercrime has now come to as much as $600 billion — about 0.8 percent of worldwide Gross Domestic Product (GDP). More stressing than that figure might be the huge development from 2014, when a similar examination demonstrated the expense was distinctly as much as $445 billion [2].

The security challenges of internet banking have risen as internet banking platforms have become commonly used by the general populace. Of all the various authentication techniques, OTP (one-time password)

is regarded as one of the most effective methods of implementing two factor authentication, and it is now widely used on online banking platforms. However, attack methods that can detour OTP have been developed that additional security for OTP is now required [3].

Cyber security is the term for the techniques deployed to maintain a strategic distance from or decrease in unauthorized access to information, PCs or cell phones. Cyber security covers shielding, secrecy and protection, yet additionally the accessibility and integrity of information, the two of which are crucial for the quality assurance. Security bridges can happen when we use paper records, send data utilizing fax machines and even verbally. Be that as it may, the results of security ruptures with advanced data are conceivably unquestionably progressively serious, as data can be circulated all the more effectively and to a far more extensive group of audience [4].

Online security is crucial. The Internet has evolved tremendously over the last several years and computer networks are becoming bigger and bigger. Cyber security has turned out to be one of the most significant elements for organizations to consider. Today we perform financial payments via the Internet using mobile money transfer services, we perform banking operations online, and we make use of online health services. As a result, our data is everywhere: on our phones, laptops, work PCs, servers, and retailers' computer networks. In addition, hackers are becoming more sophisticated and offensive hacking tools are numerous and cheap [2].

Lots of world-famous companies have been attacked, including Sony, Adobe, Evernote, and LinkedIn. The biggest data breach in history was revealed in December 2016 when Yahoo said one billion accounts were compromised in 2013 [5].

These cyber-attacks have enormous consequences in terms of cost for the involved businesses. A research that Juniper published in 2015 predicts that cybercrime will cost businesses over US$2 trillion by 2019[6].

In other mitigate the operations carried out by these Cyber Criminals different authentication processes have been put in place such as encouraging internet users to use Alpha-numeric and special character based passwords. This has its own issues, as hackers can physically eavesdrop on users or use password sniffing tools to obtain their passwords. This gave rise to the introduction of Two-Factor Authentication (2FA) and Multifactor Authentication (MFA) that can be used to validate the identity of the user before providing access or completing an operation. Popular examples of 2FA and MFA techniques is the use of One-Time-Password (OTP) and Hardware token devices in conjunction with password and Personal Identification Number (PIN).OTPs that are passed over SMS and email are vulnerable to social engineering attacks. OTPs are also indirectly susceptible to man in the middle (MITM) and man in the browser (MITB) attacks [7].

Two-Factor Authentication (2FA) is a two-step verification process that aims to provide an additional layer of security by requiring the user to authenticate himself/herself using a secondary means (ownership factor or inheritance factor). If 2FA is not deployed, an attacker could obtain access to a person's devices or accounts simply by knowing the victim's password, while with 2FA knowing only this password is insufficient to pass the authentication check [8].

The literature review showed that SMS OTPs have proven to be vulnerable to interception. Hackers can now steal OTPs from the network service providers using specialized malware. This poses a serious risk for the user especially when the first level login credentials have been stolen. Some companies do not encrypt their email before sending to the user. If the OTP sent is intercepted, the user becomes vulnerable. Also, since most users access their email via browsers, the possibility of credential theft is still very high. If this is achieved, no further action is required to snatch the OTP. Also, when a push to approve link is sent to the user's the same method explained in no. 2 can be used to hijack the link. The reviews also showed that hardware token OTP device is usually not password. If stolen by a hacker, it can be used to authenticate transactions on a user's account, after stealing their first level login credentials. The google authenticator application is not also pass worded. This presents a risk to users that do not use password or pin to lock their device.

In the article by Camenisch et al, [9] the writers propose a two-factor confirmation convention which comprises of a biometric definition known as BioHash. This joins a client explicit unique finger impression Bi with a tokenized irregular number T which thus creates a lot of n double piece strings B = {b1, . . . ,bn}. This technique makes it hard for an enemy ADV to get hold of the required verification components (B, T) to try and make the last item required for an effective validation. Biometrics would not be a practical choice to use in your framework because of the high execution cost both on our side and on the customers side, additionally there are a few downsides with the precision of such frameworks as secured by the creators, false acknowledgment rate (FRR) and false acknowledgment rates (FAR) can be an issue inside said plots and are not something which we are expecting to address or enhance [10].

II. ANALYSIS OF THE EXISTING SYSTEM

SMS and email based one-time passwords are the most commonly used method of two factor authentication due to the ease of use.

This method of authentication is implemented with the use of encryption keys to generate the one time passwords, also known as tokens. Encryption keys are unique to each user. When the token/OTP is generated and sent to the user over an email/SMS service the user keys it in to authenticate the operation. The token may be numeric or alphanumeric, depending on the design technique implemented. Each token generated is unique to the user based on their encryption key. It is usually short-lived (between one to five minutes). When a user enters a token that doesn't match their encryption key, has lived its life cycle or incorrect, the server will not grant access or authorize the action of the user.

Another method similar to the SMS/email OTP is a physical hardware token and Google Authenticator. These systems generate one minute OTPs based on the encryption key that is unique to the user. The validation process is still similar to that of SMS/email OTP. The only difference is that, one is transmitted over SMS and email channel, while the other (Hardware Token and Google Authenticator) is physically present with the user and no third party channel is required to transmit the OTP.

Sim swapping which is a very common means of hijacking a user's mobile phone number can be used to obtain an OTP to access the user's account. If a user's account login credentials are obtained from the user's browser, there is a very high tendency that the email credentials may have been compromised alongside. Therefore, the intruder can access the OTP from there.

The hardware token and Google Authenticator don't make use of passwords. Turning on the hardware token or launching the Google authenticator application gives direct access to access the token. Although if a user exercises some caution, for example, desist from the use of untrusted browser plugins, pass-wording their mobile phones and keeping their hardware tokens in a very secure location, there is a 90% chance that they may never be compromised easily.

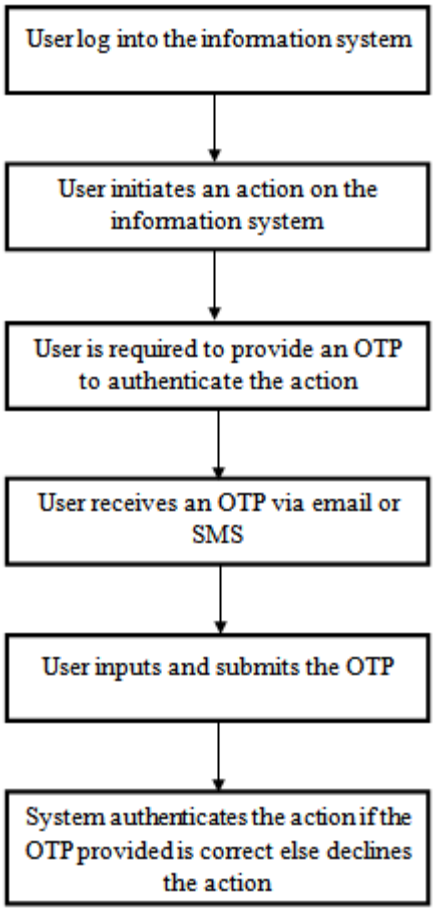

Figure 1: Block diagram of an information system that makes use of OTP

III. DESIGN OF THE PROPOSED SYSTEM

The proposed system is a basic banking portal that uses a push to approve standalone application to authenticate user operations such as login and fund transfers. When an operation is to be carried on the banking platform, a request will be pushed to the PTA application for the user to approve or decline the action. To be able to access the application, the user must use a specific time sensitive password to gain access into the approval interface. The application will have two passwords that can be used to access the interface at specific times of the day. Each password will be unique to a particular timeline within the day as defined by the user during set-up.

When a user launches the PTA application the application requests for a username and password. The user provides the password that matches the particular time of the day in other to gain access into the application.

1.1 ALGORITHM OF THE PROPOSED SYSTEM

The concept of the push to approve (PTA) application uses end-to-end encryption and password time mapping to authenticate actions in an information system. Actions on the information system, in this case; an online banking application, will be approved/authenticated using the PTA application that can only be access using either of two time sensitive passwords as specified by the user. The information system has its own first level authentication parameter which is the username and password. While the PTA application has makes use of a separate username and two passwords that can be used by the user depending on the current timeline as at the time of logging in.

Below is the workflow of the system:

1. A user visits the domain of the information system (e.g. ibank.tcomhq.com).
2. The user then inputs his/her login details (username and password) and logs into the platform. If the credentials are correct, he/she is given access into the banking application platform. If there is a credential mismatch, the user will not be granted access into the platform.
3. The PTA application makes use of two passwords that are mapped to different times of the day as set by the user (e.g. 6:00 am to 5:59pm for password one and 6:00pm to 5:59am for password two). Upon logging in, the user knows the password to access the application based on the current time of the day.
4. When the user tries to carry out a transaction on the banking system, (e.g. a bank transfer) an authorization request will be pushed to the PTA application for the user to approve the action. The request will contain a narration of the action the user wants to conduct on the banking platform. It will also give the user the options to accept or decline the action that has been initiated on the banking platform.
5. The PTA request is short-lived. If the user does not take action on the request expires after 59 seconds for security reasons.

The following procedures show the algorithmic approach adopted for the two factor authentication system that uses a push to approve standalone mobile application.

1.2 SYSTEM FLOWCHART AND ARCHITECTURE

Figure 2 depicts the architecture of the proposed system, which shows the overall process. PTA application is implemented as an intermediary consumed by web application and mobile application. Any web-based programming language can be used to implement. A database is built along with the web service to store data when users interact via website and mobile application interface. More emphasis should be placed on the mobile application that will handle the PTA request, and transmit the decoded message to the web server.

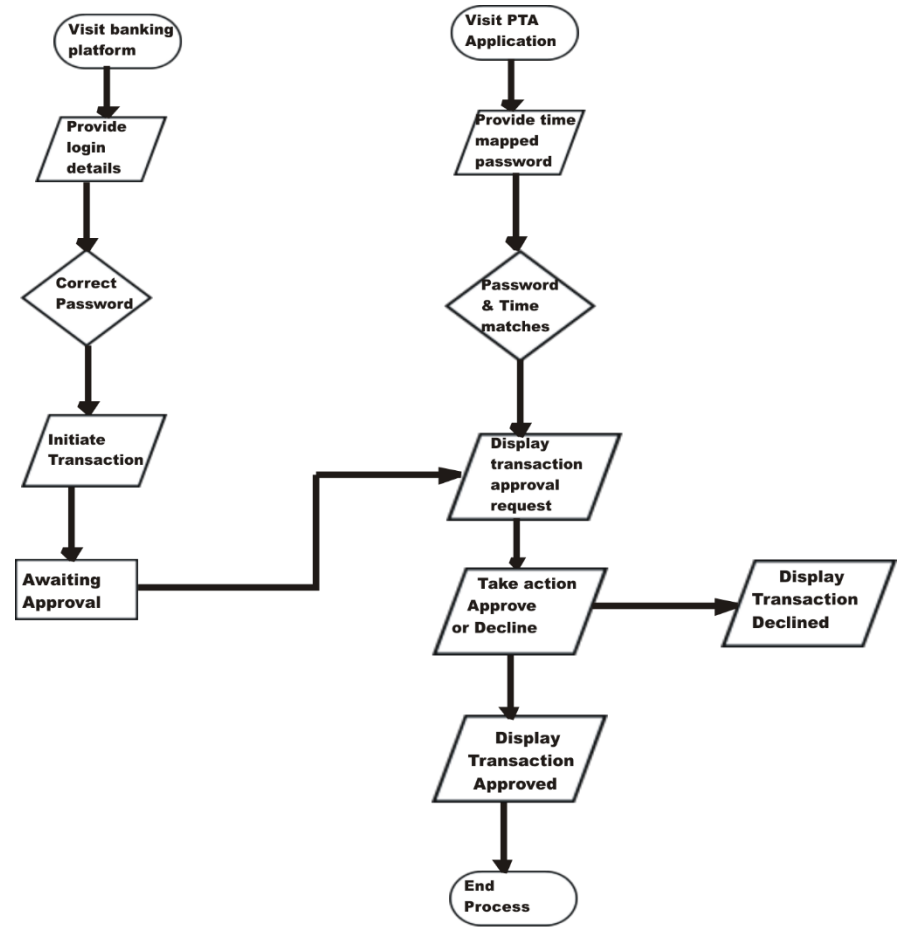

Figure 2: Flowchart of the Proposed System

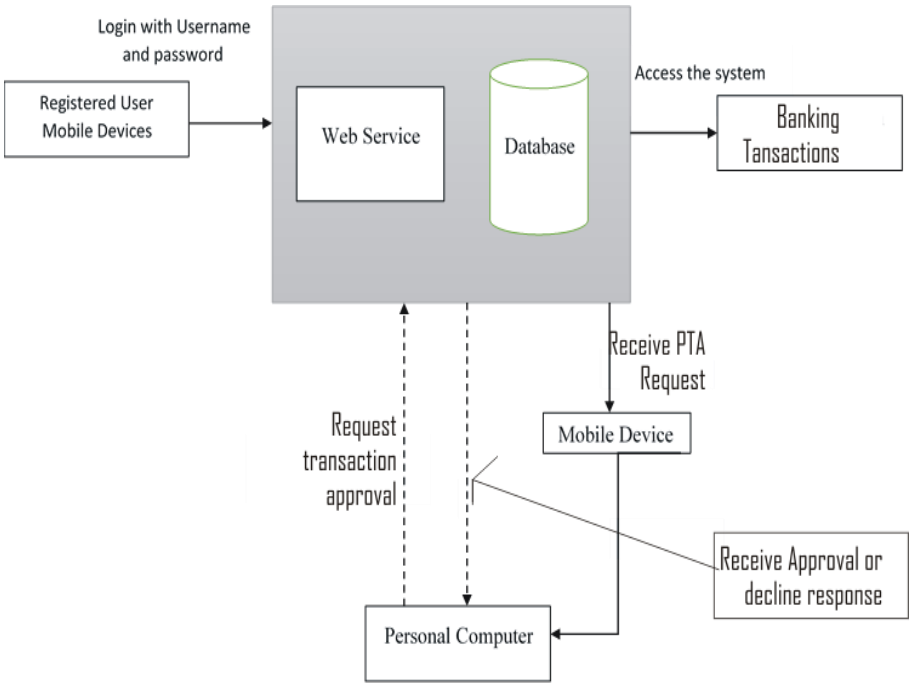

Figure 3: System Architecture

IV. CONCLUSION

The issue of cyber-crimes, especially in the aspect of credential and OTP snatching is of major concern to the cyber community and organizations that make use of real time systems. In this research, we proposed a

Push to approve application that makes use of password time mapping to give access to the user to authenticate actions on an information system. This system will be very useful in ensuring users are more secure and will be fully responsible for the actions they take on their accounts.

REFERENCES

[1] Barry M. Leiner, V. G. (s.j.). Brief History of the Internet. Onttrek Dec. 20, 2015. Available online: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License [Accessed: September 2, 2019].

[2] Lynette Lau, "Cybercrime 'pandemic' may have cost the world $600 billion last year 2018". Available online: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html [Accessed: September 2, 2019].

[3] Yoo, C., Kang, B. T., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications, 74(10), 3289–3303. Available online: https://doi.org/10.1007/s11042-014-1888-3 [Accessed: September 8, 2019].

[4] Cavelty, M. D. Cyber-security. (2017, May).Available online: https://www.researchgate.net/publication/256018865_Cyber-Security [Accessed: September 2, 2019].

[5] V. Goel and N. Perlroth, 'Yahoo Says 1 Billion User Accounts Were Hacked', The New York Times, 14-Dec-2016. Available online: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [Accessed: September 9, 2019]

[6] J. Moar, 'The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation', Juniper, Dec. 2015. Available online: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businessesover-2trillion. [Accessed: September 9, 2019]

[7] Rakesh Thatha, Limitations of two factor authentication (2FA) technology. Published on Computer Weekly: 25 Sep 2012. Available online:https://www.computerweekly.com/tip/Limitations-of-two-factor-authentication-2FA-technology [Accessed: September 5, 2019]

[8] NiklasTellini and Fredrik Vargas, Two-Factor Authentication; Selecting and implementing a two factor authentication method for a digital assessment platform. Degree Project In Computer Engineering, First Cycle and DegreeProjectin Information and Communication Technology, First Cycle Stockholm, Sweden 2017

[9] Jan Camenisch, AbhiShelat, Dieter Sommer, et al. Privacy and identity management for everyone. In DIM '05: Proceedings of the 2005 workshop on Digital identity management, pages 20-27, 2005.

[10] Costa, J. (2017). 2FA2P2: A Two Factor Authentication Scheme. (June), 11. Available online: https://doi.org/10.13140/RG.2.2.16228.99207 [Accessed: September 6, 2019].

Jovworie Tanshi "Standalone Two Factor Authentication System Using Push to Approve." International Journal of Engineering Science Invention (IJESI), Vol. 09(03), 2020, PP0 16-21.