Turkish Journal of Computer and Mathematics Education Vol.12 No.12 (2021), 948-*953*

Research Article

Multifactor Authentication On Mobile Phones UsingExisting BrightPass

Ms.Saylee Deshpande[1], Vimla Jethani[2]

[1]Computer Engineering RAIT, Mumbai, India Email:sayleedeshpande11@gmail.com
[2]Computer EngineeringRAIT, Mumbai, India Email:vimlajethani@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract—The use of smart phones have increased rapidlyin the last few years.Due to the emerging technology, Internetis a wide choice for various transactions such as e-business, e-commerce, e-banking .For this smart phones become very useful devices, so these phones are interesting targets for hackers. To maintain the extraordinary level of trust industry should adopt strong authentication mechanism . Earlier single factor andtwo factor mechanism are vulnerable to malware attack. More advanced malware can easily bypass OTP based two factor authentication by intercepting the OTP. The OTP which comes from SMS can easily be stolen. Further, SMS costs and delaysin SMS are drawbacks in this system. .There is need to developa system which generates secure OTP on the mobile device itself which is secure from attackers. With the help of out of bandauthentication which uses two different communication channels for authentication system lessen the probability of attack on the system. So, to enhance the security in transactions we are going propose a system which generates OTP on the mobile itself with the help of lie sequence in the BrightPass .We are using nested hashing function to generate an OTP which adds complexity for an attacker. With the help two channels such as internet andmobile phones the chances of attack on our system is very low. Ourproposed system presents a multi-factor authentication in which a users device produces a PIN from seed from various parameters. This proposed system reduces the limitations of the SMS system.

Keywords—*Multi-Factor Authentication, BrightPass, Nested Hashing , Secure OTP Generation on Mobile*

I. INTRODUCTION

Mobile usage increases drastically over few years. Thereis a development in information technology because of which people using it are in increasing number. People have adopted mobiles for communication and computing. With mobile ap- plication user daily life transactions become easy using smart phones. There are many advantages of one device for many transactions and rich user interactions. But with the increase in mobile communication, hackers grows their interest in such platform for their personal use. Hackers exploit these internet resources for their own purpose. In order to avoid this there is need to secure these internet resources. For this purpose strongauthentication mechanism is required. Traditional PIN based single factor authentication mechanism is vulnerable to many spy ware attacks .Current password based mechanism is not fully protected and attackers can easily crack these passwords and vulnerable to automated attacks. So the single authentication mechanism is a security weakness in transaction. To avoid this researchers have proposed two factor authentication which includes OTP received via SMS is useful to confirm users identity. But these technique for authentication purposeis vulnerable to malware attack. So there is need for multi- factor authentication mechanism for secure transaction. Toenhance security in transactions we are proposing a system which generates OTP on mobile device itself with the helpof lie overhead concept in earlier BrightPass system. We are going to propose a system which generates OTP on mobile phones uses two different hashing functions. For this purpose two nested hashing algorithms are used.

II. LITERATURE REVIEW

PassWindow [2], a method which uses digits of PIN anda already selected image as Pass-icon as

the password. [3] proposed a dummy-key password authentication mechanism known as FakePIN. [10] proposed CAPPCHA mechanism. To overcome this we are going to propose a system which involves two factor authentication techniques and create a multifactor authentication for safer transactions.

First one is earlier BrightPass system,To enhance the security of mobile transactions, BrightPass concept increases the security of classic PIN based mechanism. The basic idea isto use the concept of lie overhead where user has to enter a combination of true values of PIN digits and lies provided by Secure Element in the mobile. The high brightness value indicates that user has to enter true PIN value whereas dark circle indicates user should enter misleading value. As SE generates PIN sequence for every authentication randomly, so even mobile malware can not detect the PIN position for next authentication because of randomization PIN digits for every authentication.

III. PROBLEM DEFINITION

Usage of OTP using SMS as second factor of authentication is widely used. The security of OTP delivered over the SMS is based on network operators. But unfortunately mostof the service providers using less secure network to deliver SMSs. Because of this hackers can intercept to network and divert the OTPs. Also many times it becomes inconvenient to read sms and type it on application interface. Sometimes dueto incomplete transaction hackers can acquire OTP through SIM Swap Attack .Sms OTPs do not protect against MITM (man-in-the-middle)attacks either so an attacker take over a

connection where a user has sent an OTP. Additionally , the delay of SMS OTP delivery represents the major limitations ofthe system. While travelling if users roaming is not activated then user will not get the OTP SMS delivered , another limitation of SMS based OTP. The cost of SMSs and network coverage are other problems associated with it. So to enhance the security in mobile communication on mobile phones weare proposing a system which uses lie sequence mechanismin existing BrightPass with nested chain hashing for secure OTP generations on mobile phones itself in electronic paymentwith the help of Multi-Factor Authentication .With the this system we are going to add a layer of security in authentication mechanism.

IV. PROPOSED SYSTEM

In this section we are going to propose a new authenticationscheme for secure OTP generation using smart phones. For thiswe are proposing a system which uses lie sequence methodin BrightPass mechanism with a nested hashing function for secure OTP generation on mobile phones. With the help of thissystem , security in the transaction has been increased through multi-factor authentication .his system works as follows- Whenuser wants to start communication with server after submittingcredential online to website, ssl has been established between server and client. Server challenges the user with two variablesand server calculates own OTP using same index variablesand server side SEED at the same time .The user enters the same variables in the system which generate client side PIN on device itself. This OTP is calculated with nested hashing functions on SEED .SEED is the combination of IMSI no., IMEI no. , account number. This OTP will now enter with BrightPass mechanism to get page authenticated. Our proposaluses lie overhead concept in BrightPass method to safely insert client sided OTP with the help of lie sequence which is randomly generated by SE to enhance security in transactions while generating OTP in mobile with the help of Multi-Factor authentication. For OTP generation user and client will use nested hashing function to avoid collision. After submittingthe OTP with BrightPass method. Server will check its own calculated OTP and if its matches with client side OTP, the server will ask for predefined security questions. If the answer matches with earlier registered answer the authentication completed and the page will be authenticated.

Our proposal works as follows-

Registration-1

a. User have to register on the banks website through mobile application with these inputs as follows- - User name with Email - Passcode - Predefined Question and their Answers
b. The mobile application reads and sends the IMEI and IMSI to the server
c. After receiving inputs server will creates an account forthe user such User name, password and predefined Security Questions and their Answers
d. Server will concatenate IMEI, IMSI, account number to

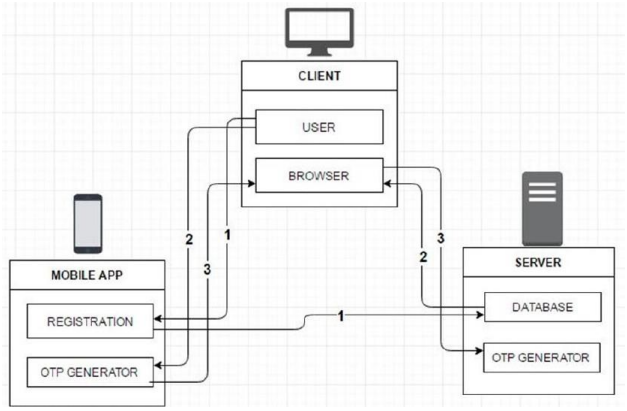

Fig. 1. Two Factor Authentication Architecture

produce a server side seedRegistration-2
a. User will allow to enter his newly created accountnumber in the PIN section of the app
b. The app will concatenate IMEI, IMSI, account Number toproduce a client seed

Login- 1

a. User access account into server website with user nameand passcode
b. Server will check users credentials and create a SSLconnection
c. Server will create and show two variables x and y and willshow on clients web page
d. Server will use these variables x and y to create a serversided OTP with nested hashing functions.

Login-2

a. User t will also use the these two variables x and y inthe systems PIN section to generate client side OTP
b. The app will create a client sided OTP using hash chainwith seed
c. This generated OTP will now enter through BrightPassmechanism and submit through our system in online mode. d. After validation of server of user submitted OTP the Fourth factor of security in our proposal is to answer pre-definedquestions

Our proposal is focuses on secure transactions which uses PIN verification techniques in e- payment applications using BrightPass and nested chain hashing both.

Example

IMEI : 813589069458989
IMSI : 415151001385048

ACNO : 1338-02
Bank Code : 1338UserID : 1

Concatenate (IMEI, IMSI, ACNO) Concatenate(813589069458989+415151001385048+133801) Seed = 813589069458989415151001385048133801

Formula : Seed $\gg$ $HBy(HAx(Seed))$ $\gg$ $FinalHashValue \gg 4digitOTP$

It is performed on server client side in parallel Hashing Function : Used by client server to generate 4 digit OTPfrom seed

HB = SHA, HA = MD5 Hashing Index (x,y) : Generatedby Server, Sent to client

x is SHA256 rounds, y is MD5 rounds

Minimum Maximum number of rounds to be applied on seed: limit of hash index Min : (x,y) = (1,1) rounds, Max :(x,y) = (10,10) rounds

e.g. : Index (x,y)=(1,1)

Seed : 813589069458989415151001385048133801

Formula : Seed $HB1(HA1(Seed))$ $HashValue$ $\gg$ $4digitOTPSeed$ $MD5(SHA(Seed))$ $HashValue$ $4digitOTP$

Seed $\gg$ $SHA(Seed)$ $\gg$ $0d63c393a9bff3d5c331263ba0b673d47999dea63de4b48a22a268a079ca81f9MD5(SHA(Seed)) \gg 2e630cb5ee25aff672d7ef1c986fc4ce$

Final Hash Value : 2e630cb5ee25aff672d7ef1c986fc4ce
$\gg Convertinto4digitOTP$

e.g. : Index (x,y)=(2,3)

Seed : 813589069458989415151001385048133801

Formula : Seed $HB2(HA3(Seed))$ $HashValue$ $6digitOTP$

Seed $\gg HA3(Seed)$: $3roundsofSHA(Seed)$
Round 1 SHA :3f4d2e67a1010fd1a2072033a5f7495f9331eca9a999f8717f67b2699b31965d

Round 2 SHA :582504e52b842be08c704df0b49ef6c0309d06ba193c78f7b27ed10f8dee04b4

Round 3 SHA :d84738654926d1ea17b2c76a9eef604bd5fc8ec0edb867928c8a8b9ec8eac0fe

HB2(SHA-3) $FinalHashValue$ $:2roundsofMD5on(Round3SHA)$
$Round1MD5$: $3265b97837c9ab2c77c8fdf099e2cc02$
Round 2 MD5 : 812961c4ea21d22f3833833f778ff26a Final Hash Value : 812961c4ea21d22f3833833f778ff26a
$» Convertinto4digitOTP$

Security Question

Pre-defined Questions to be listed on registration page

V. CONCLUSION

As the mobile transaction increases there is fear of possible attack also increases. These m-transactions are vulnerable to identity theft attack. To avoid this there is need of proper multi-factor authentication mechanism. But this authentication is the weakest element in security scenario. The earlier SMS based two factor authentication mechanism is vulnerable to malware attack. So we are going to propose a system which uses lie overhead concept in BrightPass mechanism with nested chain hashing which uses two hashing function in which OTP will generate in offline mode on the mobile device itself and predefined questions which add more security to mobile transactions. We are trying to overcome disadvantages of SMS OTP based two factor authentication by using multifactor authentication.

REFERENCES

1. Guerar M, Migliard M, Merlo A, Benmohammed M, Palmieri F, Castiglion A, "Using screen brightness to improve security in mobile social network access" IEEE DOI:10.1109/TDSC.2016.2601603
2. Choudhary, B., Risikko, J.: "Mobile Financial Services Business Ecosystem Scenarios Consequences". Mobey Forum Mobile Financial Services Ltd (2006)
3. Yi, H., Piao, Y.,Yi, J.H.: "Touch Logger Resistant Mobile Authentication Scheme Using Multimodal Sensors." In: Advances in Computer Science and its Applications, Volume 279 of Lecture Notes in Electrical Engineering, pp.19-26. Springer, Berlin (2014)
4. Kim, S., Yi, H., Yi, J.H.: "FakePIN: Dummy Key Based Mobile User Authentication Scheme." In Ubiquitous Information Technologies and Applications, Volume 280 of Lecture Notes in Electrical Engineering
5. ,pp.157-164, Springer, Berlin (2014)
6. L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum. "ReCAPTCHA: Human-Based Character Recognition via Web Security Measures." Science, September 2008
7. Reynaga, G., Chiasson, S.: "The Usability of Captchas on Smartphones."In: Proceedings of SECRYPT pp.427-434, SciTePress (2013)
8. Reynaga, G., Chiasson, S. and van Oorschot, P. C.: "Exploring the usability of captchas on smartphones: Comparisons and recommendations." In Proceedings of 2015 Network and Distributed System Security (NDSS) Symposium. pp. 8-11, (2015, February)
9. Chow, R., Golle, P. Jakobsson, M., Wang, X., Wang, L.: "Making CAPTCHAs clickable." Ninth Workshop on Mobile Computing Systems and Applications (HotMobile 2008).2008 February 25-26; Napa, CA
10. Jha, Rakesh Kumar, Suresh V. Limkar, and Upena D. Dalal. A performance comparison of routing protocols for security issue in wireless mobile ad hoc networks. Third International Conference on

Emerging Trends in Engineering and Technology. IEEE, 2010

11. Choudhary, B., Risikko, J.:" Mobile Financial Services Business Ecosystem Scenarios Consequences." Mobey Forum Mobile Financial Services Ltd (2006)
12. Guerar, M. , Migliardi, M., Merlo, A. , Benmohammed, M. , Messabih,B.: "A Completely Automatic Public Physical test to tell Computers and Humans Apart: A way to enhance authentication schemes in mobile devices."International Conference on High Performance Computing Simulation (HPCS),Amsterdam, 2015, pp.203 - 210.
13. https://duo.com/blog/answer-to-otp-bypass-out-of-band-two-factor- authentication
14. Mohamed Hamdy Eldefrawy1, Khaled Alghathbar1, 2, MuhammadKhurram Khan1:OTP-Based Two-Factor Authentication Using Mobile Phones1Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia,Information Systems Department, College of Computer and Information Sciences, King Saud University, Saudi Arabia.2011 Eighth International Conference on Information Technology: New Generations
15. www.panamaxil.com