IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 85-90
www.iosrjournals.org

Two Factor Authentication Using Smartphone Generated One Time Password

Sagar Acharya[1], Apoorva Polawar[2], P.Y.Pawar[3]
[1](Student, Information Technology, Sinhgad Academy Of Engineering/ University of Pune, India)
[2](Student, Information Technology, Sinhgad Academy Of Engineering/ University of Pune, India)
[3](Asst. Prof, Information Technology, Sinhgad Academy Of Engineering/ University of Pune, India)

Abstract:*This paper explains a method of how the two factor authentication implemented using SMS OTP or OTP generated by Smartphone- One Time Password to secure user accounts. The proposed method guarantees authenticating online banking features are secured also this method can be useful for e-shopping & ATM machines. The proposed system involves generating and delivering a One Time Password to mobile phone. Smartphone can be used as token for creating OTP or OTP can be send to mobile phone in form of SMS. The generated OTP is valid for only for short period of time and it is generated and verified using Secured Cryptographic Algorithm. The proposed system has been implemented and tested successfully.*
Keywords - *OTP, Authentication, SHA-1, Cloud, token, Android*

I. INTRODUCTION

Security is a major concern today in all sectors such as banks, governmental applications, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. The rapid growth in the number of online services leads to an increasing number of different digital identities each user needs to manage. But passwords are perhaps the most common type of credential used today [1]. To avoid the tedious task of remembering difficult passwords, users often behave less securely by using low entropy and weak passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Moreover passwords can be written down, forgotten and stolen, guessed deliberately being told to other people.

Several proper strategies for using passwords have been proposed [2]. Some of which are very difficult to use and others might not meet the company's security concerns. Some solutions have been developed to eliminate the need for users to create and manage passwords. A typical solution is based on giving the user a hardware token that generates one-time-passwords, i.e. passwords for single session or transaction usage.

Moreover token also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen. So we have a provision of OTP in Mobile, but there are major hurdles in that, we have to install OTP generation software in all clients mobile, the time in both mobile and server has to be always synchronized, if client purchase a new mobile, the mobile have to be registered and installed with the OTP generation software, updated software have to re-installed in all client mobile.

In this paper, we propose a securely generated and verified OTP using smartphone. Installing third-party applications allows mobile phones to provide expanded new services other than communication. The use of mobile phone as a software token will make it easier for the customer to deal with multiple two-factor authentication systems and will also reduce the cost of manufacturing, distributing and maintaining millions of hardware tokens. Sometimes OTP is sent to user mobile phone as a SMS with Transaction details. SMS is riveted because SMS is a ubiquitous communication channel, being available in all handsets. SMS messaging has the tremendous potential to reach all customers with a low total cost of ownership.

II. LITERATURE CITED

Online banking is a very prominent area and has many methods to make the transactions more secure. One time passwords, two factor authentication, digital certificate verification are considered to provide more security than general PIN number authentication. Authentication is the process of verifying the correctness of a claimed identity. It is a way of ensuring that users are who they claim to be when they access systems.

Three universally recognized authentication factors exists today: what you know (passwords), what you have (tokens, cards) and what you are (biometrics). Recent work has been done in trying alternative factors, for example somebody you know, a factor that can be applied in social networking.

Passwords are known to be one of the easiest targets of hackers. Therefore, most organizations are looking for more secure methods to protect their customers and employees. Biometrics are known to be very secure and are used in special organizations, but they are not used much to secure online transactions or ATM machines given the expensive hardware that is needed to identify the subject and the maintenance costs, etc. Instead, banks and companies are using tokens as a mean of two factor authentication.

A security token is a hardware device that is given to authorize user. It is also referred to as an authentication token or a cryptographic token. Tokens come in two formats: hardware and software. Hardware tokens are small devices which are small and can be conveniently carried. Some of these tokens store cryptographic keys or biometric data, while others display a PIN that changes with time. At any particular time when a user wishes to log-in, i.e. authenticate, he uses the PIN displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a PIN that change with time. Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence. The sequence should be random to the maximum possible extent, unpredictable, and irreversible. Factors that can be used in OTP generation include names, time, ATM pin, etc. Several commercial two factor authentication systems exist today such as BestBuy's BesToken, RSA's SecurID, and Secure Computing's Safeword

Using tokens involves several steps including registration of users, token production and distribution, user and token authentication, and user and token revocation among others. While tokens provide a much safer environment for users, it can be very costly for organizations. For example, a bank with a million customers will have to purchase, install, and maintain a million tokens. Furthermore, the bank has to provide continuous support for training customers on how to use the tokens. The banks have to also be ready to provide replacements if a token breaks or gets stolen. Replacing a token is a lot more expensive than replacing an ATM card or resetting a password.

From the customer's perspective, having an account with more than one bank means the need to carry and maintain several tokens which constitute a big inconvenience and can lead to tokens being lost, stolen, or broken. In many cases, the customers are charged for each token. So we propose a mobile-based software token that will save the organizations the cost of purchasing and maintaining the hardware tokens. Hence, they will only worry about their mobile phones instead of worrying about several hardware tokens.

III. SYSTEM DESIGN AND IMPLEMENTATION

In this paper, we propose a computer-based software token. This is supposed to replace existing hardware token devices. The System involves generation of Secured OTP using Cryptographic algorithm and delivering it to user's mobile in the form of SMS or user can able to create his own OTP using smartphone and validating the OTP using same Cryptographic algorithm. The proposed system is secured and consists of two parts: (1) the server software, (2) the client software: Client application on PC for transaction & android application on smartphone for creating OTP.

3.1 OTP Algorithm:

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments, so we propose a Secured Cryptographic algorithm.

The [5] unique OTP is generated by the mobile application offline, without having to connect to the server. The mobile phone will use some unique information in order to generate the password. The server will use the same unique information and validate the OTP. In order for the system to be secure, the unique OTP must be hard to predict by hackers. The following factors will be used to generate the OTP:

IMSI number: The term stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the (SIM) card in the mobile phone. This number will also be stored in the server's database for each client.

ATM PIN: Needed for verifying the authenticity of the client. If the phone is stolen, a valid OTP can't be generated without knowing the user's PIN. The PIN isn't stored in the phone's memory. It is only being used only to generate the OTP and destroyed immediately after that.

Timestamp: Used to generate unique OTP, valid for a short amount of time. The timestamp on the phone must be synchronized with the one from the server.
DOB: Date of birth of user whose going to use the application.
Username: Username of customer provided by bank.

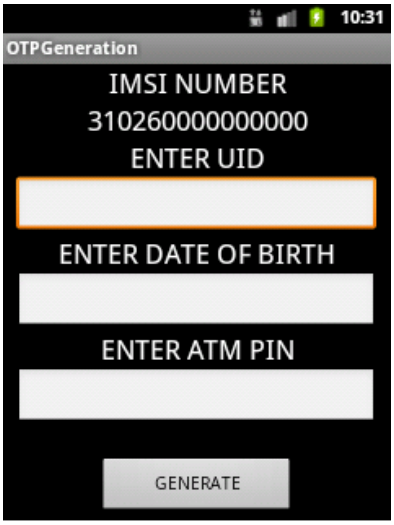

Fig.1 shows menu to generate OTP (IMSI No. taken automatically)

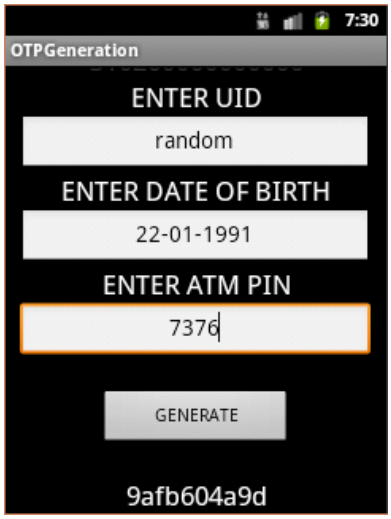

Fig.2 shows how OTP generated in Android mobile (Client Module)

How OTP Generated:

The Username, password, date of birth of user is taken from the user and then concatenated with the current date, time and the time stamp for which the one time password is valid. This concatenated string is then given as input to Secured Hash Algorith (SHA1) algorithim. SHA- 1 algorithm returns its message digest which is 20 bytes value. These 20 bytes are reduced to 5 bytes by XORing a group of 4 bytes , i.e byte no. 1, 4, 8, 12 are XORed ; 2, 5, 9, 13; 3, 6, 10, 14; 4, 7, 11, 15; 5, 8, 12, 16; 17, 18, 19, 20 are Xored.

Then from this 5 byte value, every byte is right shifted with 4 digits and then is converted to hexadecimal. Finally by converting the ASCII values to a character string, it is displayed as a onetime password to the user.

3.2Database Design:

A database is needed on the server side to store the client's identification information such as the first name, last name, username, password and the mobile phone number for each user. And also user id, details of transaction, OTP sent and date and time of transaction for every transaction. The OTP field will store the hash of the 10 minute One Time Password. It will not store the OTP itself. Should the database be compromised the hashes cannot be reversed in order to get the OTP used to generate those hashes. Hence, the OTP algorithm will not be traced.

3.3 Server Design:

A server is implemented to generate the token on the organization's (BANK) side. A server can be responsible for doing multiple activities. [1] It can be responsible for initializing database and sending of SMS. [2] A server is responsible for generating and sending the OTP and transaction details in the form of SMS. [3] A server is used to validate the OTP given by user. [4] A server can trigger the bank about the approval of transaction and payment to vendor. [5] A server can send customer's details like userid, password, and transaction password via e-mail with the help of SMTP server.

In order to setup the database, the client must register in person at the organization. The client's mobile phone/SIM card identification factors, e.g. IMSI, are retrieved and stored in the database, in addition to the username and PIN. The Android OTP generating software is installed on the mobile phone. The software is configured to connect to the server's GSM modem in case the SMS option is used. Both parties are ready to generate the OTP at that point.

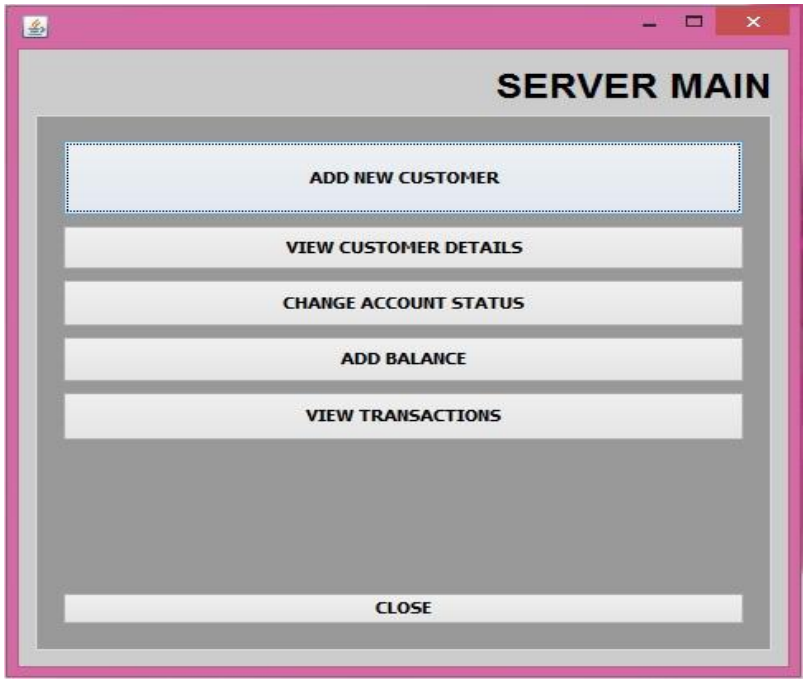

Fig.3 shows operations performed by server Admin

3.4 Client Design:

An Android program is developed and installed on the mobile phone. The programs run on any Android-enabled mobile phone. The key token program generates the dynamic key using the mobile credentials, e.g. ATM pin and IMSI numbers or requests from the server via an SMS message.

A client can able to do transaction for that purpose client need transaction password to so. After that client need OTP to complete transaction process. OTP can be generated either connection-less or connection-oriented method. Also we used cloud computing so that client can access its stored on server remotely.

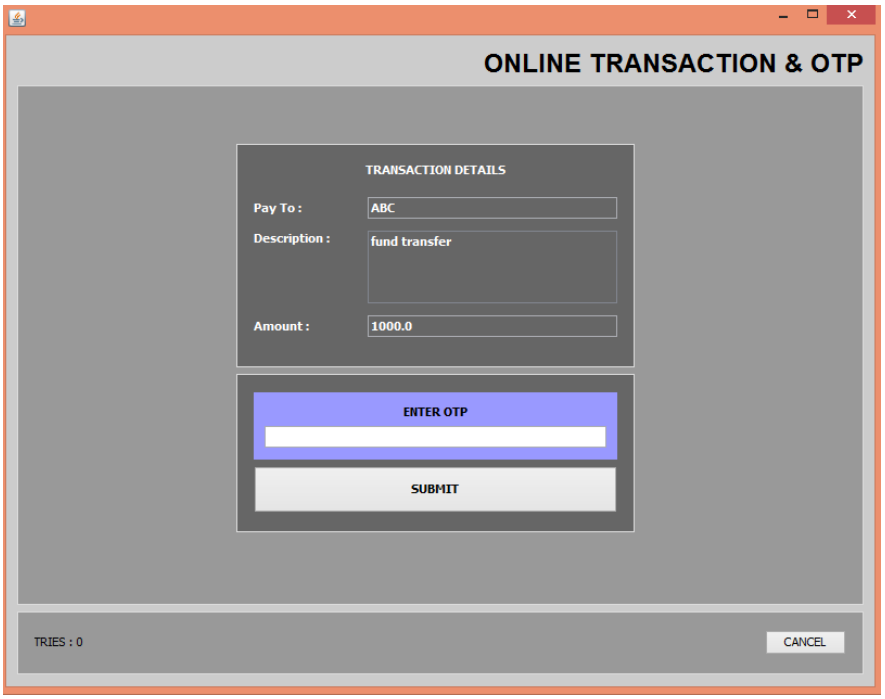

Fig.4 shows Client side transaction and OTP

Connection-Less Authentication System:

An [3] onetimepassword (OTP) is generated without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online. A program will be installed on the client's mobile phone to generate the OTP.

Connection-Oriented Authentication System:

In case the first method fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the one time password directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires.

Note that this method will require both the client and server to pay for the telecommunication charges of sending the SMS message.

IV. CONCLUSION

Single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentication methods have recently been introduced to meet the needs of organizations for providing stronger authentication options to its users.

In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is difficult for both the client and organization. Many clients carry a mobile phone now at all times. An alternative is to install all the software tokens on the mobile phone, which helps reduce the manufacturing costs and the number of devices carried by the client. The proposed work focuses on the implementation of two-factor authentication methods using mobile phones. It provides an overview of the various parts of the system and the capabilities of the system. The proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive SMS based method. Both methods have been successfully implemented and tested, and shown to be robust and secure. The system has several factors that make it difficult to hack.

Future developments include a more user friendly GUI, extending the algorithm to work on various mobile phone platforms. In addition to the use of Bluetooth and WLAN features on mobile phones for better security and cheaper token generation.

V. FUTURE WORK

Image Based Authentication: A two-factor authentication solution that delivers an image-based authentication challenge on the user's mobile phone. The user must be able to correctly solve the image-based challenge, which relies on their knowledge of a previously-determined secret, in order to use the second factor and complete the authentication.

- How it works:

- The first time a user registers with the website or creates an account with an online service, they will create a username and password as usual. They will also select a few categories of things they can easily remember – such as dogs, flowers and cars.
- When a second factor of authentication is needed (such as during a high-value transaction or when the user is logging in from an unrecognized device), TFA using Images creates a one-time authentication code and encrypts it within a randomly-generated grid of images. An application on the user's smartphone displays the grid of images.
- The user looks at the application in mobile and identifies the pictures that match their secret categories by touching/tapping the appropriate pictures. By identifying the correct pictures, the user is essentially using their knowledge of their secret categories to decrypt the authentication code. Upon successful authentication, the web page automatically proceeds with the transaction or process.

ACKNOWLEDGEMENTS

We would like to thank our Institution and faculty members, without whom this Paper would have been a distant reality. Last but not the least, we would also like to thank to our friends for listening to our ideas, asking questions and providing feedback and suggestions for improving our ideas.

REFERENCES

Journal Papers:

[1] Jøsang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities," in Proc. of the Australasian information security workshop conference on ACSW frontiers

[2] D. de Borde, "Two-Factor Authentication," Siemens EnterpriseCommunications UK- Security Solutions, 2008. Available at http://www.insight.co.uk/files/whitepapers/Twofactorauthentication(Whitepaper).pdf

[3] Fadi Aloul, Syed Zahidi, "Two Factor Authentication Using MobilePhones," in Proceedings Proceedings of the IEEE International Conference on Computer Systems and Applications, pg. 641-644, 2009.

[4] Nandagopal, Thyagarajan "Authentication and Verification for third party vendors using mobile devices", International Application No.: PCT/US2007/002996, Publication Number: WO/2007/092366. Publica-tion Date: 16.08.2007

[5] Sagar Acharya, Apoorva Polawar, Priyashree Baldawa, Sourabh Junghare, P.Y. Pawar " Internet Banking Two Factor Authentication Using Smartphone" , IJSER, IJSER, Volume 4, Issue 3, March Edition, 2013, (ISSN 2229-5518)

[6] Aladdin Secure SafeWord 2008. Available at http://www.securecomputing.com/index.cfm?skey=1713

[7] The mobile phone as multi otp device using trusted computing http://eprints.qut.edu.au/37711/

[8] H. Wang, "Research and Design on Identity Authentication System in Mobile-Commerce", In: Beijing Jiaotong University, 2007, pp. 18-50.

[9] S. Hallsteinsen, I. Jorstad, D-V., Thanh, "Using the mobile phone as a security token for unified authentication", Systems and Networks Communication. In: International Conference on Systems and Networks Communications, 2007, pp. 68-74.

[10] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services,"Communications of the ACM, 47(8), 42-46, May 2004.

[11] R. Groom, "Two Factor Authentication Using BESTOKEN Pro USBToken." Available at http://bizsecurity.about.com/od/mobilesecurity/a/twofactor.htm

Books:

[12] WikidSystem, "E-Guide To Two Factor Authentication to your corporate network", at http://www.wikidsystems.com/webdemo/Two-factor_Authentication_in_your_Network_eGuide.pdf

[13] SonicWall, "SSL_VPN-Two Factor Authentication", at http://www.sonicwall.com/downloads/SSL_VPN-Two_factor_Authentication.pdf

[14] GPayments Pty Ltd, "Two-Factor Authentication:An essential guide in the fight against Internet fraud", 02 February 2006

Theses:

[15] Christoffer Haglund, "Two-factor Authentication With a Mobile Phone", Fox Technologies, Uppsala Department of Information Technology, Lund University, 7th November 2007.