International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

SMS-Based One Time Password Vulnerabilities and Safeguarding OTP Over Network

Ms. Ankita R Karia
Student, Computer Engineering Dept.
Thadomal Shahani Engineering College
Mumbai, India

Dr.Archana B. Patankar
Asso. Prof. Computer Eng. Dept.
Thadomal Shahani Engineering College
Mumbai, India

Ms. Purnima Tawde
Student, Computer Engineering Dept.
Thadomal Shahani Engineering College
Mumbai, India

***Abstract*— User authentication is an essential step for online banking. Online banking uses remote authentication for authenticating users before granting them access to confidential data. Remote authentication means an infrastructure where client and server are connected through some potentially insecure network such as Internet. Online banking needs strong remote authentication since it contains user's sensitive data. Remote authentication is usually based on static passwords which are prone to replay attacks. One Time Passwords (OTP) is introduced to provide an additional layer of security. OTP is normally transmitted through SMS, but recent studies prove that SMS OTPs are also vulnerable to various attacks. In this paper, we are presenting vulnerabilities of SMS OTP and how it can be compromised. Based on this study, we present a mechanism to securely transmit OTP through e-mail over a network instead of SMS which suffer from various attacks.**

Keywords*— Authentication, OTP, mTAN, Smartphone, Steganography.

I. INTRODUCTION

Internet is an intrinsic part of our daily lives. In today's Internet driven society, many financial institutions offer their customers various financial services such as Bill payments, International funds transfer, money transfer etc., through Internet channel. The proportion of people, who expect to manage their accounts anywhere, anytime is constantly growing. Thus, Internet banking has quickly become an integral part of financial institutions. While Internet offers immense advantages and opportunities, it also presents various security risks. Online banking system authenticates users before granting them access to various services. Thus, user authentication is the fundamental process which is required to access secure and confidential data. User authentication is usually done using static passwords. Static password is a traditional password which is usually changed only when it is necessary. It is changed when the user has to reset the password i.e. either the user has forgotten the password or the password has expired. Static passwords are vulnerable to various attacks. To mitigate the problems associated with static passwords, One Time Passwords (OTP) was introduced.

One Time Password is a dynamic password that is valid for only one login session or transaction. It is a two-factor authentication system where the password constantly alternates. OTP system greatly reduces the risk of an unauthorized person gaining access to the account. OTP helps in preventing replay attacks, phishing attacks and other attacks which are possible to occur on static passwords. Also they offer other characteristics like anonymity, portability, and extensity and enable to keep the information from being leaked [1]. An added layer of security is provided because of the introduction of One Time Password. OTP since constantly alternates, thus for every new login session a new OTP will be generated which will help in authenticating the user. The idea of OTP was first suggested by American scientist Leslie Lamport in early 1980s of the 20th century [3].

OTP is greatly being used by many banking systems to provide their customers with excellent security. OTP is used in various banking activity such as Interactive Voice Response (IVR) transactions, money transfer, bill payments etc. OTP is also generated automatically when the system suspects an unusual activity or change in your Internet banking access pattern. This automatically generated OTP is then made available to user through various transmission techniques. OTP can be transmitted using techniques such as text messages by gateway (SMS), proprietary tokens, web-based methods; secure code devices and Grid file [1]. OTP generated on server side system is generally transmitted to the user using SMS messaging.

The rest of the paper is organized as follows:

Section II includes transmission of OTP through SMS. Section III describes vulnerabilities associated with SMS OTP. Section IV provides a solution to safely transmit OTP through e-mail. Section V presents Performance and Analysis. Section V presents Conclusion.

II. OTP TRANSMISSION

One Time Password generated is delivered to the user using various methods such as text messages, mobile phones, proprietary tokens and web based methods. With proprietary tokens user carries a device which is responsible for

generating and displaying OTP. Alternately, a mobile phone can also be used to generate OTP. But now-a-days OTP is usually provided to the user using Short Messaging System i.e. SMS. This is because; SMS is considered to be the most successful data transmission technique. With SMS OTP, users are either required to enter an OTP after logging in with a username and password or to authorize a transaction. The prime example of SMS OTP is the mobile Transaction Authorization Number (mTAN) that is used to authorize transaction for online banking services [2]. SMS OTP is promoted because it provides users with two factor authentication. Two factor authentication schemes are described as something which user owns and something which user have. Even though SMS OTP provides two factor authentication, it is now no longer considered secure. The reason for this is the fact that SMS OTP has come under heavy attack, especially smartphone Trojans [2].Wireless Interception, mobile phone Trojans, SIM Swap Attack are some of the attacks done on SMS [2]. Lately, several attacks against GSM and even 3G networks have shown that confidentiality for SMS messages cannot necessarily be provided [2].

III. VULNERABILITIES WITH SMS OTP

The only aim of an attacker is to acquire OTP. There are several ways such as Wireless interception, mobile phone Trojans, SIM Swap Attack through which he can obtain this OTP. The attacks are briefly discussed below:-

A. Wireless Threat

Wireless attack is achieved by placing an unauthorized device on the wireless network, bypassing a security process. Femtocells are network devices that people can get from their carrier to boost their cellular signal [5]. Lately, femtocells can be compromised to record many individuals' activities, such as SMS. Researchers were able to eavesdrop and record all voice calls, intercept incoming SMS and MMS messages [6].

GSM technology used for delivering SMS to the intended user is considered as insecure because of weak encryption algorithms and lack of mutual authentication. A5/1 encryption algorithm is used to provide privacy only in the air part of communication. The encryption on the air part was broken in 1998 [4]. Further research shows that the communication between mobile phones and base stations can be eavesdropped and decrypted using protocol weakness [2].

B. Mobile Phone Malware

Mobile phone Trojans are at rising threats which are specifically designed to intercept SMS messages. The ZITMO (Zeus In The MObile) Trojan for Symbian OS is the first known piece of malware that was specifically created for intercepting mTANs [2]. ZITMO is designed to steal OTP sent by banks in text messages. It is a Trojan with a very narrow specialization, its main aim is to forward incoming text messages with mTAN codes to malicious users (or a server, in cases involving ZITMO for Android) so that the latter can execute financial transactions using hacked bank accounts [7]. In February 2011, a ZeuS version for Windows Mobile was detected and named Trojan-Spy.WinCE.Zbot.a [2]. The most distinctive feature of ZITMO is most distinctive feature is its 'partnership' with the classic PC-based ZeuS Trojan [7]. Without the latter, ZITMO is merely spyware capable of forwarding text messages. The 'teamwork' between the two components enables cybercriminals to successfully bypass mTAN security measures used in online banking [7]. PCs infected with ZeuS trick users in installing the malicious app by stating that their phone needs be activated as part of extra security measurements. Once the victim entered his phone number, a text message is sent to the phone that contains a link to the malicious application [8].

SMS OTP Trojans [2] are malicious software which is installed by user. This software does not leverage security vulnerability of the affected platform but they use social engineering to deceive the user into installing the malware.

C. SIM Swap Attack

SIM Swapping is one of the latest frauds and is the second phase of phishing scam. Firstly, a criminal through phishing acquires basic personal information of the victim and then he can intercepts calls, text and other confidential information. SIM swap attack is a type of spear phishing [10] attack where in a criminal uses social engineering technique for duping the victim's mobile phone operator to port the victim's mobile number to a SIM which is in the possession of the criminal. The criminal then starts receiving any incoming calls and text messages, including banking one-time-passcodes that are sent to the victim's phone. The criminal can then perform transactions using personal information which he had gathered by techniques such as phishing or key loggers, and when the bank sends an OTP via SMS, the fraudster receives it and completes the authorization of the transaction. SIM Swap fraud has been observed in South Africa where SMS delivered TAN codes are common [9].

Banks had introduced measures such as one-time-passwords which were delivered to the intended user via SMS, to combat phishing attacks and Trojans such as key loggers. The criminals therefore required these OTPs to perform a successful fraudulent transaction which was achieved using SIM swapping. SIM swap fraud is a relatively easy fraud vector for the determined fraudster since they can capitalize on the operator's desire to provide good and quick customer service (and to preserve revenue streams) [10].

SIM Swap fraud is hitting the banks' bottom line and could erode customers' trust in the mobile, not only as a mechanism for receiving relatively simple security codes, but as a banking and payment device overall [10].

D. Additonal problems with SMS OTP

- The SMS transmission delay represents one of the major limitations of the traditional system [11].
- Disabling the roaming service prevents the bank from sending the SMS-OTP, thus disallowing the user from resuming any further processes.

- Cost associated with SMS is more when compared to the statistics of bank's transaction.
- Network coverage problem does not allow customers to complete an authorized transaction.

IV. SYSTEM FOR SAFEGUARDING OTP

SMS OTP since suffers from various attacks, in this section we present a solution which overcomes the problem of SMS OTP. The following system sends the encrypted OTP to the user through e-mail.

In the presented system, the financial organization is responsible for generating alphanumeric OTP. The OTP needs to be generated using time synchronized mechanism. This ensures that the generated OTP is unique and valid for a very short period of time. The generated OTP is then encrypted using AES encryption algorithm [1]. AES, a cryptographic algorithm is normally used to protect electronic data. AES which is the successor to the older Data Encryption Standard (DES) has become the standard for encrypting all private and electronic data. Also the time required to crack 128-bit AES key using brute force attack is approximately 1 billion years. In this proposed system, ATM pin along with last four digits of user's Credit/Debit card number and his Date of Birth in DDMMYYYY format is used as the key for the algorithm. The encrypted string is then hidden inside an image using the concept of steganography. Any steganography technique in spatial or transform domain can be used to embed the encrypted text into an image. Transform domain method is suggested since it sustains attacks. Least Significant Bit technique [12] is used here for demonstration purpose. The application used by bank for this purpose is shown in Fig.1. Thus, carrier image along with encrypted OTP generates a Stego-image which is then sent to the intended user via e-mail.

The following Fig. 2 represents the flow of the system. AES encryption algorithm [1] along with Steganography ensures secure and guaranteed delivery of OTP to the intended user. Steganography is a technique which hides information in such a way that only persons communicating know the existence of information. Thus, sending an OTP which is embedded in an image makes it difficult for an attacker to detect the presence of private information. If at all an attacker manages to retrieve encrypted OTP from the Stego-image, it will be still difficult for him to crack OTP. This is because AES encryption algorithm [1] is considered to provide higher grade of security.

Thus, by sending OTP to the intended user through e-mail will protect it from criminals who try to gain the same by attacking SMS through all possible ways. The user will be provided with an application as shown in Fig. 3 which helps in extracting encrypted text from the Stego-image. After getting the text, an OTP retrieval application has to be used by the user to decrypt the OTP. The key for decrypting OTP is ATM pin along with last four digits of user's Credit/Debit card number and his Date of Birth in DDMMYYYY format which all is available with every user. Also this number is unique for each user. The application will help in retrieving One Time Password within seconds of time. The reason for this is that, the banking system will be producing one time password using time synchronization mechanism because of which every OTP will be short-lived. Thus, a user will not be able to use the OTP after its expiry.

The application developed can be installed on user's smartphone so that the user can access his e-mail account anywhere, anytime. Through his smartphone the user can not only access his e-mail account but also use the retrieved OTP to complete his financial transactions. Sending OTP through e-mail lessens the attack done on text messages.

Fig.1: Bank Application

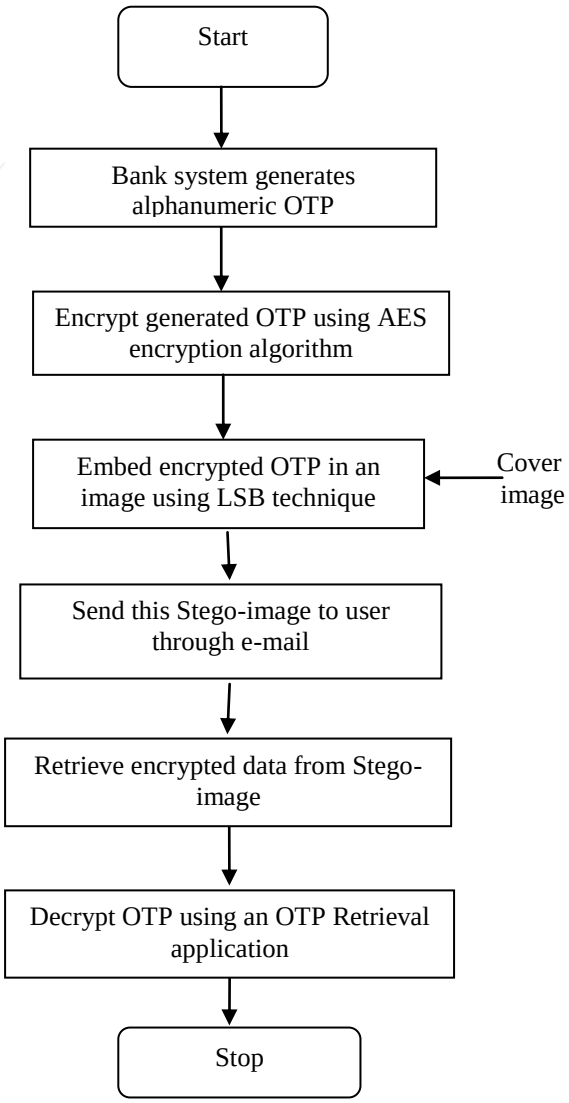

Fig. 2: Flowchart for the proposed system

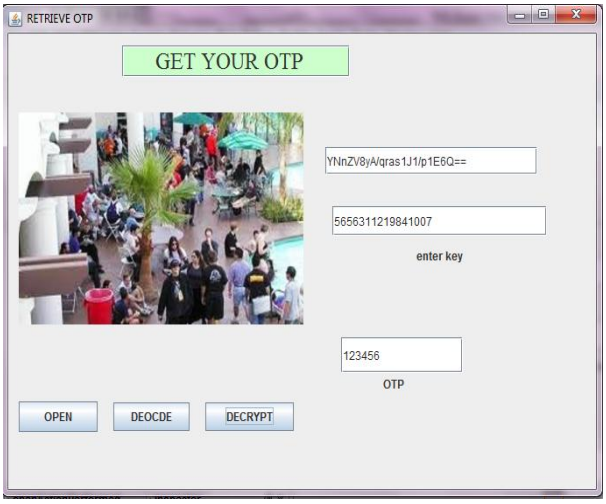

Fig 3.User Application to retrieve OTP

V. PERFORMANCE & RESULT ANALYSIS

Performance analysis for LSB steganography is done using Peak Signal to Noise Ratio (PSNR) and Root Mean Square Error (RMSE). Also, the encrypted OTP is successfully retrieved by the user once the decrypted text is retrieved from the Stego-image. PSNR computes the peak signal to noise ratio in decibels between two images. This ratio is used to measure quality between two images. If PSNR ratio is high then images are considered to be of best of quality. The cover image and Stegoimage are displayed in Fig. 4, Fig. 5, Fig. 6 and Fig. 7. Table I displays PSNR and RMSE values for 10 images of size 256 x 256 pixels.

Fig.4: Coconut Image

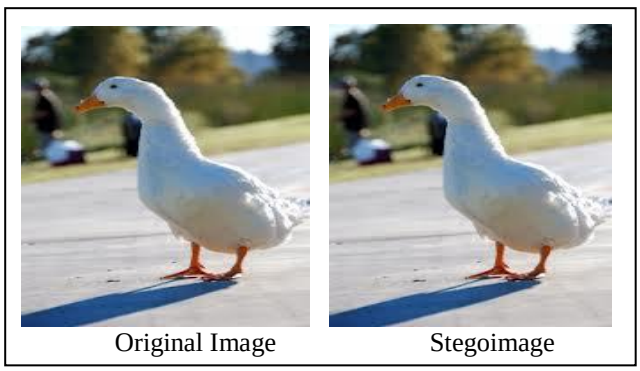

Fig. 5: Duck Image

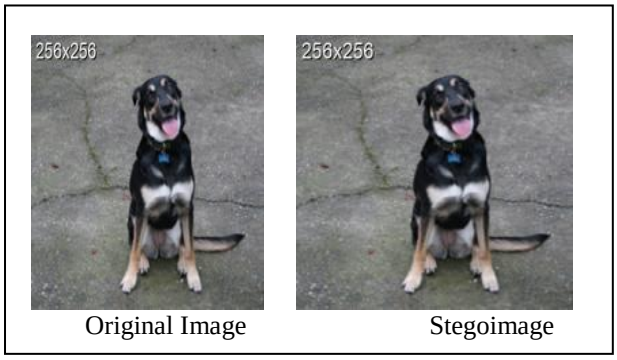

Fig. 6: Dog Image

Fig. 7: Lena Image

TABLE I: RESULTS FOR IMAGES OF SIZE 256 x 256

Image (256 x 256)	PSNR	RMSE
Coconut Image	79.3841	0.0201
Duck Image	78.0635	0.0241
Dog Image	78.3758	0.0237
Bottle Image	77.7952	0.0330
Lena Image	78.3391	0.0238
Rabbit Image	79.3174	0.0089
Apple Image	77.7592	0.0330
Heart Image	77.7592	0.0330
Leaf Image	78.3391	0.0226
Cartoon Image	77.9887	0.0314
Average	**78.3103**	**0.0253**

TABLE II: AVERAGE RESULT FOR IMAGES OF VARIOUS SIZES

Images	Avg. PSNR	Avg. RMSE
256 x 256	78.3103	0.0253
128 x 128	72.2599	0.0542
64 x 64	68.1148	0.0882

Table II displays average PSNR and average RMSE for images for various sizes. Images of size smaller than 64 x 64 pixels are not taken into consideration because these images are considered very small for user who accesses his/her e-mail through smart phone. Images of size smaller than 64 x 64 pixels will not give better clarity to users. Thus, results are generated for images of size greater than or equal to 64 x 64 pixels.

Further, if the generated OTP is ABC123 then on applying AES encryption, we get "YQoYpNMa5MNQzihyDeXwcg==" as the encrypted string. On the user side, using ATM pin along with user's Date of Birth in DDMMYYYY format and last 4 digits of user's Credit/Debit card number as key the string is successfully decrypted and the OTP is retrieved within seconds of time.

VI. CONCLUSION

This paper thus, provides an overview of One Time Password (OTP) which was introduced by bank systems to provide its customers with a better level of security. OTP is considered to provide two-factor authentication which was delivered to the intended user through text messages i.e. SMS. This paper thus focusses on vulnerabilities associated with SMS OTP and why sending One Time Password through SMS is not secure. It also describes other disadvantages associated by sending OTP via SMS. Further, a solution for safeguarding OTP over network is also presented.

This solution uses AES encryption [1] for encrypting the generated OTP and hiding that text into an image by using the concept of Steganography.

Least Significant Bit technique is used to achieve steganography. The image is then sent to user through e-mail, thus overcoming the problems associated with SMS OTP.

The presented system provides a security of better grade and overcomes various security attacks. The system is considered as user-friendly because a user since is provided with an application which will helps in extracting encrypted OTP and decrypt the same using his own ATM pin number.

The solution provided is beneficial to both customers and banking systems because of its user-friendliness and the level of security provided. The concept presented over here should be promoted to safeguard customers from facing financial loss.

REFERENCES

[1] AbhasTandon, Rahul Sharma, SankalpSodhiya, P. M. Durai, and Raj Vincent, "QR Code based secure OTP distribution scheme for Authentication in Net-Banking," International Journal of Engineering and Technology ISSN : 0975-4024, vol.5, no.3, pp.2502-2505, Jun-Jul 2013.

[2] Collin Mulliner, RavishankarBorgaonkar, Patrick Stewin, and Jean-Pierre Seifert, "SMS-Based One-Time Passwords: Attacks and Defense," Springer-Verlag Berlin Heidelberg, LNCS 796, pp.150-159, 2013.

[3] SagarGajbhar, ShrikantAher, SwapnilAuti, Shailesh Hodge, "Authentication using Mobile phone generated OTP," International Journal of Computer Science and Management ResearchISSN 2278-733X , vol.2, Issue 5, pp. 2282-2285, May 2013.

[4] Black Hat Briefing, "Intercepting GSM traffic," Washington D.C., Feb 2008.

[5] Ryan Whitwam. (2013, July 16), News, Verizon Wireless [Online]. Availabe:http://www.androidpolice.com/2013/07/16/security-researchers-use-hacked-verizon-femtocell-to-intercept-call-sms-and-mms-data-be-afraid.

[6] Fahmida Y. Rashid. (2013, Aug 01), Hacking {Online]. Available: http://securitywatch.pcmag.com/hacking/314370-black-hat-intercepting-calls-and-cloning-phones-with-femtocells.

[7] Teamwork: How the ZitMo Trojan Bypasses Online Banking Security (2011, Oct 06), Virus News [Online]. Available: http://www.kaspersky.co.in/about/news/virus/2011/Teamwork_How_the_ZitMo_Trojan_Bypasses_Online_Banking_Security.

[8] Prof. Dr. ir. Herbert Bos, Dr. Christian Rossow, " Dynamic Analysis of Android Malware," VU University Amsterdam, Internet & Web Technology Master thesis, August 2013.

[9] Anand Bajpai, "Impact of M-Commerce in Mobile Transaction's Security," Research Journal of Management Sciences ISSN 2319–1171 vol. 2(7), pp.33-37, July 2013.

[10] Suzzane Cluckey. (2013, Sep 03) Banker beware: SIM swapping con targets mobile accounts [Online]. Available: http://www.mobilepaymentstoday.com/article_print/218801/Banker-beware-SIM-swapping-con-targets-mobile-accounts.

[11] N.Harini Dr. T.R. Padmanabhan," 2CAuth: A New Two Factor Authentication Scheme Using QR-Code," International Journal of Engineering and Technology (IJET) ISSN : 0975-4024, vol 5, no 2, pp. 1087-1094, Apr-May 2013.

[12] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, Volume 3, Issue 7, July 2013.