International Journal of Computer Networks and Communications Security

VOL. 3, NO. 3, MARCH 2015, 78–82
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Model for Protecting Online Banking Using Transaction Monitoring

Md Nadeem Ahmed

Research Scholar, IFTM University, India

E-mail: mdnadeemahmed.86@gmail.com

ABSTRACT

Wonderful technique has been invented to secure the online data over the network. Online application such as banking, electronic transactions and financial services is the example which is relevant and required highly secured critical transactions. As a high-speed internet infrastructure is being developed and people are slowly digitalized, financial activities also dependent on the internet .we have so many factor authentication technique to protect over the network. In this paper we will analyze the level of security in different authentication factor and will provide a new model to enhance the financial security based on user transaction monitoring.

Keywords: *Security, Factor Authentication, Transaction, Online banking, Out of band authentication, Biometric.*

1 INTRODUCTION

Now a day's most sensitive task performed by the user is online banking. In almost all the cases bank always say they provide '100% online banking security guarantee', typically the fine print makes this conditional a user fulfilling certain security requirements [1]. An account manager at Ferma, logged in to the company's bank account for bill payment, and for more security used One time password, later analysis is performed which disclose that an earlier visit to another web application allowed a malevolent program to interrupt in his computer but the manager issued legal payments, the program done 27 transactions to different accounts, siphoning off $447,000 in a few minutes. The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds.[17] There is a exponential growth in the number of domestic user in the first quarter of 2009. The average usage of the service per day was 26,410,000 while the amount of dealings goes beyond 26 trillion 950 million. However, some banks seems to be reluctant to reimburse to user who trapped of online scams such as phishing. In 2005 the first hacking incident happen stimulate the FSS (The Korean Financial Supervisory Service) to take a comprehensive countermeasure. One of the preventive action that draw high attention of the financial agencies is OTP (One Time Password), one of the user confirmation methods is introduces, and Joint Confirmation Center of OTP is established [2]. The Online banking transaction presently uses public key certificate or security card which are the techniques authenticating a user, recently OTP (one time password) was introduced. One-Time Password is a password system where passwords can only be used once and the user has to be authenticated with a new password key each time. This almost provides guarantee of security even if the hacker trapping the password over the network. Besides, OTP features anonymity, portability, and extensity, and enables to keep the information from being leaked [3]. The type of OTP generate device is smart card, USB, fingerprint recognition and so on. Several strategies for using passwords have been proposed [4]. Some of which are very difficult to use and others might not meet the company's security policy. Two factor authentication using devices such as ATM card and tokens has been proposed to solve the password

problem and seems to difficult to hack. A revolution occur when a biometric based authentication factor also come in to the picture Biometric-based factors are physiological or behavioral characteristics of an individual that can be measured and form which distinguishing, repeatable (not necessarily exact) biometric features can be extracted for the purpose of automated individual recognition. This is the perfect and most secured security technique till now but it is difficult to implement in the online banking security model. ATM's also have changed the banking perspective of the world. But security threats repeatedly levitate around business process, ATM's lack security aspects in more generic sense. If someone lose their ATM card and PIN number is known to someone who got the ATM then there is no proposal or technique to stop the person to do any illegal financial robbery. we may think to provide security based on biometric but that will cost more and practically very difficult to implement

2 PROBLEM SCENARIO

Person 'N' has an internet banking account in Bank 'X' and logs on to their account or visit any ATM to do risky financial transaction like: Funds transfer from bank's account to any other domestic or international bank's account. Massive credit or debit of plastic money. Credit card payment. This payment refers only to credit cards issued by some bank Transaction from ATM NOW 'N' enters the amount in his online bank account and destination account number, after the process 'N' receives a e-receipt from bank 'X' which confirm the transaction happen successfully. But later after checking the bank statement confirms that the huge amount has been debited to some unknown account. Or if person 'N' loses his debit or credit card and person knowing his pin code got card and has unlawfully debited huge amount of money. online banking is exposed to the possibility of being attacked to MSW/ MITM attacks because of the below mentioned justification [5].

1) Interaction with the user is not done through the OTP only one authentication factor has been used.

2) Probably risky client PC, where communication between client and server ends.

3) No monitoring technique available to assess the record on the basis of examining the sequence of event of the authentic user in the recent past indexed from database.

3 ONLINE BANKING

The term 'Online' became popular in the late '80s and referred to the digital electronic device to access the banking system. 'Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when city's four major banks Citibank, Chase Manhattan, Chemical and Manufacturers Hanover implemented and provided home banking services using videotex system[6][7][8]. commercial failure of videotex make the banking service failure except in France where the videotex use was sponsored by the telecom provider and the UK, where the Prestel system was used.

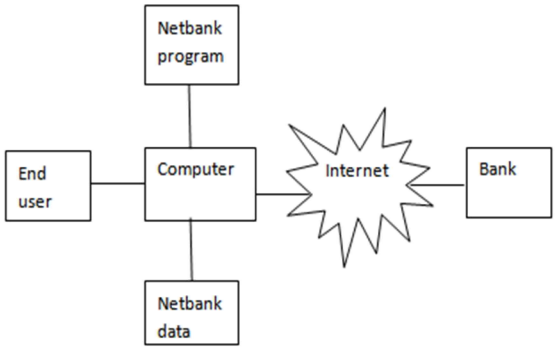

Fig. 1. Online banking model

In 1997 in china first online banking has been developed by Bank of China, online banking concept has been accepted and this expanded very rapidly that until 2007 45 bank from 100 local bank has accepted the concept of online banking and implemented for Business. However, by the end of 2002, some estimates proved that about 30 percent of Americans were using online banking [9], which jumped to 50 percent in 2003 [10]. Similarly, others [11] predicted that in UK around 20 million people will adopt e-banking by the end of 2005. This trend is also apparent in Singapore, Sweden, Germany and Norway, and the more advanced service-providing economies in the world [12], [13], [15], [14], and also in India [16]. With the unique features of time saving, cost and location, online banking has been uniquely worldwide accepted by clients. But the safety and security of this online banking is drawing more attention of the people.

4 BACKGROUND AND RELATED INSIGHTS

Authentication is any process by which a system verifies the identity of a User who want to access. Since Access Control is normally based on the identity of the User who requests access to a resource.

Category of authentication:

- Platform level authentication
- Message level authentication
- Application level authentication

We have 4 types of authentication factor:

One-factor authentication:– This is "something a user knows." The most recognized type of one-factor authentication method is the password.

Two-factor authentication– In addition to the first factor, the second factor is "something a user has." Examples of something a user is Bank card or bar code, or USB-interface device.

Three-factor authentication: In addition to the previous two factors, the third factor is "something a user is." Examples of a third factor are all biometric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar. The most recognized form of three-factor authentication is usually the retina scan.

Four-factor authentication: In addition to previous three factor authentication This is "someone whom you know". Examples using voucher system for hardware authentication tokens such as RSA Security Inc.'s SecurID.

Few major threats to for e- commerce can be classified as:

- Unauthorized access
- Data Alteration
- Spying network privacy
- Disclosure of configuration file/data
- Message replay
- SQL Injection
- Scanning and Access of WSDL
- Identity Spoofing

5 OUT OF BAND-PHONE CALL BIOMETRIC AUTHENTICATION

Out-of-Band Authentication is the use of two separate networks working simultaneously to authenticate a user and recommended by the FFIEC. The customer would be asked to initiate a call back by clicking the button on web page. The Bank out-of-band authentication server calls the customer and the voice prompt ask the user to repeat the word which is flashed in the web page and the text and the voice of the customer should be matched be matched to the to a known voice print on record. This sophisticated technology demands that the user allow the financial body to keep a voice print on file to confirm or prove the authenticity of the end user.

6 CURRENT APPROACH FOR ONLINE BANKING SECURITY

Currently almost all the bank are using two factor authentication and implementing 3 factor for all the user practically not possible in online banking system because of many factor such as cost and infrastructure availability factor. In ATM transaction also it is not practically possible to set up biometrics devices for providing 3 factor authentication. If someone illegally trying to access others account then currently we have not effective model to stop the unauthorized access. only we can detect from IP address that different system has been used and OTP has been generated for authentication. Our system currently is not much intelligent to provide security on the basis of customer login activity.

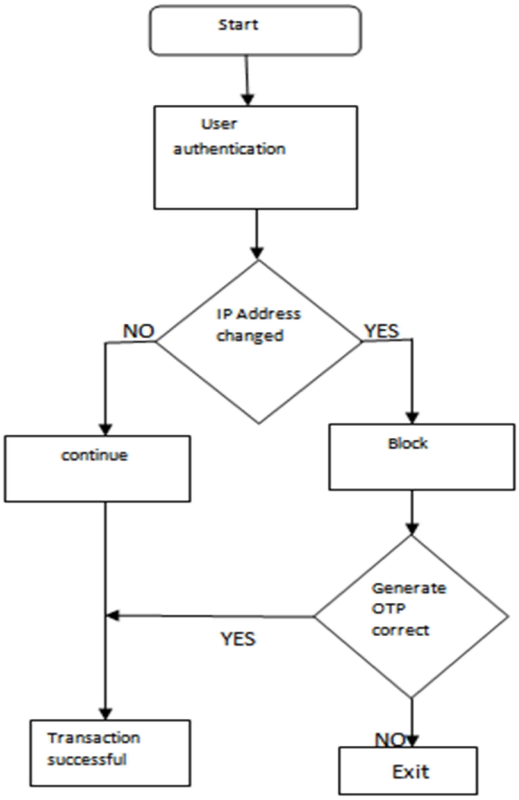

Fig. 2. Current online banking security approach

7 PROPOSED APPROACH FOR ONLINE BANKING SECURITY

Current model is that if in case OTP has been generated then server have to monitor so many event of activities which is discussed below because alone OTP is not sufficient to authenticate user as technically there is a possibility to hack session id and decode the OTP in their TTL(time to live) interval.

Factors to monitor:

- Location of accessing bank account
- Amount entered
- Duration of accessing account
- Sequence of activities
- Number of transaction

Location of accessing bank account: The most important is to determine whether the current location is changed to the location which is in the record since every machine is having different Unique IP Address when connected to the network. A new Location is suspicious hence location factor have to monitor closely.

Amount entered: The amount entered also have to monitored if the amount entered is more than last (n) transaction then again amount factor should have to monitor closely. However if amount entered is less than last (n) transaction then there is no need to monitor amount factor.

Duration of accessing account: The time of accessing the account needs to monitored the time when user login and the time when user click the button for amount transaction and should be compared with the last (n) average time interval if the deviation is more than this factor also needs to monitored closely.

Sequence of activities: This is practically true that every user perform different sequence of activities before doing the online financial transaction for example some end user may check their balance before financial transaction check their mini statement. we monitor this sequence of activity and store in the database and can monitor if the sequence of doing the activity of the end user does not match with the previous record.

Number of transaction: If there is more deviation in last (n) average number of transaction in one day then this transaction factor also need to monitor closely.

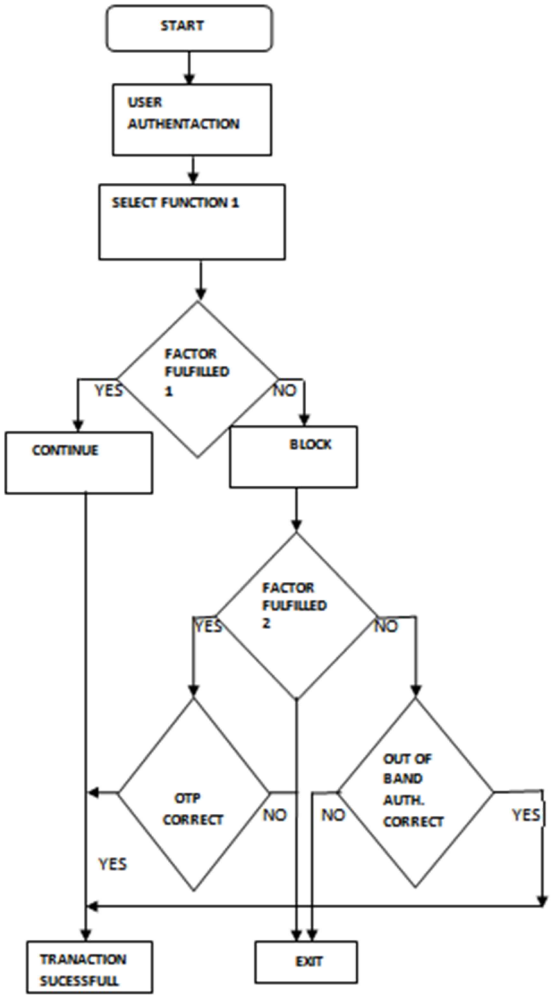

Fig. 3. Proposed approach online banking security

- If IP Address is same but (amount entered or duration of accessing account or sequence of activities or number of transaction) changed generate OTP.
- If IP Address changed but (if transaction amount entered is less than last (n) days average amount or sequence of activities or duration of accessing account or sequence of activities is same) then generate only OTP
- But if IP Address changed and (if transaction amount entered is more than last

(n) average amount or sequence of activities changed or duration of accessing account is changed)then generate out-of-band phone call biometric authentication.

- If IP Address changed and number of transaction in one day increase to a certain (n) limit and amount entered exceeds certain (n) limit then generate out-of-band phone call biometric authentication

Note: If minimum 3 factors changed then function executed.

8 CONCLUSIONS AND FUTURE WORK

This model would provide an effective way to strengthen our online financial transaction. As the number of record of transaction increases chances of misusing or hacking the individual bank account decreases. If account blocked then using OTP and out of band-phone call biometric authentication user can able to unblock their account. The possibility of implementing the current model is a challenge, need to study the statistical and mathematical calculation, need to analyze the (n) days which is mentioned in the factor and in out of band-phone call biometric authentication every customer have to register their voice in the bank database and need to develop an algorithm which matched to a known voice print on record.

9 REFERENCES

[1] Mohammad Mannan, P. C. Van Oorschot, “Security and Usability: The Gap in Real-World Online Banking”, NSPW’07, North Conway, NH, USA, Sep. 18-21, 2007.

[2] AntiPhishingGroup, “Phishing Activity Trends Report”, from: http://www.antiphishing.org, Dec. 2008.

[3] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, “OTP Authentication Protocol Using Stream Cipher with Clock-Counter”, October, 2009.

[4] A. Jøsang and G. Sanderud, “Security in Mobile Communications: Challenges and Opportunities,” in Proc. of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003.

[5] Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Horing, Peter Buhler, Michael Baentsch, "The Zurich Trusted Information ChannelAn Efficient Defence against Man-in-the-Middle and Malicious Software Attacks", In P. Lipp, A.-R. Sadeghi, and K.-M. Koch (Eds.): TRUST 2008, LNCS 4968, pp. 75-91,2008.

[6] Cronin, Mary J. (1997). Banking and Finance on the Internet, John Wiley and Sons. ISBN 0-471-29219-2 page 41 from Banking and Finance on the Internet. Retrieved 2008-07-10.

[7] Jump up^ "The Home Banking Dilemma". Retrieved 2008-07-10.

[8] Jump up^ "Computer Giants Giving a Major Boost to Increased Use of Corporate Videotex".Communications News. 1984. Retrieved 2008-07-10.

[9] Bruno, M.A., 2003. BofA’s climb to the top of the online world. US Banker, 113(6), pp.24-25.

[10] Ramsaran, C., 2003. Online banking comes of age. Bank Systems and Technology, 40(11), p.29.

[11] Mintel, 2003. Direct banking – UK (April). Mintel Market Report. London: Mintel International Group.

[12] Barto, G.L., 1999. E-Banking 1999: New Model of Banking Emerges. Stamford, CT: Gartner Group.

[13] Mulligan, P. & Gordon, S.R., 2002. The impact of information technology on customer and supplier relationships in the financial services. International Journal of Service Industry Management, 13(1), pp.29-46.

[14] Mattila, M., Karjaluoto, H. & Pento, T., 2003. Internet banking adoption among mature customers: early majority or laggards? Journal of Services Marketing, 17(5), pp.514-528.

[15] Gerrard, P. & Cunningham, J. B., 2003. The diffusion of internet banking among Singapore consumers. International Journal of Bank Marketing, 21(1), pp.16-28.

[16] Srivastava, R.K., 2007. Customer’s perception on usage of internet banking. Innovative Marketing, 3(4), pp.66-72.

[17] http://www.technologyreview.com/news/415371/real-time-hackers-foil-two-factor-security.