Multi-Level Security for ATM Transaction

Anusha Salam
Department of CSE
ICET
Ernakulam,Kerala

Asha Ali
Assistant Professor
Department of IT
GEC,Painavu,Kerala

ABSTRACT

Automated Teller Machines (ATM) have become a part of prestige of the banks all over the world. As the banks compete by opening more and more ATM's every year, research is going on of several aspects of ATM especially security. In real time ATM, user is authenticated only by a four digit Personal Identification Number (PIN) which can be compromised easily. Since this single level is vulnerable to attack, this paper proposes multiple security levels that can minimize the first financial risk to customers. The multiple security levels comprises of an extra user authentication and location aware transaction verification mechanisms Since possessing a smartphone has become a trend in current scenario, to use this functionality user is assumed to have a smartphone with good GPS functionality. Unlike prior research, this concept is a cost effective way that can be easily integrated into the current ATM functionality. Moreover, there is a provision for the user to directly block his card in context of misuse rather than dialing or contacting a third party.

General Terms

Security

Keywords

Multi-level security; ATM card misuse; location-aware transaction verification; smartphone application; GPS

1. INTRODUCTION

The pervasive deployment of Automated Teller Machines (ATM) all over the world itself highlight the importance of ATM in the current society. Eventhough transactions in ATM's are believed to be secured using PIN only, issues are reported of financial loss of atleast one transaction loss to customers when the card is lost .Sometimes customer realizes about it only when a message reaches mobile phone indicating the amount withdrawn from his/her account. Such a risk can be minimized by adding multiple levels of security for authenticating user and transaction verification based on location information.

Banks deploy more ATM's for two purposes: (1)to make money available to customers anytime anywhere, (2) reduce their own operating cost of deploying more banking personnels to serve customers. Around the world even billions of people are making use of ATM's daily. So researches are going on to improve the security of ATM transactions. As the number of hackers and their methodologies are improving day by day banks have to be more vigilant in securing ATM transactions.

In the existing system, user is authenticated by PIN only. This four digit PIN can be compromised easily by using ATM scamming devices and video cameras. Scamming devices can read the contents of a magnetic tape and capture PIN. Such devices include card readers, digital pads, video cameras. PIN can also be obtained by shoulder surfing. Once the card information is obtained duplicate cards can be generated easily. In such a situation, user even after possessing the card has to face a financial risk. Once the user is aware of the card missing, he/she has to depend on a third person to block the card.

With the increasing availability of smartphones with GPS functionality among bank customers and android applications that support mobile banking, this concept can be easily integrated to the existing ATM in a cost effective way. This can minimize the risk of financial loss faced by the customer to a considerable extend in context of a missing card.

2. RELATED WORK

The conceptual model of ATM system and transition diagram of ATM behaviors [1] gives an insight into how ATM works. The various aspects of research in ATM include dynamic user interface for ATM[7],integrity of ATM[5],transaction security[3],generation of a secure PIN[9].A misusing scenario[2] is proposed to bring light into the fact that PIN based authentication strength will weaken over time unless countermeasures are implemented. An attack is modeled to show how powerful human adversaries can be in shoulder surfing[10].Mobile phones are used for user authentication via SMS [3] and vibration [6].The security to ATM transaction is enhanced by taking biometric data[11].Location information obtained via GPS in smartphones can be used for several applications[4],[12].Location from smart phones can be used for authentication and authorization[8]Location information of credit card obtained by integrating GPS in card itself can be used for location-aware transaction verification[13].

The rest of the paper is organized as follows. A novel approach for authenticating client and location based transaction verification is described in the section 3.2.Section 3.3 describe the blocking feature. Section 3.4 describe the relevance of the solution in different scenarios. The experimental set up is covered in section 4. The idea is concluded in section 5. The main advantage of this approach is that it can be easily integrated into the existing banking security system. The approach is inexpensive and feasible compared to previous researches on providing more security to ATM transaction.

3. METHODOLOGY

3.1 Requirements

This approach is proposed in the assumption that all users possess Android Smartphones with GPS functionality. Initially user have to register with the bank for getting the mobile application and authentication code.

3.2 User Authentication and Transaction Verification

When the user wishes to use his/her ATM card in an ATM, user is requested to login to mobile application preferably prior to entering the ATM. If the username and password doesn't match with already existing username and password in the database, then the user will not be allowed to login to the application and for further process. On login, location of phone is retrieved by the application via GPS. This is transparent to user.

When the user swipes the card in the ATM, user will be asked to enter PIN as in the normal scenario. The entered PIN will then be crosschecked with the PIN in database. If it matches ,then a transaction ID is shown to user in the ATM interface and the user is instructed to proceed via application in the phone .An alert is also send to user's registered Email ID in the mean time. Else no transaction ID is displayed, user have to enter PIN again. .User can try entering PIN for three times. Once limit is over, transaction get cancelled automaticaly. After successful PIN verification,user have to enter the Transaction ID in the mobile application along with authentication code provided by the bank. On submitting these two parameters location information of phone identified via GPS is also send to the web service.

Web Service does the following functions:1)Crosscheck authentication code received with the authentication code stored in database.2)Identify ATM based on transaction ID received. Retrieve its location from database and crosscheck with the received location information from the phone.3)If both the authentication code and location matches, an alert is send to ATM to proceed the transaction.4)If either authentication code or location or both doesn't match, then alerts are send to both ATM and user for denying transaction and to attract user's attention respectively.

The overview of the proposed system is shown in Figure 1.

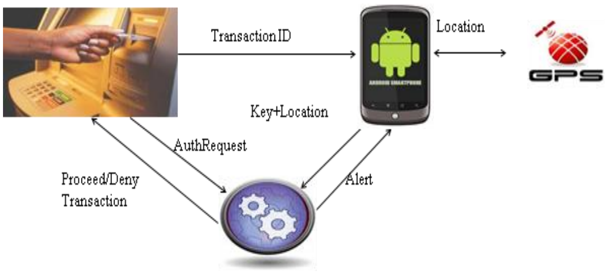

Fig 1: Overview

3.3 Direct Blocking

Once the user feel that someone get hold of his card and phone someway, then inspite of relying on the security provided by authentication code, user himself/herself can block the card directly by login onto his/her profile.

Once the card is blocked, if user get back the card and phone within short interval then he/she can request the bank to reissue the same card along with the context that leaded to decision of blocking card. Bank then after analysing the context can make a decision to reissue or not.

3.4 Relevance

Once the user feel that someone get hold of his card and phone someway, then inspite of relying on the security provided by authentication code, user himself/herself can block the card directly by login onto his/her profile. Even if the card is lost and PIN is compromised, attacker is restricted via username, password and authentication code

Even if card and mobile phone gets stolen assuming that user forgot to logout properly or preferred to stay signed in, then also attacker is hindered by authentication code. Since user will realize that phone is stolen in a short time, attacker will only get a short time prior to user blocking the card.

If some peer gets hold of your card and phone while in office ,and in fear of being tracked decide to use your own phone then transaction will be denied due to different locations. Moreover user is alerted every time while transaction is initiated. So in context of misuse he/she can block card.

3.5 Experimental Setup

An RFID tag and reader is used to simulate the event of card reading. ATM is represented as a desktop application designed in JAVA. The smartphone is represented using emulator. Eclipse IDE is used for developing mobile application. Web application is designed in JSP for user and bank using NetBeans IDE. Database used is MySQL.

Here user is allowed to perform transaction only after verifying PIN, authentication code, location of user and mobile phone. If the user is alerted of any misuse, he/she can immediately block by logging onto web.

Here location of ATM obtained from Google Map is saved in the database of the bank. This latitude and longitude values are compared with the latitude and longitude values transparently obtained from the mobile phone.

The transaction is denied either if PIN is entered more than three times or in case of PIN, authentication code and location mismatch.

3.6 Comparative Study

In the proposed solution, even if the mobile phone and card is lost the attacker gets hindered by various levels. This provide enough time for the user to be aware of the issue and he/she can immediately block the card himself or herself. The great advantage of the solution is that it ensures security in the worst case where both the card and mobile phone get lost.

Moreover the proposed solution does not demand any change in the infrastructure of the system. Since this is the era of mobile banking, the proposed solution can be easily integrated into the mobile applications that enable mobile banking. All that is needed here is some add-ons to the mobile application and inclusion of some extra functionalities to the already existing web service. Hence the solution is cost-effective. Here security is improved by integrating mobile phone into system

4. CONCLUSION

In this paper ,a novel approach to secure ATM transaction by introducing multiple levels of security is proposed. First level includes PIN and first alert. Second level include transaction ID and authentication code. Third level includes location. The attacker has to compromise all the levels to be successful. Since chance of hacking all the levels in minimum duration is less, risk of first financial loss to the user is minimized with this approach.

Here the user has to login to mobile application prior to entering ATM due to the limitation of GPS indoor. Once an indoor location provider gets common in all buildings with ATM installed, the location discussed in this paper can be obtained from such providers. Eventhough it add some inconvenience to user, it is assumed that user will be ready to compromise a little for more security than facing financial loss. The location discussed here can be spoofed in the worst case. So future work is to make sure location obtained from mobile phone is the legitimate location

5. ACKNOWLEDGMENTS

Our sincere thanks to all who helped in developing this concept that include mainly Mr.Rineez Ahmed N,CTO of Livares Technologies Private Limited and Mrs.Aity,CEO of Aiko Infotech.

6. REFERENCES

[1] Yingxu Wang, "The Formal Design Model of an Automated Teller Machine," *IEEE CCECE*, vol. 2, pp. 1255–1258, 2003.

[2] Kjell.J.Hole, Veblorn Moen,Andre N. Klingsheim ,and Knut M. Tande , "Lessons from the Norwegian ATM system," *IEEE Security and Privacy*," vol. 5,no. 6, pp. 25–31, 2007.

[3] Kopparapu Srivasta ,Madamshetti Yashwanth and A.Parvathy, "RFID & mobile Fusion for authenticated ATM transaction," *IJCA*, vol. 3, no. 5,2010.

[4] Nan Li and Guanling Chen, "Sharing Location in Online Social Networks," *IEEE Network*, vol. 24, no. 5, pp. 20–25, 2010.

[5] R.Petric, "Integrity protection for automated Teller Machines ," *IEEE 10th international Conference on TrustCom*, pp. 829–834, 2011.

[6] Nitesh Saxena ,Md. Borhan Uddin, Jonatahan Voris, and N.Asokan,"Vibrate-to-Unlock: Mobile Phone Assisted User_Authentication to Multiple Personal RFID Tags," *IEEE international Conference on Pervasive Computing and Communications*, vol. 2, no. 4, pp. 181–188, 2011

[7] Ghulam Mujtaba and Dr. Tariq Mahmood, "Adaptive Automated Teller Machines-Part II," *International Conference on Information and Communication Technologies*, pp. 1–6, 2011.

[8] Feng Zhang,Aron Kondoro,and Sead Muttic,"Location-based Authentication and Authorization Using Smart Phones," *IEEE 11th International Conference on TrustCom*, pp. 1285–1292, 2012.

[9] Yong Xiao ,Chung-Chih Li,Ming Lei,and Susan V.Vrbsky, "Differential Virtual Passwords,Secret Little Functions, and codebooks for protecting Users from Password Theft," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1, 2012

[10] Taekyoung Kwon, Sooyeon Shin, and Sarang Na, "Covert Attentional shoulder Surfing:Human Adversaries are More Powerful Than Expected," *IEEE Transactions on Systems,Man and Cybernetics Systems*, vol. PP, no. 99, pp. 1, 2013.

[11] P. Prem Kishan ,Neerugatti Vishwanath, Vasudheva Reddy Nandhigama ,K. Khamaruddeen,Anirudh Kasibhatla,D.Pavani, and G.Swetha, and "Real Time SMS-Based Hashing Scheme For Securing Financial Transactions on ATM Terminal," *IJRES*, vol. 1, no. 3, pp. 27–33, 2013.

[12] Lei Zhang, Jiangchuan Liu , Hongbo Jiang and Yong Guan, "SensTrack: Energy-Efficient location Tracking with Smartphone Sensors," *IEEE Sensors Journal* , vol. 13, no. 10, pp. 3375–3784, 2013.

[13] Di Ma, N Saxena,Tuo Xiang, and Yan Zhu, "Location-Aware and Safer Cards: Enhancing RFID security and Privacy via Location Sensing," *IEEE Transaction on Dependable and Secure computing* , vol. 10, no. 2,pp. 57-69, 2013.