Securing ATM and Card Transactions using SMS-Based Security

Kevin Alex Sam
Department of Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Liya Mary Antony
Department of Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Reenu Xavier
Department of Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Remitha Rahim
Department of Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Prof. Tintu Alphonsa Thomas
Department of Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Abstract

ATM cards and systems have changed the lives of people. Now they have access to money all round the clock. This ease of access to money has brought forth a serious problem as well. There has been an increase in the amount of credit card frauds caused due to impersonating as the owner of the card in shops and also obtaining the PIN (Personal Identification Number) of the customer through some illegal means. The system proposed here ensures that only the authorized user can do any kind of banking transactions both in ATMs and in shops. The customers must initiate a transaction request from their mobile phones using the SMS (Short Message Service) feature that is present in all mobile phones. The customer sends a message to the bank server before he actually performs an actual banking transaction. After that he will approach either an ATM system or a shop that accepts card payments. The transaction request is sent to the bank server and hence authenticated.

Keywords: ATM, credit card, security, SMS, PIN security, attacker, cyber criminals, crime

I. INTRODUCTION

Mobile phones have brought about a wave of revolution in the recent years. Now all financial transactions can be done in the palm of our hands with the help of these gadgets. The introduction of the Automated Teller Machines also known as ATMs provided the customers with faster access to cash whenever they wanted [6][8]. But these machines are prone to attacks from people. Once a person finds out the PIN of the user and is able to get hold of the card, then he is able to access all the savings of the customer. In case of using debit cards while shopping, the customer may also be a victim of credit card fraud. The PIN of the customer may be exposed to attacks from snooping etc [3].

These risks pose a major threat to the existence of the banking sector in any country. These problems can lead to huge economic crisis and losses to an economy which may fall entirely [2]. The developing nations report the major cases of frauds in transactions involving the bank cards [7]. An attacker has various means by which he can access to the confidential details of the user. He may be an online attacker or an offline attacker. The users tend to forget the security policies that the bank specifies about the PIN code. They may write it down on a piece of paper inside the wallet with the card. When the wallet gets stolen, their reluctance to call the bank officials and block the card from any further banking operations is one of the main reasons of successful card fraud. The users must be aware that such incidents are not isolated ones and that they must be ever vigilant. The need for the security mechanisms is increasing at an exponential rate. There is a need for a new approach to combat cybercrime and ATM fraud. This article presents a new approach via mobile phone's SMS alert [1].

II. TRANSACTIONS

ATM and shopping transactions follow the same strategy. There is a unique PIN which only the customer and the bank know. A successful authentication attempt of the PIN will result in the transaction to undergo processing and cash dispensed or debited from the account. Figure 2.1 shows how ATM and card transactions are carried out. Three incorrect PIN attempts will lead to blocking of the user's card and all future transaction accesses are denied.

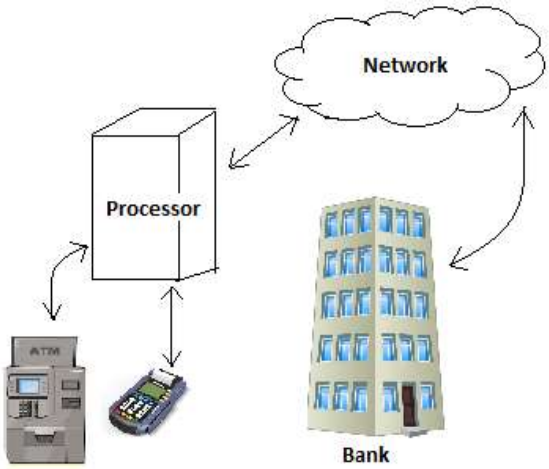

Fig. 2.1: Bank Transaction Processing

A. The Threats to PIN:

The problems of the customer arise because of carelessness. A PIN may be exposed when the user reveals the PIN to a close relative or friend. Sometimes fraudsters may pose themselves as bank officials and call them. The users thinking them to be authentic may reveal the PIN as a response to some false information provided [5]. The banks may also reveal some information in the case of some attacks to their servers or data storage warehouses. Also hackers present online may send an email to the users with the login fields [4]. The user thinking that the website is genuine, types the values needed for a successful transaction to take place. Figure 2.2 shows the various types of attackers that can take benefit of a victim's PIN.

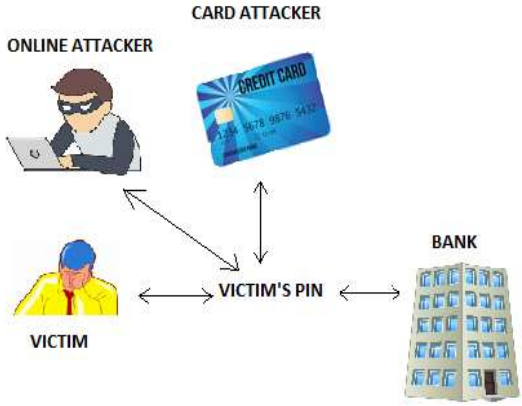

Fig. 2.2: Accesses to a Victim's PIN

B. Proposed System:

The proposed system makes use of the messaging service that is present in all mobile phones. This messaging service will be added as an extra layer of security. The messages sent will be kept on the bank servers. They will inform the servers that a new transaction in incoming.

In the case of ATM Systems, a user before he approaches a system, he will send an SMS from his phone about the details of his location, the PIN and the amount that he wishes to withdraw from that ATM system. This is the first message and it gets stored on the bank server. He then approaches the ATM and inserts his card. After he inputs his PIN and the transaction amount, the information is sent from the ATM system to the bank server. If the previous message and this message match, then the user is authenticated and the cash is drawn or other operations performed. Also a confirmation is sent back to the user's mobile device.
In the case of shopping transactions, the user sends the transaction amount and the shop id along with his PIN. This is stored on the bank server. The card is then swiped on the POS (Point of Sale) device and the amount entered. The details are again sent to the bank server and after verification, the confirmation of cash debit is sent back to the shop. Figure 2.3 shows the architecture of the proposed system.

Fig. 2.2: Proposed Architecture

III. CONCLUSION

The need for banking security is an ever growing concern within the general public. This system aims to help reduce the effects of frauds and attacks by adding a layer of security. However, ultimately the protection lies in the hands of the user. We believe that by providing a wide range of services at the ATM and at shops, depositors and customers can conveniently carry out banking transactions round the clock by confidence in this system.

REFERENCES

[1] Ugochukwu Onwudebelu, "Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems", ICAST 2011
[2] E. Aginam, "Cybercrime Can Wipe out Development Gains of a Nation – Experts", 4 March 2009, Vanguard newspaper in Nigeria.
[3] Y. Ishola, "ATM fraud: What safeguard for bank customers?" http://sunday.dailytrust.com/
[4] http://www.mydigitallife.info (2006). ATM Hacking and Cracking to Steal Money with ATM Backdoor Default Master Password
[5] Little Linda, "Attitudes towards Technology Use in Public Zones: The Influence of External Factors on ATM use" CHI of ACM, 2003, pp. 990 -991.
[6] J. J. McAndrews, "Automated Teller Machine Network Pricing – A Review of the Literature" Review of Network Economics Vol.2, Issue 2, 2003.
[7] A. Karunanayake, K. De Zoysa, S. Muftic, (2008). "Mobile ATM for Developing Countries", MobiArch'08, ACM: pp. 25-30.
[8] Triton, "Model 8100: Automated Teller Machine, User / Installation Manual, version 1.0" Delaware Capital Formation, Inc., Triton, 2005.