Abstract

With the growing number of ATM frauds, banks and customers are faced with the concern of providing security to ATM transactions. This paper presents SMS encrypted message as a media to protect ATMs against frauds and crimes. The technology includes the use of the existing PIN to provide authentication of the ATM card to the card issuer host system and the use of SMS encrypted message to authenticate the user before any transaction can take place at the ATM machine. The use of SMS encrypted message to authenticate the users can improve ATM security against frauds and crimes.

Keywords: ATM; SMS; Encryption; Elliptic curve

1. Introduction

Automatic Teller Machines (ATMs) are self service banking machines that allows customers to access their bank account without the aid of a bank teller or bank clerk [1]. They are use for financial transactions, they operate 24 hour a day helping customers to withdraw cash, deposit cash, transfer funds, check account balance, and print statement of account [2]. They are placed in convenient locations such as the retail outlets, banking premises, grocery stores, shopping malls and gas stations. [3]. They make banking transaction easier, by helping banks to meet the demands of their customers; customers do not need to go to the banking hall or even in some cases they do not need to queue in banks just to make basic banking transactions. Some ATM machines allow customers of different banks to perform basic banking transactions without going to their bank or their banks ATM machine [4]. Despite all these advantages, it has been reported in [5] [6] [7] [8] that customers and banks are faced with a lot of ATM fraud and other ATM security related problems. Therefore, there is a need to provide a means of securing ATM transaction against frauds and crimes. This study presents how Short Message Service (SMS) encrypted message can help make ATMs more secured. The proposed technology includes the use of existing Personal Identification Number (PIN) to provide authentication of the card to card issuer host system and the use of SMS encrypted message to authenticate customers before any transaction can take place at the ATM machine.

The next section explains how ATM works. ATM security threats are presented in Section 3. Section 4 describes the threat on the recent ATM security technology followed by the description of our proposed scheme in section 5.

2. How ATM Works

ATMs have a small display and either touch screen or input devices for entering inputs. To access their bank account, customers insert a plastic card into the magnetic stride reader. The plastic cards are issued by the holder’s bank. The magnetic stride card contains an identification code that is transmitted to the banks central computer
through a host computer. This identification code identifies the holder of the ATM card. The ATM asks for a PIN which is used to authenticate the user. If the user is authenticated, the ATM permits the transaction with the banking computer [9]. The basic ATM working relation is given Fig. 1

![Basic ATM Working Relation](image)

Fig. 1. Basic ATM Working Relation

3. ATM Security Problems

With the growing number of ATM put in use, ATM security breaches are now a daily occurrence around the world. Attacks on ATM include phishing, shoulder surfing and the installation of ATM skimmer [10]. ATM skimmers are used to read the ATM card number. Cameras are also installed at the ATM to read the PIN and other bank account information. This stolen information can be used to create fake or cloned ATM cards which can be used to steal money from the customer’s account [11]. The ATM security threat described in [12] [13] explains how PIN can be hacked from the Hardware Secure Module (HSM) in the ATM network. ATM PIN verification uses encryption technique. Access to PINs of some cards issued from the same bank can help an attacker determine the encryption key used by that bank hence the PIN to any ATM card issued by that bank can then be determined [14]. ATM fraudsters have become more sophisticated; they have used ATM machine to defraud banks [15] [16]. To address these issues, banks and customers are requiring new security enhancements for ATMs in order to provide improved security for financial institutions and prevent ATMs from being compromised [17].

4. Recent ATM Security Technology

With the growing security threats on banks, banking industries have been adopting new technologies to secure banking transactions. One of the recent technologies adopted by banks is the two factor authentication which often combines the use of PIN and One Time Password (OTP) for user’s authentication [17]. In two factor authentication method, first the customer enters the PIN, if the PIN is validated; the bank computer generates and sends an OTP to the customer’s mobile phone via SMS. The customer enters the received OTP. If the OTP entered by the customer corresponds to the OTP generated by the bank computer, the customer is authenticated and the transaction is permitted. This OTP password is only valid for one log on after which it is discarded [18]. The two factor authentication method is illustrated in Fig. 2.
The OTP technology includes the use of SMS message for delivery of the OTP from banks to customers. The security of OTP is based on the security of SMS which is extremely vulnerable to variety of attacks. SMS usage is threatened with security concerns such as eavesdropping, interception and modification [19]. SMS messages are transmitted as plain text. The A5 algorithm which is the GSM standard for encrypting transmitted data has been compromised. Encryption and decryption is done just between the base transceiver station and the mobile station [20]. Since SMS messages can easily be wiretapped, intercepted, and modified, it can be envisioned that OTP send via an SMS can easily be compromised by man-in-the-middle attack. If the PIN to an ATM card is earlier compromised, and the mobile number of the customer is known, compromising the OTP can be done by intercepting the OTP sent via SMS. The OTP and the PIN can then be used to make banking transactions without the customers and bank spotting any abnormalities.

5. The Proposed Security Scheme

After thorough study of the security features in ATM transaction, a security scheme is proposed. Our proposal is not replacing the existing security technology; rather it serves as an additional layer of security that protects the existing authentication system from frauds and crimes. Our concern is to provide a secure end to end communication of OTP to customer’s by encrypting the SMS message used to send the OTP from the bank server to the customer’s mobile phone.

There are two banking modules in the proposed secure model, one at the bank server and the other on customer’s mobile phone. The module at the bank server will contain a database where the entire customer’s encryption key will be stored. This encryption key will be used to encrypt SMS message containing the generated OTP before it is sent to the customer’s mobile phone. The module on the customer’s mobile phone will contain the decryption key for decrypting received encrypted SMS from the bank server. This module is password based, the customer need to enter a password before access is granted to the module. This is done in order to secure the module from unauthorized users. Both modules use Elliptic curve encryption for encrypting and decrypting the SMS message containing the OTP.

Elliptic curve is an asymmetric encryption technique. Study in [21] discusses Elliptic curve working relation. The study also explained that Elliptic curve encryption technique is a suitable asymmetric encryption technique for encrypting SMS transmitted message due to its ability of using smaller key size to obtain same security as compared to other asymmetric encryption techniques. Asymmetric encryption technique is used in the proposed model in order to prevent the decryption key from being compromised. On like the symmetric encryption technique which uses same key for encryption and decryption, the Asymmetric encryption uses two related keys, public and private key [22]. The public key will be stored in the bank server database while the private key will be stored in customer’s mobile phone. If the database containing the customers encrypting key is compromised, the decryption key will definitely not be compromised since the decryption key is stored in the customer’s mobile phone. Using asymmetric
encryption to encrypt the SMS message containing the OTP at the bank computer and decrypting it after it is received at the customer’s mobile phone will prevent the OTP against eavesdropping and interception, thereby providing security to ATM transactions.

Customer’s public and private keys can be generated by physically connecting the customer’s mobile phone to the bank computer using a cable. The public key is stored in a database at the bank server as the encrypting key while the private key will be stored on the customer’s mobile phone as the decrypting key. These keys can only be renewed if the customer’s mobile phone is physically connected to the bank's computer.

In the proposed technology, if the customer initiates a transaction at the ATM, after entering the PIN, if the PIN is authenticated, the bank server generates the OTP, gets the customer’s public key from the database, encrypt the OTP and send it to the customer’s mobile phone via SMS. Customer on receiving the encrypted SMS decrypts it using the private key to get the OTP. This additional layer on the existing security technology will help protect the OTP’s transmission from malicious attack and eavesdropping, thereby providing security to ATM transactions. This technology is illustrated in Fig. 3.

![Fig. 3. Proposed SMS encryption Authentication in ATM](image)

6. Conclusion

An asymmetric based encryption solution for securing OTP transmitted via SMS is introduced in this study. It is a scheme that provides an end to end security for SMS message containing the OTP send by bank server to customers for authentication, thereby providing security to ATM banking transaction. This scheme can be used by banks to provide confidentiality and authenticity to the bank-customer’s communications through ATM. However this scheme is not limited to ATM security, it can also be used to provide secured communication between banks and customer’s in mobile and online banking.

References