International Journal of Mathematics and Computational Science
Vol. 1, No. 4, 2015, pp. 199-205
http://www.aiscience.org/journal/ijmcs

Security Issues in ATM Smart Card Technology

Nor Fazlina Mohd Amin, Shorayha A/P Eh Chong, Nur Zafirah Abd Hashim, Hassan Chizari*

Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor, Malaysia

Abstract

A smart card is a card embedded with chip that runs dedicated applications. There are an issues related to the security in authenticity and integrity. The weaknesses of existing authentication scheme such as password and PIN number caused the leakage of information stored in ATM smartcard which lead to the lost of money in bank account and private information misuses. The security issues related to the smart card is discussed. The mitigation of the authentication issues on the ATM smart card discussed towards the biometric, cryptography and embedded biometric and cryptography approaches included communication technologies. Fingerprint biometric is one of the famous techniques for smartcard security.

Keywords

Authentication, Biometric, Fingerprint, Cryptography

Received: April 9, 2015 / Accepted: May 6, 2015 / Published online: June 3, 2015

1. Introduction

Smartcard growth from a very simple phone cards to business cards. There is a computer chip in smart card which makes it called ‘smart’ [1]. It made with inferior equipment into complex high technology security solutions which can support a large number of applications today. The usage of smartcard is actively growing over the last decade as they are many usage of them such as telecommunications (GSM), banking services and identity card. In the previous smartcards, their security features are limited to a mechanism preventing the chip on the card to be filled up again. Thus, its use is limited into a memory chip that can hold a stored value, described as write once only. Current smartcards can be used and have been used as stored value cards for pay phones.

Applications nowadays require more functionality and security which are more complex. Smartcards are re-usable, stored large quantities of data, speed transaction times, identify the card holder, and provide loyalty benefits. Smartcards are now equipped with microprocessors and a significant number of security measures. The self-containment of Smartcards makes them resistant to attack as they not need to depend up on potentially vulnerable external resources. So, smartcards are often used in applications which require strong security protection and authentication. Smart cards may also provide strong security authentication for single sign-on (SSO) in large organizations. Even the vulnerabilities displayed by Smartcards, designers of secure applications still use smartcards as one of the major technology for business transactions.

One of the most usage smart card today is ATM card. Even it is widely used, ATM card services is not considered secure 100% in order to protect the money in bank account. This paper gives a technical overview of the ATM card issues a raised and their countermeasures are also discussed.

2. Related Works

Authenticity and integrity employ a mandatory control in automated teller machine [2][3][5] in purpose to withdraw money and other bank transactions. According to [2], there

* Corresponding author
Email address: e2306@yahoo.com (N. F. M. Amin), sora_1503@yahoo.com (S. A/P Eh Chong), zafirah.hashim88@gmail.com (N. Z. A. Hashim), chizari@fc.utm.my (H. Chizari)

are three popular attacks against ATM: Skimming, PIN logging and Integrity violation. There are also attacks against mobile phone: Fake mobile apps installation, key logging software and grab PIN number during transmission. Besides that, an attack may also be a combination of both types of said attacks.

Petrlic *et al.* [2] analyze the ATM software manipulations usually done by insiders worked in the bank as they have legitimate access into the ATM. This is known as 'offline attack'. An attacker also may install fake pin pad on the ATM machine which makes full control in the attacker's hand. Normally, when ATM machine get compromised, the manufacturer will put the ATM machine as out of operation on the ATM's screen. This is how when the insider manage a chance to present any other instruction on the screen. Instead of out of operation sign, they turn it to please enter your bank card number message on the screen. This kind of tactic, normally use a software manipulation as their modus operandi regardless of the attacker's knowledge of ICT.

The attack pattern may involve spying out user's PIN number by installing tiny, hidden video camera in ATM booth location [2][14]. Lee [14] in his article re-examining the security issues of ATM systems. Just before midnight October 10, 2003 Bank of Taiwan suspended all bankcards usage and closed down ATM due to illegal withdrawals. In Australia, implanted device in card slots with tiny cameras installed resulted of illegal withdrawals total of US$436,398. Both tragedies use implanted camera as their modus operandi.

The act of mechanically pressing keys is a vulnerability to ATM. ATM PIN number can easily get through by identifying the pressed key from ATM card during entering ATM PIN number at ATM machine. A vibration of pressing key PIN number on a PIN pad may lead to reveal the actual PIN number [3]. According to Kim *et al.* [3], the natural choice to enter confidential data in electronic payment is mechanical keypads. An intrinsic vulnerability of ATM device can be caused by the act of mechanically pressing keys. Lee [14] supported [3]. A special device installed to record the sound from the pin pad when customers typing the PIN number. Different digits have different sound of frequencies. The special device is then decoded the sounds and translates them into password. The combination of both device and software manipulation is a kind of high-tech ATM scam modus operandi to get customer PIN logging.

Information also can be exploited by a side channel attack [4][5]. It is found that attackers try to get the user's account information that stored on the magnetic strip present at the back side of ATM card. Password is the only identity that can use to authenticate the owner of ATM card. It means anyone can access the account bank through ATM machine as the password entered is correct. So, once the ATM card and password is lost or stolen by anyone, they can withdraw the money from that account easily without the problem of user authentication [4][6]. Besides that, the account information in ATM card also can be getting through a fake magnetic card reader [2][6]. Thus, it can see that the most serious issue raised in ATM card security is about user authentication. User authentication is important because it lead to the integrity violation of bank account information.

Weaknesses of authentication system also lead to the leakage of account information that stored on chip in ATM card. ATM machine has keys as the input devices and card reader to read the information stored and some common gateway of ATM networks is available to users [4]. The card reader will read all information in account when the users enter the correct password or Personal Identity Number (PIN). Even each ATM needs a PIN for accessing information, it cannot consider as the information which will be access is by actual owner. This is because anyone can access the account information in ATM card when they enter the correct password [4]. Consequently, reduction in account balance may occur due to money stealing case. Most banks tried to have minimal level of security with maximum level of convenience to customer. As a customer, being a little rigid when withdrawal money from ATM is such difficulties that need to avoid. A proper balance between security and convenience need enhancement.

By reviewing on the current security issue of ATM card, the authentication mechanism is the most important rule in accessing information stored in ATM card. This is because as PIN number is the only identity that can use to authenticate the owner of ATM card. It seems that this issue is worse as anyone can access all information stored when they entered the correct password towards accessing ATM card at ATM machine. Other than that, it is strongly emphasized that the security issues need technology improvements and better security policy as a countermeasure.

3. Mitigation on the Authentication Issue of ATM Card

In order to mitigate this security issue of ATM card, many researchers come out with their idea by proposing some enhancement of ATM card security issue using biometric [4][6][10][11][12] and cryptography approach [8][9][13]. Besides that, some of researcher also proposed their idea of authentication system using biometrics combines with other technologies such as fuzzy extractor [6], Global System for Communication (GSM) and Radio Frequency Identification

in ATM smart card [12].

Researchers in [4] come out with an enhancement of ATM security using biometric and Global System for Mobile Communication (GSM) technology. They proposed this approach due to reduce the risk of authentication issue of ATM card and directly can prevent fraud activities of ATM transaction. Biometric is choose because it provide a strong and the best authentication as biometric features cannot be stole, lost, share or copy by malicious attacker. In this approach, biometric is combined with GSM technology. Based on their proposed system, once user inserted ATM card into ATM machine, the card will be process and ask user to enter pin number as normal. After pin number is correctly entered, then user need to enroll their finger on ATM provided interface for fingerprint detection. If the fingerprint recognition is match with data save in main data server, GSM will send 4 digits one time password to user mobile. So, the user need to enter one time password and then can access ATM transaction normally. If the fingerprint cannot recognized by system and it not match with the stored data, ATM card will be rejected from machine.

Yang. *et al.* [6] were proposed their biometrics authentication system using fuzzy extractor. Their biometric scheme is based on finger prints and this scheme is combined with normal passwords. Their proposed system mainly composed of three phase which are registration phase, login phase, authentication phase and key agreement phase. The general flow of their system is as follow:

1. User insert card into ATM machine.
2. Card reader read the information in ATM card.
3. Put finger print on finger print scanner and finger print sensor will authenticate the user biometric with information stored in database.
4. After finger print authentication is passed, user need to enter user ID and password for second authentication.
5. If user ID and password correct, user can access ATM transaction.

Application of biometric in secure bank transaction also has been proposed by Yadav [10]. The author stated that biometric technique using fingerprint-based is the oldest technique which is a successful method used for biometric authentication in many applications. Fingerprint is chosen because of their uniqueness features which made up of a series of ridges and furrows on the finger's surface. The uniqueness of fingerprint in this case used minutiae-based technique.

Kolhe *et al.* [11] also proposed a biometric mechanism in order to increase the security level of ATM transaction. Their proposed system is biometric palm print and transaction confirmation system. As biometric feature is a unique data, so it can be used by only one person who was the actual owner of ATM card to perform any transaction. The user's biometric palm print is taken and compare it with image that has been stored in data server. The palm print image is taken during user open a new bank account. In this scheme, a palm print biometric technique is fused with ATM for user authentication to reduce the risk of authentication security issue.

Biometric palm print recognition and transaction confirmation system work almost like the previous mechanism in [4] but, it needs to extract the principle lines of the palm print. Fig. 1 shows the flow of biometric palm print recognition and transaction confirmation system work.

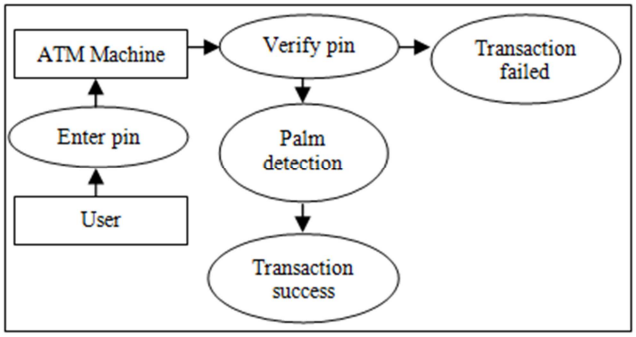

Fig. 1. Architectural block diagram of Biometric Palm Print Recognition and Transaction Confirmation System [11].

Avhad *et al.* [12] have proposed a model of authentication scheme in ATM. Their authentication model is based on three factor which are password and user ID, biometric input and one-time-password (OTP). This method includes the GSM technology for OTP and face recognition for biometric security in their authentication scheme. RFID embedded security is for password authentication scheme.

A. Biometric

Biometric is a measureable and behavioral characteristics. It can be captured and compared with another features during verification [11]. Nowadays, biometric are widely used as authentication mechanism because biometric feature is unique. Every person has different biometric characteristics and features, so biometric cannot be stolen or used by attacker to violate ATM card authentication [4][6][10][11][12]. Jaiswal *et al.* [4], Yang *et al.* [6] and Yadav [10] choose fingerprint biometric as their biometric security but the different between them is fuzzy extractor is used in [6]. Kolhe *et al.* [11] choose palm print biometric as their authentication system while Avhad *et al.* [12] used face recognition for biometric security.

As stated above, fingerprint biometric is selected to be one of

the authentication systems while using GSM technology at the same time [4]. Banker will collect customer fingerprint and mobile number for opening new bank account and store them in database. So, when user starts using ATM card by inserting it into ATM machine, machine will request user to enter their PIN number. If the PIN number entered is wrong, the card will rejected automatically. If it is correct, the user will ask to place their finger to recognize their fingerprint. Next, user will receive a 4-digits one time password through SMS if their fingerprint is match with data that stored in database during registration. Thus, user can access ATM transaction successfully after enter one-time password correctly.

Even this kind of authentication scheme seems secure but users may need to increase their access time due to the waiting time of one-time-password to be sent to them via SMS. This problem may lead to the long-queue of people that need ATM service. Some time, users may face with problem of network communication. They may fail to get one-time-password if their mobile network communication has problem or network down. Furthermore, mobile technology is not really adapted among old generations aged 60-80 years. So, GSM usage for ATM authentication may not be relevant.

The other fingerprint biometric scheme for security is proposed by Yang *et al.* [6]. The biometric scheme techniques used in their proposed system is fuzzy extractors. This scheme has three main phases which are registration, log in, authentication and key agreement phase. First phase is registration phase where user must choose their identity (ID), password and imprint their fingerprint on fingerprint sensor. Then all of this will save through a secure channel in server. Second phase is login phase. Users need to insert their ATM card into ATM machine which is card reader, and then imprint their fingerprint on fingerprint sensor. Last step in this phase is entering their ID and password. If the fingerprints, user ID and password do not match with data save in server, ATM card will reject user's login.

Final phase is authentication phase which two entities are authenticating each other. After machine receive login request, server will verify the validity of time stamp. If one of them is invalid, request will be rejected. Transaction will success if both verifications are valid. It founded that some of fingerprint may be unable to be detected and match due to unclean or unclear fingerprint texture. Sometime, it is due to fingerprint scanner problem, if the surface of scanner is unclean, fingerprint cannot be detected too. So, it is bad practice if users are urgent to use some money.

Fingerprint biometric is used because everyone has immutable and special fingerprint pattern. The minutiae points of fingerprint can be determined based on the pattern of ridges and furrows on finger's surface. There are two categories of fingerprint matching techniques which are minutiae-based and correlation-based. For minutiae-based technique, minutiae points are identified and map their relative placement on finger. Then, the Euclidean distance between the two codes will be calculated for matching the fingerprint. The algorithm to increase the robustness and accuracy in real-time is developed by the researcher but it is still not accurate enough for whole system [10].

Another type of biometric that has been proposed as authentication system is palm print. Biometric palm print recognition and transaction confirmation system is used as ATM card authentication to reduce the fraud [11]. Palm print of user bank account is integrated by storing the pattern of palm print in database. Palm print is stored as image. When user inserts their ATM card into machine, they need to enter PIN number as normal, then PIN number is verified. After PIN number is verified, user must place their hand on the palm scanner on ATM machine. Then, user's palm print will be authenticated by palm print recognition system. If the image s matched with image stored in database, user can access ATM transaction normally.

Palm print recognition system consist of several main processes which are pre-processing, region of interest (ROI) extraction, feature extraction and matching process. First, the image of palm print is capture using palm scanner.

1. After capture the hand image, the pre-processing is done to reduce the overhead. In this stage, the distortion is removed, the palm prints is aligned and the ROI is cropped. The ROI which have been crop is use for feature extraction. It begins with binaries the palm image. Then, they implement the boundary of tracking method. Next is detecting the key points and followed by establishing coordination the system. Last is extracting the central part of image.
2. In ROI extraction stage, researchers use square algorithm for feature extraction. They pass the cropped image and the minor lines through a low pass filter to suppress both of them. The composite binaries image is probe by using square structuring element.
3. Feature extraction is the third stage of palm print recognition system. In this stage, palm line is characterize by using several approaches which are line based, sub based approach, statistical approach and coding approach.
4. Last stage is matching and database verification. Users are authenticated by palm print recognition system. If the image is verified and match with the stored image in database, user can access ATM transaction as they prefer

securely.

This kind of authentication scheme also may have same problem with fingerprint biometric authentication. However, biometrics scheme for security especially fingerprint is one of the most successful authentication scheme as biometric cannot be copied or stolen by other person, only the owner of ATM card can access ATM transaction.

The other kind of using biometric for security is face recognition. This scheme is proposed by Avhad *et al*. [12]. The overall system they have proposed is the combination of RFID tag for security embedded in smartcard, face recognition for biometric security and GSM communication which is one-time-password for password security. The user will be identified by data stored in RFID tag. In the client side, the biometric (face image) data is sense using a sensor. Then this biometric data will be compared with the image stored data base in terminal side. Here, image processing is performed for extracting the feature vectors of image. If the image is same with one that stored in database, user is authorized otherwise not authorized. The third level of authentication is in server side. A random number will be generated by random generator and send these numbers (one-time-password, OTP) to user via GSM communications. If user enter the correct OTP, they can access ATM transaction otherwise it will block.

B. Cryptography

Cryptography approaches are common in smart card security. Each approach leads to an implementation either in software or hardware. Some of algorithms are commonly use in cryptography function in smart card security. However, some issues also raised up from cryptography approaches used in smart card because weaknesses in cryptography algorithms itself. Cryptography contains the encryption that process of converting the plaintext of the images towards the cipher image. While the decryption is contain the process of to get the secure plain image [8].

Below are the common algorithm used in encryption function for smart card security:

4. Private-Key Encryption Algorithm

Usually, Advanced Encryption Standard (AES) is used for cryptography function in smart card because of security, cost and implementation factors and suitable for encipher a long message as it can encrypt and decrypt a block of 128 bits. Private-key encryption is a symmetric-key cipher. Symmetric-key cipher uses a single key in encryption and decryption of plain text.

One of the modes of operations that have been used in cryptography function in smart card security is Electronic codebook (ECB) mode. It is the simplest mode of operations. In ECB algorithm, the plaintext is divided into N blocks and block size is n bits. If the plaintext is not a multiple of block size, the text is padded to make the last block the same size as the other blocks. Same key is used to encrypt and decrypt each block. So, it is not recommend encrypting big amount of block with same key. This is because message with highly structured have possible for cryptanalyst to exploit these regularities.

For example, if it is known that the message always start out with certain predefined fields, the cryptanalyst may have a number of known plain text-cipher text pairs to work with. If the message has repetitive elements with a period of repetition a multiple of n bits, then these elements van be identified by the analyst. This may help in the analysis or may provide an opportunity for substituting or rearranging blocks [9].

5. Public-Key Encryption Algorithm

Public-key encryption is an asymmetric-key cipher. It is based on personal secrecy. Asymmetric-key cipher uses two different key (one private key and one public key) in encryption and decryption of plain text. They are thought of as locking and unlocking padlocks with keys, then padlock that is locked with a public key can be unlocked only with the corresponding private key. One of the issues rose due public-key encryption algorithm in smart card security is it is more computationally cost if compare to secret-key as it has a unique nature. Besides that, keys in asymmetric cryptography are more vulnerability to brute force and man in the middle attacks.

In this situation, a malicious third party intercepts a public key on its way to one of the parties involved. The third party can then instead pass along his or her own public key with a message claiming to be from the original sender. An attacker can use this process at every step of an exchange in order to successfully impersonate each member of the conversation without any other parties having knowledge of this deception.

6. Embedded Crypto-Biometric

Embedded crypto-biometric authentication scheme is combination of the cryptography and biometric technique to improve the level of security for person authentication purposed by [7]. By combination of the cryptography that encrypted the images then transmitted to the secure channel and by using biometric that the images of fingerprint

acquired from the user encrypted for the authentication.

These include three phase in this protocol that is registration, login and authentication.

Registration Finding phase of the fingerprint of the ATM users and the templates of derived fingerprint that stored in the central server.

Login Including the fingerprint sensor detection that performed at the ATM terminal equipped.

Authentication Containing the encryption and decryption phase then transmitted to the central server in the secure channel.

There is challenge to implement the biometric cryptosystem to overcome the variation whilst harnessing of the advantages of biometrics to improve the security of encryption keys [10]. Besides that, the stems from the permanence of a biometric that apart from the physical damage, iris or fingerprints remains basically unchanged throughout a person's life.

7. Conclusions

As conclusions, this paper found that various kind of attacks on ATM smart card and ATM card reader itself have their own vulnerabilities which lead to the leakage of information that stored in ATM card. These issues have caused the reduction of money in bank account and there were many victims who faced with these issues. So, to overcome these issues, many researchers have come out with their idea to mitigate them. Some of them use biometric scheme combines with mobile technology for ATM smartcard security. Besides that, idea which used cryptography approach to mitigate these problems also has been proposed. Encrypted password can reduce the possibilities of attackers guess the password easily. For future work, some improvement on for embedded crypto-biometric approach can be done to increase the security of smart card. This is because, human biological authentication pattern are not repeated and cannot be get by others, only one pattern for each human. So, this can increase the security of authentication for accessing the information in ATM smart card.

References

[1] Taherdoost H., Sahibuddin S., and Jalaliyoon N. Smart Card Security; Technology and Adoption. International Journal of Security (IJS), 2011. Volume (5) : Issue (2).

[2] Petrlic, Ronald, and Christoph Sorge. Establishing user trust in automated teller machine integrity. IET Information Security, 2013. 8(2) p: 132-139.

[3] de Souza Faria, Gerson, and Hae Yong Kim. Identification of Pressed Keys from Mechanical Vibrations. Information Forensics and Security, IEEE Transactions, 2013. 8(7) p: 1221-1229.

[4] Jaiswal A.M. and Bartere M. Enhancing Security Using Fingerprint and GSM Technology. 2014

[5] Choudhary G.K., Sankar K. and Muthukumarawel A. ATM Technology Management System. 2014

[6] Yang, Dexin, and Bo Yang. A new password authentication scheme using fuzzy extractor with smart card. Computational Intelligence and Security, 2009. CIS'09. International Conference on. Vol. 2. IEEE, 2009.

[7] Shi, Peipei, Bo Zhu, and Amr Youssef. A rotary pin entry scheme resilient to shoulder-surfing. Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. IEEE, 2009.

[8] Ingle, Mrs Sonali S., Mrs Pratima M. Bhalekar, and Mrs Ketaki S. Pathak. Using Advanced Encryption Standard (AES) Algorithm Upgrade the Security Level of ATM Banking Systems. Rodriguez A.B., 2010. Cryptographic Function in a Smart Card.

[9] Rodriguez A.B. (2010). Cryptographic Function in a Smart Card.

[10] Yadav G. Applications of Biometrics in Secure Bank Transactions. 2013.

[11] Kolhe H., Chaudhari S., Deshphande K. and Athavle S. ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System. 2014

[12] Avhad, Prashant R., and R. Satyanarayana. A Three-Factor Authentication Scheme in ATM. 2014

[13] Sagheer, Ali Makki. Elliptic curves cryptographic techniques. Signal Processing and Communication Systems (ICSPCS). International Conference on. IEEE, 2012.

[14] Lee, Dong-Tsan. Re-examining the security issues of ATM systems. Computer Fraud & Security 2004.2 (2004) p: 13-15.

Biography

Nor Fazlina Mohd Amin, was graduated in Bachelor Degree of Computer (Science) from Universiti Teknologi Malaysia. Now is a Master candidate at Universiti Teknologi Malaysia in Computer Science (Information Security).

Shorayha A/P Eh Chong, was graduated in Bachelor Degree of Information Technology (Software Engineering) from Universiti Malaysia Terengganu. Now is a Master candidate at Universiti Teknologi Malaysia in Computer Science (Information Security).

Nur Zafirah Abd Hashim, was graduated in Bachelor Degree of Computer Science (Software Engineering) from Universiti Teknologi Malaysia. Now is a Master candidate at Universiti Teknologi Malaysia in Computer Science (Information Security).

Hassan Chizari, He is a Senior Lecturer at Universiti Teknologi Malaysia in Faculty Computing. His main research interests include wireless sensor networks, smart grid, disaster monitoring and management.