International Journal of Computer Applications Technology and Research
Volume 4– Issue 12, 943 - 946, 2015, ISSN: 2319–8656

Novel Approach for Card Payment

Amrapali.Patil
MIT College of Engineering,Pune
Pune,India

Piyush.Potdar
MIT College of Engineering,Pune
Pune,India

Swapnaja.Lomte
MIT College of Engineering,Pune
Pune,India

Abstract: The ultimate across the board user authentication approach in use today is evidently the password-based authentication. When we carry out a credit card transaction through the EDC (Electronic Data Capture) machine in the public, the user's PIN number becomes very much vulnerable to the direct observation by nearby adversaries in huddled places, promoted by vision enhancing and/or recording appliances. Devising a secure PIN entry method during the credit card transaction in such a situation is a strenuous task. Currently, there is no pragmatic solution being implemented for this problem. This paper starts with the investigation of the current status about the direct experiential attacks. Our analysis about these attacks terminates that no practical available solution at present for these direct observational attacks. This paper introduces a model which attempts to make the PIN number entry secure during credit card transactions in public places. Our model aims to use the user's mobile phone for PIN number entry rather than the merchant's user machine. The best tract about the proposed model is that the PIN number does not get revealed to any of the direct observational attacks, be it direct human observation or observation by a video camera.

Keywords: overlooking, shoulder-surfing, chip and pin, bank server, user's PIN.

1. INTRODUCTION

The chip and Pin method is carried out as follows. The Merchant or the public place where the user is paying his/her bill presents the user with the EDC machine. The user swipes his/her credit card through the EDC machine. The credit card specifics get recorded in the EDC machine. Then the user will enter his/her PIN number through the keypad on the EDC machine. The credit card details captured by the machine are matched with the PIN number. If matched, the bank will allow the merchant to carry out the transaction. For committing a credit card fraud, two things are very Crucial, one is the credit card number and the other is the PIN number. Obtaining the credit card number has become very easy these days. Credit card number can easily be obtained from the receipt produced during any credit card transaction. Or it can be recorded by a fraud person by installing a card reader in the EDC machine. So, if the credit card number is so effortless to obtain, it all comes down to the PIN number. Hence, securing the PIN number becomes very critical. Even partial information about the PIN number if leaked, can prove to be harmful as users tend to use identical passwords on multiple systems. Or, as the information is partially known, guessing the remaining part may become easier.

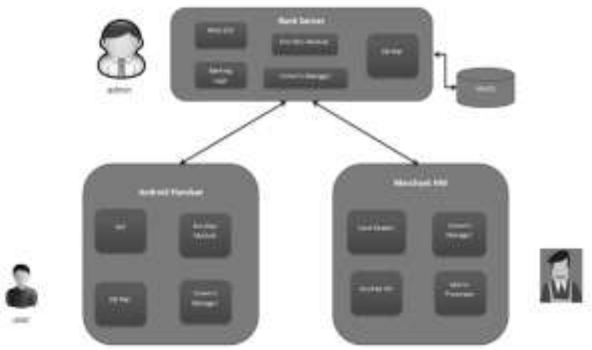

Figure 1. Schematic diagram of proposed system Model.

The problem in the chip and pin method arises during the credit card transaction when the user is entering the PIN number in a public or a crowded place such as, restaurant or a shopping mall. In this situation, the user is obliged to enter his/her PIN number in front of all those around him in the surrounding. Hence, the PIN number becomes susceptible to the direct observational attacks by humans. Or there can be a video camera or others such device which can easily capture the user entering PIN number through the EDC machine. If a user performs the credit card transaction regularly at some place, for example at a cafeteria every day, the employee by observation can learn about the users PIN number eventually. Or it may get recorded in the video Cameras at the public places. So, the PIN number is being exposed in a relatively non-technical aspect. Such kind of attacks are called overlooking or shoulder-surfing attacks. The revealing of passwords in this manner has become a security concern today due to the many cases of frauds being committed in this manner.

After the introduction of Chip-and-Pin method magnetic stripes cards were replaced with EMV cards, Chip-and-Pin method drastically reduced fraud rates in US and Europe to a certain level. This method may have reduced frauds in face-to-face transaction but we think this is not sufficient and with the implementation of our algorithm and setup this can be further reduced. Fraud losses associated with face-to-face transaction in UK itself were 198 million pounds in financial year 2008 which is pretty huge amount while the total fraud losses in UK in same year were skyrocketing high i.e. 600 million pound. World is now adapted to Chip-and-Pin method but this technique is not totally safe, as per the federal bank records in 2008 in USA fraud losses to all parties on card transaction per dollar volume were 0.13 percent or 13 basis point. This figures tells us that a lot of work can be done to reduce this losses, so we proposed a method which is capable of this. As of now, no solution is being implemented. There are some methods like BW (Black White) scheme, TictocPIN proposed for the overlooking or shoulder attacks but none of them have yet been implemented for practical use due to their respective drawbacks. So, at present all the user can do to secure his/her PIN number from being revealed is that, cover

International Journal of Computer Applications Technology and Research
Volume 4– Issue 12, 943 - 946, 2015, ISSN: 2319–8656

it while PIN number entry through the EDC machine with his/her hand or Also, review the statements after the transaction. For such attacks, we propose a model which defies overlooking or shoulder-surfing attacks. Our model uses the Users cell phone for PIN number entry instead of the user's Cell phone.

2. LITERATURE SURVEY

The solutions for making the PIN number entry during the credit card transactions are many. However, none of these implementations have brought into practical use yet. Because some have drawbacks in security whereas some others in the usability. This indicates the difficulty in securing the PIN number during offline credit card transaction.

Previously, methods have been suggested which use graphical passwords [3] [4], textual passwords [5] [6] as well a method which uses the combination of both [6]. In the method proposed by H. J. Asghar et al. [7], the user has to perform a convex hull of secret icons mentally in a set of graphical icons and then click randomly within this hull. In PAS i.e. predicate based authentication proposed by X. Baiet.al [5], predicates are used for authentication. The method described in [8] use haptic and audio signals as input for PIN number entry as these type of inputs tend to be resilient against camera attacks. The method ColorPIN [9] uses coloured letter to indicate the digits in the PIN number. But this method is not resilient against camera attacks. In one another method, pressure grids [10] are used to indicate the digit in the PIN number. However, this method has usability issues, especially in the time and efforts of the user to enter the PIN. In the method proposed by Roth et. Al [1] referred to as the BW method in [2] the user uses a simple keypad layout with half of the keys coloured white and the other half, black for entering the PIN number. The user gives input by pressing on the colours of his digit in the PIN. So the user does not give the actual digits but indicates them by colour. The entry of the PIN takes 16 rounds. It is a simple method but has practical usability issues like round redundancy, unbalanced frequencies and little protection against recording attacks [2] This method fails if sophisticated strategies and training adopted by adversaries. An improvement over this BW scheme is proposed by Kwon and Jin Hong [2] called as TictocPIN. This method assigns colours to the numeric keys. Four and three subsets of numbers are created. Unlike BW, here fixed partitions of digit space are to be used in all the sessions. It aims to receive each PIN digit through multi-round challenge round procedure. The user is informed through short vibration signals as to which of Multiple displayed challenges is to be taken as valid. This method provides sufficient security against even camera based Recording attacks. The drawback is that the time required may be considered as uncomfortable for users use.

3. OVERVIEW OF MODEL

The model aims to take the PIN entry through his mobile phone rather than the conventional method of using the same EDC machine. One of the purposes of doing this is to provide more closure to the user while entering PIN. The user swipes his/her credit card through the EDC machine. Then the merchant notifies the bank about this swipe. The bank sends notification on the user's mobile phone. The user enters his PIN through his mobile phone instead of the EDC machine. In one kind of attack, the adversary may install a card reader in the EDC machine and when the user swipes his/her card or enters the PIN number, the user's details may get recorded in the card reader. The method of entering the PIN number through the user's mobile phone deflects this possibility of such an attack. It can be called as Man-in-the-middle attack.

When at a public or cramped place the user makes a prime of paying his/her bill through the credit card the user is conferred with the merchants EDC machine through which the user swipes his/her credit card. This type of transaction is often called as the offline credit card transaction. On swiping, the credit card details are captured by the EDC machine. These specifics will be sent by the merchant to the bank through the Internet. The bank gets notified about the card swipe. The bank will immediately send a notification on the user's cell phone. The user's cell phone has an application which takes the PIN entry input. The application on the user's cell phone is the most crucial part of this model. The application aims to not to reveal the users PIN in the public place which means the user will not enter the PIN at all in the entire transaction. So, the PIN entry will be made in the application by a manner which will satisfy such condition. There are many different Methods of achieving this.

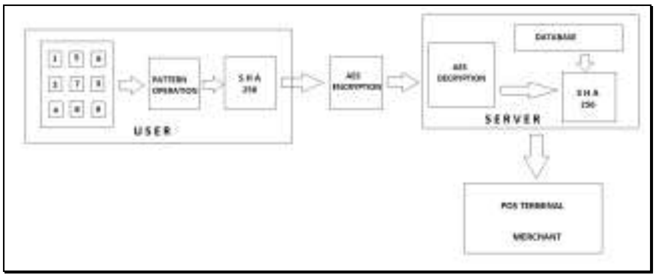

Figure 2.Detailed System Architecture of proposed Model.

The user will have the flexibility to choose any method which he/she finds suitable. Some of the methods are as follows. One way is through pattern entry like the one that is available for the phone lock. So when the user gets a notification on the mobile phone, he will enter the pattern and the PIN number stored in the mobile phone in the encrypted form will be sent to the bank. The advantage here is that the pattern is only known to the user. Also, even if it faces shoulder-surfing or overlooking attack or gets recorded by a video camera, will be of no use because knowing the pattern is basically useless .Unless the PIN number is known, the efforts of the adversary are futile. Another way of pattern entry could be to have a password entry which again will have the same advantage as the previous method .Or one can use other methods like reverse pattern or half reverse pattern. If the user uses reverse pattern, only the user knows that the PIN number to be entered has to be in reverse. For example, if the PIN number is 0793, the user will enter 3970.So the adversaries will consider the users PIN number to be the 3970
Whereas the actual PIN being reverse of it. The entered PIN after pattern analysis will be sent in an encrypted manner to the bank. The half pattern will work in the similar manner. Here, the user will have to enter 7039 i.e. half of the digits in the reverse order. One can use many such type of patterns which after pattern analysis by the application will be

converted back to the actual PIN. Thus, the actual PIN does not get revealed during the Pin number entry. Or a simpler method would be to use a yes/no pattern i.e. when the bank notifies the user about the card swipe, the user will simply press on either yes/no provided by the application. On entering yes, the PIN stored in the phone in the encrypted form will be sent to the bank. One can also use the TicTocPIN scheme proposed by Kwon and Jin Hong [2] on the phone application as it is by far the most viable method proposed. The user has a choice to use the PIN entry method of his/her choice, whichever he/she finds appropriate and secure.

3.1 Detailed Working of Model

The main purpose of this application is to keep the PIN hidden from observers and cameras. In some of the methods above, the PIN number needs to be hoarded in the phone in an encrypted manner. For security, this PIN number will be stored in the phone using SHA (secure hash algorithm) coding. SHA 256 is a cryptographic hashing function. It allows an almost unique, fixed size 256 bit (36 byte) .It is a one way function. Once operated, it cannot be decrypted back. This makes it suitable for password validation. So even if the phone comes into the hands of the adversary, the SHA coded PIN will be of no use .And if the PIN number is not stored in the phone i.e. it is entered every time during the transaction using some pattern, then the entered PIN after pattern analysis will be converted back to the actual PIN which in turn will be operated with SHA. After the SHA coding of the PIN number, It needs to be delegated to the bank, through the network. To make the PIN more secure, the SHA coded is AES encrypted. Or any such similar encryption algorithm can be used. After AES encryption, it will be directed through the network to the bank. At the bank end, the authentication will be carried out in the following manner. The incoming PIN number from the user through the network will first be decrypted back to the SHA coded PIN. As the bank database will have users PIN number stored, it will get the PIN of that particular user. The PIN will undergo SHA coding as the incoming PIN from the user is SHA coded. The incoming SHA coded PIN is matched with that from the database. Depending on the match results, the bank allows the merchant to carry out the supplementary

4. CONCLUSION

Through the proposed model, the vital objective of keeping the PIN confidential from the observer or video cameras is accomplished. PIN does not get revealed at any stage of the transaction. Thus, the model is resilient to overlooking or shoulder-surfing attacks. As the application gives the user the flexibility to choose the PIN entry method according to his/her usability and security, this makes it strenuous for the adversaries to obtain the PIN number by sophisticated approach.

Also, as the users mobile phone provides more closure to the user than the EDC machine, even observation along with the camera recording attacks become difficult for the adversaries. The bank notifying the user after the card swipe by the user serves another purpose. When the card is swiped, the bank is notified about the card swipe. The bank in turn notifies the user about the card swipe and asks for the PIN entry .In case of the card gets stolen and is used by the adversary for swiping at some place, the user will immediately be notified about the card swipe. This serves to authenticate the card owner. In case of the stolen card, the user due to the bank notification will easily come to realize about his/her stolen card if not known until then. The user can then take suitable action as soon as possible to avoid any damage. The model also delivers to make attacks other than the overlooking, shoulder-surfing or recording attacks resilient. One such attack is man-in-middle attack. If a card reader is installed in the EDC machine, all the credit card specifics entered through the EDC machine will be captured by the adversaries. In our proposed model, as the EDC machine is not used for the PIN number entry, capturing of the data by the third party is averted. The PIN number remains secure making the man-in-middle attack futile.

The proposed model has Internet dependency. In case there is no Internet available, there will constantly be an option for the user to enter the PIN number in the popular manner as our model does not change any aspects of the conventional method of the offline credit card transaction.

5. REFERENCES

[1] V. Roth , K. Richter, and R. Freidinger, “A PIN-entry method resilient against shoulder surfing”, in Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS), 2004, pp. 236–245.

[2] Taekyoung Kwon ; Grad. Sch. of Inf., Yonsei Univ., Seoul, South Korea ; Jin Hong “Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks’’ in Information Forensics and Security, IEEE Transactions on (Volume:10 , Issue: 2) Feb. 2015 pp. 278 – 292.

[3] P. Dunphy, A. P. Heiner, and N. Asokan, “A closer look at recognition based graphical passwords on mobile devices” in Proc. 6th Symp. Usable Privacy Secur. , 2010, pp. 1–12.

[4] Q. Yan, J. Han, Y. Li, and R. H. Deng, “On limitations of designing leakage-resilient password systems: Attacks, principals and usability” in Proc. 19th Symp. Internet Soc. Netw. Distrib. Syst. Secur. (NDSS), Feb. 2012.Brown, L. D., Hua, H., and Gao C. 2003. A widget framework for augmented interaction in SCAPE.

[5] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, “PAS: Predicate-based authentication services against powerful passive adversaries,” in Proc. IEEE Annu. Comput. Secur. Appl. Conf., Dec. 2008, pp. 433–442.

[6] H. Zhao and X. Li, “S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. Workshops, vol. 2. May 2007, pp. 467–472.

[7] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, “Cryptoanalysis of the convex hull click human identification protocol,” in Proc. 13th Int. Conf. Inf. Secur., 2011, pp. 24–30.

[8] A. Bianchi, I. Oakley, and D. S. Kwon, “Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry,” Interact. Comput. , vol. 24, no. 5, pp. 409–422, Sep. 2012.

[9] A. De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN—Securing PIN entry through indirect input," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2010, pp. 1103–1106.

[10] D. Kim et al., "Multi-touch authentication on tabletops," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst. (CHI), 2010, pp. 1093–1102.