International Journal of Engineering and Technology Vol. 1, No. 2, June, 2009
1793-8236

Secure Password Entry Scheme in ATM Network which Is Resistant to Peeping Attacks

Divyans Mahansaria

***Abstract* – Peeping attack is becoming an issue in the present day world with Peeping Toms looking over someone's shoulder while he/she is keying in personal data into a computer or punching password at an ATM kiosk. Also there could be the presence of any external device, which may be placed in order to trap the user and obtain valuable information, such as, his/her passwords or ATM card pin numbers, while the user types through. This form of attack is commonly known as Shoulder Surfing attack. Shoulder Surfing is a critical way to know any information, related to a person, who is doing any work in a system. It is relatively easy to stand next to someone and watch, what data the user types as an information to authenticate himself\herself to enter into a particular system. This paper provides a solution to the problem of loss in pin numbers of ATM accounts which could be obtained either through direct observation by peeping toms or due to any external vision enhancing devices. The proposed solution also avoids eavesdropper from seeking information by tapping the pin number flowing over an interconnected ATM network. No encryption technique, for encrypting the pin numbers from ATM machines to database is required. The proposed solution is also resistant to reply attack in which a user observes the movement of a person who is keying any information and then repeats his/her actions to authenticate. Thus the proposed solution is very effective.**

***Keywords* - Authentication, Shoulder Surfing or Peeping attack, Pin Number, Cryptosystem**

I. INTRODUCTION

Authentication is indeed at the heart of any secure system; a user has to be authenticated before he/she involves in online transactions, enters a secured vault, opens a safe or reach his/her email account and many other things. If sensitive information or unauthorized access is given to a wrong identity, the security of the entire system will collapse. Identity theft refers to fraudulence that involves stealing money or getting other benefits by pretending to be someone else. The person whose identity is used faces various consequences when held responsible for the perpetrator's actions. Security may not be purely technical. Hitchings asserts that treating security as a purely technical issue has led to mechanisms that are less effective than what it should have been [6]. Davis and Price add that since security necessarily involves people, human factors should be carefully considered in designing effective security mechanisms [7].

A. PEEPING ATTACK

An emerging form of security breach is due to what is called 'Shoulder Surfing' or attack due to peeping. Peeping attack is becoming an issue in the present day world with Peeping Toms looking over someone's shoulder while he/she is keying in personal data into a computer or punching password at an ATM kiosk. Shoulder Surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras could also be concealed in ceilings, walls or fixtures to observe data entry. According to other researchers on the subject, shoulder surfing is effective in crowded places because it's relatively easy to observe someone as they: fill out a form, enter their PIN (Personal Identification Number) at an automated teller machine, use a calling card at a public pay phone, enter passwords at a cyber cafe, public and university libraries, or airport kiosks, and enter a digit code for a rented locker in a public place such as the airport.

One should remain cautious of his/her surroundings if he/she is authenticating by the traditional authentication methods prone to Shoulder Surfing.

B. ENCRYPTION/DECRYPTION

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text [4].

C. REPLY ATTACK

Reply Attack is carried out by observers who do not explicitly know the password or pin number of a person typing in authentication information. But it tries to repeat the typist's actions in order to enter the password or pin number.

II. RELATED WORK

There have been some countermeasures used in a few products to prevent peeping attack. Few research proposals pertaining to it have also been proposed. But a fully functional solution which could be widely used in several applications in order to control Shoulder Surfing has not been deployed yet.

Volker et al. proposed a secure personal identification number (PIN) entry method for use against peeping attacks [2].

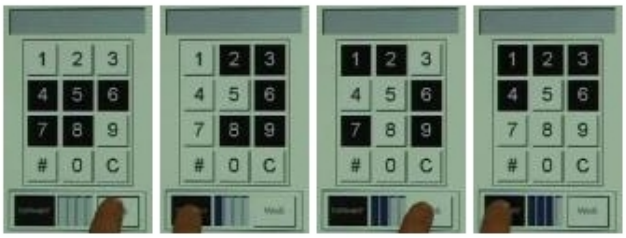

Fig1. Secure PIN entry method

By this method, the authentication system provides users with a numeric keypad with background colors of the keys as painted either black or white. These background colors are determined by the system and changed randomly after each PIN input. It is a challenge-response authentication scheme. To input a PIN, a user answers a background color of a number key of user's PIN. For each entry the color randomizes. In order to enter a 4-digit pin it is required to undergo 16 such rounds. The limitation here is that if a video recording of the login is made the password can be found out.

Another scheme to prevent peeping attacks has been proposed by Tetsuji TAKADA which uses the concept of fakePointer [1].

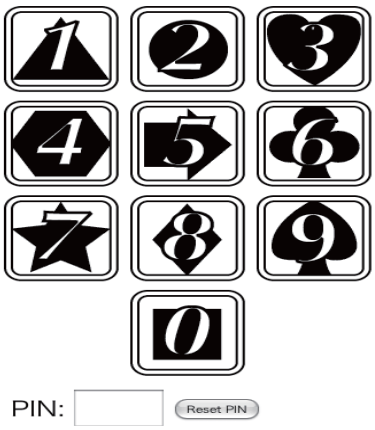

Fig.2 Screen snapshot of a secret input interface in fakePointer

The fakePointer has two unique features to ensure security against such a peeping attack. One is that fakePointer provides a double-layered interface for a secret input. This interface makes it difficult for attackers to identify a legitimate user's secret even if they have a video record showing a target user's authentication action. The other feature is that fakePointer uses two secrets: a fixed secret and a disposable secret. This feature enables change of a secret input operation in each authentication.

But this method requires more computation overhead and also the keying in time in ATM Machines increases on using this method.

Alexander et al. proposed a scheme using "PassShape". In it he says that using shapes will allow more complex and more secure authentication with a lower cognitive load [3].

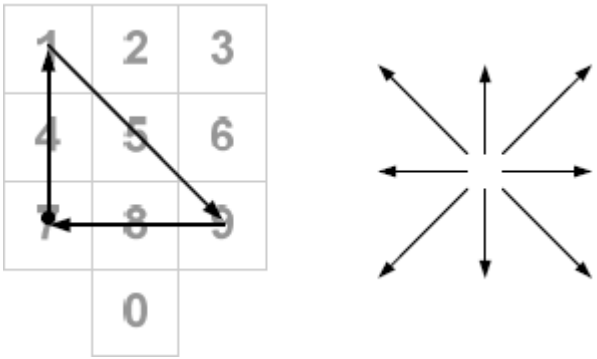

Fig.3 A shape to remember the PIN 7197 (left) and the eight possible strokes (right) of the concept.

Here the use of extremely simple or well-known shapes could be a security risk. It might be necessary to set specific requirements for the definition of shape passwords (e.g. an appropriate minimum number of strokes). A pen or touch screen based input implementation and a security-enhanced version based on the gaze gestures concept add additional complexity.

Manu Kumar et al. proposed a gazed based entry scheme to reduce Shoulder Surfing. With Eye Password, a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using only the orientation of their pupils (i.e. the position of their gaze on screen) [4].

Fig. 4 Gaze-based Password entry

But this method is expensive and takes more time than usual pin entry procedures. It also increases the complexity of a system.

Another work done in this area is by Tan et al. They propose a spy-resistant keyboard, which uses a level of indirection to prevent the observer from guessing the password However, this approach involves complex interaction techniques and also does not prevent Shoulder Surfing attack in instances when a user's keying session is recorded using Video Camera etc. [5]

The proposed method in this paper is quite different from all the preexisting solution towards the problem of Shoulder Surfing in an ATM Network. It is less complex for users to use and is also very effective in removing the Shoulder Surfing attack, which can be carried out either through direct observations or through the use of external vision enhancing devices.

III. PROPOSED SOLUTION

A user sends a SMS of ATM card number to the bank server. The bank server generates a number which we call as "FAUX" and assigns the number to the ATM card. It then encrypts "FAUX" using the password of the ATM card number as the key. To perform encryption any secure symmetric encryption algorithm such as Triple DES, AES etc. may be used. It is then send to the user who requested for a temporary pin number "FAUX" via a SMS. The user receives the SMS over his mobile phone. Now here it is mandatory for a user to have a sophisticated mobile device that has preinstalled software to perform symmetric encryption. The symmetric encryption algorithm should be a common one as is employed by server. The user then decrypts the received message on his mobile phone using his/her actual ATM pin number as the key. Only the authentic user in possession of the pin number could decrypt the encrypted message to generate the correct "FAUX". Now the user enters the decrypted number as his pin number in the ATM Machine. The ATM service provider checks the authenticity of the pin by comparing it with the assigned "FAUX". If they match then the user of the system is authentic.

After each session the "FAUX" is removed by the Bank Server as the pin number. A new "FAUX" is to be requested for each new ATM login session. Suppose that an eavesdropper obtains the encrypted form of "FAUX" by knowing a legitimate user's card number. It will be futile for the eavesdropper since he/she does not possess the correct key so they will not be able to generate correct "FAUX". A rule could be set in the server to allow a "FAUX" last for say six hours or until a login session finishes, whichever is minimum. This rule is advantageous. Another person could be given the authority by the legitimate ATM Cardholder to withdraw on the ATM Cardholder's behalf. He provides another person with the "FAUX" number which he/she has obtained through the mentioned scheme. Another person who is withdrawing on the behalf of legitimate ATM Cardholder knows only the temporarily assigned pin number which will expires after one login session. The assigned withdrawer could at the most cheat the legitimate Cardholder only at that particular time when he was assigned the job of withdrawing and not always. So he/she can be caught if extra amount is taken out at that time by going through the transaction records of the legitimate Cardholder. There could also be an optional facility available in the ATM Machine to enter the pin number directly without using the proposed scheme. This could be used for instances when the user does not want to use the proposed scheme or is not able to obtain the temporary pin number due to any unavoidable reason.

One of the other advantages of using the proposed scheme is that eavesdroppers who are eavesdropping ATM network traffic to obtain pin numbers could be avoided without using any other explicit encryption/decryption technique. An ATM Cardholder is keying in a temporary password "FAUX" which even if a wire tapping observer knows still there won't be any harm to the user since "FAUX" is not the same for subsequent login session.

The proposed scheme in this paper also reduces the transaction time by reducing the computational overhead of performing encryption and decryption of ATM pin numbers during a transaction session.

IV. SIMULATION

Step 1: A user sends his ATM Card number to an assigned server of a particular bank through his mobile phone using Short Messaging Service.

Step 2: The Server checks for the existence of a card number. If present it assigns a fake pin number "FAUX" to the corresponding card number and reply backs to the Cardholder the encrypted form of "FAUX". The encryption is performed using the Cardholder's password as the key.

Step 3: The Cardholder has a Mobile Phone which has software installed in it to perform decryption of the "FAUX". A user enters his ATM Card password as the key to decrypt "FAUX". Thus a symmetric encryption technique is been involved here.

Step 4: A user enters his/her ATM Card into ATM machine to perform a transaction. The decrypted number which is "FAUX" is entered in the ATM machine as the user's pin number. The user proceeds towards transaction. After the completion of the session and removing the ATM card from the ATM Machine his/her FAUX is not valid anymore. For subsequent transactions a new FAUX value is to be generated.

V. ADVANTAGES OF USING THE PROPOSED SCHEME

The keying time of the personal identification number does not increase. It is the same as the present time being involved in keying ATM pin number in ATM Machines. We have different FAUX number for each session which is keyed into the ATM Machine. Therefore even if a user records someone's pin number during one authentication session still it would be futile since it is changed in subsequent logins. Therefore Peeping attack on pin number is dispensed away. Using this scheme we could also hand over our ATM Card to someone else for withdrawal purpose without much of a worry. Instead of actual ATM Pin number just the temporary FAUX number needs to be told to him. Even if that person commits a fraud it would be for just one session for which he/she was requested to take out money from ATM on someone's behalf. He could be caught by verifying the transaction records by the Cardholder. Here we are performing encryption and decryption process beforehand. The requirement to perform encryption and decryption process (to prevent eavesdroppers from wire tapping the ATM Network line) by the ATM service provider is thus there. This facilitates faster transaction and reduces overhead of performing encryption / decryption during transaction. Thus we see that the proposed solution "Secure Password Entry Scheme in ATM Network which Is Resistant to Peeping Attacks" is very useful.

VI. CERTAIN CONSTRAINTS IN USING THE PROPOSED SCHEME

Extra burden of assigning "FAUX" is involved. Also the server has to receive and reply to the SMS. There may be congestion in the Mobile Wireless Network which could

involve loss of SMS or delay in the receipt of SMS by the user. In such cases user could authenticate by the traditional way which will also be present as an option in an ATM Machine. The user may be out of balance or Mobile Phone may not be charged. In such a case a user is unable to send a SMS to a server. But keeping the advantages in mind the few constraints can be overlooked.

VII. CONCLUSIONS

Pin number theft protection is of vital concern in ATM Network. Unfortunately, today's standard pin entry methods for pin number input of users is subject to a variety of attacks based on observation, from casual sneaking (Shoulder Surfing), to many other forms of attacks. The method presented by us can be very useful in controlling "Shoulder Surfing" and "Eavesdropping" of pin number over a network.

REFERENCES

[1] Tetsuji TAKADA "fakePointer: An authentication scheme for improving Security against Peeping attacks using video Cameras". In proceedings of UBICOMM08, Sept. 29-Oct. 4 2008 Page(s):395 – 400. Publisher – IEEE Computer Society.

[2] Roth, V., Richter, K., and Freidinger, R. 2004. "A PIN entry method resilient against shoulder surfing". In Proceedings of CCS'04, Washington DC, USA, October 25 - 29, 2004

[3] Alexander De Luca, Rom an Weiss, Heinrich Hussmann "PassShape – Stroke based Shape Passwords". In Proceedings of OzCHI 2007, 28-30 November 2007, Adelaide, Australia.

[4] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry". SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, July 2007, Publisher: ACM.

[5] Tan, D. S., P. Keyani, and M Czerwinski. "Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens". In Proceedings of OZCHI - Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press, 2005.

[6] Hitchings, J. "Deficiencies of the traditional approach to information security and the requirements for a new methodology". Computers and Security, 14, 377-383. (1995).

[7] Davis, Price Security for Computer Networks. Wiley: Chichester, UK. (1987).

[8] William Stallings "Cryptography and Network Security", 4th Edition. Publisher – Pearson Education Inc.

Divyans Mahansaria was born in Kolkata, India in 1987. He is a presently pursuing B. Tech in Computer Science and Engineering from SRM University, India. This young researcher has publications in many other reputed Conferences and Journals. Recently he was selected for a fully sponsored trip to Japan under JENESYS program. His research interest includes Network Security, Networking and Robotics.