IJSRCSEIT

International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307

Securing ATM Transactions Using QR Code based Secure PIN Authentication

Sumanth C M

Assistant Professor, Rajeev Institute of Technology, Hassan, Karnataka, India

ABSTRACT

With the increase of automated teller machine (ATM) frauds, authentication plays a very important role in this global world. The authentication of users at ATMs is dependent on PIN-based verification. The traditional methods relied on using card artifacts for authenticating the right user. But nowadays shoulder-surfing, physical observation, keypad overlays, ATM cloning and skimming attacks are the most common threats to the security of ATM PIN verification. In order to overcome from such attacks, here we proposed a new secure authentication mechanism Secure-PIN-Authentication-using QR code (SPAQ) -which is a card-less, secure authentication mechanism for ATM terminals using QR code and OTP. This approach protects user from transaction attacks.

Keywords : Authentication, PIN-based verification, SPAQ, QR code, OTP

I. INTRODUCTION

With the rapid growth of technology, people rely more on digital communications. The computer networks connect hosts and user terminals into a distributed computing environment, which provides the advantages of increasing reliability, sharing information and computing power, etc. Whenever a user wants to establish a secure communication channel with the server, he initiates a service request during the login process. The server first identifies the user and then checks for the legitimacy of the user. Upon a successful identification, they then negotiate a shared session key to secure the rest of the communication. Many password-based authenticated key agreement protocols [1]– [4] have been extensively investigated for a long time, where a client remembers a short password and the corresponding server holds the password or its verification data that are used to verify the client's knowledge of the password.

Our aim is to develop a secure unintelligible PIN authentication protocol for ATM terminal using personal mobile devices (SPAQ). SPAQ is mobile application allows a user to scan a QR code from the screen of a point-of-service terminal and connects to the bank's SPAQ server to obtain secure one-time-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code can be scan using a smart phone [3]. The protocol is immune to shoulder-surfing attackers, and ensures resistance against relay and replay attacks by proving co-location with the ATM terminal to the bank's server. Our design requires minimal overhead computation on the personal devices with most operations offloaded to the server and does not impose any hardware-oriented requirements on the terminals. Authentication of users at ATMs is mostly dependent on PIN-based verification [2]. Traditional methods relied on using card artefact's for authenticating the right author [1].

Nowadays, shoulder-surfing, partial observation and skimming attacks are the most common threats to the security of PIN verification [5]. People are now demanding for a more secure ATM authentication. Systems supporting card-less transactions are also getting popular. This paper aims at providing a secure authentication methodology, SPAQ, by making use of personal mobile devices.

The remaining of this paper is organized as follows: Section 2 gives existing attacks at ATM terminals. Section 3 describes the proposed system. Conclusion and future work are presented in the final section.

II. ATTACKS AT ATM TERMINALS

i. Physical obstruction attack

The fraudsters insert a folded piece of plastic film into the ATM card slot, which holds the card and does not allow it to be expelled by the machine. The victim believes his card to be caught in the machine and does not notice the card slot has been tampered. Once an inserted card is struck, a fraudster pretending as a genuine cardholder will suggest re-entering his or her security code, at this moment the fraudster reads that PIN code. When the cardholder leaves the cabin in frustration, fraudster takes the card and makes transaction using the captured information.

ii. ATM Skimming attack

It is a method used by criminals to capture data from magnetic stripes on the block of an ATM card. Devices used for skimming are smaller than deck of card and they put very close to or over the top of ATMs card reader as shown in Figure.1.

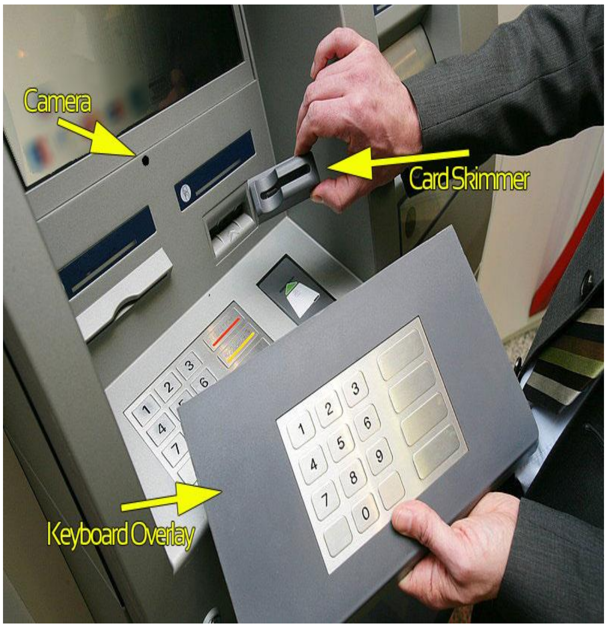

Figure 1 : Card skimmer, keyboard overlays at ATM Terminals

iii. Keypad overlays

It is a new technique designed to go unnoticed and blend in with the standard ATM keypad. It captures keystroke (i.e. steals customer PIN) when the customer enters his/ her PIN into the dummy keypad placed over the existing ATM keypad as shown in Figure.1. At the same time, the ATM card slot overlay facsimiles/records the confidential data from magnetic strip of ATM cards. Hackers/fraudsters assemble information in their computer to clone the ATM card by using blank card stock.

iv. ATM cloning

It is a process of making a duplicate card using the data captured from the original card. Fraudsters attach a skimming device on POS holder/ATM machine. Whenever a user swipes his/her card, the information from magnetic stripes goes to the skimming device, which can capture all details such as subscriber name, account details and other security details etc. after this, the user is asked to enter the PIN, which is read by the fraudster either through camera or manually. The fraudsters use this information to make a duplicate card.

v. Phishing attack

Phishing frauds are designed to attract the user to provide the card number and PIN.

i. Using Mobile: Attackers pretends himself as bank representative and claims victim's account/ card is being blocked citing security reasons and to avoid it, the user is asked to give the card and bank account details such as bank account number, card number, CVV, PIN etc., using these details attacker makes an online transaction and then user is asked to tell the One time Password (OTP) received on his/her mobile. As soon as the user reveals the OTP, the transaction is carried out using user's banking credentials.

ii. Using Email: The user is asking to click on a link and follow the directions provided. The link however is a fraudulent one and directs the user to a site set up by the attacker and designed to look like the user's bank's website. The site detects the user input sensitive information such as card numbers and PINs. Thieves, criminals, collect the information or hackers are used to create fraudulent cards.

III. PROPOSED SYSTEM

In order to overcome from all above attacks, here we proposed a secure unintelligible PIN authentication protocol for ATM terminal using personal mobile devices (SPAQ). The new approach works as follows.

i. Registration via bank's SPAQ website

The user can register in the SPAQ website by providing his personal details. Upon registration, a randomly generated password will be sent to his email. The website has further options like update profile, reset password, block and unblock account.

ii. Secure Authentication via SPAQ app

There is absolutely no need to carry the ATM card for authentication. Once connected to the network, the user can login to the app using his username and the password generated. Upon successful login, he can scan the QR code generated on the ATM screen. An 8-digit OTP is generated of which, the first 4 digits would appear on the ATM screen. The last 4 digits will be sent to the application on scanning.

SPAQ is dependent on four entities:

1) SPAQ Website: The user has register in the website beforehand. A password is generate randomly and sent to his email automatically. Using this password, user can login to the SPAQ app. Furthermore, functions like update profile, reset password, block and unblock account, are available in the website.

2) SPAQ User: The user uses a Smartphone instead of ATM card. He can log onto the SPAQ app installed on the mobile device and use SPAQ service.

3) ATM Terminal: The ATM terminal ensures the network security and it communicates with the bank server.
   SEPIA user has two options-
   1) Perform transaction using ATM card or
   2) Using SPAQ app

4) Server: The server is owned by the bank and plays an important role in the verification process. The server stores the user database and the transactions involved.

The mutual interactions between the artefacts involved in the SPAQ protocol have been depicted in Figure. 2.

There are five steps to be followed in SPAQ protocol:

Step 1: Registration and Login:

The SPAQ user must register with SPAQ application through the bank website. A system generated password will be sent to the user's email id. The user can login to the SPAQ app using the username and password.

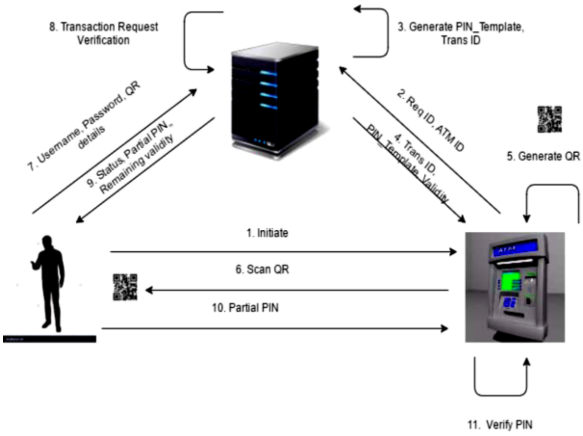
8. Transaction Request Verification
3. Generate PIN_Template, Trans ID
7. Username, Password, QR details
9. Status, Partial PIN, Remaining validity
2. Req ID, ATM ID
4. Trans ID, PIN_Template Validity
5. Generate QR
1. Initiate
6. Scan QR
10. Partial PIN
11. Verify PIN

Fig. 2 : Secure PIN Authentication for ATM terminals using QR code (SPAQ)

Step 2: ATM Transaction

If the ATM_ID is present in the server database, the ATM is authenticating once it initiate by touching the start button. The server generates a PIN and Trans_ID. The PIN is an 8-digit number.

Step 3: QR Code Generation and Scanning

A QR code is generated on the ATM terminal. The ATM_ID, Req_ID, Trans_ID is encrypted in the QR code. This QR code is scan using the SPAQ app and the encrypted details along with the username and password and those details will sent to the bank server.

Step 4: User Transaction

Three-level verification is at the bank server.

1. Checking the username and password entered are correct or not.
2. Verifying the ATM_ID is valid or not.
3. Checking the app_status is blocked or unblocked.

The last four digits are sent to the application upon successful verification and these digits will entered on the ATM screen.

Step 5 : PIN Authentication

If the entered PIN is correct, then the user is authenticated and can proceed for further transactions.

IV. CONCLUSION

ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing and skimming attacks. The goal is to protect ATM from theft using counter measures for security. Firstly in this paper shown the various possible attacks at the ATM terminals and later in this paper presented the new protocol for ATM terminal that ensures the security of ATM transactions by making use of three-level verification. Since SPAQ is based on one-time PIN and QR code, it addresses the security vulnerabilities involved in PIN-based ATM authentication. In case of loss of the mobile device, the user has the option to block the SPAQ service for his account as well. This makes SPAQ service simple and user-friendly.

V. REFERENCES

[1]. L. Coventry, A. De Angeli, and G. Johnson, “Usability and biometric verification at the ATM interface,” in Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2003, pp. 153–160

[2]. A. De Luca, M. Langheinrich, and H. Hussmann, “Towards understanding ATM security: a field study of real world atm use,” in Proceedings of the 6th Symposium on Usable Privacy and Security. ACM, 2010.

[3]. Y. Liu, J. Yang, and M. Liu, “Recognition of qr code with mobile phones,” in Control and Decision Conference, 2008. CCDC 2008. Chinese, July 2008, pp. 203–206.

[4]. M.Priyadharshini1, G.Manisha,Assistant Professor, Dept. of CSE, Valliammai Engineering College, Chennai, Tamil Nadu, India,” Quick

Response code for ATM transaction Using Face Recognition",in International Journal of Innovative Research in Computer and Communication Engineering Vol.3 special issue 8,October 2015

[5]. S. Raj and A. Portia, "Analysis on credit card fraud detection methods," in Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on, March 2011, pp. 152–156.

[6]. N. Sethi and A. Gera, "A revived survey of various credit card fraud detection techniques," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 780 – 791, April 2014.

Author :

Mr. Sumanth C M received his B.E degree in Computer Science and Engineering from Sai Vidya Institute of Technology, Bangalore in 2012. He is received his M.Tech degree in Computer Science and Engineering at Canara Engineering College, Mangalore in 2014. And he is currently working as Assistant Professor, RIT, Hassan. His areas of interest are Network Security, Information Security, IOT, and Data Science.

Cite this article as :

Sumanth C M, "Securing ATM Transactions Using QR Code based Secure PIN Authentication", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 289-293, May-June 2019.
Journal URL : http://ijsrcseit.com/CSEIT1952342