ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 2, February 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Survey of Reliable PIN confirmation for ATM's using Smartphone and Wearable Devices

Saurabh S. Sharma[1]
B.tech, (Cloud Technology & Mobile Applications)
Ajeenkya D.Y Patil University
Pune – India

Teja Bhutada[2]
Sr. Faculty
Ajeenkya D.Y Patil University
Pune – India

Abstract: In the 21st century due to the vast increase in the internet world, it has become very easy to cheat the highly secured technologies. Debit and credit card hoax is very common in today's time. Monetary centers are reporting huge losses due to operators being revealed to their credit card information. Card skimming attacks, video recording with hidden and pre-setup cameras while users execute the PIN-based transaction at ATM's is one of the common problems for the real and regular users. Many solutions came up to make it more secure, but every time that it becomes secure the hackers come up with new tricks again to reveal the PIN information. Now a days new age devices and wearables, in the form of Google Glass, have proved newer opportunities in this research area.

In this paper, we have surveyed Reliable PIN confirmation for ATM's using Smartphone and Wearable Devices like Google Glass. This serves as a secure obscured PIN confirmation convention for ATM's using cloud-connected smartphones and easy to access wearable devices. This technology is quite innovative, easy and understandable for the user to be safe and secure from the hoax or cheats happening in this practical world. The user using this technology needs a Google Glass / Wearable or simply a smartphone for scanning a QR code on the screen of the system to prove co-location to the cloud-based server and obtain a secure PIN template for point-of-service confirmation. It is simple to understand and also provides complete tough and secure connectivity to the cloud. This PIN confirmation protocol serves to protect against varied attacks.

Keywords: Carpool ATM, Confirmation, Credit/Debit Card, Google Glass, Obscured PIN, OTP, PIN Template, Smartphone, Security.

I. Introduction

Confirmation of PIN of the users at the automatic teller machines i.e. ATM's is subject to a digit-based validation. A lot of research has been done to keep these digit-based validations safe and secure.

However, the advent of technology and its growth has increased the number of hackers who will use the ATM based PIN validation process for malicious purposes. There are various attacks which can take place in such ATM based validation mechanisms. Few of them are replay attacks, card cloning, and unintentional PIN sharing. Many companies and organizations maintain a team of engineers who look into such attacks and prevent them from happening in the first place, but to no avail.

There has been a lot of research on the current scenario of credit and debit card cheats. Systems supporting card-less transactions are becoming popular, where users can use their own personal devices which they trust, such as their smartphones, to perform their monetary transactions. However, even today, incidents in the spotlight of credit card frauds and malpractices are rampant and are common news. [1]

The total loss from consumer cyber-attacks in 2013 was projected at approximately 38 million USD in the US, including 13 and 37 million in Europe and China correspondingly. Such credit and debit card hoax due to identity thefts are growing every year. [2, 3]

One very prominent attack in the above category is the Shoulder-surfing attack, also known as observation attack. They are observed to be very frequent for the ATM PIN entering process. In this case, the attacker simply observes the PIN entered by the user to get a hold on it. Although there has been a lot of research in preventing the attacks in the first place, shoulder surfing attack remains ingrained in the core of the ATM entering process. No research has yet been able to avoid it completely.

In this paper, we have studied the Reliable PIN confirmation for ATM's framework to enable obfuscated PIN confirmation for ATM and other point-of-service system using cloud-connected personal mobile and wearable devices. This system proves to be very effective against shoulder surfing attacks. It allows a user to examine a QR code from the screen of a point-of-service system and connects to the cloud-based bank's server to get secure one-time-use PIN templates also called as OTP. Here, a PIN template is a string of digits with distinct positions for the user which he uses to enter the actual PIN. The QR code scanning is done using wearable devices, such as the Google Glass wear or a simple smartphone. [4]

II. Literature Survey

The Literature survey for Secure ATM point-of-service user confirmation using PIN based templates has been done and in this section, a few of the prominent attacks have been mentioned. [5, 6, 7]

The PIN based template model identifies the ATM PIN as the main type of asset around which the entire array of attacks takes place.

Once the attacks have been identified the attacker's capabilities come to the fore as follows:

1. The shoulder surfing attack which allows the attacker to be vigilant when the ATM user is entering his/ her PIN. He observes the PIN over the ATM user's shoulders. He thus comes to know of the PIN and uses it for his gain.
2. There is also a rapid increase in the card cloning devices now a days. Whenever the authentic user needs to swipe his credit/ debit card, it is fed to such card cloning devices. This results in stolen user credentials.
3. There are also card skimming devices which fit perfectly well in the ATM card slot. When the user enters his credit or debit card, he unintentionally enters them in the card skimming device and thus results in stolen credentials.
4. There can also be framed ATM terminals which are used for stealing user's information. Such fake ATM terminals which send across user credentials to a remote terminal are called relay attacks.

III. System Architecture

This section covers the architecture of the Secure ATM point-of-service user confirmation protocol.

In the architecture, there is a cloud based server which is privately owned by the banks and shared with the costumers i.e. the credit/debit card holders. The users are also provided with local credentials by the organizations called as the Local ID's with the passwords which can be changed whenever needed and kept secretly only with the user of the cards.

The user owns a credit or debit card and a wearable device like Google glass or he/she can simply use their smartphones for Reliable PIN transactions. [9]

The model shows the complete architecture of the designed prototype model. The interaction between all the three models in the process i.e.: the user, the bank server and the ATM Machine.

The interactions and the communications are shown below step by step in the system model Figure 1.

[1] Touch the Screen to initiate: The ATM machines will display ‘Touch to Begin’ message to the user. He/ she will have to touch the screen to begin with the PIN validation process.

[2] ATM Location verification: This message sends the location of the ATM to the bank server. This helps in identifying genuine and legitimate ATM’s. A location ID of the ATM is sent to the bank server. Along with the location a Request ID is also sent.

[3] Generate PIN Template: The PIN template is an N-digit numeric pattern. The PIN template is generated using a random N-digit generator, with a total of P number of digits marked as ‘*’, where P is the ATM PIN length. The PIN of any ATM being a 4 digit number, P will be 4 and placed at random places. For example, 8-digit PIN templates for a 4-digit PIN may look like [4 8 * * 2 9 * *], [* * 4 0 2 * * 6], etc. This PIN template is generated by the Bank server after verifying the Request ID and the location ID of the ATM. [1, 8]

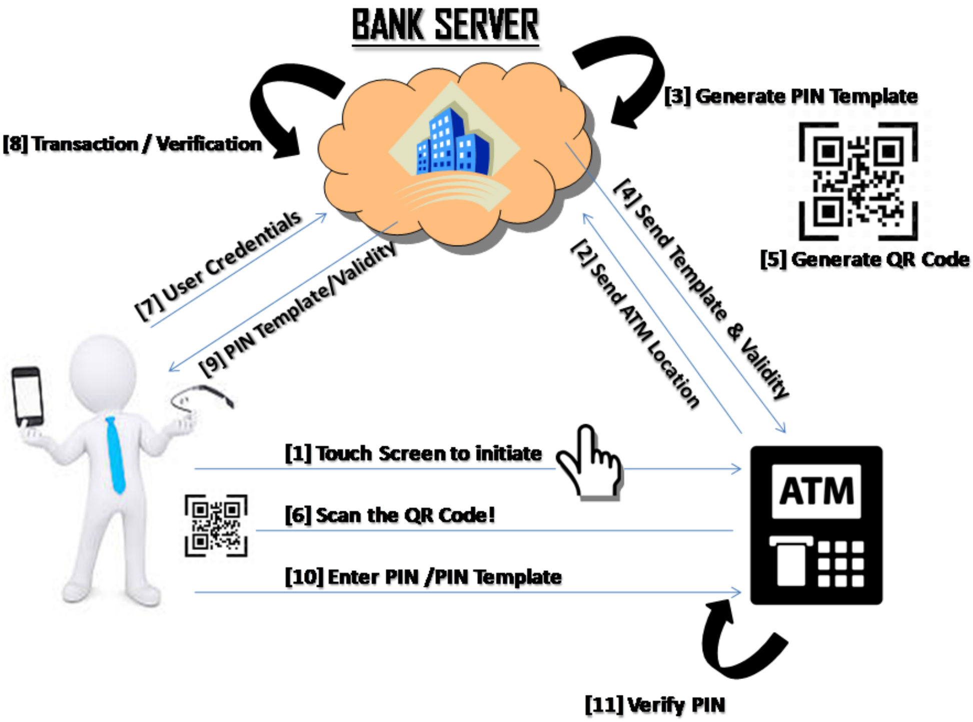
BANK SERVER
[8] Transaction / Verification
[3] Generate PIN Template
[5] Generate QR Code
[7] User Credentials
[9] PIN Template/Validity
[4] Send Template & Validity
[2] Send ATM Location
[1] Touch Screen to initiate
[6] Scan the QR Code!
[10] Enter PIN /PIN Template
ATM
[11] Verify PIN

Figure 1: System Model

[4] Send Template and Validity:

After the PIN template has been generated, it is now sent to the ATM. Along with the PIN template a validity field is also sent. This validity helps in the completing the entire “PIN entering process” within a stipulated time period. This avoids attacks which can take place after the valid user has left the ATM terminal. The user should complete the entire PIN entering process within the given validity time period. [10]

[5] Generate QR Code:

Next, the ATM generates the QR code. This QR code is a combination of the location of the ATM i.e. the location ID, the Transaction ID and the Request ID.

[6] Scan QR Code:

This is the step where the QR Code is displayed to the user. The user then scans the QR code using his smartphone or a wearable device like Google glass. The advantage of using Google glass has already been discussed i.e. the messages entered and exchanged after this will be visible only to the person wearing the Google Glass. Once the QR scanning is done, Location ID of the ATM, the current transaction ID and the Request ID are passed to the user's device from the ATM screen. [7]

[7] Send user Credentials:

This step involves verification of the user credentials. The username and the password of the user is now send to the Bank Server. To verify that it is a correct and valid transaction, the Location ID of the ATM, the current Transaction ID and the Request ID of the ATM are all sent to the Bank Server. All the 3 mentioned fields are passed onto the user's device in the step 6. [11]

[8] Transaction/verification by the Bank Server:

The Bank performs many different types of verification processes in this step. The first verification is of the username and the password received from the user. Incorrect values will send an "invalid user" message. Again the Location ID, Transaction ID and the Request ID are compared to check whether the ongoing transaction is valid or not. Any mismatch in the above results in an "invalid transaction message". Again the validity field is checked to compare if the transaction has expired or not. Expiration of a transaction results in an "expired transaction" message.

[9] Sent PIN Template/validity:

If all the validations hold true a success message is sent to the user along with the PIN template generated in step 3. A validity field is also sent along to affirm the remaining time for the transaction to be completed.

[10] Enter PIN/PIN Template:

After the user receives a Success message, the PIN template is now visible on the user's smartphone or Google Glass. If using a smartphone to enter the PIN it is the user's headache to prevent against shoulder surfing attacks. In case of Google Glass, only the user will be able to see the obscured PIN template. The user then enters the P- digit PIN code obscured within the N-digit PIN Template on the ATM's input screen. For example, if the user is displayed with the following 8-digit PIN Template: [4 8 * * 2 9 * *]. Assuming that the 4-digit PIN for the user is [1 2 3 4], the user enters the following obfuscated PIN [4 8 1 2 2 9 3 4].

[11] Verify PIN:

The PIN template along with the PIN is then given to the ATM machine. The ATM then extracts the valid PIN from the PIN template and compared it with the PIN template that it received from the Bank Server. On successful verification of the PIN, the transaction stands completed.

IV. Conclusion

The endowments and contributions of this paper are encapsulated as follows:

The Reliable PIN confirmation for ATM's is an obscured PIN-based transaction treaty for point-of-service systems using cloud-connected devices such as Smartphone. The composed treaty works with a wearable device (Google glass) or Smartphone to allow an obscured PIN template entry and is against the hoax or reply attacks by the hackers' or the attacker.

We have studied the tougher sketch for the same, via a cloud-based bank server and user applications for both Google Glass and Smartphones.

References

1. Rasib Khan, Ragib Hasan, and Jinfang Xu, "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices," 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015.
2. G. Stanley, "Card-less financial transaction," Apr. 21 2014, US Patent App. 14/257,588
3. S. N. White, "Secure mobile-based financial transactions," Feb 2013, US Patent 8,374,916.

4. E. Weise, “Home depot’s credit cards may have been hacked,” Online at http://www:usatoday:com/story/tech/2014/09/02/home-depotcredit- cards-hack-russia-ukraine/14972179/, Sep 2014, uSATODAY.
5. R. Khan, M. Mizan, R. Hasan, and A. Sprague, “Hot zone identification: Analyzing effects of data sampling on spam clustering,” Journal of Digital Forensics, Security and Law (JDFSL), vol. Vol. 9, no. 1, pp. 67–82, 2014.
6. Bureau of Justice Statistics, “Identity Theft Supplement (ITS) to the National Crime Victimization Survey,” Online at http://www:bjs:gov/ ontent/pub/pdf/vit12:pdf.
7. M. Roland and J. Langer, “Cloning credit cards: A combined pre-play and downgrade attack on emv contactless.” in Proceedings of The 7th USENIX Workshop on Offensive Technologies, 2013
8. R. Anderson and S. J. Murdoch, “Emv: Why payment systems fail,” Communications of the ACM, vol. 57, no. 6, pp. 24–28, Jun 2014. [Online]. Available: http://doi:acm:org/10:1145/2602321
9. S. Schaible, “How thieves clone your credit cards,” Online at http: //www:wfla:com/story/26074193/credit-cards-cloned, Jul 2014, wFLA News Report.
10. M.-K. Lee and H. Nam, “Secure and usable pin-entry method with shoulder-surfing resistance,” in HCI International 2013-Posters Extended Abstracts. Springer, 2013, pp. 745–748.
11. M.-K. Lee, “Security notions and advanced method for human shoulder surfing resistant pin-entry,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695–708, April 2014.