ISSN 2348 – 7968

ATM Custodian

Justin Joseph[1], Jaisan Mathew[*2], Ghilby Varghese Jaison[#3]

Student, CSE Department MBCCET, Peermade, Idukki
[1] justin11joseph91@gmail.com
[2] jaisanmathewm3@gmail.com
[3] gilbyvarghesejaison@mbcpeermade.com

Abstract
Credit card fraud is one of the common problem in today's economical world. Many Credit card fraud issues are reporting every day in the field of finance. Shoulder-surfing, observation attacks, including card skimming and video recording using hidden cameras at ATM terminals are common threats for common users. Even if many security solutions are suggested by researchers, none of them gives a permanent solution. In this paper, we propose a new security measure for ATM as ATM CUSTODIAN, a more secure ATM authentication protocol. Our system protects the user from shoulder-surfers and partial observation attack. ATM CUSTODIAN user utilizes a mobile device for scanning a QR code on the ATM screen and obtain a secure PIN template for authentication. ATM CUSTODIAN ensures minimal task for the user to perform the transaction.

I. INTRODUCTION

User authentication at ATM machines (ATMs) is generally supported PIN-based verification. Several Socio-physical factors, such as, queue length, distractions, length of your time for the interaction, urgency, physical hindrance, acquisition of PINs, co-located user show, speed of interaction, and also the setting area unit all determinants of the secureness for the procedure[2,3].The most impo- rtance from all of those factors area unit related to shoulder-surfing attacks, replay attacks, card biological research, and unintentional PIN sharing [3].Security of credit Associate in Nursingd open-end credit authentication is also thought-about as an evolving field to fight against the skillful fraudsters obtaining old of recent and simpler means that every day[5]. Researches have analysed the present state of affairs of master card fraud[7].Systems supporting card-less transactions are becoming standard, wherever users will use extra personal devices like mobiles phones, to perform the monetary. Even though chip-based (EMV) cards square measure recently gaining quality, cards still associate with the magnetic strips, and it'll be a short while until all point-of-service devices and banks square measure upgraded to support solely EMV cards .sadly, such EMV cards square measure still prone to biological research of the bank's certificate and relay attack [16,17]. Analysis on shoulder-surfing resistant PIN entry has not been new [20, 21].

Shoulder-surfing attacks, additionally called observation attacks, are most typical for ATM authentication. during this case, the assaulter merely observes the entry procedure of the PIN by the licensed user to urge hold of the key data. Credit and charge account credit frauds because of identity thefts are increasing each year [11, 12].

Credit or debit cards might have magnetic strips on them to store the PIN data. Cards with magnetic strips are simple to clone with without delay accessible and low cost card readers [18, 19]. even if chip-based (EMV) cards are recently gaining quality, cards still go along with the magnetic strips, and it'll be a short while until all point-of-service devices and banks are upgraded to support solely EMV cards. sadly, such EMV cards are still prone to biological research of the bank's certificate and relay attacks [16, 17].analysis on shoulder-surfing resistant PIN entry has not been new [20, 21]. Newer technologies, like Omni present wearable devices an mobile phones have additionally been utilised in developing secure PIN authentication technologies [22]. However, such devices also are thought of as a chance for a lot of advanced attacks by malicious users [23].

In this paper, we tend to propose the ATM CUSTODIAN to alter complicated PIN authentication for ATM. ATM CUSTODIAN permits a user to scan a QR code from the screen of a point-of-service terminal and connects to the bank's server to get secure one-time-use PIN templates. Here, a PIN template could be a sequence of digits for the user to enter the particular PIN code. We have projected ATM CUSTODIAN, a secure complicated PIN-based authentication protocol for terminals. The projected protocol works with a mobile device to permit associate obfuscated PIN guide entry and is proof against shoulder-surfing, relay, and replay attacks.

II. ATM CUSTODIAN MODEL

The ATM CUSTODIAN architecture is a protocol for secure ATM point-of-service user authentication using obfuscated PIN codes. In this section, we present the threat and system model to illustrate the functionality of the proposed ATM CUSTODIAN architecture.

A. Threat Model

The usual threats in the field of banking is as follows our present world

1) ***Assets:*** The quality for ATM point-of-service authentica-tion is primarily the user's PIN code. The PIN could be a secret data identified solely to the user of the cardboard and is employed by the user to certify at the ATM at the side of the credit and/or charge account credit.

2) ***Attacker's Capability:*** within the state of affairs wherever a user has bestowed a credit or charge account credit at associate ATM and is near to gift the PIN code for authentication, the subsequent area unit thought-about to be the potential attacks by a malicious entity:

i. The offender is standing in queue behind the au-thenticating person and looking out at the PIN entry and execute a shoulder-surfing or observation attack [20]. The offender may additionally install atiny low camera on the highest surface of the ATM terminal to record PIN entries of users at the point-of-service.

ii. A viewer could also be roaring in a very partial observation attack, wherever he's solely ready to see the partial PIN entry for the user. as long as most PIN codes area unit 4-digits long, the likelihood of a PIN-guessing attack still persists.

iii. The offender works at an area eating place and owns an inexpensive and pronto accessible card biological research device. A user could visit the eating place, and once paying with the credit or charge account credit, the offender clones the customer's card [15, 18, 19].

iv. The offender has put in a card skimming device on the ATM machine to induce hold of the user's card data. Such devices match at the cardboard slot on ATM machines and record the cardboard data because the user slides in their card [24].

v. The offender will execute a relay attack on the user's card. The offender operates a changed ATM terminal, associated uses relayed card data from an actual mastercard user to form payments at another remote station [17].

vi. The offender has put in a legitimate-looking ATM terminal. Users area unit so tricked into thinking the terminal as a sound ATM and puts in their credit/debit card and loses the cardboard data.

vii. The user uses a complicated credit/debit card PIN protection service supported memorability and graphical image recall [14]. associate offender keenly follows the entry procedure of the user, or uses a movable camera to record and gain information regarding the user's graphical countersign entry and is roaring in death penalty a shoulder-surfing attack.

viii. An offender will execute associate intermediate interaction attack. during this case, the offender finds his thanks to steal the data because the user has been distracted for a few reason and exposes the credentials to the offender.

B. System Model

Next, we define the ATM CUSTODIAN system model, which will allow credit/debit card users to perform secure confused PIN authentication at ATM point-of-service terminals. ATM CUSTODIAN dependent on 3 entities: the user, the ATM terminal, and therefore the bank server.
Bank Server: The bank server stores the username and passwords of different users. The generation of OTP pin template is also done is bank server.

1) ***Point-of-Service Terminal:*** The ATM point-of-service terminal encompasses a distinctive location symbol, Loc ID, that is approved and appointed by the bank. The ATM incorporates network property and might communicate with the bank over secure affiliation.

2) ***User:*** The user owns a credit/debit card together with a legitimate PIN code for authentication at the point-of-service terminal. The user owns a mobile phone device for secure obfuscated PIN authentication. The ATM CUSTODIAN application is put in on the mobile device. Initially, the user generates a username and secret key to be used for ATM CUSTODIAN on the app. The mobile application needs the user to log in to the application using the username and secret key. The web-based service on the bank server permits the user to store and save the username/password data, that is later used throughout the ATM CUSTODIAN protocol. The user will produce a replacement secret at any time, and update it on the bank web site.

The ATM CUSTODIAN protocol involves mutual interaction between all 3 pairs of entities: the user and also the ATM, the ATM and also the bank, and also the user and also the bank, as shown in Figure 1. The sequence of

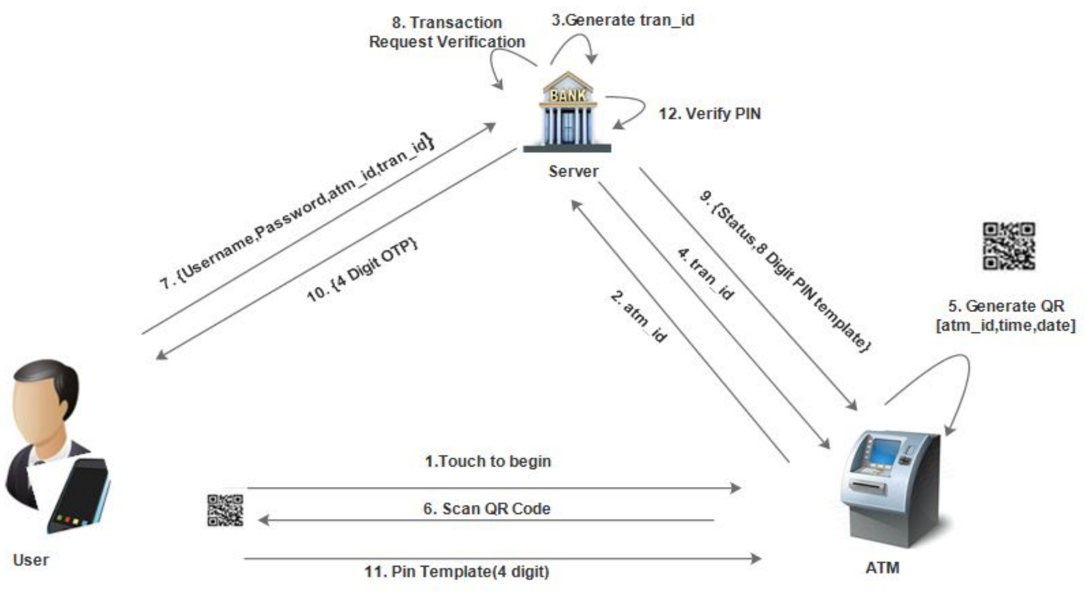
8. Transaction Request Verification
3.Generate tran_id
BANK
12. Verify PIN
Server
7. {Username,Password,atm_id,tran_id}
10. {4 Digit OTP}
9. {Status,8 Digit PIN template}
4. tran_id
2. atm_id
5. Generate QR [atm_id,time,date]
User
1.Touch to begin
6. Scan QR Code
11. Pin Template(4 digit)
ATM

Fig. 1: The ATM CUSTODIAN for Obfuscated PIN Authentication for ATM using Personal Mobile

interactions and messages within the ATM CUSTODIAN protocol is delineated as follows.

1) ***Step one [Initiation]:*** The user, in conjunction with the non-public mobile approaches the ATM to perform a secure dealing. The ATM screen displays a “Touch to begin” data screen by default. The user touches the screen (or presses the button) to initiate the protocol.

2) ***Step two [ATM dealing Request]:*** At now, the ATM sends Associate in Nursing ATM TRAN REQ message to the bank’s secure server. The structure of the message is outlined as:

ATM TRAN REQ ⇒ [ATM_ID]   (1)

Here, the Req ID could be a request symbol that is generated by the ATM for this current dealing request. The Loc ID is a distinctive and verified unque symbol for the actual ATM point-of-service appointed by the bank.

3)***Step three (atm_id verification and transaction id generation)***: at the server end,it checks whether it is a valid atm_id and will generate a transaction id for the same.

4) ***Step four [Transefering transaction id]:***The transaction id generated at server will be passed to the atm.

5) Step five QR code Generation]: Upon receiving the ATM TRAN REQ message from the ATM, the bank generates a dealing symbol, Tran ID, for this explicit ATM dealing request. The ATM thus generates a QR code on receiving the Tran ID using the Loc ID and current date and time.

6) ***Step six [Scanning QR code]:*** Once the user gets a QR code on the ATM screen, he has to scan it using the mobile ATM CUSTODIAN application. Along with that he has to give his bank’s username and password.

7) ***Step seven[transferring values to server]:***In this step, the customer’s user name, password, and atm_id will be send to the server. atm_id is encoded in QR code.

8) ***Step eight[verification at server]:*** At the server end, server checks whether the username, password, ATM loc are correct or not.

9) ***Step nine[Pin Template generation]:***The PIN guide is generated employing a random 8-digit generator, with last four digits marked as ‘*’. as an example, eight-digit PIN templates for a 4-digit PIN might seem like [4 8 2 9 * * * *], [1 2 3 9 * * * *], etc.

The bank stores the Validity for the at most amount of your time (e.g. thirty seconds) among that the PIN guide must be used. A Validity worth too low would force the user to perform the ATM authentication in no time, whereas the next worth can create the system at risk of relay and replay attacks.

10) ***Step ten [OTP process]:*** The last 4 digits of the pin template will be send to the users ATM CUSTODIAN application as OTP.

11) ***Step eleven[Obfuscated PIN Input] :*** In this last step ,the user has to input the 4 digit pin received in ATM CUSTODIAN application to complete the authentication.

12) ***Step twelve[verification at server]:***At the server end,server checks wherther the password users inputs is correct or wrong.if everything fine ,the authentication is complete and he can perform the rest of the transaction.

III. DESIGN ANALYSIS

This section presents the safety and style analysis for the planned ATM CUSTODIAN design with relation to the threats mentioned within ATM CUSTODIAN . The ATM CUSTODIAN protocol needs a private device, like a Smart phone, for performing arts the confused PIN authentication. However, because it has already been mentioned, the larger screen on the mobile device needs the user to be a lot of careful since they may support partial observation a bit extend, provided that the show of the PIN guide is protected. Any witness observant or recording the PIN entry procedure won't be able to decipher the particular PIN code that pertains to the authentication.

Let us assume that a non-authorized user scans the QR code whereas the user is performing arts the authentication method. There are 2 potential event scenarios: the user has already scanned the QR and sent the USR TRAN REQ before the criminal has scanned it, or the wrongdoer scans it initial before the user. within the initial case, the REC for that specific dealings and therefore the PIN guide can already be flagged as used. The wrongdoer can so receive a ‘Repeated transaction’ error code. within the second case, the user can receive the ‘Repeated transaction’ error, within which case, the entire procedure is restarted firmly. just in case an wrongdoer makes an attempt to perform the terminal authentication with the PIN code of a cloned card, the attacker can still need a username/password data. while not the ATM CUSTODIAN service username/password data, that is registered on the bank’s web site, the wrongdoer can receive the ‘Invalid user’ error standing.

Video recording bugs on an ATM terminal or bystanders recording the PIN entry procedure with mobile cameras can still defend the user from being exploited as a result of the one-time-use PIN guide. to boot, the 8-digit PIN guide offers a lot of numeric combos for the PIN entry procedure. This makes the task of PIN-guessing with partial observation attacks far more tough. The user proves co-location with the ATM terminal to the SEPIA server mistreatment the corresponding Req ID, Loc ID, and therefore the Tran ID. Therefore, authorisation data to an overseas terminal and execution of a relay attack becomes not possible. A tainted ATM terminal won't be holding a sound Loc ID that are assigned by the bank. As a result, the Tran ID for the requested dealings won't be valid by the bank and can be responded with a ‘Invalid dealings request’ error from the bank server.

Similarly, the one-time-use PIN guide bank server generated Tran ID also protects the user from replay at-tacks. to boot, the regular validity amount for every transaction and therefore the corresponding PIN guide prevents users from intermediate interaction attacks provided that the ATM CUSTODIAN service solely permits the PIN guide to be used for Validity time (e.g. twenty seconds), the dealings request gets terminated and therefore the user has got to begin the method from the start. Therefore, solely an energetic interaction of the user at the point-of-service can permit the authentication method to achieve success. Finally, provided that the user loses his personal mobile or wearable device, the credentials ar still safe with the user. not like alternative works [22], the devices don't store any data, like certificates, to decipher the one-time PIN. Instead, the username/password data is employed to retrieve the PIN guide firmly from the ATM CUSTODIAN service , so the PIN code is mapped by the user on the PIN guide for obfuscated authentication. The user can block the device if needed using the banks site.

The user’s personal mobile simply acts as a requestor and receiver of the PIN guide from the bank server. Moreover, ATM CUSTODIAN doesn't need any hardware upgrades to presently operative ATM or point-of-service terminals. The ATM package is simply upgraded to include the ATM CUSTODIAN service for users with Internet-enabled devices.

IV. IMPLEMENTATION

We have enforced a essence for the planned ATMCUSTODIAN protocol. The epitome consisted of a bank server, a Java primarily based desktop application to imitate the ATM terminal, and SEPIA user applications for humanoid . during this section, we have a tendency to gift the main points and therefore the experimental results from for epitome implementation.

A. Bank Server internet Application

The ATM CUSTODIAN service was enforced as a web-based application. The back-end was enforced victimisation MySQL info, that was running on constant cloud instance. The response and management logic was developed victimisation Java Server Pages. the applying generates 8-digit PIN Templates supported the Java random generator. the primary step creates associate 8-digit random variety, and so replaces four random places to form the PIN guide.

B. User Application

We developed the ATM CUSTODIAN user application for the personal devices like mobile phones. The mobile phones are one of the most user friendly and fast access personal device which is easy to carry and maintain. The device so inherently filters off the upcoming threats for observation attacks. The user management for the mobile interface is so easy and convenient. The system make use of a mobile application which operates by displaying the necessary actions to be performed by the user. Once the application is launched, the ATM CUSTODIAN bank sever will provide the username and password for the login and to continue banking.

The ATM CUSTODIAN make use of a dedicated mobile application for the secure transaction and communication with the server. The server provides a unique username and password for each of the user for using the application. Once the user touch and initiate the process at the ATM, a QR code will be displayed on the screen, the next action is to activate the mobile application. When the application on the personal device is activated it reads and measure two inputs like the username and password of the corresponding user. After the authentication is successful, the next action to be performed by the user is to scan the QR code displayed on the ATM screen using the camera read on mobile application. We enforced a secret creation and verification of transaction for our system in terms of usability. It’s not a trivial task to scan and send the details by using personal device. Therefore, a user is predicted to form a secure and secret verification for the ATM CUSTODIAN by mobile application. After the successful verification, the protocol is mechanically triggered and therefore a four digit randomly generated secret PIN guide is then displayed on the screen of the user, that he/she will enter it along with the four digit PIN displayed on the ATM screen. If the verification of the eight digit PIN is successful then further transaction is proceeded. The humanoid mobile application follows the same user flow. However, the mobile application doesn't have the new secret creation possibility. Rather, it's a username/password primarily based login panel to log in to the application.

V. CONCLUSION

ATM authentication mistreatment PIN-based entry is very susceptible to shoulder-surfing or observation attacks. Credit/Debit cards are not resilient to relay and alternative skimming and biological research attacks. during this paper, we have a tendency to propose the ATM CUSTODIAN a cloud-based obfuscated PIN-based authentication service for ATMs or point-of-service terminals mistreatment personal mobile . We’ve targeted the safety style for ATM CUSTODIAN supported visual privacy of users for a one-time-use PIN guide and address the safety vulnerabilities in PIN-based authentication. The protocol doesn't need any extra hardware support for presently operational ATM terminals and employs offloaded computation from the mobile device for substantiative the trans-action requests. A proof-of-concept example implementation was accustomed perform experimental analysis and a usability study. Results show that users area unit simply tailored to the method of template-based authentication. Our future work involves applying the ATM CUSTODIAN service to newer application fields, such as, PIN-enabled doors and visual authentication mechanisms.

REFERENCE

[1] Rasib Khan, Ragib Hasan, and Jinfang Xu,”SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices”, 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering

[2] Coventry, A. De Angeli, and G. Johnson, “Usability and biometric verification at the atm interface,” in *Proceedings of the SIGCHI con-ference on Human factors in computing systems*. ACM, 2003, pp. 153–160.

[3] A De Luca, M. Langhinrich, and H. Hussmann

[4] “Towards understand-ing atm security: a field study of real world atm use,” in *Proceedings of the 6th Symposium on Usable Privacy and Security*. ACM, 2010.

[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.

[7] M. Dlamini, J. H. Eloff, and M. M. Eloff, “Information security: The moving target,” *Elsevier Computers & Security*, vol. 28, no. 3, pp. 189– 198, May 2009.

[8] T. P. Bhatla, V. Prabhu, and A. Dua, “Understanding credit card frauds,” *Cards business review*, vol. 1, no. 6, 2003.

[9] G. Stanley, “Card-less financial transaction,” Apr. 21

2014, US Patent App. 14/257,588.

[10] S. N. White, "Secure mobile-based financial transactions," Feb 2013, US Patent 8,374,916

[11] E. Weise, "Home depot's credit cards may have been hacked," Online at http://www.usatoday.com/story/tech/2014/09/02/home-depot-credit-cards-hack-russia-ukraine/14972179/, Sep 2014, Usatoday.

[12] Bureau of Justice Statistics, "Identity Theft Supplement (ITS) to the National Crime Victimization Survey," Online at http://www.bjs.gov/ content/pub/pdf/vit12.pdf.

[13] R. Anderson, "Why cryptosystems fail," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*. ACM, 1993,

a. 215–227.

[14] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in *Proceeding of The 26th Annual SIGCHI Conference on Human factors in Computing Systems*. New York, NY, USA: ACM, 2008, pp. 183–192.

[15] 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.

[16] 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

[17] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks." in *Proceedings of The 16th USENIX Security Symposium*, 2007, pp. 87–102.

[18] S. Schaible, "How thieves clone your credit cards," Online at http: //www.wfla.com/story/26074193/credit-cards-cloned, Jul 2014, wFLA News Report.

[19] J. Kegley, "Financial crimes: Credit card 'cloning' is a growing form of identity theft," Online at http://www.kentucky.com/2012/06/24/ 2236535/financial-crimes-credit-card-cloning.html, Jun 2012.

[20] M.-K. Lee and H. Nam, "Secure and usable pin-entry method with shoulder-surfing resistance," in *HCI International 2013-Posters Ex-tended Abstracts*. Springer, 2013, pp. 745–748.

[21] 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.

[22] J. Hsu, "How google glass can improve atm banking security," Online at http://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/how-google-glass-can-improve-atm-banking-security, Mar 2014, iEEE Spec-trum.

[23] S. Safavi and Z. Shukur, "Improving google glass security and privacy by changing the physical and software structure," *Life Science Journal*, vol. 11, no. 5, pp. 109–117, 2014.

[24] B. Krebs, "Would you have spotted the fraud?" Online at http: //krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/, Jan 2010, krebs on Security, In-depth security news and investigation.

[25] L. Richardson and S. Ruby, *RESTful web services*. " O'Reilly Media, Inc.", 2008.

[26] 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.

[27] A. De Luca, E. von Zezschwitz, and H. Hu*β*mann, "Vibrapass: Secure authentication based on shared lies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '09. New York, NY, USA: ACM, 2009, pp. 913–916.

[28] A. Vukotic and J. Goodwill, *Apache Tomcat 7*, 1st ed. Berkely, CA, USA: Apress, 2011.

[29] N. Asokan, H. Debar, M. Steiner, and M. Waidner, "Authenticating public terminals," *Computer Networks*, vol. 31, no. 8, pp. 861–870, 1999.

[30] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*. New York: ACM, 2004,