ATM CUSTODIAN: A NEW TYPE OF AUTHENTICATION FOR ATM'S

ABHISHEK G MENON
Student, Dept. of Cse
Mbccet, Peermade
Idukki

ARUN V MOHANAN
Student, Dept. of Cse
Mbccet, Peermade
Idukki

GHILBY VARGHESE JAISON
Assistant Professor, Dept. of Cse
Mbccet, Peermade
Idukki

ABSTRACT

***Abstract*—Credit card fraud is a major problem in today's world. Financial institutions has registered field loses currently due to users being unprotected of their assets and card information. The present system of authentication of ATM is mostly dependent on pin-based verification. Factors such as urgency, memorization of pins, speed of interaction, unintentional pin sharing affect diversely for the current system. There are many threats regarding ATM like shoulder-surfing or observation attacks, including card skimming and video recording with hidden cameras while users perform PIN-based authentication at ATM terminals is one of the common threats for common users. Cards with magnetic strips are easy to clone. Card-less transaction are getting popular, where users can use mobiles phones to perform the financial transaction. Researchers have struggled to come up with secure solutions for secure PIN authentication. A ATM custodian user utilizes a mobile device for scanning a QR code on the terminal screen to prove co-location to the server and obtain a secure one time PIN for point-of-service authentication. ATM custodian ensures minimal task overhead on the user's device with maximal computation offloaded to the cloud.**

General Terms

Authentication, Credit/Debit Card

Keywords

ATM, Shoulder surfing, card skimming, card cloning, QR code, PIN.

1. INTRODUCTION

As Automated Teller Machine (ATM) is becoming common ATM frauds also are increasing. New authentication mechanisms area being developed

to beat security issues of ATM personal identification numbers (PIN). Those mechanisms are judged on speed, security, and memorability compared with ancient PIN entry systems. It remains unclear, however, what appropriate values for PIN-based ATM authentication really area unit. A field study and two smaller follow-up studies on real-world ATM use was conducted so as to produce each a stronger understanding of PIN-based ATM authentication, and on however different authentication ways are often compared and evaluated. The results show that there's a giant influence of contextual factors on security and performance in PIN-based ATM use. Such factors include distractions, physical hindrance, trust relationships, and memorability. From these findings many implications for the planning of other ATM authentication systems were found, like resilience to distraction and social compatibility.

Automated Teller Machines (ATM)[2] has become more relevant to the mankind in day-to-day operations. The Automated Teller Machines have been installed in all the locations around the globe. The majority of the cash withdrawal transactions are handled only by the ATM. ATM offers a wide range of financial services and are well-equipped to provide a

high level of satisfaction to the end users. The main aim of financial institutions is to utilize the same Automated Teller Machines for non-financial services. Many initiatives have been made by the financial institutions to carry out the same. One of such initiative is to perform the mobile recharge through the ATM.

In this work, we propose a system for efficient authentication of automatic teller machine (ATM) by QR code system. Quick Response (QR) codes are two dimensional barcodes that can be used to efficiently store small amount of data. They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. While QR codes have many advantages that QR code is an image of a matrix barcode that stores data in two dimensions. Data is presented as square dots with specific pattern in both horizontal and vertical dimensions. Specific imaging devices (QR scanners) can read this image and retrieve the stored data based on the pattern of square dots. There are several standards for data encoding in QR codes, the last standard is ISO/IEC 18004:2006 Information technology -- Automatic identification and data capture techniques. Smart phone devices can be used as QR code scanners. The embedded camera in the smart phone captures an image of the QR code, then an application analyses the pattern of square dots to retrieve the encoded data and display it in a useful form make them very popular.

The main attempt here is made to provide a system that will provide a well security and propose a convenient way of using the automated teller machine for the purpose of a secure and efficient transaction. This system consideration is also helpful in providing an alternative and a secure way for accessing ATM using QR custodian method rather than depending on a ATM cash card and PIN.

The proposed system makes use or QR code and a smart phone for scanning it. The system mainly consist of a QR code at the ATM screen which contains the location ID of the ATM, in this an android application is associated with the user with which he/she enters the user name and password for authentication and scans the QR code on the ATM for getting the location ID of the ATM. All the entered data is being forwarded to the banks server for verification purpose. After verification had been successfully done, the transaction details and amount for withdrawal had to be entered through the smart phone. Upon receiving all the details the bank server creates a corresponding QR code, and is being send to the ATM screen. The user uses the smart phone to scan the QR code for verifying the account transaction, and is being send back to the bank's server for checking weather both the QR code send to the ATM screen and which is received by the server are same .If the they matches each other the transaction becomes successful. The this system the QR code which is generated is different in each transaction and

This will also provide security from shoulder surfing and partial observation attacks. Since in this system the use of ATM card is completely avoided, therefore the card skimming and card cloning attacks is completely avoided. The QR code which is displayed on the ATM screen which contains the location ID of the ATM is also continuously changing in order to provide a better security for the system.

In this paper literature survey about the topic is done. Here we discuss about the disadvantages of the existing system and how we came into the current solution. This paper consists of the technologies used in the current ATM system and the threats associated with the present system.

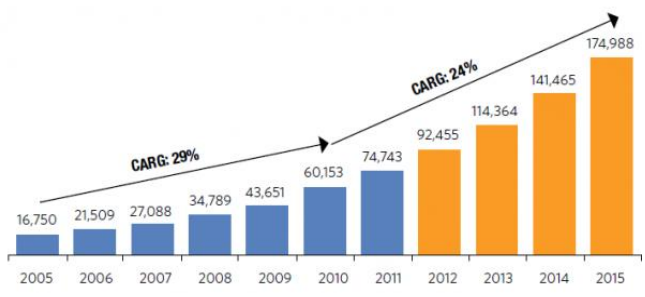

Fig 1.1 ATM users growth rate

2. LITERATURE REVIEW

2.1 PIN BASED AUTHENTICATION

A PIN pad or PIN entry device is important in a very debit, credit or sensible card-based dealings to simply accept and cipher the cardholder's personal selection (PIN). PIN entry technique is usually used for cash dispenser machine, associate integrated purpose of sale devices among that associate electronic till is chargeable for taking the sale quantity and initiating/handling the dealings. The PIN is employed to verify a client (the user of a bank card) at intervals associate degree electronic funds transfer system, and (typically) to authorize the transfer of funds, thus it's necessary to guard it against unauthorized access or misuse. fashionable banking systems want ability between totally different card issuers, effort banks and retailers – as well as transmission of PINs between those entities – thus a standard set of rules for handling and securing PINs is required to confirm technical compatibility and a reciprocally in agreement level of security.

Information and laptop security area unit supported for the most part by passwords that area unit the principle a part of the authentication method. The private number (PIN) is common authentication technique employed in varied devices like ATM's, mobile devices and electronic door locks. This PIN entry technique is injured to shoulder surfboarding attack (SSA). Once user enters their number in inhabited place, assailant observes the number over their shoulder. This is often referred to as shoulder surfboarding attack.

2.2 QR CODE

QR code stands for Quick Response Code, Which is the trademark for the type of matrix barcode which was invented by the Japanese corporation Denso Wave. QR[15] code has a number of features such as large capacity data encoding, dirt and damage resistant, high speed reading, small print out size, 360 degree reading and structural flexibility of application. QR codes have already overtaken the popularity of classical barcode in many areas because of several advantages like increase in capacity, reduced size, etc. Combined with the diversity and extendibility offered, it makes the use of QR code more appealing than that of the barcodes. Statistically, QR codes are capable of symbolizing same amount of data in approximately one tenth the space of a traditional barcode. Information such as URL, SMS, contact information and plain text can be embedded into the two dimensional matrix. Moreover, with the explosive increment of the trend to use smartphones has also played an important role in the popularity of QR codes. They are easy to use and versatile. The code itself stores huge amounts of information that is easily scanned and stored onto a mobile device. Many businesses are now adopting this code as a means of marketing and as another way to attract customers to the internet for more information. QR codes have both advantages and disadvantages and both benefits and drawbacks of the code should be understood before using the QR code as a marketing technique.

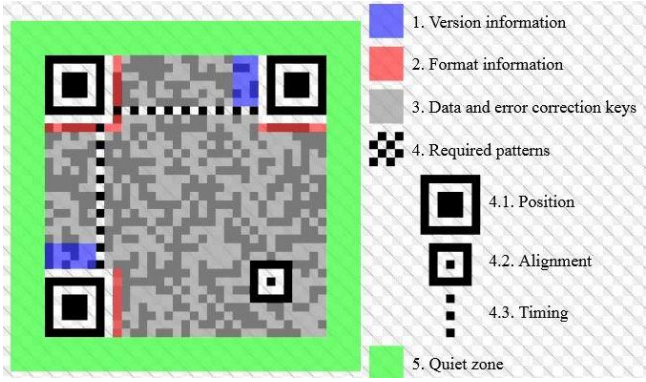

Fig 2.1 Functioning of a Quick Response code

2.1.1 Advantages

The main advantage of a QR code is its versatility. QR codes can be used for anything and everything. They are also beneficial for both customers and businesses. For example, a business saves money and advertising costs by distributing a QR code to their website or URL. A customer can scan this QR code and this allows them to store the information for future reference. What's also greater about QR codes is that they bridge different forms of marketing streams together. For example ecommerce and mobile commerce are both used for QR codes. QR codes acts as the link and it also exposes customers to other forms of advertising the business or service of the QR code has done. This maximizes exposure and can potentially generate revenue.

This novel technology is now used in many new areas and according to latest measurements has been adopted by millions of smartphone users. This explosive growth in the last years indicates that that QR codes are not just a momentary fashion but a very powerful and versatile tool for the future.

2.3 BIOMETRIC VERIFICATION FOR ATM

Biometric[1] verification is a technique by which a person can be uniquely identified by evaluating one or more distinctive biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. The oldest form of biometric verification is fingerprinting. Historians have found samples of thumbprints getting used as a method of distinctive identification on clay seals in ancient China. Biometric verification has advanced significantly with the arrival of computerized knowledge bases and also the digitization of analog data, granting nearly instant personal identification. Biometric verification is used in position of the username-password authentication theme, because it is almost not possible to duplicate a person's biological signatures, in contrast to usernames, which might be guessed or taken.

The process starts with the retrieval of a biometric sample via a scan of the attribute chosen for identification, such as fingerprints, hand geometry, iris patterns, facial geometry or voice patterns. The sample is then compared to a database of known authorized personnel, and when that sample comes out positive, the user is asked to authenticate using the unique identification code associated with the sample. When both parameters match, access is granted. This is standard for what is called a two-step verification process, where access requires two parameters.

The sample is then compared to a info of identified personnel, and once that sample comes out positive, the user is asked to evidence the distinctive identification code related to the sample. Once each parameters match, access is granted. This can be customary for what's known as a two-step verification process, wherever access needs two parameters.

3. THREATS TO ATM NETWORK

There many threats related to ATM security[2,3,4] as the popularity and usage is increasing day by day. New ATM's are being installed in different locations daily and the users are also increasing. Some of the threats are discussed below.

3.1 SHOULDER SURFING

Shoulder surfing[2,3] is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

3.2 SPOOFING

Spoofing attack means that an attacker tries to impersonate another user to the third part therefore can get access to resources belonging to the victim to take advantages or just destroy them. Spoofing might need special tools to manipulate the protocol data unit. And sometimes it might require the attacker has special access permission, say, must be the super user in UNIX environment. However, since a network will be connected to many untrusted networks via the Internet, it's impossible to prevent a hacker from getting this access permission or even trace the people with this particular access permission. ATM is being implemented in public domain. Therefore, it is subject to this kind of attack also.

3.3 SKIMMING

ATM card skimming[6] is the most prevalent and well known attack against ATMs. Card skimmers are devices used by perpetrators to capture cardholder data from the magnetic stripe on the back of an ATM card. These sophisticated devices smaller than a deck of cards and resembling a hand-held credit card scanner are often installed inside or over top of an ATM's factory-installed card reader. When the consumer inserts his card into the card reader, the skimmer captures the card information before it passes into the ATMs card reader to initiate the transaction. The transaction continues in a normal fashion. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used the ATM. An inexpensive, commercially available skimmer can capture and retain account numbers and PINs for more than 200 ATM cards. Typically, criminals design skimming devices to be undetectable by consumers.

3.4 CARD TRAPPING/FISHING

Card trapping and fishing[10] attempt to steal consumers' cards as they are inserted into the card reader during a transaction. The purpose of this type of attack is to steal the card and use it at a later time to make fraudulent withdrawals from the consumers' compromised accounts. Card trapping is conducted by placing a device over or inside the card reader slot to capture the consumer's card. These can be devices such as plates over the card reader, thin metallic strips covered in a plastic transparent film, wires, probes and hooks. These devices are designed to prevent the card from being returned to the consumer at the end of a transaction. These attacks are sometimes combined with other fraudulent devices such as cameras or keypad overlays to capture the consumer's PIN as it is being entered on the keypad during a transaction.

3.5 REPLY ATTACKS

Replay attacks are the network attacks in which an attacker spies the conversation between the sender and receiver and takes the authenticated information e.g. sharing key and then contact to the receiver with that key. In Replay attack the attacker gives the proof of his identity and authenticity.

4 SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Present ATM banking system are working with ATM cards with PIN/ Biometric systems, in feature we have chance to perform ATM transactions without having any ATM cards by help of One Time Password (OTP) and PIN combination to remove security concern to authenticate user.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe. The magnetic strip on the ATM consists of the account number and other user details. This ATM card is used for identifying users. Along with the card a four digit pin is provided from the bank. The user inserts the ATM card in the machine and enters the pin thus authentication will be performed.

There are various threats for this type of authentication. We propose a system which overcomes most of these security problems.

4.2 PROPOSED SYSTEM

The main objective of this system is to develop a secure ATM in future. In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication which has been a most prone threat for ATM's.

In this system, ATM custodian enable authentication for ATM using personal. ATM custodian allows a user to scan a QR code from the screen of a machine and connects to the server to obtain ATM ID. The QR code scanning is done using users personal mobile. 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.

In our system ATM will be having a unique id. This unique id will be displayed as a QR code on the ATM machine. There will be a touch button on the ATM screen. When the user touches this button a request will be send to the server requesting the atm's id. Using the ATM id a QR code will be generated on the ATM screen. Using a smartphone user can scan the QR code. A mobile application is used in our system. In order to login to the application user has to enter the username and password. If the username and password is valid, an 8 digit pin will be send to the ATM in which only four digits will be displayed on the atm screen. The remaining four digits will be sending to the mobile application. The user has to enter this 4 digit number on the atm screen. Thus the authentication will be complete, The remaining process has to be done in order to perform the transaction.

Because of increasing threats to networked computer systems, there is great need for high security innovations. Text based password is easy to hacking OTP [5] can be get easily by hacking email account. In image based authentication, selecting image and taking its click points can be easily understood to hacker by shoulder surfing attack in our authentication system we have integrated alphanumeric password, OTP generation via e-mail or mobile, graphical authentication. New user should have register his/her id p/w mobile no. e-mail id ,key for image authentication and other personal details such as name ,address .In our system graphical authentication we have used Pair-based Authentication scheme to select click points on image matrix. No system has been developed so far which uses such technique in image based authentication.

The ATM custodian for ATM threat model

includes the definition of the assets and the attackers' capabilities in the process of ATM authentication using PIN codes.

1) Assets: The asset for ATM point-of-service authentication is primarily the user's PIN code. The PIN is a secret information known only to the user of the card and is used by the user to authenticate at the ATM along with the credit and/or debit card.

2) Attacker's Capability: In the scenario where a user has presented a credit or debit card at an ATM and is about to present the PIN code for authentication

ADVANTAGES

It is more reliable and time saving system when compared to the manual system. It is more efficient and faster to use. ATM card is not used so no need to take care of the card and no need to memorize the PIN. It is secure against shoulder attacks, relay, replay attacks, skimming, partial observation and cloning.

5. CONCLUSION

This paper recognizes a model for the modification of existing ATM systems by QR code [15] system and mobile application. The Proposed idea will confuse the Password guessing and password thieving in future from unauthorized person. Therefore this kind of additional technique preventing pin theft in future. ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing or observation attacks. Credit/Debit cards are also not resilient to relay and other skimming and cloning attacks. In this paper, we propose the ATM custodian for ATM, a unique QR code-based authentication service for ATMs using personal mobile. We have focused the security design for this system is based on visual privacy of users for QR code scanning and address the security vulnerabilities in PIN-based authentication. The protocol does not require any additional hardware support for currently operating ATM terminals and employs offloaded computation from the mobile device for verifying the trans-action requests. A proof-of-concept prototype implementation was used to perform experimental analysis and a usability study. Results show that users are easily adapted to the process of QR-based authentication. Our future work involves applying this system service to newer application fields, such as, PIN-enabled doors and visual authentication mechanisms.

6. 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] 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.

[4] 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.

[5] Mohsin Karovaliya,Saifali Karedia,Sharad Oza, Dr.D.R.Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features", International Conference on Advanced Computing Technologies and Applications(ICATA 2015).

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

[7] G. Stanley, "Card-less financial transaction," Apr. 21 2014, US Patent App. 14/257,588.

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

[9] S.T. Bhosale and Dr. B.S.Sawant "security in e-banking via card less biometric atms", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012

[10] 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.

[11] A Survey on the Security of an ATM Transaction Joyce Soares1, Dr. A. N. Gaikwad2 1, 2Zeal College of Engineering and Research, Sr.No 39,Off Mumbai-Bangalore Express Highway, Narhe, Pune, India

[12] Diebold, "ATM Fraud and Security White Paper", 2003.

[13] Michael S. Scott, "Robbery at Automated Teller Machines", Guide No.8, 2001

[14] 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.

[15] Wikipedia, Retrieved May, 22, 2014, from http://en.wikipedia.org/wiki/QR_code

[16] ISO/IEC 18004:2006 Information technology -- Automatic identification and data capture techniques.