Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey Paper on Wireless Authentication in ATM System Using GSM Technology

Kranti Narayan Gule*, **Rohit N. Devikar, Sudeep K. Hase**

I.T.& Pune University, Pune, Maharashtra,

India

Abstract— Public terminals for service provision provide high convenience to users because of their constant availability and public location. Due to that they can easily fall victim to manipulation. With the increase of automated teller machine (ATM) frauds, new authentication mechanisms are developed to overcome security problems of personal identification numbers (PIN). All those mechanisms are usually judged on the basis of speed, security, and memorability in comparison with traditional PIN entry mechanism. It remains unclear, what appropriate values for PIN-based ATM authentication. Here doing the survey of real-world ATM use, in order to provide both a better understanding of PIN-based ATM authentication, and on how alternative authentication methods compared and evaluated. From these findings, draw the several implications for the design of alternative ATM authentication systems, such as resilience to distraction and social security.

Keywords— Security, PIN Entry, Mobile devices, ATMs, Authentication.

I. INTRODUCTION

In our day today life Public terminals provide high level of convenience that many people would not like to miss. 24 hours, 7 days in a week services can be accessed easily. No longer bound to opening or working times for customer. There are various terminals include for like train ticket vending machines, check-in terminals at airports, cash machines (ATMs). The main part of these services require customers to authenticate to the given system[2].

In year 2009, a spectacular case of automated teller machine (ATM) fraud took place in Russia and Ukraine. The particular of this case was the course of action taken by the defrauders to attack ATMs at large scale they employed a 'software integrity violation'. Although there are some known software manipulations of ATMs targeted at stealing money, this is the first case that was published in which malware was set up on ATMs to grab user data. The main question was 'who' could carry out such a sophisticated so-called 'offline attack' where direct access to the system computer that works within the ATM is needed. It is assumed that the attack was carried out by an insider who worked at the bank and who had legitimate access to the ATM[1].

Based on semi-structured interviews, helped to identify basic factors that influence the decision to use an ATM, like privacy, social density, and time pressure. Nevertheless, the actual use of ATMs was not explored. Consequently, we decided to perform a number of field observations involving ATM use, in order to explore how people actually interacted with ATMs. As it has been previously shown in the domain of public display interactions, studies have the potential to uncover important facts and practices that otherwise cannot be asserted. The main focus of our observations was on the ATM authentication process, i.e., how people enter their PIN, whether and how people protect their PIN entry from skimming attacks, and what contextual factors affect security and secure behavior. As online banking or ATM machines, is done in a very secure manner. This paper presents the survey of the observations and the interviews, and derives a number of implications for the design and the evaluation of authentication mechanisms for ATMs. For example, our observations indicate that contextual factors have a high influence on security and usability of PIN authentication. A large number of observed interactions (11%) featured one or more distractions during ATM use like phone calls, discussion with friends, or handling shopping bags. Maybe not surprisingly, also found that a majority of users (65%) did not take any precautions against PIN skimming attacks such as shielding PIN entry. During last two decades researchers have applied information and communication technology concepts to solve banking problems. E-Commerce and M-Commerce concepts have been introduced as alternatives to traditional methods. Examples of such solutions are ATM services, credit card/debit card services[4].

II. LITERATURE SURVEY

An attacker is able to carry out a skimming attack against an ATM.

The observations were performed in various European cities, Munich (Germany) and Delft (the Netherlands). Chose ATMs that were available 24 hours a day, seven days a week. This allowed for unobtrusively observing actual ATM interactions.

Fig. 1. A typical Automated Teller Machine (ATM)

The data for the primary observation was collected over a period of nearly two months. Each ATM was at least visited four times, with at least one observation session on a Sunday and at least one session during rush hour means mid-mornings, noon, or early evenings. This was to ensure that the data collected was as broad as possible.

That only include off peak times, which could have biased the results. Rush hours and off peak times were identified in pre observations. Depending on the location e.g. close to a supermarket these times differed not only between cities, but also between locations within the cities. For instance, the rush hour close to a supermarket was between 5pm to 7pm while the rush hour at an ATM in a pedestrian area with shops and restaurants was during lunch time around 1pm[4].

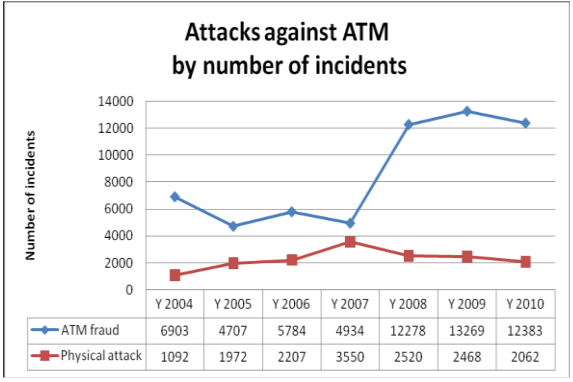
A. Various Attacks

1. Attacker I

Your We can assume that an attack carried out by such an attacker also involves spying out the users PIN, for example, video surveillance, shoulder surfing or fake PIN pads come into question. This is basically the type of attacker that causes the most substantial harm for banks nowadays.

2. Attacker II

A more skilled attacker is able, besides carrying out a skimming attack, to compromise a users mobile phone as well. The goal for the attacker is to spy out the user PIN, which is now entered at his mobile phone and not at the ATM terminal which can be spied out much easier. An attacker may drive a user into installing a fake ATM application on his mobile phone. This could be done by sending a text message with a link to the download page that houses the fake application to the user. Such an attacker is limited in the scalability of an attack, although. Spying out the PIN entry directly at an ATM affects all the users. However, spying out the PIN entry on a large scale of users mobile phones means for an attacker to compromise all of those devices separately.



	Y 2004	Y 2005	Y 2006	Y 2007	Y 2008	Y 2009	Y 2010
ATM fraud	6903	4707	5784	4934	12278	13269	12383
Physical attack	1092	1972	2207	3550	2520	2468	2062

Fig. 2. ATM related attacks.

Security-enhanced authentication mechanisms can be roughly divided into two categories. The first includes systems that, like Mobile PIN, try to increase the security of traditional authentication approaches like password and PIN. An example is the spy-resistant keyboard Tan et al.(2005). Using the Spy-Resistant Keyboard rather than a standard soft keyboard resulted in a significant increase in their ability to protect their passwords from watchful observer. This keyboard randomizes the spatial location of all characters as each password character is entered. The Spy-Resistant Keyboard is composed of 42 Character Tiles, two Interact or Tiles, a feedback textbox, a backspace button, and an enter button . Each Character Tile is randomly assigned a lowercase letter, an uppercase letter, and either a number or a symbol, all positioned vertically on top of each other. Lowercase letters are always on the top row of each tile and have a red background, uppercase letters are placed in the middle and have a green background, and numbers and symbols are positioned on the bottom and have a blue background. Since there are exactly 42 numbers and symbols combined, but only 26 letters, some letters are repeated. It uses a two-step character selection that is hard for an attacker to follow, but also increases the time and the complexity to input a password. Furthermore, it is not resilient against observation attacks based on camera recordings.

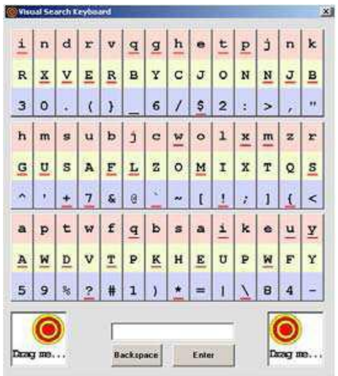

Visual Search Keyboard
i n d r v q g h e t p j n k
R X V E R B Y C J O N N J B
3 0 . ( ) _ 6 / $ 2 : > , "
h m s u b j c w o l x m z r
G U S A F L Z O M I X T Q S
^ ' + 7 & @ ` ~ [! ;] { <
a p t w f q b s a i k e u y
A W D V T P K H E U P W F Y
5 9 % ? # 1) * = | \ 8 4 -
Drag me...
Backspace
Enter
Drag me...

Fig. 3. The mapping phase, the user first finds the character they would like to type and notes its location.

A similar approach of adding overhead to the input has been taken by Roth et al. (2004). Towards a PIN entry method that is robust against shoulder surfing, proposed two variants of an interactive challenge-response protocol to which refer as cognitive trapdoor games. The essential feature of such a game is that it is easily won if the PIN is known, and hard to win otherwise. The cognitive capabilities of a human are generally not sufficient to derive the genuine PIN through observation of the entire games input and output. As a defense against automatic recording like by miniature cameras, proposed another variant which maintains a certain level of uncertainty about the genuine PIN even if automatic recording devices are deployed. Due to its probabilistic nature, this variant as a probabilistic cognitive trapdoor game. In order to assess the security and usability of our PIN entry methods, conducted two user studies. The results of these studies support our hypothesis that our methods provide superior resilience against shoulder surfing which is of significant value when entering PINs in a public environment.

Eye-tracking technology for PIN and password entry has been evaluated by Kumar et al. (2007). Eye tracking technology has come a long way since its origins in the early. State of the art eye trackers offer no encumbering, remote video-based eye tracking with an accuracy of 1 of visual angle. Eye trackers are a specialized application of computer vision. A camera is used to monitor the users eyes. One or more infrared light sources illuminate the users face and produce a glint a reflection of the light source on the cornea. As the user looks in different directions the pupil moves but the location of the glint on the cornea remains fixed. The relative motion and position of the center of the pupil and the glint is used to estimate the gaze vector, which is then mapped to coordinates on the screen plane. Since muscle memory from typing does not translate to on screen keyboard layouts, the users visual memory for the spatial location of the keys becomes a more dominant factor in the design of on-screen keyboards. The trade off here is between usability and security it is possible to design random keyboard layouts that change after every login attempt. These would require considerably more visual search by the user when entering the passwords and therefore be a detriment to the user experience, but would provide increased security.

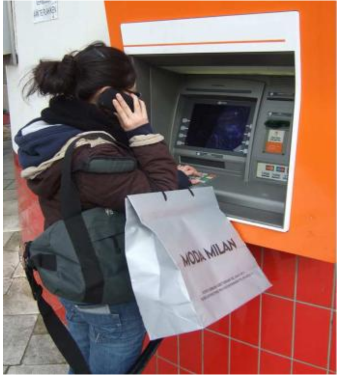


Fig. 4. A staged example of a user that cannot hide the PIN entry due to physical hindrance.

Interesting research has also been performed on completely different authentication approaches. The best known being biometric authentication as evaluated for ATM usage by Coventry et al. (2003). While biometry performs rather well on usability and speed, it is hard to deploy and more expensive than other approaches. The main advantage of biometry is that users do not have to recall any secret information like a PIN. It is clear from our experiences with the on going development of the iris verification prototypes, that there exists a gulf between those general pre-usage attitudes, and subjective opinion following iris-ATM use. Our ability to predict consumer acceptance of new technologies and services requires that we acknowledge some of the inherent limitations of focus groups and surveys.

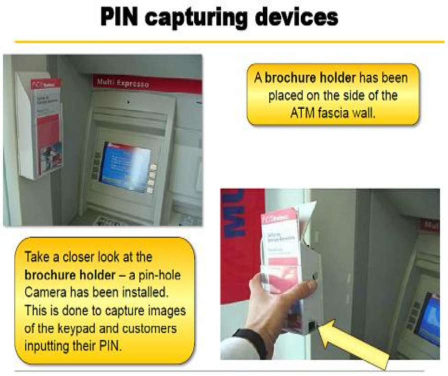
The earlier engage consumers with prototypes of the intended system, the better. Some of the main issues emerging from our research with the iris verification technology are specific to this type of non contact approach, whilst others relate to more general. Every biometric device has its own set of usability issues and more work is required to ensure to understand the nature of permanent and transient exclusions to any biometric technology as well as how to maximize the usability of a biometric to enable it to be utilised within public technology. Biometric technologies do not resolve the usability, security trade off. Biometric devices have to establish fault tolerance limits. Setting these narrowly maximises security but means the ease of use could decline. Further research is required to understand the relationship between security and issues such as false rejects and failure to acquire.

Tactile feedback provided by the terminal is used to share secret information with the users and increase the systems security by Deyle et al. (2006). The tactile PIN entry mechanism requires palpable actuators that can be controlled by a computer process. In our prototype, we use solenoids with pins that can be raised or lowered by applying an electric current to the embedded electromagnet. Overall, eight solenoids are required, four per hand. Users position their index, middle, ring and pinky fingers the indicated states in each round. The overall procedure is repeated for the next finger and so forth until all fingers are input. With only the button presses being perceivable, a shoulder surfer gains no information about the entered PIN. Unless the positions of the solenoid pins can be measured as well, the device offers perfect secrecy even if the entire process is recorded by a camera. A tactile PIN entry device that uses computer-controlled solenoids as palpable actuators. Users enter their PIN as a sequence of fingers by responding to raised and lowered solenoid pins. Responses consist of button clicks with the thumbs, which indicate whether the pin under the current PIN finger is raised or lowered. Based on our experiences with the first prototype built an improved PCB for the second generation controller. In a commercial-grade implementation, the mechanism would offer perfect security against shoulder surfers even if the entry procedure is recorded with a camera. Moreover, the mechanism can be operated by blind persons. If found usable, the mechanism could improve the accessibility of ATMs for handicapped people.

III. RELATED WORK

A. Shoulder Surfing Attack

When user reach to ATM center for doing transaction swapping of card is essential. If user swap card & giving PIN no.via the fix PIN pad, someone do direct observation towards the user. Or looking over one’s shoulder. Observing what number that person enters onto the keyboard of device. With the help of using miniature video cameras easily obtained the number which is discretely installed close to the PIN Pad of device. Ergonomic design means systematic design of study of the ATM to prevent shoulder surfing attack is used. On the fascia of the ATM Fix mirror is placed. Cover the area of pin entry with the help of body. A secure and nice environment given to the customers by providing illuminated signage panels and surrounding street lights. Also keep or place ATM in high-traffic area of city[3]. Strategically attaching or positioning cameras and other imaging devices to ATMs to fraudulently capture PIN numbers. Once captured, the electronic data is put onto a fraudulent card and the captured PIN is used to withdraw money from accounts. PIN capturing is a world-wide problem.



PIN capturing devices

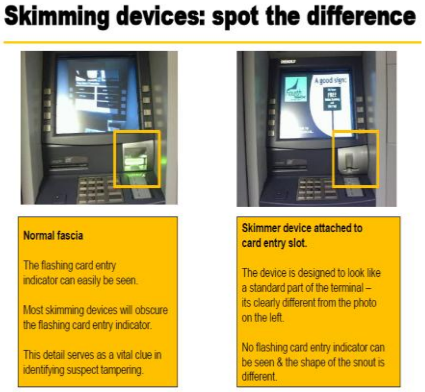
A brochure holder has been placed on the side of the ATM fascia wall.

Take a closer look at the brochure holder – a pin-hole Camera has been installed. This is done to capture images of the keypad and customers inputting their PIN.

Fig. 5. PIN capturing devices.

B. ATM Fraud Techniques with Skimming Devices

Illegally obtaining card track data the frequently used method is with skimming devices. By the criminals to capture the data which is stored in magnetic strip of card the idea is used. Firstly, read and then decipher information on the magnetic stripes. Through the small card readers which is placed on top of the actual card reader input slot work is done. Deck of cards are larger than skimming devices. With the help of that easily capture the account numbers, verification codes ,balances[1].



Skimming devices: spot the difference

Normal fascia

The flashing card entry indicator can easily be seen.

Most skimming devices will obscure the flashing card entry indicator.

This detail serves as a vital clue in identifying suspect tampering.

Skimmer device attached to card entry slot.

The device is designed to look like a standard part of the terminal – its clearly different from the photo on the left.

No flashing card entry indicator can be seen & the shape of the snout is different.

Fig. 6. Skimming Devices.

Skimming devices are normally attached to ATMs during quiet periods, e.g. early morning or late evening. Length of time skimming devices are attached can vary, but normally no longer than 24 hours. Successful skimming requires both a card skimmer (card reader) & camera (PIN capturing device) to be fitted to the ATM in order to steal card data. Criminals may loiter nearby to observe customers & remove equipment after machine use. Downloaded information can be transmitted wirelessly to other devices.

C. Fake PIN Pad Overlay

Devices used by criminals to capture the PIN there is use of fake PIN pad which is keep over the original keypad. Firstly overlay captures the PIN data and then stores information into its own memory. After that fake PIN pad removed. And recorded PINs are get downloaded. Those PINs are identical in the appearance and size of the original keypad. For that aware people & educate. Familiarize yourself with the look & feel of the ATM fascia on machines. While pay attention to the screen when enter PIN[5].

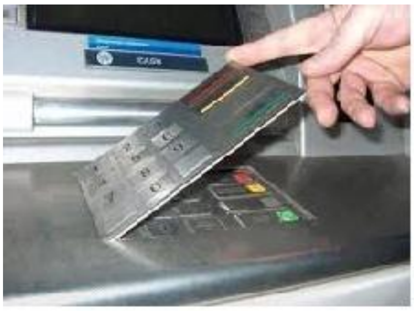


Fig. 7. Fake PIN pad.

D. Problems in the Existing System

Securing PIN entry against cameras and shoulder surfers typically requires a second hand to shield the keypad. We observed several instances where users simply did not have a free hand to spare to protect their input. For instance, they were holding shopping bags that they did not want to put down. Other users were holding their mobile phone, having calls or even holding children in their arms. Four out of the six ATMs in study displayed users at such ATMs were not more likely to protect their PIN entry. The remaining users that applied security measures did not hide the PIN entry, but instead checked their surrounding and verified that no one was standing nearby[10].

IV. CONCLUSIONS

In this survey paper, we have done survey of various Automated Teller Machines (ATMs) authentication scheme attacks. Towards a PIN entry method that is robust against shoulder surfing. As a defense against automatic recording e.g., by miniature cameras, another variant which maintains a certain level of uncertainty about the genuine PIN even if automatic recording devices are deployed. In order to assess the security and usability of our PIN entry methods, conducted user studies. These studies provide superior resilience against ATM attacks.

The large number of frauds on public terminal shows that there is need for new authentication methods. It only requires minor software updates at the terminal and possibly additional modules for wireless communication.

ACKNOWLEDGMENT

I take this opportunity to express my intense gratitude and deep regards to my Guide Prof. R. N. Devikar for their exemplary guidance, monitoring and constant encouragement throughtout this paper.

I also express a deep sense of gratitude to Prof. S. E. Pawar, Head of Information Technology Engineering Department for her valuable guidance and encouragement.

I would like to express deepest appreciation towards Prof. Dr. G.J.Vikhe Patil., Principal of Amrutvahini College of Engineering, Sangamner, and Prof. B.S.Borkar (ME Coordinator) who's valuable guidance supported me in completing this paper.

REFERENCES

[1] Ronald Petrlic, Christoph Sorge, "Establishing user trust in automated teller machine integrity," Computer Science Department, University of Paderborn, Paderborn, Germany, Vol. 8, Iss. 2, 2014, pp.132–139.

[2] Bernhard Frauendienst, Alexander De Luca, Sbastian Boring, Heinrich Hussmann, "My Phone is my Keypad: Privacy-Enhanced PIN-Entry on Public Terminals," Media Informatics Group, University of Munich Amalienstr, Munich, Germany, 2009, pp. 854-858.

[3] Richter, K., Roth, V., Freidinger, R., "A PIN entry method resilient against shoulder surfing," In: CCS '04: Proc. 11th ACM Conf. on Computer and Communications Security, New York, NY, USA, ACM, 2004, pp. 236-245.

[4] Alexander De Luca, Marc Langheinrich, Heinrich Hussmann, "Towards Understanding ATM Security: A Field Study of Real World ATM Use," Faculty of Informatics, University of Lugano, Via G. Buffi, Lugano, Switzerland, (2010).

[5] ATM Marketplace, "ATMs reprogrammed to print out ATM, debit details on receipts," (2009).

[6] ATM Marketplace, "Reprogrammed ATM helps minn. man get away," (2009).

[7] Berger, S., Cáceres, R., Goldman, K.A., Perez, R., Sailer, R., van Doorn,“vTPM: virtualizing the trusted platform module,” In:USENIX-SS’06: Proc. 15th Conf. on USENIX Security Symp.Berkeley, CA, USA, USENIX Association, 2006.

[8] Stumpf, F., Benz, M., Hermanowski, M., Eckert, C., “An approach to a trust-worthy system architecture using virtualization,” vol. 4610 of lecture notes in computer science, Springer Berlin Heidelberg, 2007, pp.191-202.

[9] Berger, S., Cáceres, R., Pendarakis, D., et al, “TVDc: managing security in the trusted virtual datacenter,” SIGOPS Oper. Syst. Rev., 2008, pp.40-47.

[10] De Luca, A., Langheinrich, M., Hussmann, H., “Towards understanding ATM security: a field study of real world ATM use,” In: Proc. Sixth Symp. on Usable Privacy and Security (SOUPS ’10), New York, NY, USA, 2010, pp.16:1-16:10.

[11] De Angeli, A., Coventry, L., Johnson, G., Renaud, K., “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems,” Int. J. Hum.-Comput.Stud., 2009, pp.128-152.

[12] GRGBanking Equipment (HK) Co.,Ltd, “ Best Practice for ATM Security,” 2011.

[13] Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S.,Wolf, C., “Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices,” In: 2011 IEEE Symp. on Security and Privacy (SP), 2011, pp .96-111.

[14] Tan, D., Keyani, P., Czerwinski, M., “Spy-resistant keyboard: more secure password entry on public touch screen displays”, Microsoft Research One Microsoft Way, Redmond, Washington 98052, USA.

[15] Deyle, T., Roth, V., “Accessible authentication via tactile pin entry”, CG Topics, Issue 3, March (2006).

[16] Kumar, M., Garfinkel, T., Boneh, D., Winograd, T., “Reducing shoulder-surfing byusing gaze-based password entry”, In Proc SOUPS(2007).

[17] Coventry, L., De Angeli, A., Johnson, G., “Usability and biometric verification at the ATM interface”, In Proc Chi (2003).

[18] Roth, V., Richter, K., Freidinger, R., “A pin-entry method resilient against shoulder surfing”, In Proc CCS (2004).

[19] Sasamoto, H., Christin, N., Hayashi, E., “Undercover:authentication usable in front of prying eyes”, In Proc CHI (2008).

[20] Rogers, J., “Please enter your 4-digit PIN”, Financial Services Technology, U.S, Edition, Issue 4, March (2007).

[21] Andrea Bianchi, “Authentication on Public Terminals with Private Devices”, Korea Advanced Institute of Science and Technology Daejeon, Korea, Jan (2011).

[22] Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr.D.R.Kalbanded, “ Enhanced security for ATM machine with OTP and Facial recognition features”, International Conference on Advanced Computing Technologies and Applications (2015).

[23] Rupinder Saini, Narinder Rana,Rayat, “Comparison of various biometric methods”, Institute of Engineering and IT, International Journal of Advances in Science and Technology (IJAST),Vol 2,Issue I, March (2014).

[24] Aru, Okereke Eze, Ihekweaba Gozie, “Facial Verification Technology for Use In Atm Transactions”.