SHODH SAMAGAM

Online ISSN : 2581-6918

ATM CARD DATA SECURITY BREACH BY PERISCOPE DEVICE : A REVIEW

MOHD SHADAB, Research Scholar,
Department of Information Technology,
Dr. C.V. Raman University, Bilaspur, Chhattisgarh, India
DR. RAGINI SHUKLA, Research Supervisor,
Associate Professor, Department of Information Technology,
Dr. C.V. Raman University, Bilaspur, Chhattisgarh, India

ORIGINAL ARTICLE

Corresponding Autor's :
MOHD SHADAB, Research Scholar,
DR. RAGINI SHUKLA,
Research Supervisor, Associate Professor,
Department of Information Technology,
Dr. C.V. Raman University, Bilaspur,
Chhattisgarh, India

shodhsamagam1@gmail.com

Received on : 26/03/2019
Revised on : -----
Accepted on : 29/03/2019
Plagiarism : 14% on 28/03/2019

Abstract :-

Magnetic stripe ATM cards are continuously applied by banking as well as other financial industries to offer both advantage and security. These models of ATM cards are usually keeping faith on recognition and individuals authentication. (Guo, h. and Jin, b. 2010).

Frauds related to Automated Teller Machines (ATMs) are rising rapidly in both volume and sophistication manner so it is important to identifying several skimming frauds and data security threats belonging to the use of ATM card. (Adepoju.et al., 1970, Solomon, Adelowo.et al., 1970 and EnagiAlhassan, Mohammed.et al., 1970).

According to the U.S secret service agency "There is an alert for banks and ATM vendors for the new ATM skimming technique so-called periscope skimming." Periscope skimming uses a device which is made up of skimming probe and this device is use by the criminals to connect the internal circuit board of ATM's for the purpose of information collection from ATM cards.

Keywords :- ATM, Fraud, Information, lawbreakers, Magnetic stripe, Periscope device, Security, Skimming.

Introduction :-

Expeditious growth in the field of technology has improve the working approach of banking sectors like use of automated teller machine (ATM) for rapid withdrawal of cash money. On the other hand uses of ATM Withdrawal techniques shorten the workload of bank employee. ATMs provides several activities such as cash withdrawal, transfer of money, personal identification number (PIN) change and many other functions/ transactions. An ATM allows fast and quick access to their users for financial transactions so the use of ATMs is increasing day by day. The ATM's transaction is done through plastic card which contains magnetic stripe and their personal identification number (PIN). A magnetic stripe consists of customers unique account information. (Das, s.s. and Debbarma, j. 2011) (Okechukwu onyesolu, Moses. and Majesty Ezeani, Ignatius. 2012).

In the present scenario, ATMs card are becoming the major payment source for self and online purchases. Because of popularity of ATMs cards, the industry of credit and debit cards is constantly rising. As the uses of ATMs card are increasing, Frauds on ATMs card are also increasing continuously day by day. (Sullivan, R.J. 2010).

These ATM frauds could become as a security risk in the form of card cloning or PIN release. There are various types of attacks which are continuously noticed in the past decades including as: (Dastur, navroze. 2017).

I. Card skimming.

II. Cash trapping.

III. Keypad jamming.

IV. Jackpotting attacks.

V. Card swapping.

VI. Periscope skimming.

Among these skimming on ATM cards is the most recurrent form of ATM attack and currently represents 97 percent of all losses by using these types of card as shown in Fig. 1 (Statistics, fraud.).

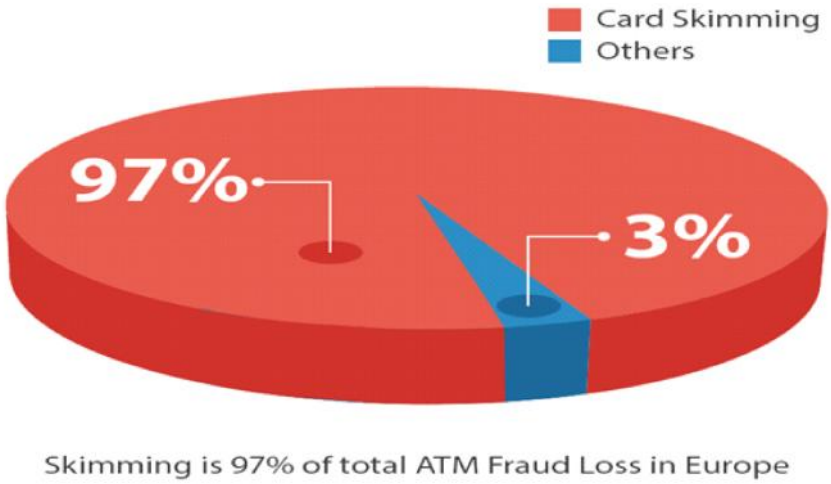

Fig. 1. Pie chart of card skimming loss in Europe.

ATM Card Skimming :-

ATM card skimming is a technique used by lawbreakers to capture information from the magnetic stripe on the back of the plastic card. (Commonwealth Bank of Australia. November 2009).

Devices used by lawbreakers are compact in comparison to the area of the deck where cards are inserted. These devices are frequently fastened in near accessibility to, or over the peak of the ATM's industry-installed card reader. (Commonwealth Bank of Australia. November 2009).

Lawbreakers apply the skimming devices on the light diffuser area, Card reader entry slot, ATM keyboard area, ATM side fascia and speaker area. (Commonwealth Bank of Australia. November 2009).

Fig.2. ATM skimming devices & ATM's different regions.

Lawbreakers fix the cameras and other image capturing devices to ATMs for illegal capturing of personal identification number (PIN). (Commonwealth Bank of Australia. November 2009).

Once captured, the electronic information is apply onto a clone/duplicate plastic ATM card and illegally captured PIN is apply to withdraw cash from accounts. (Commonwealth Bank of Australia. November 2009).

ATM skimming is a world-wide issue. (Commonwealth Bank of Australia. November 2009).

Fig.3. Year wise skimming incidents in Europe.

According to the European ATM Security Team (EAST), the average loss of cash money per ATM card skimming attack in Europe is more than 48.000 EUR. In 2010, it was 25.500 EUR and frequently rising every year. Whereas the Bank Info Security said that the average loss in US is approximately 50.000 USD. This was 30.000 USD in 2010. It appears that, ATM card skimming is harming banks and their customers more and more every year as shown in Fig.3. (Statistics, fraud.)

Review of Literature :-

Technique applied by fraudsters to copy personal data from the magnetic strip on an ATM card is known as ATM skimming.

Ultimately the world's most sophisticated ATM skimming technique called periscope skimming is started to seen in America. According to the Krebs, this is the first time that the periscope skimming is spotted by the police in the United State. The modern periscope skimming is capable of storing up to 32 thousand payment card numbers, only one time installed on automated teller machine (ATM), it has power capability up to 14 days. (Secret Service, U.S. 2016).

The police have already found two cases of periscope skimming. First one is in Greenwich on august 19 of year 2016 and another is spotted in Pennsylvania on September 3 of year 2016. On examination of both cases by police is find out that the skimmers had access to the insides of the cash machine (referred as the top portion of the machine) by using a key and they attached two devices with the help of wiring. (Secret Service, U.S. 2016).

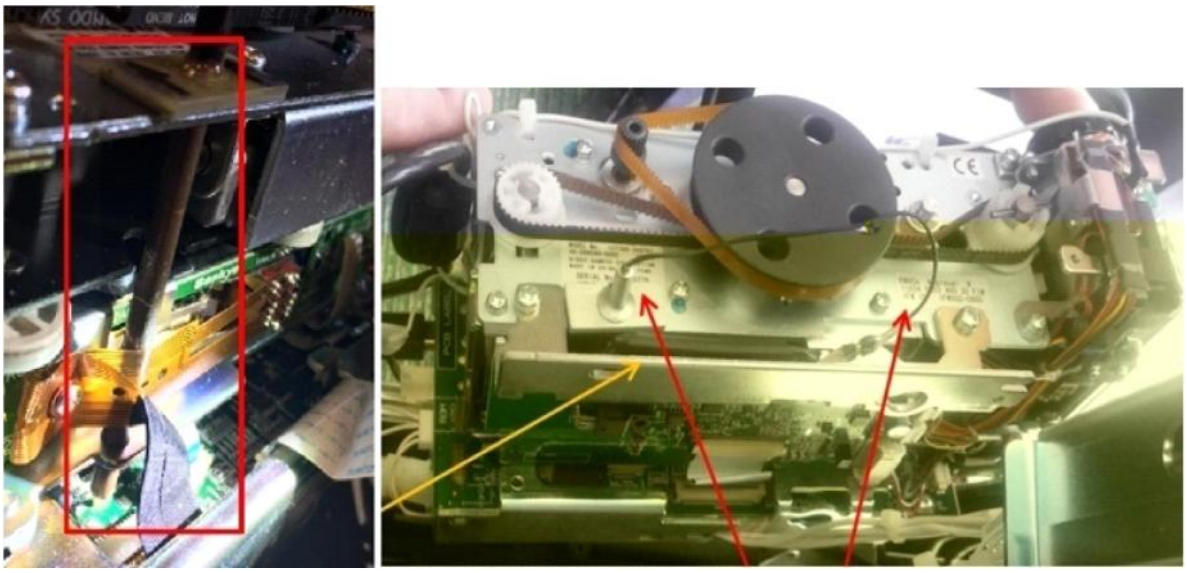

Fig.4. The wires prognathous from the periscope device.

BRIAN KREBS, a famous cyber security expert released the photos of the periscope skimming, the photos exhibit the wires prognathous from the periscope as shown in Fig.4. (Secret Service, U.S. 2016).

The first device is the periscope skimming probe that is attached to the hole on the frame of the card reader and the probe connects the pad to the circuit board where as the second device is “skimming monitoring device”, which is directly appended to the skimming probe and consisting of battery source as well as data storage unit as shown in Fig.5. (Secret Service, U.S. 2016).

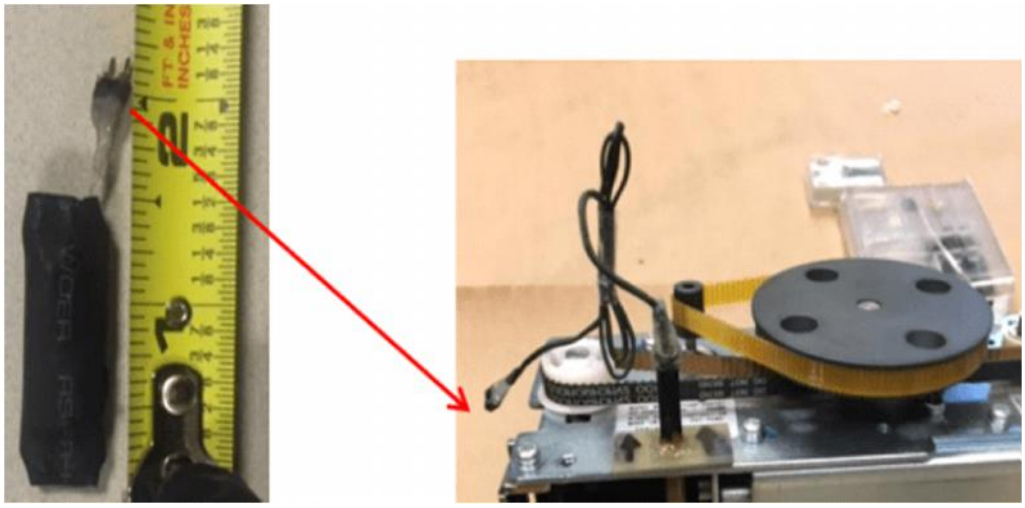

Fig.5. Periscope skimming probe & circuit board is attached directly onto the pad

The circuit board is attached directly onto the pad that fetch ATM card’s confidential information stored on the magnetic stripe on the back of ATM cards by the help of skimming probe.

The U.S secret service said that the only noticeable portion of this skimming device once the top part of automated teller machine (ATM) is opened will be the wire goes from periscope probe that leads to the other part of this skimmer called skimming monitoring device.

Research Gap :-

There is a lot of need to aware ATM cards users as well as our banks about this new type of ATM skimming so called skimming by periscope device. we know all other types of skimming technique and our banks also aware their customers time to time but this periscope device skimming technique is very new and the literature on it is also very less so it is important in term of data security our banks need to understand this skimming technique for the purpose of increasing awareness of the ATM card users.

As the Krebs says that the frauds of these types of skimming will not decrease as more banks choosing this chip-based payment cards that's why our banks need to enhance their data security as well as public awareness.

Periscope skimming are very sophisticated type of ATM card data skimming because it is completely within the Automated teller machine, so it is not possible to identify. (Schneier on security. September 2016).

Objective :-

The objectives of the study are as follows :-

1. We have to recognize several frauds and security threats concerned with the use of ATM.
2. We have to evaluate the users opinion on ATM fraud and how offender robs the victim of his/her ATM card, gets the PIN and then uses the card.
3. We have to understand the frequency and incident of ATM fraud.
4. We have to examine the grade of security put in place as regards the use of ATM.

Methodology & Proposed Plan :-

The proposed title encompasses the tasks of establishment, development and evaluation nature. Initially the establishment of a Security Development Framework (SDF) is supposed to be accomplished through infrastructure setup followed by explorations, identifications, procurements, installations and operationalization activities. Secondly, the development of security procedure in the absence of pertinent ready-to-use framework is to undertaken. It is supposed to accomplish through several phases including following:

- Conceptualization
- SDF Design and Development
- Expert-Review and Revision of SDF
- Implementation-Level Specifications
- Implementation, Preview and Pre-Tryout
- Assessment of Effectiveness
- Documentation and Finalization

Evaluation of effectiveness of SDF at components level and as a whole will be accomplished through an experimental design.

Summary & Conclusion :-

At least this paper will be an example for awareness and security system, such as magnetic stripe based ATM cards applied by banks and financial institutions and their loophole. (Utakrit, Nattakant. 2007).

As the numbers of ATM customers are increasing day by day, they becoming more desirable targets for skimmers. These frauds could be counted as a security risk in the form of card cloning or PIN capturing, etc. (Sankhwar, Shweta. and Pandey, Dhirendra. 2016).

According to the Reserve bank of India (RBI), pecuniary cyber crime in our country India has been raising day by day over the years. The RBI reported 16,468 frauds cases concerned to debit/credit ATM cards and net banking in year 2015-16. In year 2013-14 and 2014-15, the fraud cases were reported 9500 and 13083 respectively. The central bank is alert with the circumstances and has taken energetic steps to learning the banks. (Dastur, navroze. 2017).

In India most surprisingly, over 3.2 million debit card information were eventual stolen by the criminals from ATMs and POS (point of sale) machine in October 2106. According to the national payment corporation of India (NCPI), the grievances of untrustworthy cash withdrawal are restricted to cards of 19 banks and 641 customers. The affected amount is 13 million rupees. (Dastur, navroze. 2017).

In this investigation, we identifying skimming attacks on ATMs via periscope device. (Dicks, Alexander.et al., 2016 , Lohweg, Volker.et al., 2016 and Sahar, Torkamani.et al., 2016). According to the Krebs, the scams of such skimming will not reduce as more banks choosing this chip-based payment cards. Most banks and financial institutions will keep faith on the magnetic stripe to use modern ATM cards. It is eventually that bank will keep on use of magnetic stripe at ATM's to examine the correct insertion of the card in slot of cash machine. Experts said that the periscope skimming probes are just sample, actually they absent of hidden cameras or other mode of stealing bank customer's personal identification number (PIN) at the ATM's. (Secret Service, U.S. 2016).

Reference :-

- Adepoju., Solomon, Adelowo. and EnagiAlhassan, Mohammed. (1970). Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria Ã¢ Â Â A Case Study of Selected Banks in Minna Metropolis. The Journal of Internet Banking and Commerce, 15.2, pp.1-10.
- Commonwealth Bank of Australia. (November 2009). ATM Card Skimming & PIN capturing Customer Awareness Guide Group Security. https://www.commbank.com.au/personal/apply-online/download-printed-forms/ATM_awareness_guide.pdf/

- Das, s.s. and Debbarma, j. (2011). Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System. International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203.
- Dastur, navroze. (2017). ATM frauds will continue, but here are a few steps card holders can follow to safeguard their money. https:// www.firstpost.com/business/ATM-frauds-will-continue-but-here-are-a-few-steps-card-holders-can-follow-to-safeguard-their-money-3505527.html
- Guo, h. and Jin, b. (2010). Forensic analysis of skimming device for credit fraud detection. 2010 2nd IEEE international conference on information and financial engineering, Chongqing, pp.542-546.
- Okechukwu onyesolu, Moses. and Majesty Ezeani, Ignatius. (2012). ATM security using fingerprint biometric identifer: An investigative study. International Journal of Advanced Computer science and applications, 3.4, pp. 68-72.
- Sankhwar, Shweta. and Pandey, Dhirendra. (2016). A safeguard against ATM fraud. 2016 IEEE 6th International Conference on Advanced Computing (IACC). IEEE.
- Schneier on security. (19 September 2016). Periscope ATM skimmers. https:// www.schneier.com/blog/archives/2016/09/periscope_ATM_s.html
- Secret Service, U.S. (2016). Secret Service Warns of 'Periscope' Skimmers. https://krebsonsecurity.com/2016/09/SECRET-SERVICE-WARNS-OF-PERISCOPE-SKIMMERS/
- Statistics, fraud. Brief data analysis about card skimming. https:// www.antiskimmingeye.com/fraud-statistics.html
- Sullivan, R. J. (2010). The Changing Nature Of US Card Payment Fraud: Issues For Industry And Public Policy, Federal Reserve Bank of Kansas City. Workshop on the Economics of Information Security, Harvard University, May. Vol. 21.

****