Master Vlada Živanović
State Audit Office, Kragujevac, Serbia

BUSINESS WITH ATM

Abstract. *Payment system is representing all fund transfers and money free way fore domestic and foreign subjects. Fundamental character of payment system is mirrored in his significant impact incorporated at financial sector of the economy, and is indispensable for modern and reliable functioning of money and capital market.*

Regularly based and organized payment system provides smooth business flows, both in enterprises sector and in civil sector. This work is focus on patchwork machine ATM and to increase the safety of the user when raising money from an ATM.

New types of mal ware that attacks the ATM aims to enable the theft of the original payment card, by making the first "capture" the ATM, and then release when the attackers want.

Operation ATM is supported by Star Net computers that they contain and which, like every other has an operating system installed. Another thing common in ATMs and computers desktop or laptop PC is Windows, hence the danger that ATMs are easily infected with malicious software. Of course, the computer is infected ATMs is somewhat harder than ordinary computer, but it is not impossible that have so far been successful hacker attacks showed.

Key words: *Canvas operations, payment cards, the use of electronics, modern fraud at ATMs, the protection of citizens.*

1. INTRODUCTION

The development of banking through greater application of electronics, computer technology and databases tendency toward ever-smaller direct contact between bank customers and banking officials. The most frequent occurrence in the banking business with clients is payments and payments of money in cash.

To reduce the involvement of human resource banks and automate job time, resulting in the appearance of devices that in this business change man - ATMs.

The first man who came up with the idea to make money from your bank account raises with the help of machines, called [1, pp. 19].

He came up with the idea back in 1939, and thus delighted the bank Citicorp, which has decided to offer the service to their customers.

However, after only half a year, the bank said it has suspended the project due to lack of interest of customers for this service. The turning point occurred in 1967 when Barclays Bank in London installed ATM, and thus began the expansion of ATMs and their increasingly frequent use throughout the world.

To withdraw money from an ATM using the card with a chip or a magnetic stripe. Despite the fact that more and more in use appear 'chip card' 'to pay for that increase the safety of users, criminals continue to find ways how to reach the PIN code, and copy the data from the same.

Therefore, below we explore: How to increase the safety of the user when raising money from an ATM?

2. METHODS OF ABUSE ATMs

Advancing technologies have emerged and modern ways of theft. Instead of stealing a wallet thieves are diverted to pull money with payment cards and the most perfidious methods and modern techniques.

In the last few years, thieves have perfected the most modern techniques of theft at ATMs or POS systems that involve the use of a variety of devices, ranging from micro cameras, scanners to false keyboard.

Basic fraud at the ATM used carelessness cardholder, while more sophisticated methods based on the use of various devices which are copied sensitive data from the card and/or PIN.

New types of malicious that attacks ATMs aims to allow the theft of the original payment card, by making the first "capture" the ATM, and then release when the attackers want.

Operation ATM is supported by Star Net computers that they contain and which, like every other has an operating system installed. Another thing common in ATMs and computers desktop or laptop PC is Windows, hence the danger that ATMs are easily infected with malicious software. Of course, the computer is infected ATMs is somewhat harder than ordinary computer, but it is not impossible that have so far been successful hacker attacks showed.

Advanced malicious code [2] is called SUCCESSFUL, and was discovered by researchers from Fire Eye. SUCCESSFUL appeared a couple of months ago, and recently was widely used.

2.1. "Trap" or "jamming"

This method is used so that the space provided for inserting the card inserted suitable subject with a view to being trapped inside the ATM. The simplest technique is called. "Lebanese loop" (the first technique that was used for these purposes).

Use the Tab loop is very simple and effective method that uses a "device" (often just enough rubber or plastic tape) which is inserted into the space card reader at an ATM in order to keep the inserted card.

Because of the embedded plastic strip ("Lebanese loop"), the card reader can not retract and process it, and the card remains active in plastic tape and inaccessible to the user [3].

Once the user ATM withdraws from the transaction and leave the ATM card into leaving him, criminals removed the guts and card. If some of the methods of detecting and PIN for further abuses card is simple and convenient without risking criminal (Figure 1).

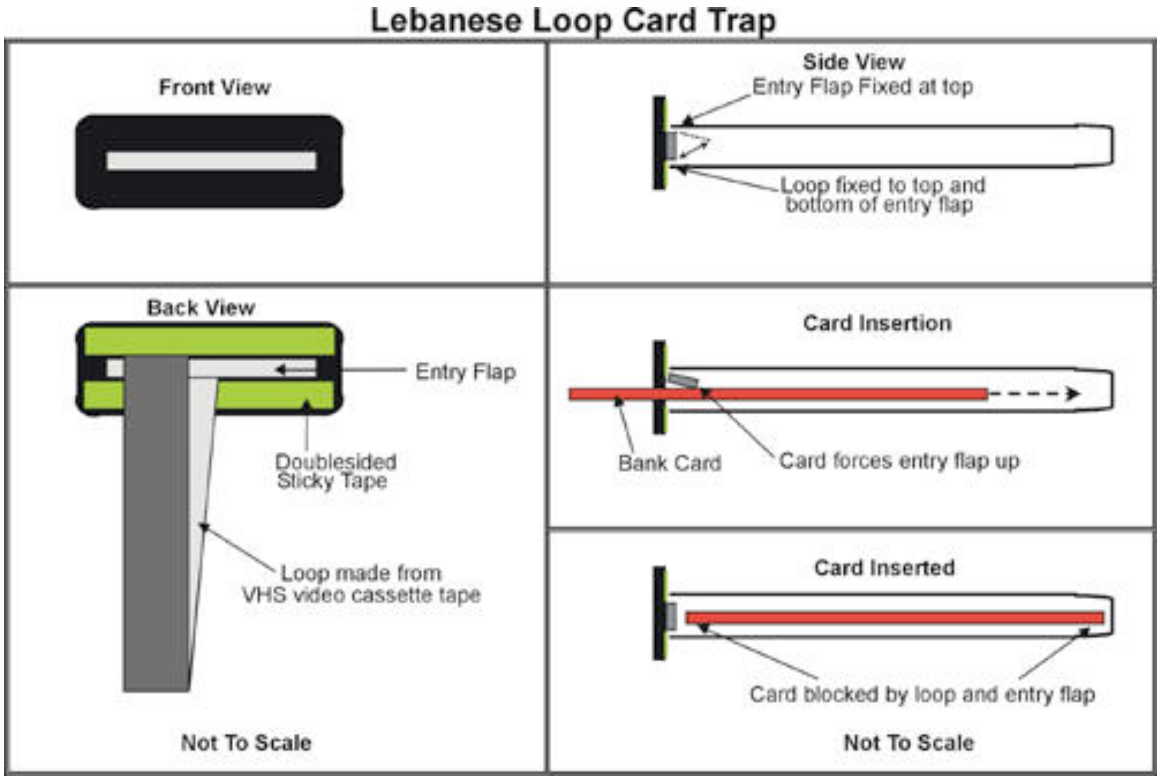

Fig. 1. Principle of operation «Lebanese loop»

2.2. Using the «skimmer»

It is necessary to specify the basic of skimmers and dangers that these devices pose to the safety of our cards. Usually we think of first teller machine (ATM) with dual keypad and magnetic reader installed by fraud [4].

Skimmers are sophisticated ''high tech'' solution which, put simply, copied magnetic track data on the pin code, which is later used in the production of false cards. Masked so that after the installation seems to have been an integral part of the ATM (Figure 2).

Fig. 2. Skimmers

Recent information security expert Brian Krebs City banks draw attention to a less known about the use of skimmers which certainly should take into account. These are skimmers POS (Point Of Sale terminals as those devices that have the shops that take credit cards) [5].

2.3. Theft PIN code

Theft PIN number is done by placing miniature cameras, or other devices that will record the number of users who knocks. A pinhole camera is set to the ATM and is masked as an integral part of the ATM or near the keyboard, and even a bucket to throw lane (slips) that we receive after raising money.

The camera can be set up within a couple of minutes at an ATM is usually held for a few hours or less. People who have a set can be placed in close proximity to make sure that the machine is not detected, which would have been exposed to the arrest during his takeover. Data from " skimming 'devices can be wirelessly sent [6].

The PIN can be obtained and social engineering under the pretext of aid when raising money, setting additional keyboard on existing (Figure 3).

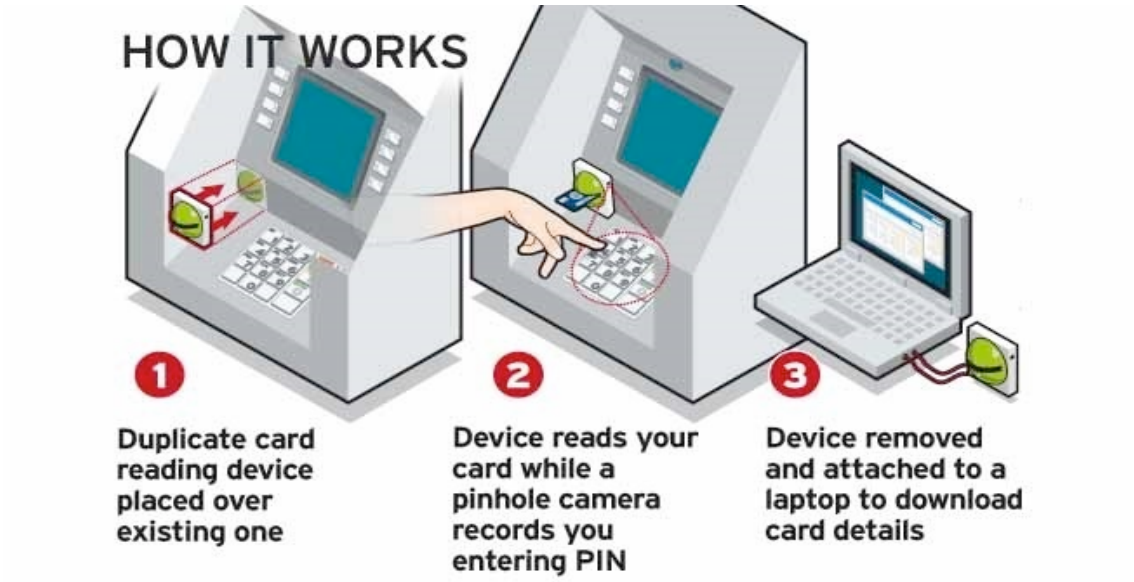

Fig. 3. The principle of operation of the reader data and camera which records the PIN code

2.4. "Cash trapping" devices

"Cash trapping" devices are put in place for the payment of money and is a physical barrier between the client and the door for payment. Upon successful completion of the transaction [7], ATM pays money, which remains trapped between an ATM and a special device that is mounted on the door for payment. After the client away, approached the ATM fraudster captured and taken the money.

In payment, will be heard counting money and raising money door presenters, but the client will not be able to physically see your money. The device can be set up by cutting part of the ATM [8] (Figure 4).

Fig. 4. Cash trapping device

3. METHODS OF PROTECTION FROM ABUSE ATMs

There are three basic ways that can reduce the chances of fraud:

1. Before you put the card in the ATM needs to take a good look, observe and hand-
checked the place in which the card is inserted.
2. Before than the PIN try to raise the keyboard to determine if the law
3. When you enter your PIN blocked leading arm types in a PIN other hand, that is to
protect the keyboard from view or recording [9].

4. CONCLUSION

A safe and efficient payment system is a key factor in the functioning of the financial system. In economy which claims a well developed payments infrastructure, the central bank needs to lay the foundation, monitors, identifies important events, directs and builds participants and network that will result in a synergistic effect.

The development of electronic banking and the introduction of the use of ATM as one of the primary means for the work there has been increased misuse of the same. As ATM is not only a machine that is installed next to each bank offices and branches, where it is possible to protect it with a camera or the actual physical security, but also in the areas of independent and distant from the banks themselves, and thus becomes susceptible to fraud.

Now the most sought after commodity - money becomes very interesting persons' 'beyond the law' 'that use all possible methods, both primitive and contemporary to him' access to ATMs.

Educating clients by demonstrating the methods thieves use when misuse of data from an ATM or plastic cards, the banking sector is its level of business leads to a safer level. The tendency in the development of the protection of banks on one hand and customers on the other hand, in light of the opposition to the possibility of fraud that follow the trend of introducing innovations in the banking business.

References:

1.Simijan,L.G The attack on ATMs and theft of payment cards, Retrived 2014, pp - 13-17.
2.www.smedia.rs/it3465976
3. http: // www. unglobalcompact.rs/dokumenti 2010 / working% 20grupa% 20for% 20 kDa% 20u% 20Bankarstvu% 20and% 20finansijama / Payment 20promet%%% 20sa 20inostrans5tvom% 200542012.pdf
4. Pavlovic, Z., 943 criminal protection of payment cards, XLIII Savetocanje for Criminal Law and Criminology of Serbia and Montenegro
5. Law, Official Gazette of RS No.61/2005th
4.1119PP16-17i182011 Interbank calculation Fifth
6.http://content.yudu.comaA1zg1ya1RetNovi12resourcesindex.htmreferrerUr1=http%3A%2F%2Fcontent.yudu.com%2FA1RetNovi12%2Fres
7. Core Principles for systemically important payment systems (2001)., Bank for International Settlements Information, Press & Library Services CH-4002 Basel Switzerland
8. Review of Theory and Practice of Finance, 2010 www.mfin.gov.rs
9. Xiaonan Che. (2011). Markov type models for large-valued interbank payment systems, the Department of Statistics, The London School of Economics and Political Science No. 1-6, pp.14-21