Attacking POS:

History, Technique and a Look to the Future

When we talk about credit and debit card we should remember that this kind of payment was think and launched after the second war from American Express and the card as we know with magstripe was introduced in the market from 1979. Since the beginning of the '90 years we've seen an increase in card fraud, before using the ATM terminals and subsequently affecting the Point of sale terminals (POS). Before talk about fraud we will try to understand how is composed a credit or debit card.

Debit and credit card are plastic made with two faces: the front shows the logo of the payment circuit (MasterCard, Visa, Maestro) the number of credit cards and as well as the expiration date, the embossed numbers correspond to the standard ANSI X4.13-1983 type XXXX-XXXX-XXXX-XXXX. The first number indicates the payment circuits membership and is set to

- 3 for cards in the tourism industry (American Express or Diners Club)
- 4 for Visa cards
- 5 for MasterCard
- 6 Discover Card

The number of card is a combination of structured data. From the second through sixth numbers we have the identification number of the bank that issued the card. From the seventh to the twelfth or the seventh to the fifteenth we have the unique account number. The last digit is called a check digit. In the back face of the card is present the magnetic stripe. The magstripe can be *written* because the tiny bar magnets can be magnetized in either a north or south pole direction and is very similar to a piece of old cassette tape. The magstripe is divided in three tracks as follows:

- Track 1 (upper area) 79 character alpha-numeric coding density: 210 bpi (bit per inch)
- Track 2 (middle zone) 40 digits, coding density: 75 bpi
- Track 3 (lower area) 107 digits, coding density: 210 bpi

Your card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorized), but its usage is not standardized among banks. The information on track one is contained in two formats: A, which is reserved for proprietary use of the card issuer, and B, which includes the following:

- Start sentinel – one character
- Format code="B" – one character (alpha only)
- Primary account number – up to 19 characters
- Separator – one character
- Country code – three characters
- Name – two to 26 characters
- Separator – one character
- Expiration date or separator – four characters or one character
- Discretionary data – enough characters to fill out maximum record length (79 characters total)
- End sentinel – one character
- Longitudinal redundancy check (LRC) – one character LRC is a form of computed check character.

The format for track two, developed by the banking industry, is as follows:

- Start sentinel – one character
- Primary account number – up to 19 characters
- Separator – one character
- Country code – three characters
- Expiration date or separator – four characters or one character
- Discretionary data – enough characters to fill out maximum record length (40 characters total)
- LRC – one character

So let's see how it works when you are on a merchant and you chose to pay with your card. After you or the cashier swipes your credit card through a reader, the software at the point-of-sale (POS) terminal dials a stored telephone number to call an acquirer.

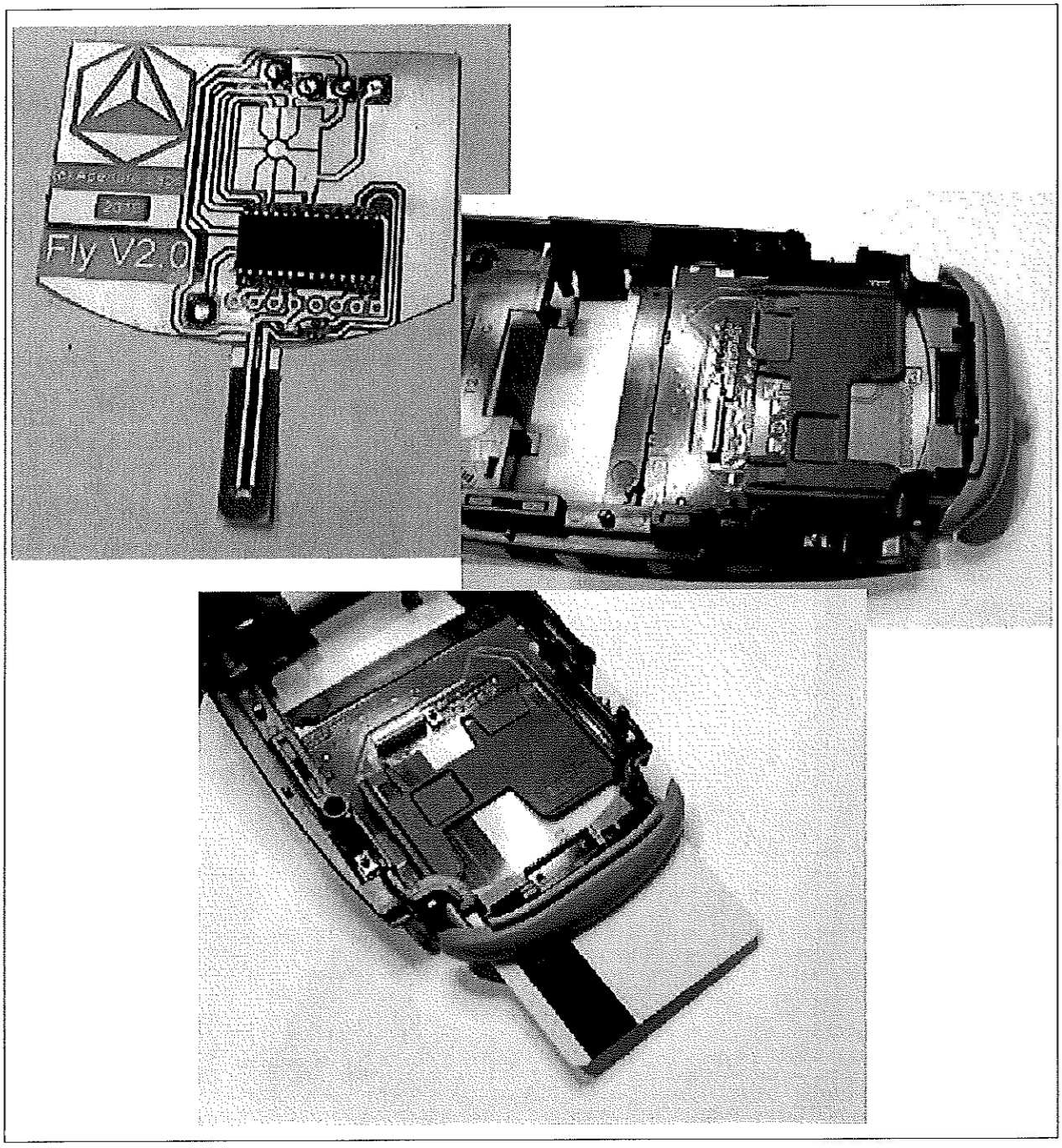

Figure 1. *Look from inside*

An acquirer is an organization that collects credit authentication requests from merchants and provides the merchants with a payment guarantee.

When the acquirer company gets the credit-card authentication request, it checks the transaction for validity and the record on the magstripe for:

- Merchant ID
- Valid card number
- Expiration date
- Credit-card limit
- Card usage

Depending on the card may be required that cardholder enters a *personal identification number* (PIN) using a keypad, or sign the receipt.

We have seen how a crad is made and how it works on payments, now it's time to understand how it is possible to clone a card to steal money. The oldest method of cloning cards on a POS was based on inserting a microchip inside the POS terminal; this is a particular chip built to record the data of the card that come from magstripe and the one come from keypad of POS. Typically this was possible with employees complacency, but when this was not possible criminals was simulated robbery to a merchant to insert microchip inside POS end subsequently recovered it with full data. Today this type of attack is very hard to do because almost all vendor of POS terminals use burglary systems. This not means that is not possible to get data of cards. Improvement of technology push criminals to found other ways to steal data from POS. In recent years have been developed micro skimmer that are inserted and glued to the inside of the nozzle where it is swiping the magstripe of card. this type of attack is particularly insidious because it is very difficult to notice the presence of the micro skimmer and there is no sign of tampering. Micro skimmer, have a Wi-Fi or Bluetooth connection for steal data from POS.

Meanwhile card have become chip card and POS have become more sure for merchants. We can find wireless POS that uses Bluetooth or Wi-Fi, or POS that use GSM networks or Internet. Chip cards seems to be more security oriented than few years ago, but they go on taking magstripe on the card with all data. When a chip card is used, the card advertises to the terminal to use chip instead of magstripe. One of the weakness of new cards is the backward compatibility, so they can work with modern POS that have e chip reader, but can also work with the old POS that have only two track reader of the magstripe and this is a great weakness of payment security. In fact you can force a card to work with an old method that means less security.

To steal data from chip card in recent years have been developed attack that consist of "hooking" a special circuit card in the nozzle of chip reader, this circuits do not need power because is powered by POS. Chip interface is inherently accessible and

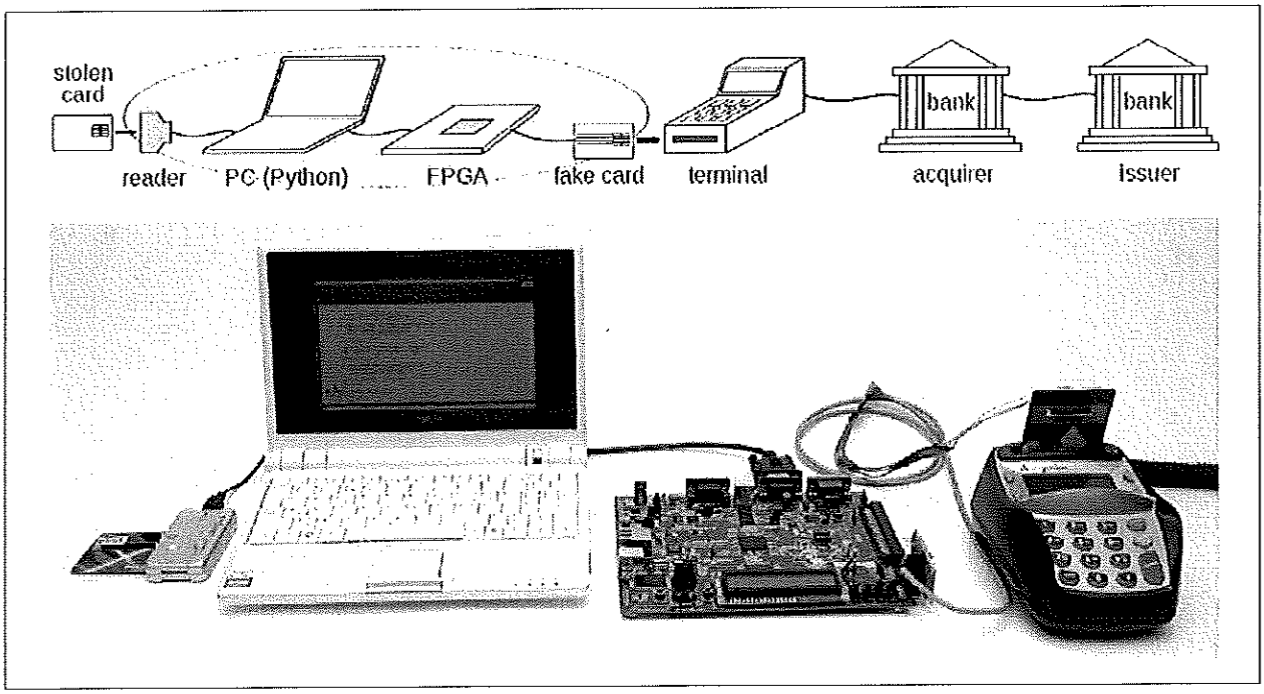

Figure 2. *Sequence - how does POS terminal work*

becomes impossible for the user to verify if the terminal has been tampered as the chip interface is not visible. This kind of skimmer could go undetected for a very long time is cheap and requires little installation effort. Data captured can be downloaded with a special card recognized by the skimmer.

So using last POS and chip cards do not means have a security payment system. In 2010 a paper from Cambridge (*http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf*) explain how a criminal can use a stolen card without knowing the PIN. The flaw is that when you put a card into a terminal, a negotiation takes place about how the cardholder should be authenticated: using a PIN, using a signature or not at all. This particular sub protocol is not authenticated, so you can trick the card into thinking it's doing a chip-and-signature transaction while the terminal thinks it's chip-and-PIN. The upshot is that you can buy stuff using a stolen card and a PIN of any number. An excellent video on *http://www.bbc.co.uk/blogs/newsnight/susanwatts/2010/02/new_flaws_in_chip_and_pin_syst.html.*

After the *Chip and PIN is broken* paper was published some contra arguments referred to the difficulty of setting up the attack but on October 2010 another students, Omar Choudary (*http://www.lightbluetouchpaper.org/2010/10/19/the-smart-card-detective-a-hand-held-emv-interceptor/*) developed a card-sized device (named Smart Card Detective – in short SCD) that can monitor Chip and PIN transactions that can be use to analyze and modify any part of an EMV (protocol used by Chip and PIN cards) transaction, using the SCD was tested the No PIN vulnerability and was proof that arguments discussed in the paper were founded and require not so difficult settings.

Another type of attack can be conducted involving attention to communications channel between the POS and the bank. The modern POS implement Bluetooth or Wi-Fi communication channel, often without any kind of encryption of data. A criminal sniff the data on the air and decode data from protocol obtaining access to card data sent by POS terminal, and in some cases also the access to the bank front end. The same arguments are valid for the newer POS SSL that use Internet to connect to the bank. This choice is generally used in shopping centers to reduce the cost of an infrastructure, they use the Internet connection instead of create an infrastructure of n-telephone lines for POSes. For this kind of POS we can take care of the same arguments of Wi-Fi and Bluetooth, the only thing different is that data are encrypted, and this should sound good for security, but if the SSL channel is not checked correctly could be inserted a MITM attack. Looking to recently advice of ssl insecurity should be more easy to access to data inside ssl tunnels.

Other type of attack could target the software of POS. The first risk is malware. In fact is begin to spread malware for POS systems (like for ATM systems) that could be targeted to get a specific type of data and send it, why not via Internet, of via Bluetooth or Wi-Fi to the criminals. The second risk is software developed and injected in the POS terminal. If someone could insert a backdoor or a Trojan inside the software of POS should be result could be very dangerous. A similar bug should be very hard to be detected, and meanwhile the man know how to access to a similar bugs could harvest millions of data

Let's take a look to the future. Bank push contactless card and NFC payments for mobile. I think they are good for increase electronic money use but are very insecure channel, all is in the air, wireless, could be heard by anyone, could be intercepted with a specific technology and the data exchanged stolen. I believe that build contactless secure infrastructure could cost too much than build an efficient anti-fraud system on the backend of POS and ATM. We also have to remember that card as for bank are used for loyalty program, on oil market and by some brand to retain customers. As some could think to steal data form debit or credit card, some other could think to use the same mechanism to unlawfully gain points and gift of the loyalty program, some of which are very expensive gift.

ALESSANDRO FIORENZI

Information Security and Forensics expert
alessandro@alessandrofiorenzi.it
www.alessandrofiorenzi.it