Trust No One. ATMs and their dirty little secrets.

Olga Kochetova & Alexey Osipov

Olga.V.Kochetova@gmail.com, giftsungiv3n@gmail.com

August 2016

1. Abstract

In this paper we will concentrate on different aspects of network and internal security problems of ATMs. We will cover some basic controls that are already there and why they are important, as well as we will provide some advices to be implemented.

We will dig into technical details of attacks on ATMs produced by more wide spread vendors. There are concentration on two aspects: network communications of ATMs with processing centers and communication of host with it's peripherals. We will describe how attackers transform ATM into skimming device without any physical access to it or steal all money without any forensic evidence in ATM logs.

2. Introduction

During several years, ATMs were jackpotted so many times with malware. They had various names, but equal possibility – malware based on financial applications standard. However, when banks tried to protect their ATMs from malware attacks, fraudster continued the cat-and-mouse game by ignoring host and using different attack vectors.

For last year, banker’s minds were full by other pain. Sometimes ATMs become empty and it looks like a miracle for banks. Malicious guys use so called “black boxes” to connect directly to dispenser to eject money. Such attack circumvent all software protections on the host machine.

But host to dispenser is only one side. On the other side, we have all kinds of connections to the outer world. From X.25 to Ethernet and cellular networks. Thousands of ATMs can be attacked by MiTM-attack called fake processing center. Or many of them can be identified with Shodan and then be attacked due to security misconfiguration, administrators laziness and lack of communication between different departments in banks.

3. Background

An ATM is basically a construction kit. The manufacturer builds them from a dispenser, a card reader and other units produced by different companies. The units are placed in a housing which usually consists of two parts: the top box called the cabinet, or the service zone, and the lower section called the safe.

All devices are connected to the system unit, which in this case performs the function of the host (as we shall refer to it) via the USB or RS232 ports (often referred to as a COM port). Sometimes these ports are located directly on the system unit; if there aren't enough ports, a USB/COM hub is used. Older ATM models can still be found that are connected via the SDC bus.

To carry out financial functions an ATM must be connected by any available means to the processing center and control host, e.g. the ATM Active Directory.

ATMs can be considered as an entry point for attackers to conduct attacks on an ATM network, or even an ATM processing center. Such attacks can provide an attacker with a base for leveraging different financial applications.

4. The hardware attacks

Black box

So-called black box attacks are another type of attack that is getting increased coverage in the news. On surveillance camera videos the following occurs: someone opens the service zone, connects a magic box to the ATM, closes the cabinet and leaves. A little later several people who appear to be customers approach the ATM and withdraw huge sums of money. Of course, the criminals retrieve their little device from the ATM once they have achieved their goal. Usually, these black box attacks are only discovered a few days later when the empty cassettes and the withdrawal logs don't tally, leaving the bank employees scratching their heads.

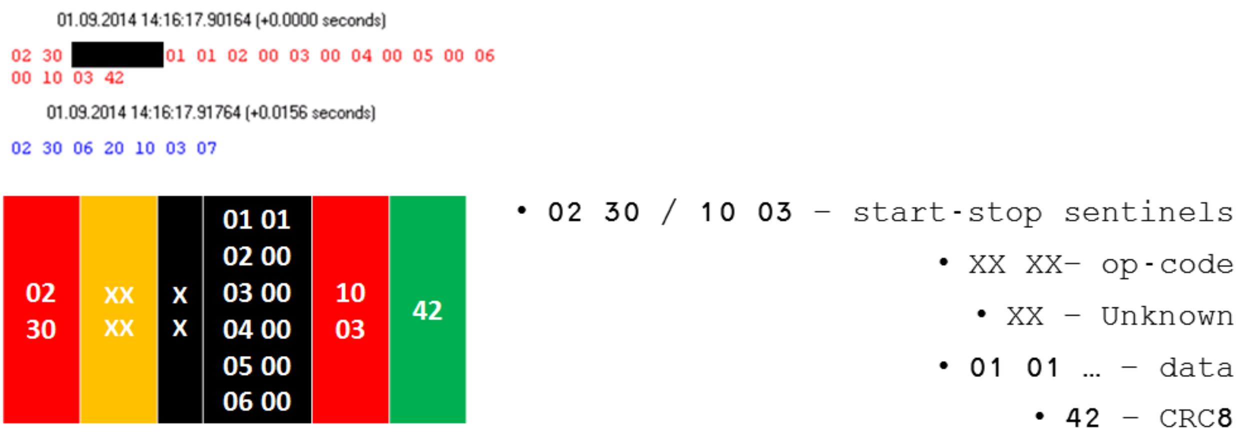
However, there is no magic involved – the attackers connect a specially programmed microcomputer (like Raspberry Pi) to the dispenser in such a way that it bypasses the security measures implemented on the host (antivirus, integrity control, full disk encryption, etc.).

Communications insecurity

As mentioned above, USB, RS232, or SDC can be used as a data transmission channel between the system unit and the devices. It's likely that nothing will prevent the attackers from sending the necessary commands directly to the device port bypassing its service provider. The standard interfaces often do not require any specific drivers. Authorization is not required either, which basically makes these insecure proprietary protocols an easy target – just sniff and replay. The result is direct control over ATM units, the use of undocumented functions (e.g., changing the unit firmware). The criminals may also use a software or hardware traffic analyzer, installing it directly on the port of a particular device such as a card reader in order to obtain the transmitted data. And this analyzer will be difficult to detect.

Direct control over the dispenser means the ATM cassettes can be emptied without any entries being made in the ATM software logs.

=



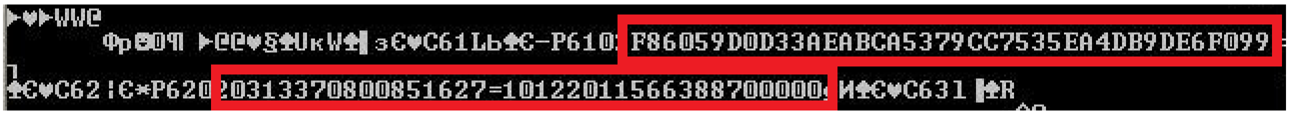
```
01.09.2014 14:16:17.90164 (+0.0000 seconds)
02 30 [redacted] 01 01 02 00 03 00 04 00 05 00 06
00 10 03 42
01.09.2014 14:16:17.91764 (+0.0156 seconds)
02 30 06 20 10 03 07
```

- 02 30 / 10 03 – start-stop sentinels
- XX XX– op-code
- XX – Unknown
- 01 01 … – data
- 42 – CRC8

Figure 1 – A typical packet – the command to dispense a banknote from the first cassette of the dispenser

For those who are unaware, it may look like magic. Every great magic trick consists of three parts or acts. There are dispensing money from the cassette, opening the shutter, and presenting money to the client.

Hardware skimmers are ‘so yesterday’. Direct connection makes it possible to read and record the magnetic strip of a credit card. Traffic analyzers, which are freely available on the Internet, can also be used as a direct connection. Rumor has it that in one fairly large bank all the ATMs were used as skimmers: the attackers had found vulnerabilities in the bank’s network and installed a USB sniffer on the ATMs, allowing them to collect bank card data in plain text for five years! Who knows, maybe your card was among those affected.



```
▶♥▶WW@
     Φp◘0¶ ▶@@♥§↟UкW↟▌зЄ♥C61Lь↟Є–P610: F86059D0D33AEABCA5379CC7535EA4DB9DE6F099
↟Є♥C62¦Є*P620 20313370800851627=10122011566388700000 И↟Є♥C631 ▌↟R
```

Figure 2 – The intercepted data of a Track2 card

5. The network attacks

The last mile of connection between ATMs and the processing center can be divided in various categories:

1. By media type:
   1.1. Wired
      1.1.1. Phone line
      1.1.2. Ethernet
   1.2. Wireless
      1.2.1. Wi-Fi
      1.2.2. Mobile
         1.2.2.1. CDMA
         1.2.2.2. GSM
         1.2.2.3. UMTS
         1.2.2.4. LTE
2. By implemented security features
   2.1. VPN

2.1.1.Software

2.1.1.1. OS internal

2.1.1.2. Third-party

2.1.2.Hardware

2.2. SSL/TLS

2.2.1.ATM application specific

2.2.2.Third party

2.3. Encryption

2.4. Message authentication

3. By PCI DSS definition

3.1. Public

3.2. Private

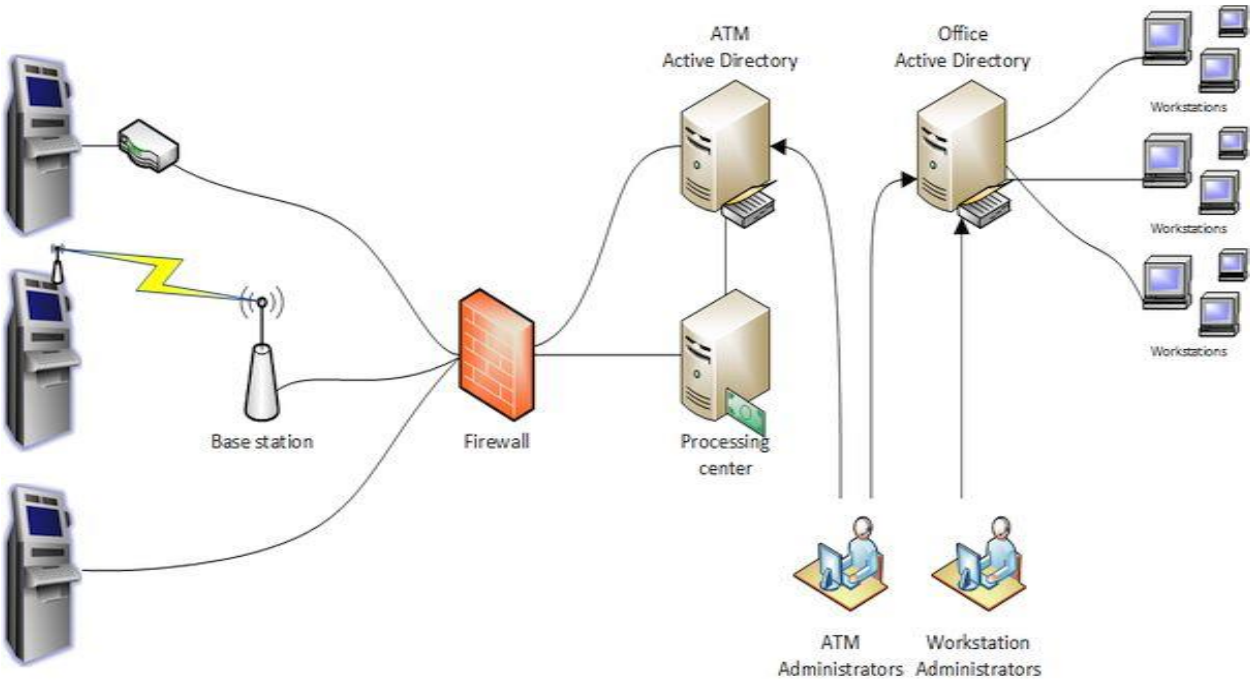


Figure 3 – Typical ATM network

We have regulatory requirements (like PCI DSS), that define minimal set of security features, that should be implemented. But, when we speak about big organizations, it is accustomed, that a lowest bidder will build the system. It is easier to implement the system that will comply with such requirements, but would be vulnerable to different attacks.

One of the major rule – all sensitive (i.e. cardholder data) information in public network should be encrypted. We have networks, that have encryption implemented by design and it is tempting to say, that data is encrypted, because one is using Wi-Fi or GSM connection. But many of such connections don't provide sufficient protection. CDMA is completely broken and there are companies, which provide commercial solutions for data interception. GSM has the pretty much the same situation. A5/1 encryption – is compromised and can be decrypted by enthusiasts.

The connection between ATMs and the processing center can be protected in various ways. For example, using a hardware or software VPN, SSL/TLS encryption, a firewall or MAC-authentication, implemented in xDC protocols. However, all these measures often appear to be so complex for banks that they don't bother using any network protection at all or they can be implemented in erroneous way.

In "best" case scenario in the bank – ATM connects to VPN server and inside such private network connects to processing center. The problem is, that banks often use site-to-site connection, where all ATMs see other ATMs. In such situation, ATMs are not connected physically, but become interconnected logically.

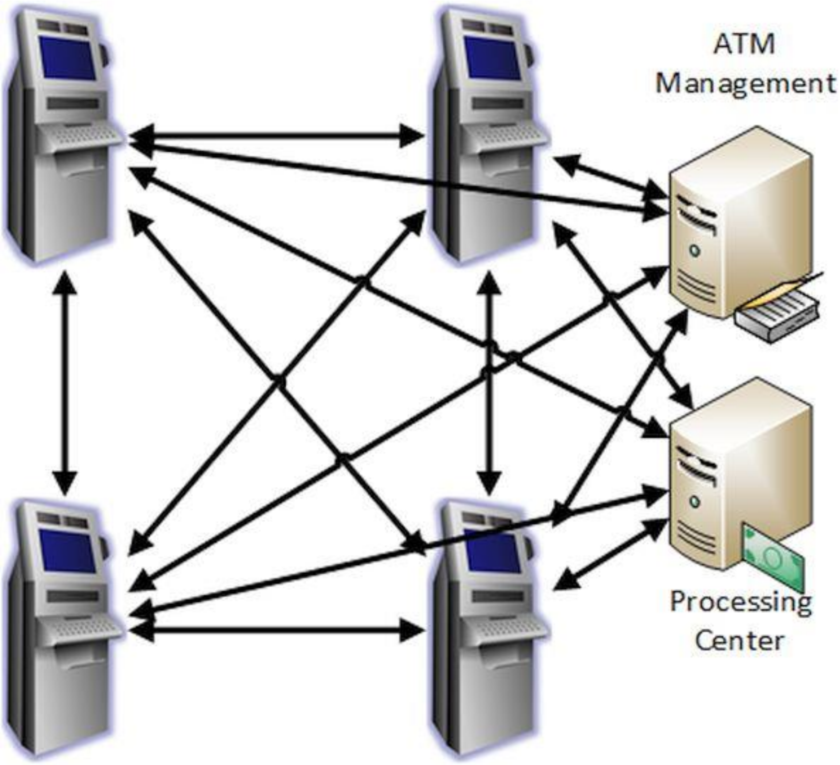
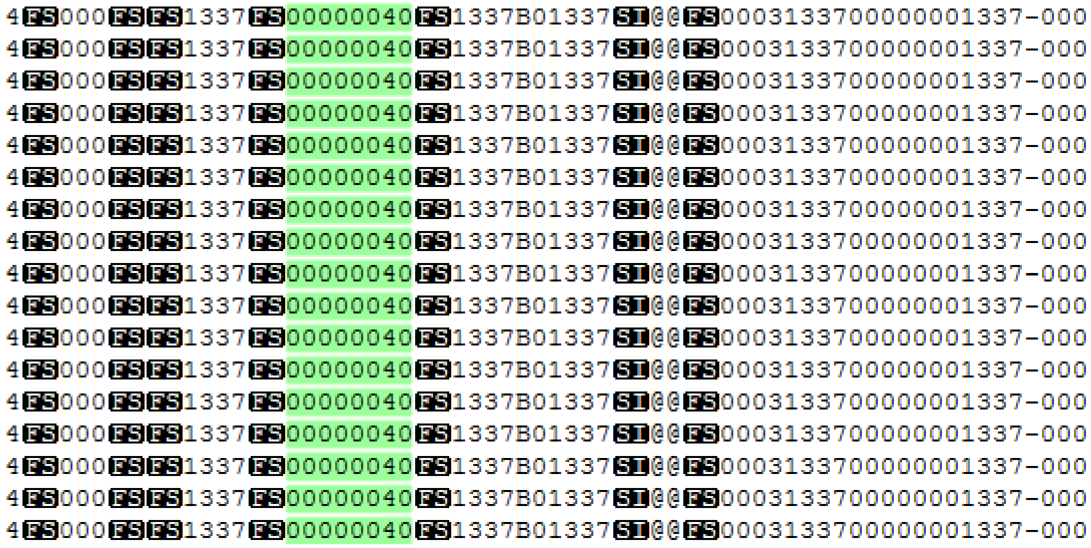


Figure 4 – ATM interconnection inside logical network

Either with insecure wireless communication or by creating private network with common broadcast domain for different ATMs, a MiTM attack can be launched that will result in the attacker getting data transmitted between ATM and bank. Such information contain card data and commands to withdraw money in the ATM. This requires remote access to the device, which is usually obtained by using vulnerable services that can be accessed from the Internet, as well as social engineering techniques. Physical access to the network hardware, including the ATM Ethernet-cable will also suffice.

On the way to the real processing center a fake one pops up; it sends commands to the ATM software to dispense banknotes. Withdrawing money is possible with any card, even one that has expired or has a zero balance, as long as the fake processing center "recognizes" it. A fake processing center can be either "homemade" software that supports communication with the ATM via the xDC-protocol, or a processing center simulator originally designed to check network settings (yet another "gift" from the vendors to the cybercriminals).



```
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
4FS000FSFS1337FS00000040FS1337B01337SI@@FS0003133700000001337-000
```

Figure 5 - The commands for giving out 40 banknotes from the fourth cassette sent from a fake processing center and stored in the ATM software logs. They look almost like the real thing

Where do the criminals find ATMs that can be attacked via the network? Do they scan all the nearby networks or buy the information on underground forums?

It turns out that you just need to enter the correct request in a search engine – https://www.shodan.io/ (this Internet of Things scanner is well-known by the experts). The data collected by this scanner is usually enough to launch such attacks.

Or you could just take a closer look at the ATMs in retail and business centers. Sometimes the ATM system can be accessed without even opening it – all the communications are located on the outside.

6. Conclusions

ATM manufacturers can reduce the risk of attack on cash machines.

- Implement "authenticated dispensing" to exclude the possibility of attacks via fake processing centers.
- Implement cryptographic protection and integrity control over the data transmitted between all hardware units and PC inside ATM.

And what should banks do? They need to take action!

Encourage those who sell ATMs and software to make them secure. The manufacturer must eliminate vulnerabilities as soon as possible; it is necessary to tell them about it as often as possible. To prevent hacking of ATMs it is necessary to make use of all the available protection tools. A completed PCI DSS Self-Assessment Questionnaire is not a silver bullet and won't protect ATMs from attacks, or banks from financial and reputational losses. Proactive protection, including regular ATM security assessment and penetration testing, is better (and often much cheaper) than security incident and the subsequent investigation.