PROTECT YOUR AUTOMATIC TELLER MACHINES AGAINST LOGICAL FRAUD
FROM SKIMMING TO THE LOGICAL FRAUD, THE NEW COMING ATM AND KIOSK RISK
ABSTRACT

WHICH ARE THE RISKS ASSOCIATED TO AN ATM NETWORK

ATM EMERGING THREATS

ATM SECURITY TECHNOLOGIES

WHY IS MY ATM SO VULNERABLE? SECURITY CONTROLS

SECURING YOUR ATM NETWORK, SECURITY POLICIES

COMPREHENSIVE PROTECTION

BEYOND AUDIT

CONCLUSION
ABSTRACT
Do you believe your ATMs or Kiosks are secure? If you do, you should take a look at the recent news related with ATM hacking that have been published during the last year, and then, you should not ask yourself “HOW” your ATM could be vulnerable but “WHY”, and then and only then, you will find the appropriate answers.

Nowadays, cybercrime is one of the main government’s security agencies concerns. Initiatives like CyberStorm or CyberEurope demonstrate that critical infrastructures protection against cybercrime is considered one of the most important security issues. Recent cyber attacks like Stuxnet or Skimer in Russia and the Ukraine to the ATM Financial infrastructure have demonstrated that targeted attacks against valuable assets are becoming more and more sophisticated. Do you think your ATM network is a valuable asset? Are you aware of the new techniques employed to attack ATM networks? New risks are arising and new protection paradigms must be deployed in order to minimize the consequences.

This whitepaper will try to show you the new risks on ATMs, the causes, motivations, and which are the necessary elements that an ATM needs in order to minimize the risks of logical fraud.

Checker ATM Security product will provide you all those elements, since Checker ATM Security is a product specifically design to solve this problem, being compliant with the most advanced regulations as PCI-DSS.

WHICH ARE THE RISKS ASSOCIATED TO AN ATM NETWORK
The arrival onto the financial self-service scene of the Microsoft Windows operating system together with the use of IP networks, for communications services, has resulted in a considerable increase in security risks for Automatic Teller Machines (ATMs) as a direct consequence of the vulnerabilities which are common to open systems.

At the same time, the world is experiencing a paradigm shift regarding cyber attacks. Worldwide criminal gangs are currently pursuing low risk, sustainable sources of revenue and it is a matter of time before many criminals in modern countries join this emerging “criminal value chains” and target attractive assets in an organized manner. In this respect, there is no doubt that an ATM network is an attractive asset. Thus attacking ATM networks in a well organized and highly sophisticated way is a clear trend nowadays in Eastern Europe and Latin America, and will become an uncomfortable reality in the most advanced countries very soon.

Several options are available on the market to help controlling and mitigating the risks associated with ATM security. After all, an ATM is a hardened Windows-based PC with specific peripherals, and software to secure PCs which has existed for a long time. However, the majority of PC security products have evolved for typical office computer environments, whose particular characteristics (stability, updating frequencies, connectivity and service needs, performance etc.) are quite different to those of the financial self-service environments.

Traditionally, a lot of attention has been paid to preventing thieves from stealing the most evident asset in an ATM: cash. Many physical security controls are in place in modern ATMs, and most ATM network managers believe their ATM network’s security is reasonably managed, since the ATM controls in place obviously face the evident threats an ATM is subject to (things like breaking the ATMs using trucks or explosives).

More recently, the raise in card fraud has resulted in the appearance of an associated credit card data market. Today, criminals can easily sell credit card data over the Internet for a profit, and thus it is only natural that they wonder how they can obtain those data. Of course ATMs are an obvious source of PINs and magnetic stripe data. Due to these facts, ATM security focus is slowly shifting to ensure that proper security controls are also in place to prevent card and PIN data stealing from the self-service network. However, in order to select the proper security controls, it is necessary to understand the threat. Well known attacks such as card skimming are already being addressed (like for instance through EMV initiative). Still, there are new threats which are far from evident and are also rapidly evolving.

ATM EMERGING THREATS
ATM networks are currently subject to emerging threats which are usually poorly understood by ATM network managers. Part of the problem probably is that data stealing from an ATM does not immediately result in a loss for the ATM network itself, but for the financial entity behind the data. There is no clear liaison from ATM data compromise and ATM
loss expectation. Furthermore, many security incidents in ATM networks are currently not detected and thus the rate of occurrence of breaches is usually underestimated. It seems contradictory that what appears to be a new promising business for criminals is getting so little attention from ATM network managers.

In order to understand how this is possible, let us first discuss what would be the best strategy that a criminal could follow, for instance to obtain some credit card data from an ATM, data that he could later sell on the market. Criminals focus on three basic aspects:

- The effort must be worth the risk of being caught.
- This risk must not surpass some acceptable level, and
- They prefer tactics that would provide sustainable revenue better than actions that would result in punctual profit.

And sustainable revenue usually comes from a situation where assets (data or cash) are stolen regularly and without notice.

Now, if criminals would come with a truck and steal a single ATM (or, less dramatically, install some hardware device on it, like a dispenser trap), they would get money and/or data, but this would require a great effort and would provide limited profit. On the other hand, if they could somehow, and without being noticed, get their hands on ATM data on a regular basis, they would sell the data and thus have a source of sustainable revenue at a very low risk. Surely this possibility deserves some attention.

One could think of two ways to achieve this goal. If the criminal (or an accomplice) has periodic access to an ATM (say he is in charge of some sort of maintenance task) all that is needed is some knowledge and/or tools in order to get these data (provided of course they know where it is). This has been the main approach for some time. However this possibility is reduced to a limited number of people and therefore the associated risk of being caught is higher. At the same time, the card fraud market is becoming commoditized and the price of the stolen magnetic stripe data is decreasing. This, as in any other business, is demanding from the criminals a higher degree of sophistication, in order to decrease risk (of being caught) and increase the amount of stolen data (or its quality, e.g. knowledge of customer profile associated to the data) and also decrease the effort to obtain it.

In this way, as in most technology based “businesses”, the threat is rapidly evolving. For instance, if they just manage to have access to the ATM at one particular time (instead that on a regular basis), they can inject some malicious software and later collect the data using the ATM printer or sometimes send it over the network. The well known “Skimer” malware that expanded in a few countries at the end of 2008 does just that. And, once you manage to introduce malware in the ATM, why not use it to withdraw cash? Indeed that is what Skimer malware is able to do: By means of a particularly built card you can instruct the infected ATM to dispense cash. The cash that “disappears” does not belong to a particular customer, and tracing the loss is sometimes difficult. Moreover, in the very near future this type of malware is expected to behave as a “worm” and be able to self-replicate in a network, thus reducing the exposure of the criminals and increasing their revenue expectations.

At a first glance it may seem that building this kind of malware is quite a sophisticated task, and it is indeed, even for a well known open system like Windows. However, most criminals do not build their malware, they can buy it from organized criminal gangs just the same as they can later sell the obtained credit card data. These malware kits are available and are quickly becoming inexpensive. This criminal “specialization” is at the very core of the new threat model that we are facing.

**ATM SECURITY TECHNOLOGIES**

New generation of ATM-focused malware coexists with a crisis in the classic anti-malware solutions (a.k.a. antivirus) that have so far protected Windows-based systems. This crisis has three aspects.

- First, new malware is expanding exponentially so as to render eventually unmanageable the number of patterns that a classic antivirus solution needs to cope with.
- Second, so called zero-day exploits cannot be effectively dealt with using pattern recognition technology which is the technology widely used by most antivirus manufacturers.
- Finally, malware is evolving to use self-compiling technologies that result in customized versions with unique patterns, so that all instances of the malware look different for a classical antivirus which yields pattern based recognition ineffective.
So essentially new anti-malware technologies are required to secure Windows-based ATMs.

The solution must then include a combination of white listing, application level firewalls, signature based validation, peripheral devices control (ranging from cash dispenser to external USB drives) and keyboard hooking, among others. At the same time, these software security technologies must be as manageable and reliable as required for all ATM software; they must have a minimum footprint to prevent interfering with the ATM application software and must work in unsupported operating systems like Windows NT4. Also, they must evolve following a roadmap suited to the needs of ATM networks which are, and will continue to be in the future, quite different from regular Windows based PCs security needs. For instance they must provide specific traceability features, must adapt to regulatory conditions and must integrate with existing and future fraud management platforms.

Traditional PC security vendors are quickly adapting their products to secure ATMs, but usually this adaptation involves a lot of marketing and very little understanding of relevant issues like fraud prevention or regulatory compliance. Their technology has always been focused in securing high performance PCs with novel operating systems, and the PC market is their most important source of revenue. While they are certainly teaming with ATM manufacturers, it is unlikely that their products will bother to extend their newest technology to run in low performance computers (widely deployed in ATMs) with unsupported operating systems, and it is even less likely that they would evolve to cope with new foreseeable demands like secure software control of cash dispensers or integration with secure pin pads.

Take care, not all that glitters is gold! Common PC white listing solutions aren’t most of the times the right ones for ATMs or Kiosks.

WHY IS MY ATM SO VULNERABLE? SECURITY CONTROLS

We have seen that new threats related to some form of malware will be gaining importance in the near future. One could wonder how difficult is indeed to secure a Windows-based ATM. As already stated, the fact that Windows is a well known, open operating system plays against us in this arena. No doubt the use of Windows in ATMs has a number of advantages but one could reasonably argue that security is not one of them.

In light of the arrival of Windows to self-service networks, it is fair to consider whether the ATM equipped with this operating systems presents new “vulnerabilities”; this is to say, if the ATM would be more susceptible to malicious attacks which open up new situations of fraud or theft.

Vulnerability is essentially a “weak point” in the computer, its programs or its concept, which could be used to overcome the security of the ATM. The ATM includes a set of hardware and software products (the devices, drivers, operating system, application programs, etc.) which operate in an ordered manner following a chain of processes. The security of the ATM depends upon the security of the weakest link in the chain. In many cases, the operating system is this weakest link, both due to its design as well as its central control position in the ATM.

The nuts and bolts on how vulnerabilities are used by hackers in order to break into a Windows system are technically sophisticated, and a detailed discussion is out of the scope of this whitepaper. But the reader should be aware at this point that the adoption of Windows as the operating system for ATMs, while providing several benefits in other aspects, has certainly brought a security issue.

Specifically, it is easier than it seems to take control of an ATM device from a remote user station with access to the ATM’s network. It is uncomplicated to introduce malicious processes in the ATM, processes
that might be storing sensitive information (for example card numbers and associated transaction data) which can later be retrieved on a regular basis and be used in fraud attempts. It is also easy to download already existing files containing sensitive information to USB storage devices. It is easy to inject code that intercepts peripheral drivers and, for instance, dispenses cash.

As a consequence, there is an urgent need to install suitable security controls in ATMs. Naturally, security controls cannot have the intention of making Windows more secure than it is. But they can, depending on the situation, avoid, counteract or minimize security risks.

When ATMs first appeared around 1968 they quickly became one of the most influential technological innovations of the century. Believe it or not, ATMs were the first large-scale example of commercial use of cryptography, and actually they contributed to establish a number of crypto standards. ATMs security-by-design was a main concern at that time. Time has, however, turned a highly sophisticated, distributed, retail transaction processing technology into a legacy system. Today many ATMs feature unsupported versions of Windows and their RAM memory is almost ridiculous when compared with the standard offer in a PC store. Surely there are new modern machines available every year, but large networks cannot be changed as fast as the evolution of technology would suggest. There are around 2 Millions ATMs in the world today, and changing all of them every three years would be absurd. On the other hand, current ATMs might not be the most modern machines, but certainly they are quite stable systems, much more reliable than your office PC. Software upgrades are well controlled, and some ATMs even feature sophisticated monitoring and failure-prediction systems. Essentially, an ATM is not a machine where one wants to introduce a source of unreliability or a performance problem.

It is in this context that ATM network managers are facing the urgent need to install security controls. Since an ATM is essentially a PC, one might argue, they should be equipped with the same security controls that we have in our PCs: antivirus (or something of the sort). But the threats to ATMs, as we have seen, are not viruses. And even if they were, could you imagine the risks associated to installing an antivirus in an almost unattended environment such as an ATM? How could their resource consumption affect the ATM? Have you ever experienced degradation of your PC environment and blamed the antivirus? Clearly, Windows-based antiviruses or personal firewalls were not developed to secure ATMs. How does one go about selecting a proper security control for an ATM?

Fortunately for us, one of the main features of an ATM, its stability, is here to help us with the answer. An ATM is a very specific environment which has a clear advantage with respect to other Windows environments such as desktop PCs from a security perspective: Its configuration (programs, files and generally required resources) and its behavior (for example, permission for writing, reading or execution) may be precisely defined, and it generally remains stable (or with few alterations) for a longer time than office computer environments.

We can thus imagine an ATM specific security product as some sort of software that is installed between the operating system and the resources which it handles in the ATM, in order to ensure that actual use of resources conforms exactly to the expected use in the ATM. Here by resources we are meaning files, peripherals, everything controlled by the operating system. In this way, a large quantity of attacks may be detected as “unexpected use” and the countermeasures immediately taken in order to avoid damage and to warn managers. It is this concept, that of conformance or compliance in the use of the resources, which leads us to the quite interesting concept of “ATM security policy”.

SECURING YOUR ATM NETWORK, SECURITY POLICIES

In a general manner, we could define a Security Policy as a set of rules, principles and practices which determine the manner of implementing and managing security in a particular environment (such as, for example, a financial self-service network). Once a security policy is established, it is possible to design and implement a well-reasoned set of security controls. Controls will be selected so as to ensure compliance with policy, and when this is not the case, detect and inform about non-compliances.

The power of security policies is that they allow you to select the security controls that you need. A security policy should also be able to help in the selection of a balanced set of procedural, administrative and technical controls for a particular scenario.

Specifying a security policy for our ATM network will enable us to select the proper security controls. This selection is an important task which is often disregarded. In many cases it is relatively common to introduce
security controls into the information systems without having previously specified a security policy. Sometimes one could argue some “best practices” reason, but quite often this is just a sign of the threat being poorly understood. In fact, it is not easy to define policies for complex environments, since they intrinsically involve difficult cost-benefit analyses. In some cases, regulatory compliance poses a time pressure which, possibly combined with the apparent inexistence of security incidents (rather we should say of detected security incidents) could conceivably force managers to install some generic control which later is shown to be inadequate.

A final problem arises when, even with a good understanding of the threat, the controls required would be numerous and complicated. And this is indeed the case of ATMs, where one should control execution, file access, peripheral access, communications and a number of other subtleties which would imply the installation of several (four or more) generic security products, which in turn would result in a security management nightmare.

So ideally, we would require just one ATM security product that would do three simple things:

- Provide for the generation and management of ATM-specific security policies, that could automatically be translated into rules for security controls,
- Enforce these rules (being it regarding execution, access, communication or any other security requirement) using one single, low footprint security product in the ATM, and
- Provide for centralized monitoring of compliance, including all required audit features.

The state-of-the-art of security today allows such a product. We have seen how an ATM is a stable environment where the use of resources is predictable. One could just conceive a security product that would monitor the ATM, generate security policies based on its expected behavior, and then enforce that security policy embedding, for this purpose, all necessary controls. For example, one could think of a security policy expressed as a set of rules that limit the access and usage of ATM resources, which could be structured and centrally stored in a file which is in turn securely sent to the ATM in order to become enforced. A security policy would not be an abstract concept, but a very specific concept which allows bringing security to the ATMs in an understandable and manageable way. The rules admitted should have to be quite diverse; some examples could be “no process except for xxx may modify file yyy”, “only Java class zzz may access the library for access to the dispenser”, or “no system outside of the ATM may access communications port 12345”. These rules must be organized so as to cover all required security protections the ATM would need.

Once we have conceived an ATM-specific security product, and recalling the threats and vulnerabilities exposed in previous chapters, let us analyze what these protections would be.

**COMPREHENSIVE PROTECTION**

The following is a (non exhaustive) list of the type of protections that an ATM Security Policy must be able to specify and automatically translate into ATM enforced controls:

- Protection against unauthorized software execution. Since an ATM is (or at least should be) a well understood and controlled environment, this should be achieved by means of **white listing technology**. This technology is used to permit execution of software only when it is included in a so called “white list”, as opposed to “black listing”, which is the current antivirus technology that allows execution of any software except that on the “black list”. Today criminals can (and do) deploy custom pieces of malware, i.e. malware with different patterns so that every single instance has a new pattern, and often cannot be detected with classical black listing technology.

- Protection against unauthorized use of libraries and drivers.

- Protection against unauthorized access to ATM hardware devices. This for instance, controls the use of USB drives to enter or extract software or data to/from the ATM, or the access to the cash dispenser.

- Protection against unauthorized access to ATM’s files and folders. This prevents both reading of sensitive data and storing programs into the ATM file system.
- Protection against unauthorized execution of Java code. The specific mention to Java arises from the fact that all Java applications run using one process, the Java Virtual Machine, and thus process-based white listing technology is insufficient to control which particular classes (or other Java resources) are actually allowed to run on the ATM.

- Integrity validation of executable files, libraries and drivers. This is a complement to the protection against unauthorized software execution. It provides for a secure means to identify process with some suitable signature. In this way replacement of authorized software by malware is prevented.

- Integrity validation of any sensitive file in the ATM. This is the capability to validate, using signatures, any relevant file in the ATM.

- Integrated Firewall to control network communications on a per process basis. A firewall controls both access to the ATM (for instance from an external source that is trying to exploit a vulnerability) or from the ATM to the external world (for instance malware in the ATM that would try to send data outside). This firewall must control communications per process, per destination and per IP. For instance, “only process xx with signature yyy is allowed to connect to port aaaaa and listen from such IP”.

- Configurable keyboard hook. Additionally to execution control, disabling some keys in the keyboard would enormously difficult some attacks. This, which in usual PCs would be inadmissible, makes sense in an ATM that need not enable some particular keys (say Ctrl or Alt) in order to provide service.

- Configurable access control based on user. Since we must assume that users that access the ATM need not be necessarily trustworthy, it follows that different users should be provided different access rights and execution permissions (even if running as Administrator), depending on what they need to run specifically to do their jobs.

- Prevention of generic users and weak passwords. Last, but not least, user-custom control is useless if an operator is able to mask as another user, due to default or weak passwords in the ATM. A security control must be in place in order to prevent this.

Some of the mentioned features might seem redundant in their purpose, for instance why control communications to prevent malware exporting sensitive data, when the malware cannot be executed in the first place? Well, this approach, known as “defense in depth”, is a common strategy in the security scenario, and essentially consists in deploying several layers of defense just in case the attacker is able somehow to bypass one of them.

The above list of features is quite extensive, and indeed only ATM specific security products could be expected to provide them all in a single product. The main reason for this extensive list is that, an ATM must prevent attacks from people having physical access to the ATM. This is an unusual situation, and indeed some security experts would argue (convincingly) that it is quite impossible to secure a Windows-based machine from someone that has physical access to it.
This argument leads us to a final requirement for an ATM security product: all relevant actions performed on the ATM must be traceable.

While this might look like a typical security requirement, there is one interesting feature that we want to propose for our ATM security product. In addition to registering all failed attempts, we would like in some cases to relax security in order to understand what the attacker is doing.

For instance suppose that an ATM maintenance operator tries to install some malicious software. We could, in principle, disable all unauthorized software installation. On the other hand, if we let the installation proceed and provide the impression that the malware will work properly, we would get in turn full access to the malware. This course of action is uncommon, but it is intriguing to consider its advantages given the fact that ATMs attackers are in most cases insiders, and that other usual security tactics (such as deploying “honeypots”) are not easy to follow in the case of ATM networks.

So essentially we propose that an ATM specific security product should under some controlled circumstances allow unauthorized software execution in order to follow the “track” of the criminal and understand exactly the approach he is following in his attack.

We will not elaborate more on this topic, we will just say that a fully controlled, remotely managed surveillance of the ATM when it is under attack (as opposed to just denying all access in the first place) is a powerful tool which can result in deeper understanding of new threats.

CONCLUSION

In this paper we have discussed the emerging security threats and we have proposed an ATM security concept summarizing the reasons why such a far reaching security product is a real need for self-service networks, and why a typical PC-focused product solution, no matter how advanced, would certainly not provide the required assurance. This concept has been implemented by GMV in its product Checker ATM Security, a product that will help you to protect your ATM network and being compliant with most of the PCI-DSS requirements.

For more information on Checker ATM Security:
http://www.gmv.com/checker.html