ATM crime

August | 09

Overview of the European situation and golden rules on how to avoid it

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

ATM Crime:
Overview of the European situation and golden rules on how to avoid it

August 2009

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. The information includes contributions from members of the ENISA Awareness Raising Community (AR Community).

ENISA wish to acknowledge the efforts of the members of the AR Community and their organisations, ADICAE, Arjen de Landgraaf of E-Secure-IT, Daniel Blander of InfoSecurityLab Inc., David Barroso of S21sec, Fabio Guasconi of @ Mediaservice.net S.r.l., Fabrizio Cirilli, Gerasimos Ntouskas of KPMG Limited, INTECO, Joao Brites Moita, Lachlan Gunn of European ATM Security Team Ltd, Neal Ysart of PwC, Sissel Thomassen of InfoSecure, William Beer of PwC, Yves Le Roux of CA, who provided valuable inputs, material and prompt support for the compilation of the paper.

Finally, we would like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions, and fixes. In particular, we would like to thank the members of the European ATM Security Team. While this is undoubtedly not a complete list, this content would be incomplete and incorrect without their help.

Contents

About ENISA 2
Acknowledgments 4
CONTENTS 5
EXECUTIVE SUMMARY 7
PART 1: ATMS AND RELATED SECURITY IMPLICATIONS 9
ATM 10
A definition 10
The use of ATM machines: the European overview 10
ATM CRIME AND ITS FINANCIAL IMPACT IN EUROPE 11
Estimated losses worldwide 12
Among recent incidents worldwide 12
TYPES OF ATM CRIME 12
A definition 12
Theft of customer's bank card information 13
Card Skimming 14
Fake ATM machines 15
Card trapping 16
Distraction theft or 'manual' skimming 16
Shoulder surfing 17
Leaving transaction 'Live' 17
Cash trapping 17
Computer and network attacks 17
Network attacks against ATMs 17
Viruses and malicious software 18
Phishing 18
PIN cash-out attacks 18
Physical ATM attacks 19
SECURITY IMPLICATIONS 19
What happens when a customer's details have been captured? 19
Risks and threats 19
Security implications for ATM cardholders 20
Card protection 20
Personal protection 20
Protecting your PIN 21
ATM card details and the Internet 21
Other security precautions 21
Keep the bank's emergency number at hand 21
PART 2: GOLDEN RULES 23
GOLDEN RULES 24
CONCLUSIONS 26
APPENDIX 27

ATM USAGE AND FRAUD: CASE STUDIES 28

CYPRUS 28
Recent incidents occurred in Cyprus 28
Risks and threats 29
ITALY 30
Methodologies used during attacks 30
PORTUGAL 32
The ATM network 32
Threats and fraud levels 33
Towards a more secure environment 33

REFERENCES AND SOURCES FOR FURTHER READING 35

Executive summary

The number of ATMs in Europe is raising every year. ATM's can increasingly be found in many remote site locations other than banks, such as convenience stores, airports, petrol stations, airports, railway stations, department stores and so on. With the rise in the number of ATMs in Europe there has also been a significant rise in the total number of reported ATM crimes with the total losses reaching EUR 485.15 million in 2008. Organised crime is behind many of these attacks and the recession is seen as a likely driver of this increase. As a result, the ATM industry has placed the safety of users and protection against fraud as a high priority in order to help protect user's confidence in the system.

This white paper aims to provide a set of recommendations to raise user awareness about the different types of risks faced when using an ATM, along with advice on how to identify and counter them. ENISA believes that increasing user awareness of the risks is the first line of defence when tackling ATM crime, and can result in a significant reduction in ATM attacks and fraud. Citizens need education and guidance on what they can do to reduce these risks, by taking the necessary precautions when using an ATM, such as shielding their PIN when entering it, and by being alert to any signs of tampering or suspicious activity at an ATM.

ATM crime is constantly evolving, as are the countermeasures required to control it. This document can not cover all risks associated with the use of ATMs, nor can it offer complete advice on how to safely use them. This document should instead be seen as a useful and necessary starting point to increase overall user awareness of the issues they face when using ATMs, both within the European Union and elsewhere in the world, of data security and industry good practices. ENISA is committed to providing educational information to ATM's users about potential vulnerabilities and urges further information and advice are provided nationally in EU Member States by banks, financial institutions, payment schemes and law enforcement agencies.

This document does not cover any matters relating to legal requirements for the installation, operation, and maintenance of ATMs, for the processing of ATM transactions or for the movement and dispensing of bank notes.

Lastly, this document does not provide any advice or guidance with regard to the suitability, availability and effectiveness of any systems or devices that can be used to prevent or deter attacks on ATMs.

PART 1: ATMs AND RELATED SECURITY IMPLICATIONS

ATM

A definition

An automated teller machine (also known as an ATM or Cash Machine), is a computerised device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller.

Most modern ATMs identify the customer by the plastic card that the customer inserts into the ATM. The plastic card can contain a magnetic stripe or a chip that contains a unique card number and some security information, such as an expiration date and card validation code (CVC). Authentication of the user is provided by the customer entering a personal identification number (PIN).

When using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and can check their account balances as well as purchasing mobile phone prepaid credit, paying bills and so on.

The use of ATM machines: the European overview

In 2008, the European ATM Security Team (EAST) estimated that there were 383,951 ATMs in Europe and more than 1.5 million ATMs around the world ([1]). Seventy-two percent of the total number of European ATMs is located in five countries: UK, Spain, Germany, France and Italy. The total number of European ATMs has increased by 6 % from the previous year.

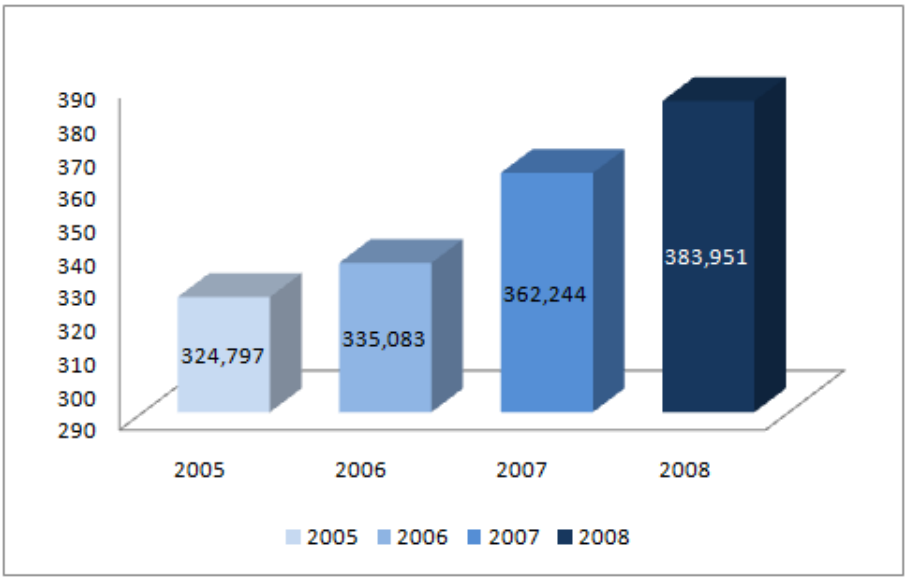
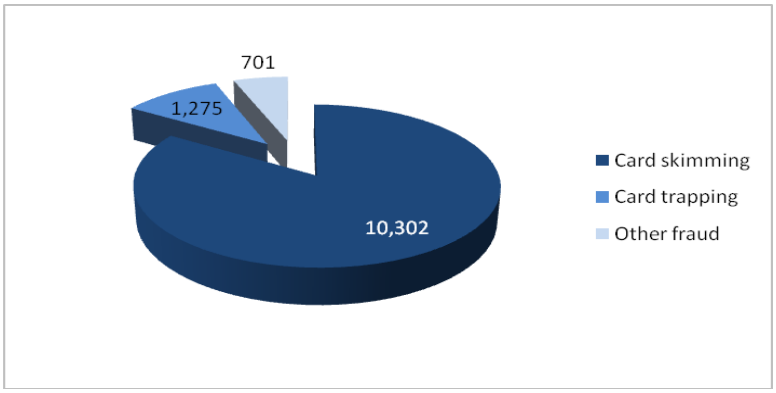


Figure 1: European ATM numbers. Source: EAST & EPC.

([1]) *https://www.european-atm-security.eu/Welcome%20to%20EAST/*
According to an EAST poll relating to the use of ATMs, which was conducted in May/June 2009, 49 % of the respondents had a basic knowledge of likely risks and threats but needed more information, while 14 % of the respondents were unsure of the risks and threats and would value guidance in how to identify them.

ATM crime and its financial impact in Europe

With the growth in the number of ATMs there has also been dramatic growth in ATM crime. A recent report released by EAST says that in 2008, fraud related ATM crimes in Europe jumped 149% when compared with the previous year. According to the report, this increase in ATM fraud is linked primarily to a dramatic increase of so-called ATM-skimming attacks. During 2008, a total of 10,302 skimming incidents were reported in Europe. However more disturbing are recent reports of attacks that are leveraging readily available and advanced malware ([2]) that has infected the ATM networks and ATMS themselves.



According to the same report, physical attacks on users of European ATMs have fallen by 29 % mainly because of a decrease in the number of reported robberies. However cases of ATM physical attacks against the ATMs themselves have risen by 32 %. While the cash losses for such attacks are lower than other ATM crimes, these attacks continue to remain of great concern to the industry.

Figure 2: ATM related fraud attacks by number of incidents 2008 (full year). Source: EAST & EPC

Despite the dramatic increase of incidents, the actual losses due to fraud increased only 11 % when compared to the previous year. The losses due to ATM fraud were still significant and a total loss of almost EUR 500 million was reported last year despite the countermeasures taken in all European Countries. Figure 3 shows the loss breakdown in more detail.

Of this loss nearly EUR 400 million was due to international losses, which is the result of fraud committed outside national borders by criminals using stolen card details. These losses are mostly occurring outside Europe primarily due to the rollout of EMV ([3]) technology in Europe.

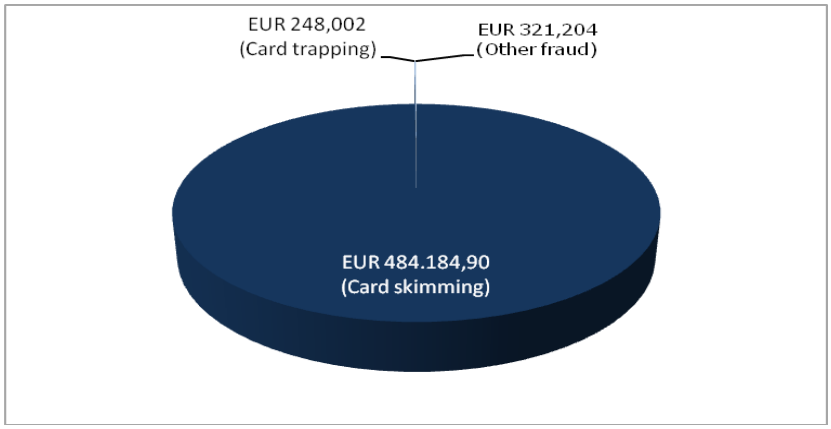


Figure 3: ATM related fraud attacks by total reported losses 2008 (full year). Source: EAST & EPC

([2]) Malware is software that is designed to infiltrate or damage a computer system without the owner's informed consent.

([3]) EMV is a standard for interoperation of IC cards and capable POS terminals and ATM's, for authenticating credit and debit card payments. The name EMV comes from the initial letters of *Europay*, *MasterCard* and *VISA*, the three companies which originally cooperated to develop the standard.

Estimated losses worldwide

The U.S. Secret Service estimates that annual losses from ATM fraud totalled about USD 1 billion or USD 350,000 a day in 2008.

In 2007, the cost of credit and debit card fraud in the UK soared to a record high of GBP 535 million. APACS reported that card fraud increased by 14 % in 2008 to almost GPB 610million. ATM specific fraud increased by 31 % and accounted for GBP 45.7million in losses in 2008.

Among recent incidents worldwide

Cases of ATM crimes continue to occur globally. Incidents have been reported not only in Europe but also in Asia-Pacific, the Americas, Africa, Russia and the Middle East. Some examples include:

- ✓ USD 500,000 were stolen from an Australian bank using a skimming device attached to an ATM in Melbourne ([4]);
- ✓ Devices capable of scanning bank and credit cards details were placed on cash machine outside a supermarket in UK ([5]);
- ✓ Ten ATMs were used to clone cards and steal more than USD 1 million from banking accounts in Melbourne ([6]);
- ✓ USD 500,000 were stolen from more than 250 victims in Staten Island by placing cameras directly onto the ATM keypad and filming victims typing in their PIN codes ([7]);
- ✓ Around 4,000 pages of data containing Cypriot credit cards were found on a computer belonging to thieves ([8]).

Types of ATM crime

A definition

ATMs are attractive to criminals because they provide direct access to currency, bank notes, and in some cases even user's personal information which can be used for identity theft. While an ATM may contain a significant amount of currency, bank cards themselves can give thieves access to customers' bank accounts which can easily exceed the value of the money contained in a single ATM. A stolen card, provided that the PIN has also been obtained, can be used by criminals to withdraw money from a bank account until the daily withdrawal limit is reached, or the card is blocked by the issuer. While thieves continue to attack ATMs and the currency they contain, they have increasingly focused on ways to collect bank card information and expand their gains.

([4]) 'ATM scam nets Melbourne thieves $ 500,000', 24 March 2009, available at *http://www.atmmarketplace.com/article.php?id=10808* (last visited on 20 April 2009).
([5]) 'Shoppers are targeted in ATM scam', BBC News, 11 March 2006, available at *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.*stm (last visited on 20 April 2009).
([6]) 'Australian police suspect Romanian gang behind $ 1 million ATM scam', 14 April 2009, available at *http://www.atmmarketplace.com/article.php?id=10883* (last visited on 20 April 2009).
([7]) 'ATMs on Staten Island rigged for identity theft; bandits steal $500G', 11 May 2009, available at http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D
([8]) 'ATM scam targets hundreds of credit cards', New Europe, issue: 793, 4 August 2008, available at *http://www.neurope.eu/articles/89221.php* (last visited on 20 April 2009).

There are three basic types of ATM attacks:

- ✓ Attempts to steal a customer's bank card information;
- ✓ Computer and Network attacks against ATM's to gather bank card information;
- ✓ Physical attacks against the ATM.

Theft of customer's bank card information

The main focus of ATM crime is the theft of the data stored on the bank card. Until recently bank cards used a magnetic stripe to store information to identify the customer and a PIN code to authenticate them and allow them to perform transactions at an ATM. Unfortunately the magnetic stripe information is simple to copy and counterfeit. As a result thieves have focused on methods of collecting this information.

This weakness has been partly addressed by the introduction in Europe of EMV smartcards (also known as Chip and PIN cards or Chip cards). According to EAST, 90 % of European ATMs are now EMV compliant.

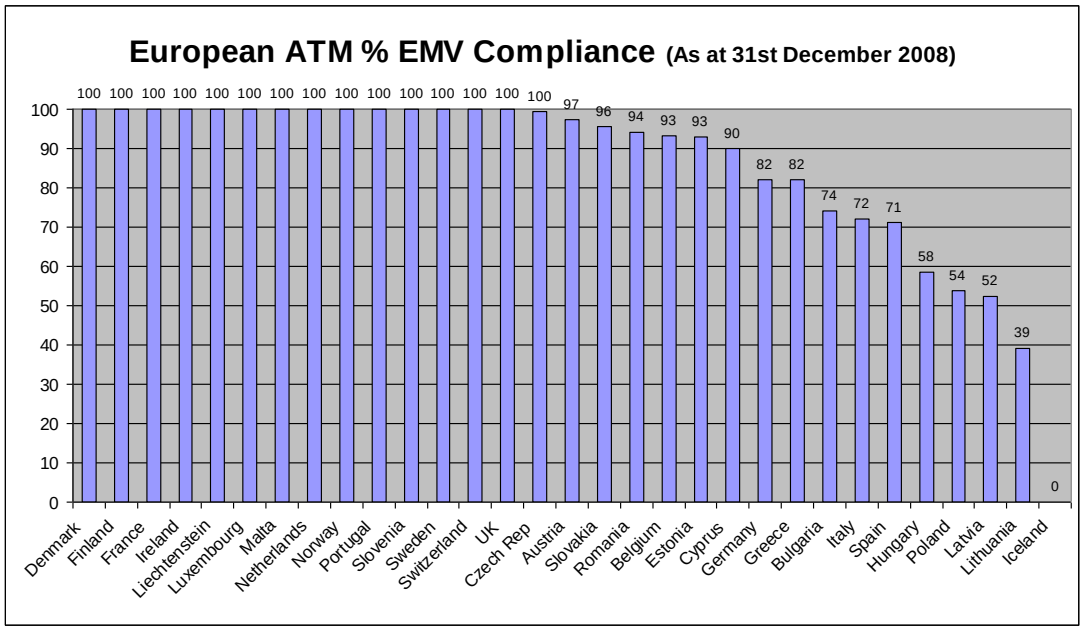


Figure 4: European ATM % EMV compliance. Source; EAST & EPC.

While these cards also have magnetic stripes, the magnetic stripe alone is not sufficient to allow a transaction to take place at an ATM with a card reader that has been modified to read an EMV Chip (unless the card issuer allows such a transaction takes place). Thus counterfeit copies of these EMV cards cannot be used to withdraw cash from EMV compliant ATMs.

As most of Europe will have EMV compliant cards by the end of 2010, this means that criminals will have to use counterfeit cards outside of Europe and in countries where ATMs do not have EMV compliant ATMs. Until that time, however the threat of counterfeit bank cards still exists.

Card Skimming

This is when the card magnetic stripe details and PIN are captured at the ATM by a modified card reader known as a skimming device. The skimming device is placed on the ATM in such a way that disguises its presence but allows it to capture the information on the magnetic stripe of the card and the input of the customer's PIN. The customer inserts their card into the ATM that has been modified with a skimming device, performs a normal transaction, and retains the card. The customer leaves the ATM unaware that their card has been compromised. The captured information is then used to produce counterfeit cards for subsequent fraudulent cash withdrawals. The customer will only become aware of the fact when unauthorised cash withdrawals/transactions are made from their bank account. Because the skimming devices are very sophisticated, and often difficult to detect, multiple cards are compromised.

Several different methods are used by criminals to do this, and the PIN is obtained either by the usage of a small spy camera, or by a PIN pad overlay (false PIN pad). Increasingly blue tooth wireless technology ([9]) is used to transmit card and PIN details to a laptop at a remote location. This information can then easily be sent anywhere in the world to allow the fast production of counterfeit cards.

Typical methods used to skim cards

A small skimming device placed over the mouth of the card reader (or a false panel over the card reader), with a fake PIN pad overlay (or a small spy camera) to capture the PIN.

Figure 5: Image is Courtesy of EAST

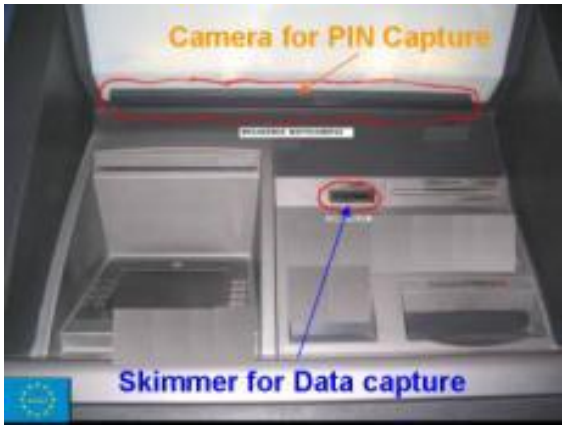


Figure 6: Image is Courtesy of EAST

([9]) Blue tooth technology enables electronic devices to communicate with each other by using a short-range radio link.

A complete false front panel is placed over the fascia of the ATM.

Figure 7: Image is Courtesy of EAST

A skimming device placed in a card reader designed to open the door of a bank lobby (typically the camera used to collect PINs will be located above the ATMs in the bank lobby).

Figure 8: Image is Courtesy of EAST

Skimming devices can also be mounted beside the normal ATM card slot with a sign that says, "slide card here first.", although this is not so common in Europe.

Figure 9: Image is Courtesy of Naples Police Department

Fake ATM machines

Criminals have been known to place fake ATM machines in and around shopping centres and other public locations. These look like real ATM machines, and some have even been known to dispense cash. All cards used at these machines are copied, and the PIN information is obtained from the PIN pad. As these machines are not connected to a network, the criminals can place them anywhere there is a power source.

Recent ATM skimming incident

In April 2009, a 33-year-old Microsoft employee, who lives in New York City, stopped in the closest Chase bank to get some cash to pay his barber. When he inserted his ATM card in the machine, he noticed a bit of resistance. The screen said the machine was unable to read his card. So he tried again. But a second time, the machine gave him an error message.

He was about to give up and try another machine, when a thought popped into his head. He had heard about devices that fraudsters attach to the outside of card readers on ATM machines and, though it seemed unlikely, wondered if that was the source of his problem. He tried to pull on the green plastic surrounding the card slot and found that it peeled right off. Behind an extra mirror attached to the machine, he also found a hidden camera positioned right over the key pad, to capture the PIN codes as victim's type them in ([10]).

Figure 10: Skimming incident.

Card trapping

This is when a card is physically captured by the ATM combined with any number of methods used to capture the customer's PIN. When the customer leaves the ATM without their card, the card is retrieved by the thieves and used to make fraudulent cash withdrawals or to make other purchases (either in store, telephone, or online). Typically only one card is lost in each attack. The criminals have to withdraw the whole device each time a card is trapped, although recently a card trapping device has been seen that can stay in place for a period of time and that allows removal of trapped cards without the removal of the device.

The most common variant is known as "Lebanese Loop". Thieves place a device fitted with a loop of tape, wire, or strong thread over an ATM card reader. This allows a card to be inserted and read by the ATM, but not returned. The criminals obtain the PIN by watching the user entering the PIN (shoulder-surfing), and retrieve the card after the victim has left the ATM under the impression that the card has been retained by the ATM for other reasons.

There are multiple techniques used to capture the customer's PIN including the use of video cameras, offering advice and distracting the customer while they input their PIN. Another variant of card trap is known as the Algerian V.

Distraction theft or 'manual' skimming

This is similar to card trapping, the difference being that instead of a trap capturing the card it is actually removed from the card reader by the criminals. Having observed the entry of the PIN, a group of criminals distract the user and cancel the transaction. While two criminals keep the user busy (often by dropping a bank note and asking the user if belongs to the user) another criminal hits the stop key and takes the customer's card. When the user turns back to the ATM they are informed that the ATM is faulty and will not return their card.

([10]) http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

Shoulder surfing

This is a method used by criminals to obtain a PIN, typically when trapping cards, or when stealing cards by distraction theft. Standing behind the victim, a criminal reads the PIN as it is entered and either memorises it, writes it down, or enters it straight into a mobile phone.

Leaving transaction 'Live'

This when a criminal completes an uncompleted transaction after the victim has left the ATM. This is typically done by making the victim believe the ATM is out of order while they are in the middle of a transaction, or any other means of moving the victim away from the ATM while in the process of withdrawing funds.

A recent incident in the USA

Two men robbed unsuspecting customers of USD 1800 in cash within half an hour of stealing their ATM cards in the middle of a transaction. In one of three known robberies, police believed the criminals walked less than two metres to a neighbouring ATM and withdrew USD 900 in three separate transactions, all before the victims made it into the bank to cancel their card. On another occasion, the pair stole USD 900 through credit card transactions and cash withdrawals within half an hour of stealing a bank card.

Police believe the first offender watches a bank customer enter their PIN into the machine and keys it into a mobile phone. The second offender then distracts the customer by dropping a USD 20 note at their feet and tapping their shoulder, while the first offender steals their card as it is ejected from the ATM. The stolen card is used in another machine, leaving the ATM customer to wonder why the machine has not returned his card ([11]).

Cash trapping

Criminals fix a device to the cash-dispensing slot, causing notes to get stuck inside when customers attempt to do a withdrawal. The customer leaves assuming that the machine is out of order or goes inside the bank to report the incident and the thieves return to retrieve the notes.

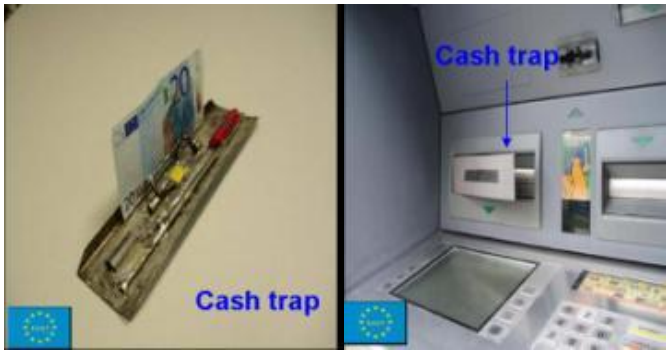


Figure 11: Images are Courtesy of EAST

Computer and network attacks

The Internet provides world-wide access and connectivity. It provides each of us access to individuals around the globe. It also provides thieves with access to systems and people. This threat manifests itself the same way.

Network attacks against ATMs

ATMs communicate with the banking systems through a network connection. Some of these connections use private networks and proprietary network protocols but more often these connections now occur via the Internet and using standard network protocols. Thieves will use

([11]) Robinson G., 'Bondi banks scam: ATM alert', *The Sydney Morning Herald*, October 2008, available at http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (last visited on 2 July 2009).

computer programs (malware) to attack the ATM in order to gain access through a software or computer flaw. Once they have gained access to the ATM, the thieves will install software that collects card information and PINs. An ATM that has been compromised is not physically recognisable from one that has not and often users will be unaware of the danger.

Viruses and malicious software

ATMs often now use publically available operating systems and off the shelf hardware and as a result are susceptible to being infected with viruses and other malicious software. The malicious software is injected into the ATM through network attacks, or through other infected devices. Once installed on the ATM, the malicious software will collect card information and PINs.

Recent incident

In April 2009, ATMs in Russia were discovered to have been infected with sophisticated malware. The malware was able to not only collect card details but also the PIN. While one specific ATM vendor's machine was successfully targeted, intelligence reports received in March indicated attempts were made to infect other vendors ATMs ([12]).

Phishing

Fraud and scams using mail communication have existed for many years. With the advent of email and the Internet this scam has quickly spread worldwide and earned the name "Phishing". Phishing scams are designed to entice the user to provide the card number and PIN for their bank card. Thieves will send an email representing them as a bank and claiming that your account information is incomplete, or that the user needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and directs the user to a site set up by the thieves and designed to look like the user's bank. The site directs the user to input sensitive information such as card numbers and PINs. The information is collected by the thieves and used to create fraudulent cards, withdraw funds from the user's account and make purchases.

PIN cash-out attacks

Thieves use sophisticated programming techniques ([13]) to break into websites which reside on a financial institution's network. Using this access, the thieves access the bank's systems to locate the ATM database. The thieves collect card numbers, and if necessary, alter the PIN for the cards they are planning to use. The thieves then sell the cards and their data to other thieves. Those thieves create ATM cards using the stolen information, and use the cards to withdraw cash from the accounts. The original thieves usually receive a percentage of the proceeds.

Recent incident

During January and February 2008, the US Secret Service has revealed that they were investigating two breaches - one against OmniAmerican Credit Union and the other against Global Cash Card. In April and May of 2008, it is also known that there were breaches of this nature against Symmetrex, a transaction processor, and 1st Source Bank. Symmetrex cards were used by MetaBank. Actual losses of more than USD 4 million were experienced just by those brands ([14]).

([12]) http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html
([13]) *Thieves use SQL injection techniques.*
([14]) http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

Physical ATM attacks

ATM physical attacks are carried out with the intention of gaining access to the cash within the ATM safe or the ATM security enclosure. Some of the most common methods include ram raids, explosive attacks (gas and non-gas) and cutting (e.g. rotary saw, blow torch, thermal lance, diamond drill). Robbery can also occur when ATMs are being replenished or serviced. Staff are either held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cassettes replaced.

Security implications

What happens when a customer's details have been captured?

Once criminals have captured card numbers and PINs, the information can be used in any number of ways. The details from compromised cards can either be used to make withdrawals from the customer's bank account, or the card details can be used to make purchases in retail outlets, over the Internet or over the telephone. Counterfeit credit and debit cards can be made for use by other individuals.

The criminals normally operate in highly organised gangs and can be acting on behalf of larger criminal syndicates. There has been a recent upsurge in criminal gangs coming from overseas to carry out such deception.

Risks and threats

Summarising the potential risks and threats that citizens could face following a successful ATM crime is a significant task. This is mainly because a successful ATM crime may not only result in unauthorised access to a victims' bank account but it could also equip the criminal with the information and tools to commit a broader variety of offences ranging from simple impersonation frauds to more complex identity related frauds such account take over.

This is perhaps best illustrated by considering the growing range of services that are available via the typical ATM served bank account. If, for example the details of your debit card were compromised together with the PIN, the criminal may then have the ability to access, not only funds from your account but they could potentially perform a range of account management functions specifically directed at the commission of further offences.

As a result, the number of risks and threats are almost infinite, however at the highest level there are two broad categories of risks and threats to be considered.

The first risk category centres around more immediate forms of attack such as note traps, the Lebanese Loop where the victim's bank card is immediately obtained by the criminal, or direct physical attacks on either ATM users or the ATM's themselves for example pick pockets or ram raids.

The second risk category is focused on longer term damage and is arguably the most prevalent due to the broad range of attack signatures. This type of crime invariably results in the subsequent exploitation of the information and identity of the victim although there are also often primary gains such as immediate access to funds. A range of frauds including identity theft, account takeover and extortion may result and for the victim, apart from the financial losses, there are often undesirable impacts such as impaired credit ratings or adverse court judgements.

Looking ahead, ATM crime is likely to become even more attractive to the criminal, as the types of services and products that are delivered via the latest generation of ATM's continue to develop and

evolve. As well as increasing numbers of ATM's being designed to take a variety of different types of deposit for example cash and cheques, many are now being used to dispense other products which will also be attractive to the criminal, such as postal stamps. In these circumstances it is reasonable to expect that the variety of attacks will also keep evolving and ATM crimes in all their different forms will continue to be a cause for concern thus making the need for public awareness all the greater.

Security implications for ATM cardholders

ATM fraud has become more technically sophisticated and criminals have found new and innovative ways of withdrawing money from cash accounts using fake or counterfeit cards with real cardholder data on them. Although the criminals' methods of getting to the money have become more advanced technically, the issues for the cardholders are still the same as they were when ATM fraud first became a major issue.

The main aim for account holders is to keep their money safe in the bank. Information security has, for too long, been focusing on technical solutions to maximise protection. With regard to ATM security incidents over the recent years, the human element has increasingly attracted more attention. Cardholders must be aware of the risks they are exposed to and how to prevent fraud occurring, or what to do to minimise the damage should their card details fall into the wrong hands. ATMs are used by criminals both to gather card information and to fraudulently withdraw money from customer accounts. Cardholders must constantly be aware of both issues when using their cards, when observing people withdrawing money, and when checking their own bank statements.

Card protection

Cardholders must be aware of the risk to their cards, and also of how they can help to prevent money being withdrawn fraudulently from other cardholders' accounts.

The first sign of something not being quite right is when a cardholder visits the ATM. It is important for cardholders to be aware of their surroundings; to stand close to the ATM and shield the key pad to avoid anyone seeing them enter their PIN. The best way for cardholders to protect their own card and card details is to be alert when using an ATM. For example, using the same ATM regularly will make cardholders aware of how the ATM should look and to observe normal, expected behaviour. Should there be anything unusual with the machine, cardholders must ensure that they don't use the machine and notify their bank of their observations and suspicions.

Personal protection

If cardholders see suspicious behaviour around ATMs, then it is important that they immediately notify the bank if possible. It is important that they never try to further investigate a suspicious looking ATM or one that is not behaving as expected; fraudsters are often close by, and may try to intervene, should anyone start to investigate the ATM more closely. There are examples of situations where ATM cardholders have been physically assaulted when trying to find out what may be wrong with the machine. Be aware of other people around the ATM; if you see someone is behaving suspiciously or it feels uncomfortable to be using an ATM, then pass your suspicions and observations on to the bank and use another ATM.

Protecting your PIN

Fraudsters use many different methods to get to card details, and the first line of security to protect cardholders from being defrauded is to ensure nobody knows the PIN. When fraudsters get to know the PIN they can easily get to the money. ATMs do not have the same security measures all over the world, and it is a good rule for cardholders to change their PIN every time they've been abroad. Fraudsters will also try the PIN they have to access accounts on other cards, so a good rule is always to have a different PIN for different cards.

ATM card details and the Internet

Another way of gaining access to personal banking and authentication details e.g. PIN numbers is via the Internet. Once this information is obtained duplicate cards can be produced. Phishing incidents, where cardholders receive an email asking them to click on links and provide bank and personal details, are on the increase. The emails often come from sources that look legitimate, because the fraudsters have found very sophisticated ways of simulating correspondence between cardholders' banks such that it may sometimes be difficult to spot a fraudulent message. A good rule is never to click on hyperlinks received by email asking to confirm bank details. Another good rule is to use good anti-virus and firewall software on the PC used for Internet banking.

Other security precautions

Another security precaution might be to investigate the use of rechargeable banking cards that have limited amounts of money put on them. This will prevent the fraudsters from withdrawing a huge sum of money that a cardholder may have deposited in a bank account.

Moreover, consumers should also be vigilant when providing bank details over the phone as someone nearby may be listening in. Always try to find a quiet area when contacting your bank using the phone.

To enable to spot a fraudulent withdrawal, a cardholder should regularly check his bank transactions and account balances.

Keep the bank's emergency number at hand

The fraudsters will try to withdraw money as quickly as they technically can, after they have gained access to card details and PIN numbers. It is important to notify the bank and sometimes the local law authorities as quickly as possible after a cardholder suspects that his PIN and/or card details have been disclosed, to enable the bank to put a block on the account(s) thus preventing fraudulent withdrawals. Keeping the bank's emergency line details always to hand is crucial; remember that with when a card has gone missing, the emergency number will also be lost if it is not written it down somewhere safe. Also, find out which number to call from abroad, as the number used at home may not work from a hotel switchboard.

PART 2: GOLDEN RULES

Golden rules to reduce ATM crime

These safety tips draw on analysis of data and available research. This section of the paper is intended to provide, in one convenient place, recommendations to raise awareness about the various types of crimes being carried out, with advice on how to spot them.

These rules offer maximum protection for the least amount of effort. By following these rules interested parties will increase their protection when they using an ATM.

Category	#	Recommendations	Description
Choose a safe ATM machine	1.	Don't use ATMs with excessive signage or warnings	Don't use ATMs with excessive signage or warnings posted on the machine as they are often used by fraudsters to try and assure the public that ATMs that have been tampered with are safe. Be especially cautious of unusual instructions on how to operate the ATM.
	2.	Use ATMs inside banks	When possible use ATMs inside banks, other buildings and enclosed areas, rather than on the street. ATMs on the street are easier for criminals to access.
	3.	Don’t use free standing ATMs	Avoid free standing ATMs that are in the open. Avoid ATMs that are not bolted to the side of a building or secured inside a facility. If the machine offers no fees but it is attached to a building and everything processes properly, you are probably fine.
Observe your physical surroundings	4.	Be aware of the surroundings	Always be aware of your physical surroundings. Use an ATM which is in clear view and well lit. Be extra careful of machines in dark areas or in places that don't look well guarded and monitored.
	5.	Check that people in the queue are at reasonable distance	Check that other people in the queue are a reasonable distance away from you. Be cautious if strangers offer to help you at an ATM, even if your card is stuck or you’re having difficulties. Do not allow anyone to distract you.
	6.	Protect your PIN by standing close to the ATM and shielding the key pad	Shield the keypad with your hand as you enter your PIN to prevent a hidden camera or a person from capturing your information. Never reveal your PIN to anyone.
Observe the ATM	7.	Pay attention to the front of machines	If the front of the machine looks different from others in the area (for example, it has an extra mirror on the face), has sticky residue on it (potentially from a device attached to it) or extra signage, use a different machine and notify bank management with your concerns.
	8.	Pay close attention to the slot you slide in your card	If you're visiting an unfamiliar ATM machine that is not inside a bank, examine it carefully for devices. Even if you are familiar with an ATM machine, pay attention to any differences or unusual

Observe the ATM			characteristics of the card reader. If the slot looks strange or bulky, try to push on it with your hand. If something has been stuck over the real reader it will wiggle or even come off. Card or cash trapping devices need to be glued or taped to the card reader or cash dispenser. If the ATM appears to have anything stuck onto the card slot or keypad, do not use it. Cancel the transaction and walk away. Never try to remove suspicious devices.
	9.	Pay close attention to the ATM's PIN pad	Even if you are familiar with an ATM machine, pay attention to any differences or unusual characteristics of the ATM's PIN pad. If a fake PIN pad has been stuck over the real pad it will appear "incorrectly attached" when being moved a bit back and forth.
	10.	See if there are extra cameras	Look for 'extra' cameras beyond the basic and generally obvious ATM security camera.
	11.	Report confiscated cards immediately	Report confiscated cards immediately. If you can, don't leave the machine. Instead call the bank from the ATM where your card was taken. Never rely on the help of strangers to retrieve a confiscated card. In addition notify your local law enforcement.
	12.	Beware if the ATM does not dispense cash or charge fees	If you use an ATM that doesn't dispense cash, it is much more likely to be a fake and you should notify your bank of the potential risk to your account. If you are using an ATM that is not associated with a bank (often in service stations and bars) beware if it does not charge you a fee. Private ATMs that are not associated directly with banks make their money through fees. Not charging a fee is an indication that the ATM may be fraudulent.
Review your statements	13.	Frequently review your account statements	Review your card statements frequently for any activity you do not recognise. While most fraud happens quickly, some may not occur for weeks or months after your card information is captured. Frequent reviews will help reduce the potential impact of any fraud.
Report suspicious activity	14.	Report confiscated cards immediately	Report confiscated cards immediately. If you can, don't leave the machine. Instead call the bank from the ATM where your card was taken. Never rely on the help of strangers to retrieve a confiscated card. In addition notify your local law enforcement.
	15.	Report any suspicious activity immediately	If your bank card is lost or stolen, or if you notice fraudulent activity in your account, report it immediately in order to prevent any further loss.

Conclusions

ATMs are an important part of commerce throughout Europe and provide a valuable service to customers. With the growth of the use of ATMs there has also been a dramatic increase in ATM attacks and fraud. Techniques such as skimming, phishing, and network attacks against ATMs have caused nearly EUR 500 million in losses in Europe last year. These techniques have become more sophisticated over time, and have resulted in a 149 % rise in ATM attacks during 2008.

This paper has presented numerous ways that ATM attacks are carried out, as well as simple techniques and guidance that ATM users can use to detect and prevent against these attacks.

ENISA believes that an important step to reducing ATM fraud and attacks is to raise the awareness of likely threats and ways in which to counter them. This information can significantly reduce the incidence and financial impact of ATM attacks, and result in improved confidence in the use of ATMs.

APPENDIX

ATM usage and fraud: case studies

ENISA gathered some case studies and experiences from a few European countries dealing with different ATM usage and fraud, to enable readers to identify key problems, issues and solutions, making the suggested rules more effective and presented in concrete ways.

Cyprus

Currently on the island (in the part that is controlled by the Republic of Cyprus), about 560 ATMs are installed. There is no information about the number or type of ATMs installed in the Turkish Occupied area of the island. The majority of the 560 ATMs are installed as through-the-wall. A number of 2-3 ATMs are installed as cash-kiosks. A significant number of ATMs installed on the island are equipped with special plastic shields at the card slots , plus an anti-skimming device to prevent the placement of skimmers (and the subsequent capture of Magnetic Stripe information), which could play a significant role in eliminating the card skimming cash machine fraud ([15]).

Recent incidents occurred in Cyprus

The following information was captured by the JCC Payments System Ltd Fraud Monitoring System.

Case No. 1

Some individuals were using counterfeit, top up and re-encoded cards at ATMs. 26 cards were used and EUR 2,310.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. One fraudster was arrested at the airport.

Case No. 2

Two individuals were using counterfeit, top up cards at ATMs. 131 cards were used and EUR 15,830.00 was withdrawn. The individuals were arrested by Police while using counterfeit cards and after the fraud monitoring system identified them.

Case No. 3

An individual was using counterfeit top up cards at ATMs. 43 cards were used and EUR 1,860.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudster was arrested.

Case No. 4

Two individuals were using counterfeit top up cards at ATMs. 76 cards were used and EUR 7,950.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudsters were arrested.

Case No. 5

Several individuals were using counterfeit top up cards at ATMs. 53 cards were used and EUR 10,700.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. One fraudster was arrested.

([15]) All the information disclosed are provided by the Risk Management department of JCC Payments Systems Ltd, the sole acquirer/processor of Cyprus for VISA, MasterCard, AMEX and Diners.

Case No. 6

Two individuals were using counterfeit top up cards at ATMs. 122 cards were used and EUR 21,980.00 was withdrawn. The individuals were arrested by Police while using the counterfeit cards and after the fraud monitoring system identified them.

Case No. 7

An individual was using counterfeit top up cards at ATMs. 41 cards were used and EUR 28,340.00 was withdrawn. The individual was arrested by Police while using the counterfeit cards and after the fraud monitoring system identified him.

Case No. 8

An individual was using counterfeit top up cards at ATMs. 82 cards were used and EUR 12,330.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudster was arrested.

Case No. 9

Two individuals were using counterfeit top up cards at ATMs. 21 cards were used and EUR 10,980.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudsters were arrested.

Risks and threats

ATM fraud development

ATM fraud activity is steady and decreasing in 2009 mainly due to the EMV chip rollout within Europe and the effective and proactive fraud counter-measures as used in Cyprus.

An increasing number of fraudsters have been identified. The main reason for that is they wrongly assume that Cyprus is a country with limited technological advancement (Limited EMV terminals and Weak Card Monitoring Systems) and it is Europe's most distant island which is consider by fraudsters as a place in which they cannot be caught. In fact there is only one acquirer so it is much easier to get caught in Cyprus, whereas in the UK or Greece where there are 5-6 different acquirers that do not share data between them it is much more difficult to get caught

ATM fraudsters capabilities

Fraudsters identified on the island were characterised by an intelligent approach during the commitment of fraud and showed great ability to circumnavigate the banks' security defences. They also act resourcefully and seem much organised. Furthermore, fraudsters' skimming technologies are superseding vendors' technologies (e.g. 'Jitter', 'FDI').

ATM fraud impact

Fraud is currently affecting the 'brand integrity' and cardholder confidence; however it is compensated by the Card Systems' actions as these effectively counterattack the fraudsters' actions during a credit card fraud case.

Italy

In Italy the ATMs are mainly used with debit cards, which allow the immediate withdrawal of cash from the bank account and also payment and query features such as telephone charges, information retrieval on the personal account, donations, etc. The BANCOMAT circuit (main Italian debit card circuit) and its protocols were designed more than twenty years ago and, even though today they are evolving towards new concepts, security issues are still present related to design choices and solutions applied to technologies that nowadays are dismissed in favour of more modern ones.

The first cards of this type, still widely used, are based on a magnetic strip on which various information are stored. Authentication is based on a PIN code of 5 digits, which is given directly by the bank. However, in the recent years, the companies managing the circuit are trying to replace these cards with the new chip-based generation ones (smart cards), more robust with regards to cloning attempts. The whole environment is evolving: the old ATMs based on proprietary systems are being replaced and the new ones provide advanced functionality, such as multimedia content, payments with the automatic recognition of notes, touch screen, keyboard and more extensive opportunities for customisation of the operational software.

All ATM devices are controlled by closed circuit video surveillance equipment to avoid physical attacks like using cranes to uproot the ATMs from their basement, using stolen cars as rams or placing explosives. Sophisticated systems of attack are using a false front-end with a "skimmer" to clone the card. Italian Banks, to limit the damage of theft (in addition to the cost of the ATM system, which is still high), supply ATMs with only the strictly necessary cash amounts, and with devices that permanently alter the notes (colour ink, etc.).

Until today, those frauds carried out in Italy were mainly limited to the categories described above, since there have not been any documented logical attack on the ATMs. Nevertheless, it is possible to assume that in the near future this trend will dramatically change.

One of the main problems encountered while working on the security of ATMs, is related to the number of players in the field: often the communication between these parties is weak and it is not easy to understand if a bug is due to the hardware manufacturer (ATM vendor), to the software manufacturer, to the protocols being used or to the configuration of the ATM infrastructure itself.

Methodologies used during attacks

The latest generation ATMs are basically industrial PCs with specific serial connections or USB devices (PINPAD, dispenser for notes, keyboards more or less customised, etc.) communicating with the bank via IP or via SNA protocols (now encapsulated over IP). Banks have also saved money by reducing investments in dedicated data lines decreasing the security of the ATM systems themselves. It has often been pointed out that these devices are directly connected to the internal network (LAN) of the bank or to the branch network and are rarely separated from the network segment where there are other corporate systems (from the workstation to the server systems).

Generally speaking, ATM systems are used as industrial equipment and not as ordinary computers. This also means that, once installed, are rarely updated and poorly managed. Furthermore, as industrial products, patches of the operating system (mainly Microsoft

Windows) first have to be tested, licensed and distributed by the manufacturer, introducing an additional obstacle. This choice exposes ATM systems to various types of well-known threats, such as worms and viruses, which could compromise the infrastructure, resulting unavailable (e.g. the mass crash of Diebold ATMs in 2003, due to the Slammer worm). An agent of external or internal threat to the bank could also attack the systems by exploiting vulnerabilities in the operating system, software or password management (often, "known") to access the ATM and modify the software in order to provide more cash, if specific conditions are met.

Moreover, the analysed communication protocols have revealed numerous security problems. Although in the recent past newer and safer-considered specifications have been released, usually are not fully implemented. For example, communications between the ATM and the back.end (mainframe, etc) are often not encrypted and there are no features that will ensure the legitimacy of the data. During some attack sessions it has been demonstrated how it is possible to intercept and edit these notifications, allowing the attacker to withdraw more money than the account current availability, or modify the amount of withdrawn money.

From the different analysis carried out, another serious problem was found (that also exacerbates what done before), which is the placement of ATM systems: in case of mobile ATMs located in unprotected areas, the power connections and network links are often accessible by the end-user (even if the ATM is located inside the bank). An artificial lack of power would cause a reboot of the system, providing several information to the attacker; on the other hand the possibility to reach network cabling could allow installing a TAP system able to intercept network traffic and forward through a wireless network.

In order to better understand how many security issues are possible, not just related to technology, we can think about how ATM systems are deployed. They are spread throughout the country, often not transiting the banks headquarters and being installed directly at branches or at other points of interest by external parties that are provided with encryption keys.

Management procedures for those systems are usually less detailed than the ones of IT systems, even if they are now using more and more similar platforms: we are speaking about security tests after deployment, password management, security monitoring and alerting, vulnerability and patch management, malware protection and so on.

It has to be repeatedly pointed out that many of these attacks are not just aimed to debit cards but can also be effective with credit cards being used through ATMs, even if the specific impacts still have to be fully assessed.

Security issues related to the ATMs are too often not recognised, very few if no banks have conducted a formal and complete security risk assessment to their ATM infrastructures. The use of the concept of "security through obscurity" that has long gone along with dedicated devices is conceptually wrong, and is proving to be so as the global trend of bank fraud rises. More and more people are studying such infrastructures to find security issues, which could provide access to cash dispenser and to the real final aim of these new forms of organised crime: notes.

In the future logical attacks to the ATMs will almost certainly grow: overlooking these risks during this delicate, transition stage, will mean, in practice, starting to lose a definitely critical fight, much important to the national security of every country and economical system of the world.

Portugal

Portugal has one of the highest penetration rates of ATM machines *per capita* in Europe. This is, in most part, due to the advanced functionalities that are available to the population in general, including the payment of public and private services (such as gas, water, taxes or mobile phone services) or the possibility to buy tickets for concerts, apart from the more traditional financial services such as withdrawing money or consulting the balance.

In the following paragraphs, we will present an overview of the ATM network in Portugal, the main threats and types of frauds, as well as what is being done and what needs to be done in order to improve the security of the ATM environment.

The ATM network

The ATM network in Portugal is managed by SIBS, a company owned by the majority of banks that have a presence in the market. SIBS ranks as the sixth biggest automated clearing house (ACH) in Europe, processing over 2.000 million transactions / year totalling about 6.000.000 million Euros, and has been responsible for the development of an integrated ATM and POS network, common to all the banks in the market.

Regarding the usage of credit and debit cards, the Portuguese indicators are above the average in the EU, both in cards, ATM machines and POS terminals *per capita*. Also, Portugal has the highest level of card usage in Europe, when compared to other forms of payment, representing over 60 % of the transactions.

All the ATM machines in the country are now EMV compatible (Europay, Mastercard and Visa), as well as 83 % of the POS terminals. An effort is also being made from the financial institutions to make available EMV compliant credit and debit cards, representing about 44 % of the cards in the country as of 2008.

In terms of communications, the ATM network is supported by dedicated communication lines (VPN) through SSL, with additional security mechanisms in place such as 3DES encryption and MAC (Message Authentication Code). In addition to that, the philosophy behind the development of the ATM network takes a security approach into consideration, where no equipment can initiate a communication directly with an ATM machine; instead, is the ATM machine that communicates with other equipment (including SIBS systems).

PayWatch

In late 2008, a new company was formed – Paywatch – with the responsibility to monitor 24/7 the ATM network, identify card usage patterns, and detect fraud patterns at ATM and POS terminals.
This will allow Paywatch to identify frauds perpetrated with Portuguese cards and/or at the ATM / POS network in real time and rapidly limit the damages. This is only possible due the abovementioned fact that the network is integrated and can be seen as whole as opposed to a fragmented network. Not so long ago, these monitoring activities were seen by the population in general as some sort of a "Big Brother", and people could not understand why someone was looking to his/her own transactions. However, probably due to the fact that more cases are made public every year (not only in Portugal, but all over the world) the mentality has changed in the last couple of years and people now see this as an advantage to the system and as a protection to themselves and to their own money.

PayWatch is able to detect in real-time where a cloned card is being used in the ATM network, through the analysis of cryptograms – this is limited to Portuguese cards and ATM machines.

Basically, if a card is supposed to be an EMV card, but only the magnetic track is being used (fallback), the card is most likely a clone, and the transaction is rejected.

PayWatch has an overview of all the usage of Portuguese credit / debit cards, both in the Portuguese ATM network, as well as abroad. This makes it possible for PayWatch and SIBS, to block the usage of certain cards, or even block transactions from a certain area in the world, in case a surge on the fraudulent usage is detected – for example, transactions from any Portuguese card made from, say, the city of Barcelona, can be blocked.

If PayWatch detects a cloned card or other fraudulent usage in real time, SIBS or the bank can contact the client immediately and proceed with the appropriate actions in order to mitigate the risks.

Threats and fraud levels

Fraud levels in the country are generally low, with one to two situations reported a year. Physical attacks to ATM machines are the biggest threat, which grew significantly in 2008, due to the specialisation of a group of people from Eastern Europe in this type of attacks.

However, the number of unsuccessful attacks is also growing at a faster rate. This is due to the fact that an increasing number of ATM machines now have banknote ink/dye staining systems and are fixed to the ground.

In terms of attacks on cards, skimming is still the #1 threat. The copy of the card occurs at the ATM machine itself, or at the lobby of the banks where some ATMs are installed where citizens have to swipe the card to open the door, the latest representing 10 to 20 %. The PIN is usually captured through the use of a camera placed on top of the ATM machine, through a fake keyboard or through shoulder surfing.

All ATM machines in the country have now some sort of anti-skimming mechanisms. The most common is the use of a reader that slows down the entrance of the card, making it more difficult for the card to be read by a fake reader.

From a technological point of view the ATM machines could have a camera incorporated in order to try to detect if someone was placing fake equipment on top the ATM, but that is not possible in Portugal due to privacy issues, as stated by the National Commission of Data Protection.

Although the relationship between SIBS and the police is very cooperative and with mutual trust, the same cannot be said about the Justice. People, who commit fraud repeatedly, are sometimes condemned only for one particular action, and the fact that they are re-incident is not taken into account. Also, the Portuguese legislation only condemned people caught with cloned credit cards, and not debit cards which is seen as a problem given the number of this type of cards (Visa Electron) in the country.

In terms of trends, since the introduction of EMV cards, it is foreseen an increase on the usage of cloned Portuguese cards abroad, in countries where EMV is not yet fully deployed.

Towards a more secure environment

SIBS has on its website the precautions that citizens must have when using ATM or POS terminals, including, but not limited to, not losing the card from sight, do not repeat operations unless the terminal presents a message stating that the first try was unsuccessful and do not transmit the PIN to third parties. With this respect, the ATM terminal itself shows a message to the user to protect and hide the introduction of PIN from third parties.

The introduction of banknote ink/dye staining systems helped on preventing physical attacks to ATM machines, and awareness is being made to merchants that an inked banknote is a robbed banknote – up until now, only one case has been detected of an inked banknote being used at a merchant.

Given the mechanisms that are being implemented at the ATM machines, attackers are focusing on the doors at the lobby of the banks where ATM machines are located. Any card with a magnetic stripe opens the door, making the mechanism useless in regards to controlling access to the lobby, while introducing a new vulnerable point for skimming. A button to open the door, which provides the same level of control as the one that exists today, could eliminate this vulnerable point. While the card is needed to access the lobby, people are advised to use a card to open the door, and a different one to make the transaction at the ATM machine.

Also, people are advised to use, whenever possible, the same ATM machine every time, in order to detect abnormal things (such as fake keyboards or card readers).

An increase of fraud levels at the virtual world is also foreseen. In order to tackle this issue, SIBS developed a system – MBNet – which allows for people to associate an MBNet account to a bank account, operation that can be performed at the bank. From here, when someone wants to pay for something online, it is possible to access MBNet website and generate a virtual visa card number, which has a limited amount of money available, and an expiration date due in one month.

References and sources for further reading

'ATM scam nets Melbourne thieves $ 500,000', 24 March 2009, available at http://www.atmmarketplace.com/article.php?id=10808 (last visited on 20 April 2009).

'ATM scam targets hundreds of credit cards', New Europe, issue: 793, 4 August 2008, available at *http://www.neurope.eu/articles/89221.php* (last visited on 20 April 2009).

'ATMs on Staten Island rigged for identity theft; bandits steal $500G', 11 May 2009, available at http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D

'Australian police suspect Romanian gang behind $ 1 million ATM scam', 14 April 2009, available at http://www.atmmarketplace.com/article.php?id=10883 (last visited on 20 April 2009).

http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

http://cert.inteco.es

http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

http://www.adicae.net/

http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html

http://www.computerworld.com/securitytopics/security/story/0,10801,111158,00.html

http://www.denverpost.com/headlines/ci_12276447 (last visited on 5 May 2009).

http://www.europol.europa.eu/index.asp?page=news&news=pr090731_2.htm

http://www.mydigitallife.info/2006/09/25/atm-hacking-and-cracking-to-steal-money-with-atm-backdoor-default-master-password/

http://www.theregister.co.uk/2006/11/18/mp3_player_atm_hack/

http://www.wired.com/threatlevel/2009/04/pins/

https://www.european-atm-security.eu/Welcome%20to%20EAST/

Marks P., 'Cash machines hacked to spew out card details', *NewScientist magazine*, issue number 2713, available at http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html?full=true (last visited on 8 July 2009).

McGlasson L., 'ATM Fraud: 7 Growing Threats to Financial Institutions', *BankInfoSecurity*, available at http://www.bankinfosecurity.com/articles.php?art_id=1523 (last visited on 9 June 2009).

Peretti K. K., 'Data Breaches: What The Underground World of "Carding" Reveals', *Santa Clara Computer & High Technology Law Journal*, volume 25, issue 2, available at http://www.chtlj.org/volumes/v25 (last visited on 2 July 2009).

Reuters, '*Cyberthieves steal millions from banks'*, May 2009, available at http://uk.reuters.com/article/idUKTRE54I6CK20090520 (last visited on 20 May 2009).

Robinson G., 'Bondi banks scam: ATM alert', *The Sydney Morning Herald*, October 2008, available at http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (last visited on 2 July 2009).

'Shoppers are targeted in ATM scam', *BBC News*, 11 March 2006, available at *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm* (last visited on 20 April 2009).

SIBS, 'Relatório e Contas 2008', *SIBS*, 2009, available at http://www.sibs.pt/export/sites/sibs_publico/pt/documentos/relatorioecontas/Contas_SA_2008.pdf (last visited on 5 May 2009).

Sydney Morning Herald, October 2008, available at http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950

Trustwave, *Automated Teller Machine (ATM) Malware Analysis Briefing*, 28 May 2009, available at https://www.trustwave.com/pressReleases.php (last visited on 13 July 2009).

VISA Business News, *Data Security Alert – Compromise of ATM PIN Transactions*, 3 June 2009.

Zetter K., 'ATM Vendor Halts Researcher's Talk on Vulnerability', *WIRED*, June 2009, available at http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/ (last visited on 8 July 2009).

ATM crime: Overview of the European situation and golden rules on how to avoid it

ISBN-13: 978-92-9204-023-9

Catalogue number: TP-80-09-736-EN-N

DOI : 10.2824/11262

TP-80-09-736-EN-N

ISBN-13 978-92-9204-023-9

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu