ATM

A LOOK AT THE FUTURE

AND

EMERGING SECURITY THREATS LANDSCAPE

Finito di stampare nel mese di settembre 2016 presso

Pioda Imaging S.r.l., Roma

1 Sommario

1 Executive summary

In the last few years the typology and numbers of attacks against Automated Teller Machine (ATM) systems have increased. The traditional physical attacks have given way to cyber attacks. ATMs are connected to Internet and to banks network. They often run obsolete operating systems with more or less known associated vulnerabilities. The attack tactics, techniques and procedures could vary from the physical introduction of malwares onto the hard drive, to the point of stealing prepaid card numbers from database.

ATMs deployers are aware that advanced security devices and regulatory compliance are not sufficient to face the "creativity" of criminals. Advanced Persistent Threats are seriously threaten several kinds of infrastructures and ATMs systems could be a profitable target.

The future of ATMs should consider how to update the countermeasures to the new attack typologies, above all considering the new services ATMs could deliver. The report "ATM Future Trends 2015", published by ATM marketplace and Auriga, shows U.S. consumers' interest in enlarging the ATMs services. Some examples are: check cashing at the ATM; bill payment; real-time transactions; cardless cash withdrawal using mobile app; virtual currency exchange and so on.

The ATMs market probably will not be negatively impacted by new technologies, on the contrary it could benefit from them.

The aims of this study are:

- To provide an overview of current security situation of ATMs, considering the classic and emerging threats;
- To consider the evolution of the ATMs systems and services and the security concerns it implies.
- To describe techniques, tactics and procedures of attack against ATM
- To identify potential countermeasures, useful to mitigate

the threats and vulnerability of the ATM system.
This publication is intended to share experts' recommendations in order to aware all ATMs stakeholders of security implications behind the services delivered nowadays and in the future. The aims of this study are to provide an overview of current security situation of ATMs, considering the classic and emerging threats and to analyse the evolution of the ATMs systems and services and the security concerns it implies.

This study has been conducted in collaboration with Braintech, Consorzio Bancomat, Diebold Nixdorf, Kaspersky Lab, NCR, Security Brokers.

Diebold Nixdorf provides an overview of threats scenario considering physical, logical and fraud and manipulation attacks and their impact at worldwide level. It shows a growth trends of cyber attacks and losses sustained in ATM attacks (Chapter 3).

Consorzio Bancomat describes the ATM functioning in terms of services provided by the ATM and their evolution, technology, components, network infrastructure and information flows (Chapter 4). It is clear that the majority of ATMs now offer advanced authentication services and are integrating the new technologies (IoT, contactless, biometrics, ...) exposing the ATM to new threats and vulnerabilities. For these reasons, the experts of Kaspersky Lab illustrate cyber security issues and examples of cyber pattern attacks suggesting countermeasure to prevent attacks to ATM authentication systems and cyber security challenges (Chapter 5 and 6).

NCR researchers provide the point of view of an ATM operator describing the main attack techniques actually used around the world and the strategies and solutions needed to guarantee an effective protection from attacks (Chapter 7).

Security Brokers presents a new trend of attack that in some part of the world already happens: the use of ATM as a bridge for attack (Chapter 8). The capillarity of ATM represents an opportunity to become the access point for a whole series of additional services. In future, for example, ATM could deliver e-government services to citizens. This scenario represents a new opportunity for attacks targeted to other infrastructure. In this section, experts of Securi-

ty Brokers describe possible cyber attack scenarios and suggest countermeasures.

The security compliance challenges are discussed by Braintech experts that analyse existing security standards, guidelines, regulations, laws involved, at different grades and levels, with ATMs and evaluated the standardization needs (Chapter 9).

The last part of this study provides recommendations to face all challenges described. In this section is presented the Consorzio Bancomat Security Framework, a framework based on the main international standards to contrast fraud.

2 Terms and Acronyms

ABI	Italian Banking Association
Acquirer	Party, which by virtue of a special Licence, finalises and manages transactions made with a card on devices and terminals for which they are responsible. Generally, these are Banks, Financial Intermediaries or other parties, such as Payment Institutions, authorised by the country's Central Bank to accept payment cards at POS and ATM terminals.
Applications Centre	Party that, on behalf of individual Members and by virtue of a specific agreement, is responsible for arranging the acquisition and formal control of flows / messages entered by the sender's bank and delivering them to the beneficiary if they are in the correct form or rejecting them in case of errors, with appropriate warning.
ATM (Automated Teller Machine)	Automatic counter that enables various operations to be performed, including cash withdrawals and payment and information operations and is equipped with a safe for the management of cash being paid in or withdrawn, or both function
Authentication	Procedure allowing verification of the identity of the Holder of the card or account from which payment is made. In Italian debit Circuits BANCOMAT® and pagobancomat®, the holder authenticates and expresses their intention to carry out an operation by inputting their PIN.
Authorisation Centre	Unattended terminal, which does not have banknote drawers, dedicated solely to payment operations.
Bill payment	Payment operation that responds to the specific purpose of discharging an obligation (e.g. Utilities, duties, taxes or other commercial invoice) and which is carried out through a party appointed by the creditor to handle collection (e.g. A supplier or the public administration).

Biller or Creditor Entity	Credit holder against a named party, which benefits from the bill payment.
CAP (Chip Authentication Program)	MasterCard initiative and technical specification for using EMV banking smartcards for authenticating users and transactions in online and telephone banking.
Card	Card issued by authorised parties, such as Banks, Financial Intermediaries, Payment Institutions, and Electronic Money Institutions. It is a tool that enables a series of operations (withdrawals / payments at ATMs, payments at merchants with POS, request for bank statement or other information regarding the account position). There are three types of payment cards (credit cards, debit cards and prepaid cards).
CIPA (Interbank Convention on Automation Problems)	Association established by Banca d'Italia and ABI which seeks to promote the adoption of technical standards and the performance of joint projects in the field of telematic infrastructures and interbank applications
Circuit	Set of processes and rules that enable, among others, withdrawal or card payment operations.
Circularity	Operating mode through which a Circuit allows the cardholder to make payments and withdrawals at any POS / POI and any ATM, regardless of which party manages the device.
Clearing	Activity dedicated to the development and provision of the data required for settlement
EMV	A technical standard for smart payment cards and for payment terminals and ATMs that can accept them.
ESCB (European System of Central Banks)	Comprises the European Central Bank and the national central banks (NCBs) of all EU Member States whether they have adopted the euro or not.

Holder (card holder)	Party whose name is on the physical / virtual card. The card is issued to the holder on the basis of a contract, which shows the costs applied and the procedures / conditions of its use, which will also depend on the circuits present on the card.
Host	Centralised computer systems for aggregating and processing transactions. The host would typically be operated by the acquiring processor but may be operated by the merchant. Payment terminals connect to and are "hosted by" these systems. The issuing processor's back-end transaction-processing systems are sometimes included in the definition of "host."
Issuer	Party maintaining the contractual relationship with the cardholder and responsible for the process of issuing payment cards
Kiosk	Unattended terminal, which does not have banknote drawers, dedicated solely to payment operations.
NFC (Near Field Communication)	a short-range wireless technology that enables the communication between devices over a distance of less than 10 cm.
OLCA (On Line Applications Centre) Authorisation Process	Circular authorisation process in which the authorising entity is not the Issuer but a delegated entity (typically an Applications Centre).
OLI (On-line to Issuer) Authorisation Process	Process that allows the Issuers to verify the liquidity of each account holder in real time, and to authorise payments and / or the provision of cash according to the actual availability of funds in the payment account.
OLTP (On line transaction processes)	Class of software programs capable of supporting transaction-oriented applications
OTP (One Time Password)	A password valid for only one login session or transaction and that must be used within a certain amount of time

Payment account holder	Party that has a relationship with one or more financial institutions for establishing a payment account that can be linked to one or more physical or virtual cards.
PIN (Personal Identification Number)	Secret personal code that, together with the card, identifies and validates the holder for the purpose of operations.
Settlement	Activity consisting of the transfer of cash flows within the system and carrying out the settlement of debit / credit positions against the Issuer and Acquirer.
SNA (System network Architecture)	Communication architecture established by IBM to specify common conventions for communication among the wide array of IBM hardware and software data communication products and other platforms.
System	The set of parties, infrastructure and unitary and organic processes.
Terminal manager	Approved body that manages transactions originating from terminals by carrying out routing to the authorization mechanisms (Banks or Application Centres).
Third Parties	Any organisation outside the company with any contractual relationship or agreement in place for conducting business in part or entirely carried out on behalf of the party which is its direct owner or manager
Virtual card	Means of payment similar to a physical card although not reproduced in physical form, used for internet payments.

3 ATM cyber attack trends

The retail banking business is facing many challenges, and one of its main concerns is the security of ATM fleets and financial infrastructure. A lack of security may have serious financial consequences for a bank, and losing customers' trust can harm its business even more. Especially at a time when issues such as customer experience go hand in hand with security. This is even amplified by increasing media coverage of security incidents and vulnerabilities regarding ATMs. The need for banks to protect their assets as well as their customer data is immense. However, when it comes to cash, there seems to be no shortage of criminal ingenuity. Whether it is cash or customer data that criminals intend to steal, the number and the technical level of attacks has increased dramatically over the last few years.

The availability of modern technologies additionally impacts the threat landscape. Fraudsters have access to the latest equipment like 3D printer in order to create high quality fraud devices. Moreover they can share knowledge and sell equipment or card data easily on a worldwide base.

It can be assumed that the more common and known threats like Skimming will still be present and create substantial losses for years. In addition to this, rather new and highly sophisticated logical attacks are the next challenge for the banking industry.

In 2014, the European ATM Security Team (EAST)[1] reported more than 17,700 physical attacks on Europe's some 400,000 ATMs. Total damages reached €306.5 million, up 13 percent from the year before. During the same time, EAST collected statistics for ATM malware after the first incidents were reported in Western Europe. The 51 incidents reported incurred losses of €1.23 million from 'cash out' or 'jackpotting' attacks.

In many cases logical attacks are developed by organized crime groups, which are experience in the field of financial malware tar-

[1] EAST European ATM Crime Report 2014

geting for example online banking networks. Based on this background several Malware Families like Skimer, Ploutus or Tyupkin were created and used during incidents.

Delivering protection and security is a never-ending battle, which can be costly from both a financial and time perspective. Having a clear understanding of the main threats and attack scenarios, the available countermeasure and the best practice in terms of security processes and procedures is a necessary prerequisite to put in place an effective security strategy to protect the ATM fleet and the customer and financial data. This can only be achieved by a layered approach consisting of several individual measures within an aligned security concept including hardware, software as well as processes and procedures. Single measures focusing only on hardware for example, will not offer substantial protection.

Apart from technical discussions, security awareness starting at the top level management down to the end-customer is the key factor of increasing the overall situation.

3.1 Attack categories

Essentially, ATM attack scenarios fall into three categories:

- Physical,
- Logical
- Fraud and manipulation.

Common **physical** attacks include brute force attacks where heavy equipment is used to tear out an entire ATM from the wall and high-impact attacks using gas or solid explosives or other mechanical tools are used. **Logical** attacks range from attacks to the backend and office environment of a bank with Advanced Persistent Threads (APTs) to local attacks at the ATM with Malware or Black Boxes. Known methods of **fraud** and **manipulations** of ATMs include skimming, cash and card trapping, as well as Transaction Reversal Fraud.

3.1.1 Physical attack

In the Physical attack category we generally find:

- **RAM Raid** where the ATM ripped out.
- **Burglary** when the safe is attacked in-situ
- **Explosive & Gas attack**
- **Robbery**, when the persons replenishing the ATM are attacked either when moving the cash to / from the ATM, or while conducting cash replenishment activities.
- **Other**, typically referring to vandalism and sometimes also to Cash trapping at the ATM shutter.

According to the EUROPEAN ATM CRIME REPORT 2015 [2] in Europe the total number of physical attacks to ATM has increased 32% compared to the previous year and the number of incident per year reached 7,2 per 1000 ATM in 2015. The pictures below show the trend of the physical attacks in the last years and the breakdown by incident type.

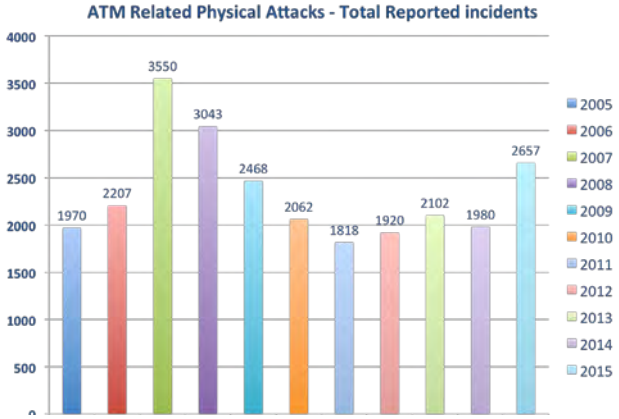


Figure 1: ATM Related Physical Attacks - Total Reported Incident 2005-2015 (source: EAST)

[2] Version: 1.1 – Issued by Lachlan Gunn; Date: 12/04/16 - PREPARED BY:THE EUROPEAN ATM SECURITY TEAM

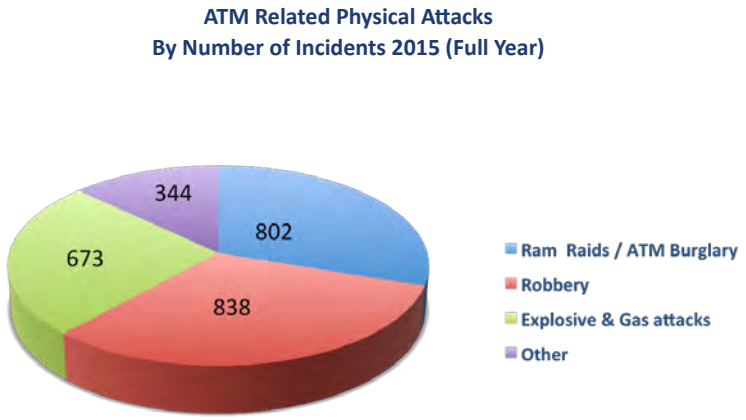


Figure 2: ATM related physical attacks by Number of Incidents 2015 Full Year (source: EAST)

Robberies have been the highest incident in 2015, with a strong increase compared to the previous year, but most countries continue to have difficulties in obtaining statistics on this type of attack; in particular only six countries were able to supply such data for this report, and one country, a major ATM deployer, was able to supply statistics for such attacks for the first time in 2015, so the data are not complete and not easy to compare.

The second highest type of attack is represented by Ram Raid/Burglary, but compared to 2014 there has been a 12% decrease in the number of such incidents and in 2015 it was the lowest level seen for 10 years.

Solid explosive and gas attacks have increased again, by 9% when compared to 2014; the majority of attacks continue to be explosive gas attacks and just 19 solid explosive attacks were reported in 2015 but not all respondent were able to provide the split between solid and gas. This type of attack, even when is not successful, can be quite costly and has high image impact: collateral damage to buildings causes financial damage that is far greater than the loss of the ATM or, for that matter, the money contained within.

In addition to the EAST report, which is focusing on Europe only, also ATMIA has done security analysis and surveys with a wider international view. In particular in the last years ATMIA has conducted several Global Fraud and Security Surveys with the objectives of monitoring the security landscape on the ATM channel, foresee new emerging threats and to highlight trends and investments around this topic. In the 2015 edition there were 87 respondents representing all the main regions. In the 2015 survey banks were also asked to give their estimation on the different types of attack, their evolution compared to previous years both in terms of volumes, methodology and cost impact.

The picture below shows the indication the participating banks gave related to the common physical attack scenarios**.**

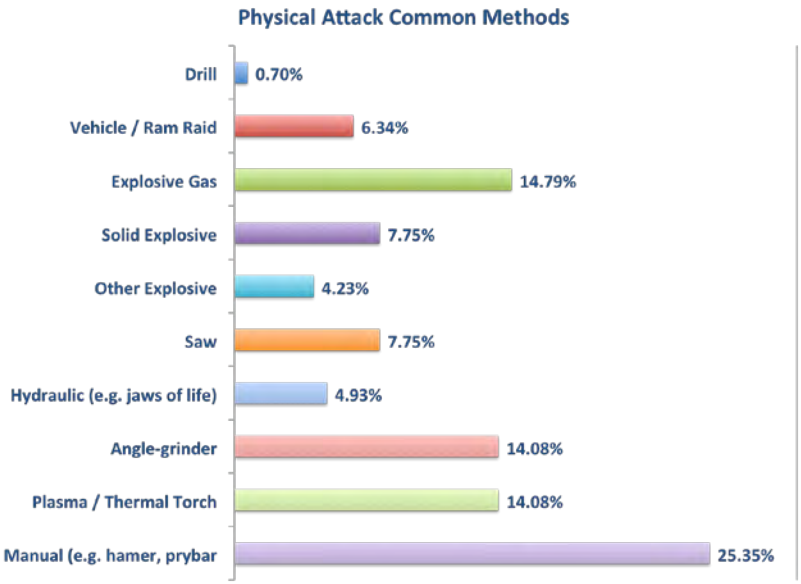


Figure 3: Physical Attack Common Methods (source: ATMIA 2015)[3]

[3] Fraud and Security Survey 2015

3.1.2 Logical attack

In the ATMIA survey mentioned before, the 3 methods of logical Attacks were quantified as reported in the table below:

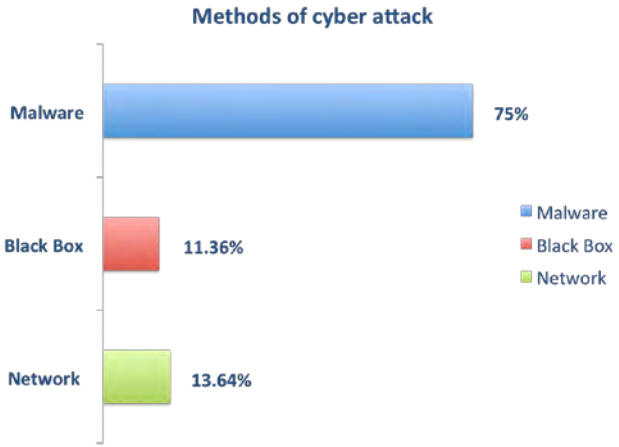


Figure 4: Methods of cyber attack[4]

At European level EAST started to collect statistics on ATM Malware in 2014, when the first attacks appeared initially in Western Countries and were mainly "cash out" or jackpotting attacks.

As shown in the picture below, the first malware families, which are used for 75% of the total cyber-attacks, were identified in 2006/2007 and over time they have evolved both for their high level of sophistication, both in relation to geographical areas of application / implementation.

In fact, initially two different criminal groups operated mainly in Eastern Europe (Russia and Ukraine) and Latin America (Mexico, Brazil, ...) probably due to lack of appropriate security measures put in place by the retail banks in those areas, or taking advantage of obsolescence of installed operating systems.

[4] From: ATMIA Global Fraud and Security Survey 2015

More exposed to cyber attacks are essentially “peripheral” ATM, i.e. installed in areas where the physical security measures can be circumvented, since the first infection requires physical access to the ATM in order to insert the malware by means of a CD or USB memory stick.

Also, in recent years these criminals are importing their technique in other countries around the globe.

In any case it’s clear that they are organized and a high level of IT know how.

The strength of cybercrime activity lies in its ability to adapt and evolve with the same speed of the technological evolution and of solutions for threat detection, as well as the strong determination to obtain personal data in every way.

But let’s see what are the latest malware discovered in recent years.

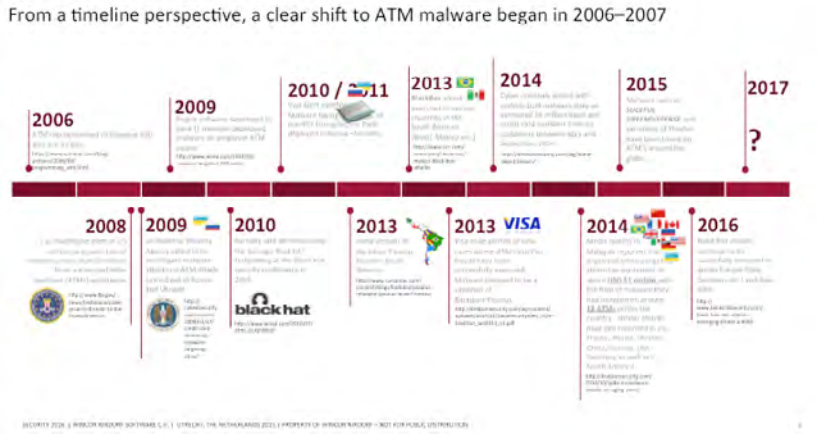


Figure 5: Timeline perspective of ATM malware

In 2013, Symantec discovered in Mexico **Ploutus** a malware code that, exploiting a bug in the Windows XP O.S. still in use by many ATMs around the world, allows to remotely the cash withdrawal of a specific amount by using a smartphone connected to the PC USB.

There is also the Ploutus B variant that exceeds the limit to specify the cash amount withdrawal; the malware checks the number of notes in each cassette and dispenses cash to the present repeating the process n-times.

Padpin was first discovered in May 2014 by Symantec and its updated version **Tyupkin** in October 2014 by Kaspersky Lab in South East Asia and across Europe.

Padpin hooks the ATM's PIN pad and allows control of the malware installed on PC via the PIN pad. By default, Padpin is set to be active between 1 a.m. and 5 a.m. from Sunday to Monday, so that criminals can operate at night to avoid raising suspicion. Both Padpin and Tyupkin allows cash dispense from the ATM.

Suceful seems not to be a working ATM malware, but only a test utility maybe for prototyping; it is missing major functions known from other malware families and it seems to be hardly manageable within a possible incident. First information comes from FireEye report published in September 2015 by, two Suceful samples were uploaded from France and the other one from Russia. It is assumed it can do: establish a connection with the XFS Manager, read debit card track data, open sessions with the peripheral devices (Epp, card reader, sensors), interact with the malware via Pin Pad.

In April 2014 was discovered **NeoPocket** malware, that, unlike the majority of ATM malware, does not steal cash from the ATM as it focuses on data theft only, stealing transaction data using a Man-in-the-Middle (MitM) attack and keylogs user input from specific application windows. This stolen data can be sold in Deep Web markets, used to create counterfeit payment cards, and used for fraudulent fund transfers out of victims' accounts. Because no cash is stolen from the ATM, the compromise tends to remain undetected for prolonged periods and thus allows the criminal group behind NeoPocket to collect large amounts of sensitive data.

Discovered in 2015 by Kaspersky Lab., **Carbanak** had been used to steal money from banks primarily in Russia, followed by the United States, Germany, China and Ukraine. The malware was

said to have been introduced to its targets via phishing emails. The criminals were able to manipulate their access to the banking networks in order to steal the money in a variety of ways, for example dispensing cash without having to locally interact with the ATM.

Carbanak is biggest coup to date found on the IT systems of at least 100 banks in 30 countries. The spyware allowed hackers to infect computer systems with malware that allowed them to observe the functions and tasks that users performed on their systems. Cyber criminals broke into bank systems, observed employees over a long period of time and then imitated their typical behaviour patterns. The warning mechanisms failed to detect the fraudulent transactions. According to various reports, the criminals not only transferred money to their own accounts but also manipulated ATMs to dispense money at selected ATMs at a certain time to be collected by an accomplice.

3.1.3 Fraud and manipulation attacks

For many years, skimming has been a popular technique to manipulate ATMs. With this technique, data from the card's magnetic stripe is captured by a concealed reading device that is attached to different position a the card reader. To record the respective card's PIN, an overlay is placed over the ATM's PIN pad or a hidden camera is used on or near the ATM.

Another approach to record customer data is eavesdropping on legitimate components of the card reader like the PCB.

In addition to this latest devices are also focusing on chip data, which is called Shimming. This MO depends on the data exchanged between the chip card and the PC and if for example an SDA card or clear text track 2 data is used.

Under the skimming category we will include all the mentioned type of attacks.

Card-trapping involves the use of a simple fixture to prevent the card that has been inserted into the card reader from being re-

turned to the customer after a successful cash transaction. As with cash-trapping, the card-trapping devices must be harvested and re-fitted after every successful attack.

Another form of ATM manipulation is cash-trapping. This technique entails placing a cash-trapping device in front of the cash output tray thereby blocking the cash from being presented and additionally the fraudster prevents a successful retract. Unlike card skimmers, which can be positioned and operated over a long period of time, cash trappers must be collected after every successful attack and placed back on the ATM fascia after the cash has been harvested.

A widespread type of ATM fraud is the misuse of copied or skimmed cards. In this fraud, stolen card data is written to the magnetic stripe of a card and can be used to carry out transactions at the cost of cardholders. The introduction of the EMV chip, commonly referred to as Chip and PIN, has reduced this type of fraud, but in most cases, the copied cards are used in non-EMV countries where card data is still read exclusively from magnetic stripes. If the misuse remains undetected, cardholders can face enormous losses on their accounts.

A spectacular hacker attack of this kind happened two years ago on an IT service provider, when criminals cancelled the limits for credit card withdrawals and withdrawal teams swarmed out around the world using copies of only 20 credit cards to withdraw a total of €34 million in 23 countries within just a few hours.

Another type of manipulation is known as transaction reversal fraud. Within a Transaction Reversal Fraud attack the fraudster creates an error condition at the ATM during a transaction, which signals that the cash was not presented to the customer. This leads to a re-credit of the amount withdrawn back to the account when in fact the criminal gets the cash. To get the money the fraudster often opens the shutter by force upfront to or during the transaction. The fraudster performs the transaction by himself with an anonymous pre-paid credit card without leaving useful traces. An automated reset after a still successful HW test gives the fraudster the chance to repeat the attack at the same ATM. At end of the day, large sums of money are missing, since the actual amount of cash in the ATM is lower than it should be according to the software protocol.

In Europe the number of fraud incidents has increased 19% in 2015 compared to previous year, as shown in the table below taken for the ATM Crime report produced by East in 2015.

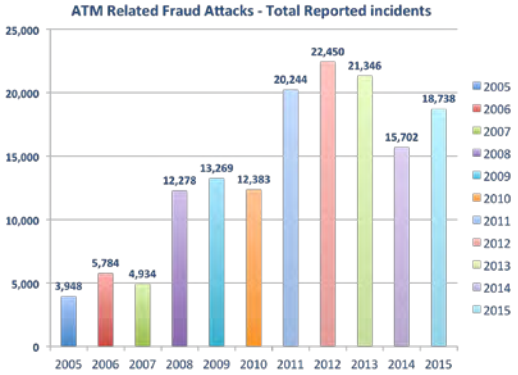


Figure 6: ATM related fraud attacks- total reported incidents (source EAST)

The breakdown of the incident type in 2015 is represented in the side picture, where the "other fraud" group is mainly made by cash trapping and transaction reversal fraud attacks.

As we will see more in details in the next paragraph the manipulation attacks are changing; while skimming is starting to decrease, also thanks to the investments done in these years in anti-skimming devices and in the migration from magnetic cards toward EMV chip card, the more simple fraud of cash trapping is becoming more and more popular.

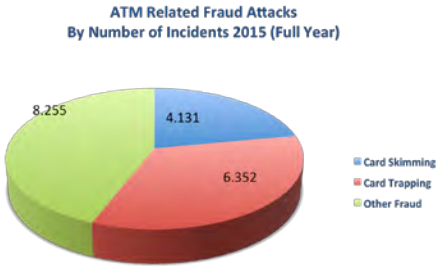


Figure 7: ATM related fraud attacks by number of incidents 2015 (source EAST)

3.2 Trends of Attack

The outcome of the ATMIA Global Fraud and Security Survey 2015 is that the total volumes of attack is still increasing according to the majority of the respondents:

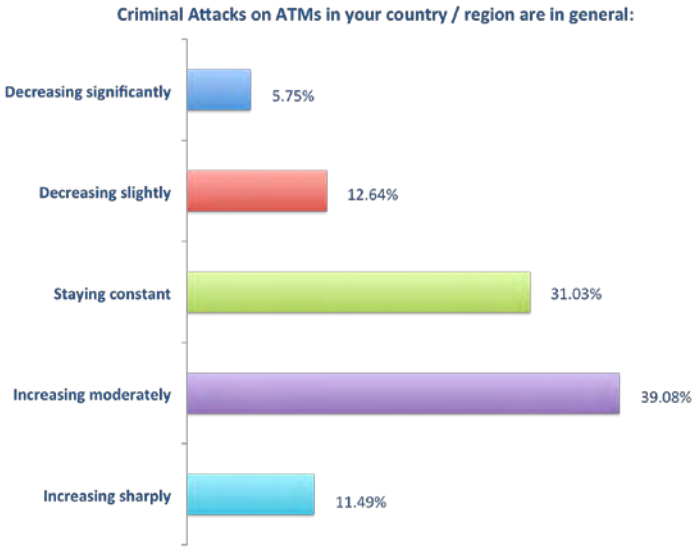


Figure 8: Criminal Attacks on ATM by country/region (source ATMIA 2015)

When we go deeper in which types of attack are increasing or decreasing we see different answers, also depending on the geography:

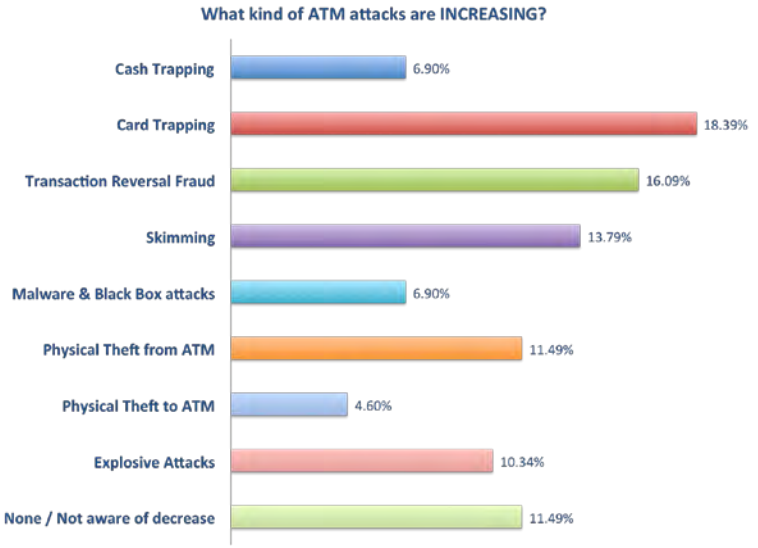


Figure 9: Increasing kind of ATM attacks (source ATMIA 2015)

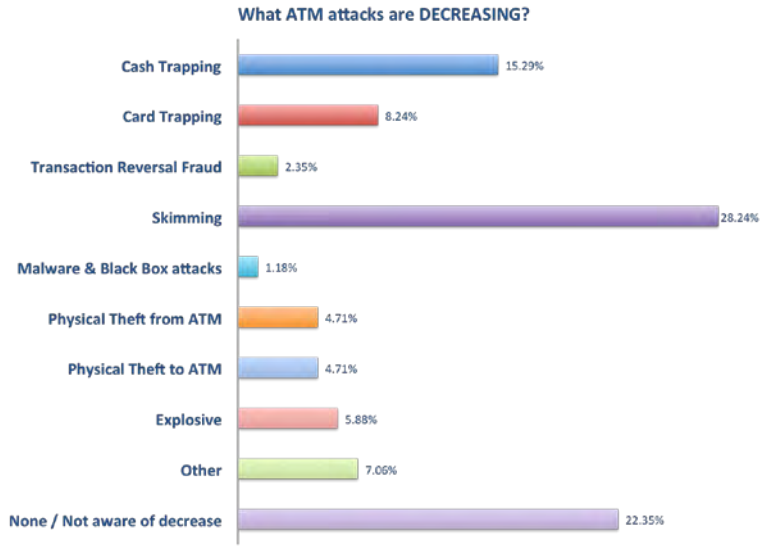


Figure 10: Decreasing kind of ATM attacks (source ATMIA 2015)

As general trends, also in comparison with the previous editions of the survey, we can see that Cash and Card trapping are the emerging threats while Skimming was perceived as strongly increasing in the previous years and now start to be seen as decreasing.

In terms of sophisticated methods of attack, the respondents identified malware as the dominant threat, far above the danger of network compromises and Black Box attacks.

This is very evident in Europe where EMV introduction together with other anti-skimming solutions has helped to reduce this type of attack, while less sophisticated fraud, like card trapping, cash trapping and Transaction Reversal Fraud (in the EAST report below under the category other fraud) are growing

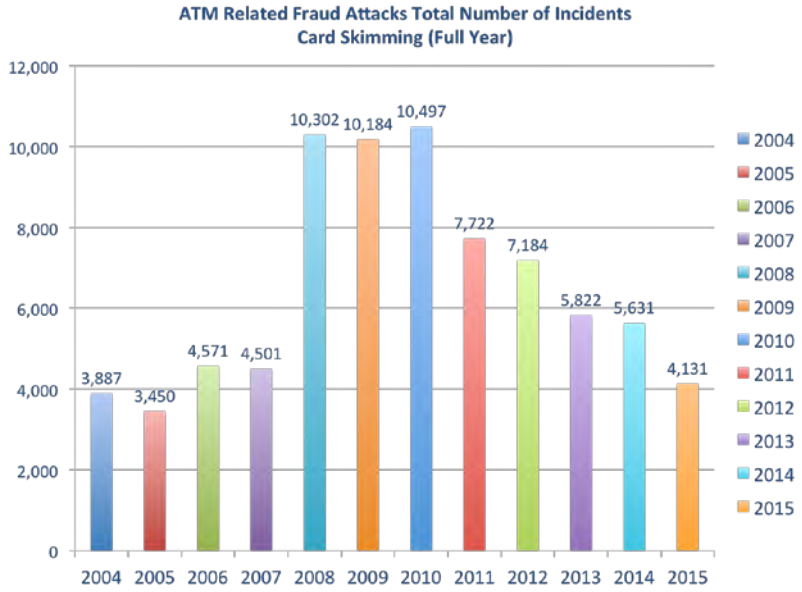


Figure 11: Total number of Incidents Card Skimming (source EAST)

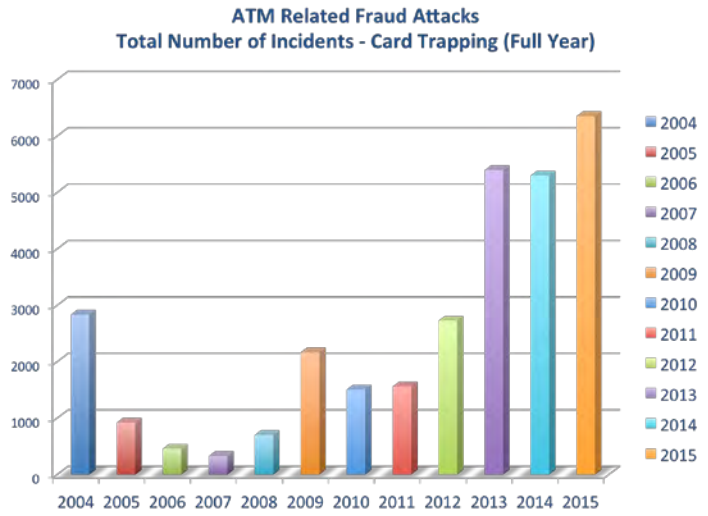


Figure 12: ATM related fraud attacks. total number of incident - Card Trapping (source EAST)

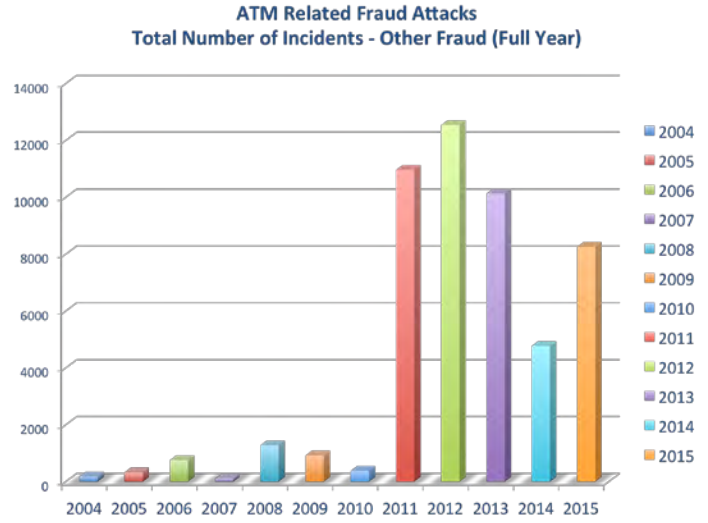


Figure 13: ATM related Fraud Attacks Total Number of Incidents - Other Fraud (source EAST)

The situation in Italy is a little different; here the total number of fraud incidents in 2015 has reached 1.015 cases, but the number of card trapping incident is very, very low (only 2 cases in 2015) compared to the European statistics. Regarding the other 2 type of manipulation the Italian market show a trend similar to the rest of Europe, with skimming attacks that are starting to decrease (-1% compared to previous year) while cash trapping is strongly growing (+586% compared to 2014). [5]

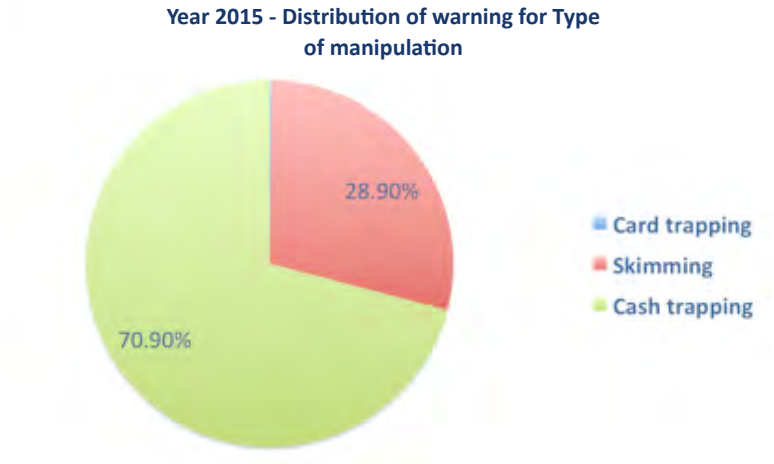


Figure 14: Distribution of warning for type of manipulation, year 2015 (source EAST)

3.3 Economic impacts & investments

It is generally very difficult to evaluate the economic loss related to ATM security attacks, and in fact, as shown the picture below over 35% of the respondent to the ATMIA survey were not able to accurately attribute a financial cost to ATM crime.

[5] Source: Centro Antifrode Bancomat

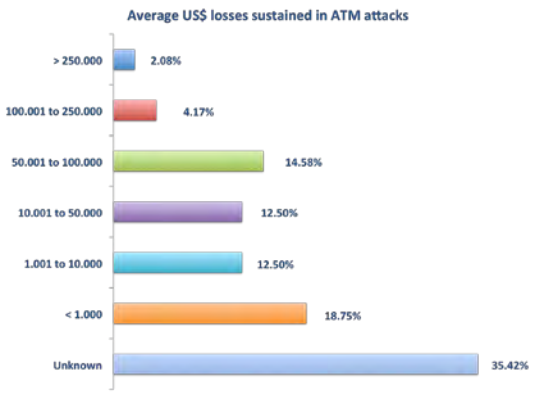


Figure 15: Average US dollar losses sustained in ATM attacks (source ATMIA)

In the same study there has been also an effort to go deeper and to estimate the US Dollar Losses related to each type of attack. Below are the outcome summarized in report:

- Skimming:
  - Average of $650 per card,
  - Range of $5,000 to $100,000 per incident
- Malware & Black Box:
  - Average of $104,000 per incident
- Physical Attacks:
  - Range from $200,000 to $2,000,000 per year,
  - Average of $41,400 per incident (including collateral damage)
- Explosive:
  - Average of $150,000 per year
  - Average of $63,000 per incident (including collateral damage),
- Phishing:
  - Average of $10,000 per incident
- Transaction Reversal Fraud:
  - Average of $500 per transaction,
  - Average of $165,000 per incident
- Card Trapping:
  - Average of $300 per card,
  - Average of $150,000 per year
- Cash Trapping:
  - Average of $150 per incident

When asked to estimate the investment intentions and trends, the participant to the ATMIA survey has shown their intention to have the same or higher level of budget and resources allocated to the ATM security topics.

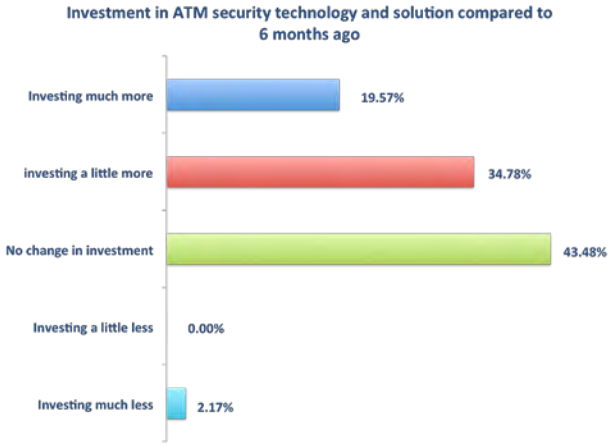


Figure 16: Investment in ATM security technology and solution compared to 6 month ago (source ATMIA 2015)

Let's now go more in detail in the analysis of the losses related to the different security areas.

3.3.1 Physical Security

In 2014, overall reported losses due to physical attacks on ATMs in European countries rose by more than 13% to €307 million compared to the previous year (the losses from gas attacks and explosives do not include collateral damage to equipment and property, which can incur significant additional costs, as the 2014 European ATM Crime Report states).

The picture below taken from the 2015 EAST report shows that the number of incident and the losses related to physical security has again increased significantly in 2015 in Europe.

3.3.2 Logical security

Various statistics have identified that, over the last few years, the growth in cybercrime or logical attacks has continued, if not accelerated, in the financial services industry.

So, while the number of incident and reported losses related to jackpotting attacks have decreased in 2015, also thanks to the countermeasure put in place by the European Financial institutions, according to a study by Europol, in 2015 the ATM malware attacks increased by 15% compared to 2014, with a total loss of 150 million € in the first half of 2015.

European banks have to keep high their attention on security, because organized crime – while also targeting back office, payment and core banking applications – focuses on points of customer interaction such as ATMs and POS terminals.

The biggest coup to date was in early 2015 when the malware Carbanak was found on the IT systems of at least 100 banks in 30 countries and the warning mechanisms failed to detect the fraudulent transactions. According to various reports, the criminals not only transferred money to their own accounts but also manipulated ATMs to dispense money at selected ATMs at a certain time to be collected by an accomplice. It is suspected that the criminals were able to steal between $2.5 and $10 million (€2.2 to €8.8 million) from each bank, representing a potential total loss of up to $1 billion.

3.3.3 Fraud Attacks

The following picture shows the evolution of the fraud attacks in Europe in terms of incidents and related losses.

In fact, talking about fraud losses, skimming is by far the biggest issue as represented in the following table:

Figure 17: ATM related fraud attacks total reported losses 2015 - €/full year (source EAST)

And while the number of skimming attacks is starting todecrease as we have seen in the previous paragraph, this is not the case for the loss amount, as shown below:

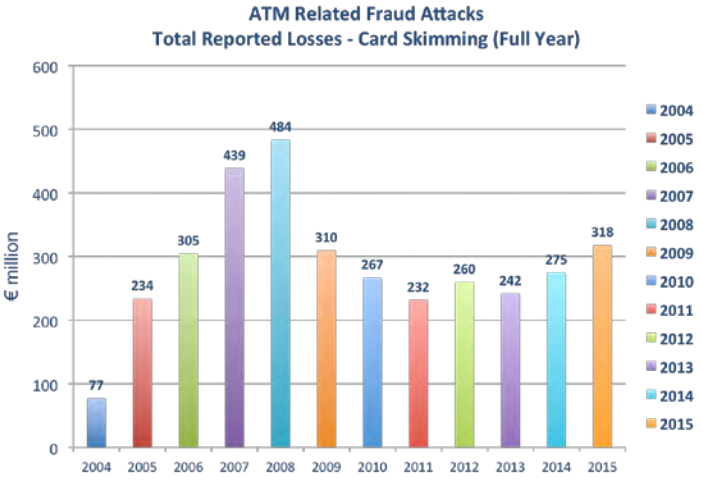


Figure 18: Total reported losses - Card Skimming (source EAST)

4 ATM operating model and services: a look at the present and future capabilities

Automated Teller Machines (ATM) are now one of the clearest indications of the presence of banking institutions in Italian territory, as their distribution is widespread and well organised.

In 2015, the network of terminals in Italy had around 50,000 ATMs, representing 14% of all ATMs installed in Europe *(source of data: EAST).*

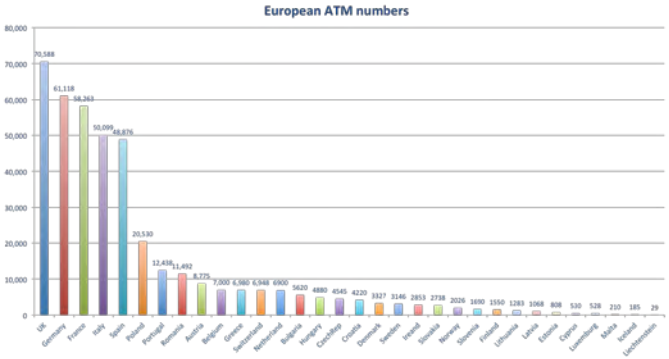


Figure 19: European ATM numbers as at 31st December 2015(source EAST and ECB)

The ATM, as part of the extensive network in which payment cards are accepted, can be enabled for the processing of transactions from different Circuits – whether national or international - that are identified by the logos shown on the machine or on the display screen.

The cards in circulation are generally multi-brand (co-badging), which means they take on board two or more payment circuits, represented on the plastic by the relevant Brands. Each ATM is under the responsibility - directly or indirectly - of a party in the role of Acquirer, which is identified by a unique code at the Circuit level, which is always transmitted in transactional messages, and which is required to finalise transactions. To understand the mechanisms that underlie the provision of ser-

vices and identify any vulnerability that would hinder its normal operation, it is good to begin by first distinguishing between the terminals according to their "morphology"; the physical characteristics of ATMs may, in fact, also have some bearing on exposure to the risks that will be addressed in subsequent chapters.

The BANCOMAT Consortium classified ATMs based on location type, as described below:

- Counters inside branches (indoor): ATMs that customers can access during the branch's opening hours
- Counters outside branches (outdoor): ATMs that customers can access regardless of the branch's opening hours (installed facing the street or placed in the 24hour self-service area)
- Counters in public places (positioned): ATMs installed in hospitals, public offices, stations, local health authorities, commercial enterprises, etc.;
- Counter inside a company: ATMs installed inside companies and therefore bound by particular rules of access;
- Seasonal: temporary ATMs operating for a limited period linked to particular events such as trade fairs and temporary events. These represent a variable share of the installed machines.

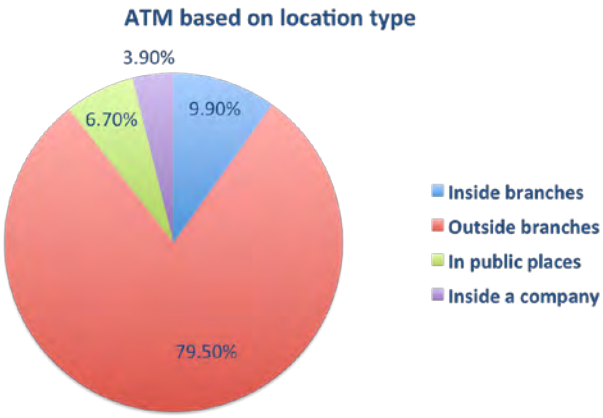


Figure 20: ATM classification based on location type

4.1 The Infrastructure

To describe the ecosystem in which the ATM operates, we must illustrate the infrastructure, applications, services and parties that contribute to its operation.

The infrastructure, which forms the basis for the ATM network, can be split into two levels:

- The **solution** based on the network layer
- The **network** layer

4.1.1 The solution

Starting from the solution, considering that this is the combination of hardware plus software with different purposes.

99 % of ATM terminals in Italian territory perform at least one financial function, such as dispensing cash or payment for goods or services.

The definition of ATM is in fact only suitable for terminals that are equipped with at least one drawer for cash management, whether this is managed via dispensing or via payment.

Then there is a wide range of terminals which, because of their hardware features, are comparable to ATM equipment even if they do not have drawers / safes. These devices, often referred to as Totems or Self Service Kiosks, do not have a cash teller function and are enabled solely for payments or questions and therefore can be compared to POI / POS terminals.

Consequently, below we will illustrate only the infrastructure provided by Italian PSPs for the management of ATM equipment.

Figure 21: ATM

Some core elements of ATM hardware components influence user transactions:

- Display
- Monitor
- EPP (Encrypting PIN PAD, a tamper-responsive security device that provides secure PIN entry and storage of cryptographic material. It is designed to be integrated into ATMs or self-service POS terminals)
- Card reader (The part of a chip payment terminal where the chip card is inserted or tapped to initiate a chip transaction. There are three types of card readers; motorised contact and manual contact and contactless. A motorised reader has a mechanism that transports the card into, and ejects the card from, the reader. A manual reader requires the card to be manually inserted into, and removed from, the reader. A contactless reader requires the cardholder tap the card near the device)
- Banknote dispenser (an electromechanical device that permits authorised users to withdraw banknotes, typically using a machine readable plastic card)
- Keyboard
- Printer

Other components are basic or additional structures which are not necessarily essential for the completion of a transaction.

Components that condition transactions are subject to approval processes prior to the implementation of the solution.

Various bodies and organisations exist to control the processes for certifying / approving solutions with different responsibilities and purposes.

ATMs assigned on Italian territory and operating within the infrastructure of the Banking network must all have undergone the following product approval steps:

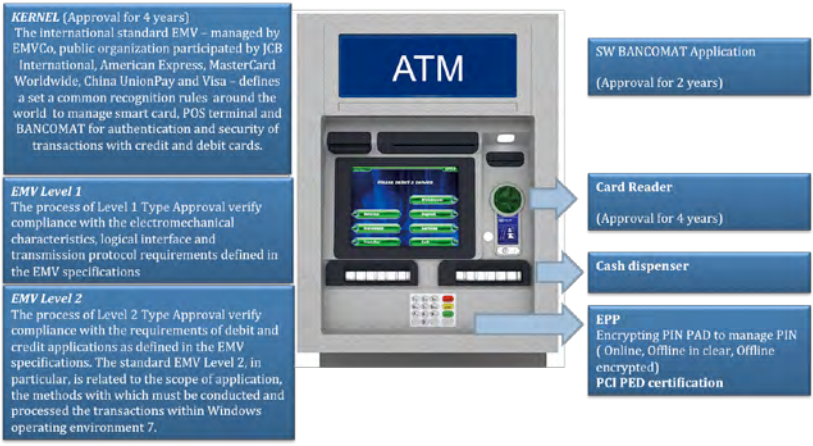


Figure 22: ATM components

4.1.2 The network

The Italian interbank network established, on the basis of the system requirements for the telematic transmission of data carried out with the incentive of the CIPA, the **Interbank Convention on Automation,** an association established in 1968 by Banca d'Italia and ABI which seeks to promote the adoption of technical standards and the performance of joint projects in the field of telematic infrastructures and interbank applications, in particular in the area of payment services, in line with guidelines published by the

European System of Central Banks (ESCB) and Banca d'Italia, and considering the issues represented by the ABI.

The requirements issued by the CIPA are mandatory for all operators carrying out management operations on telematics infrastructures in the System and are organised as described below:

- **Technical requirements**:
  - Architectural
  - Communication protocols
  - Transfer capacity
- **Operating requirements**:
  - Interoperability
  - Continuity
  - Service levels
- **Safety requirements**:
  - Authorisation
  - Privacy
  - Integrity
  - Authentication
- **Auditability**
- **Business continuity**

The physical connection that enables communication between different parties, thus ensuring the "circularity" of authorisation requests, is based on the use of routers with NAT (network access translation) functions that enable the switching of packets through the network of one banking party or several different parties operating in one System.

The "System" shall be understood, henceforth, as a group of parties, infrastructures and unified, organic processes.

The "Italian interbank system" is therefore represented by parties, infrastructures and processes which, for various purposes, work together to realise, in the case in question, the functional elements of performing ATM transactions.

The most widespread network framework in place between members of the System is still based on SNA (system network architec-

ture), an IBM system maintained above all for applications known as OLTP (on line transaction processing) which are today integrated with internet protocol (TCP/IP transfer control protocol) where TCP divides the data to be sent into many independent, numbered segments and reassembles them once they arrive at the other end, presenting them, again, as a flow of bytes.

The framework set out below explains the typical connectivity of a Bank.

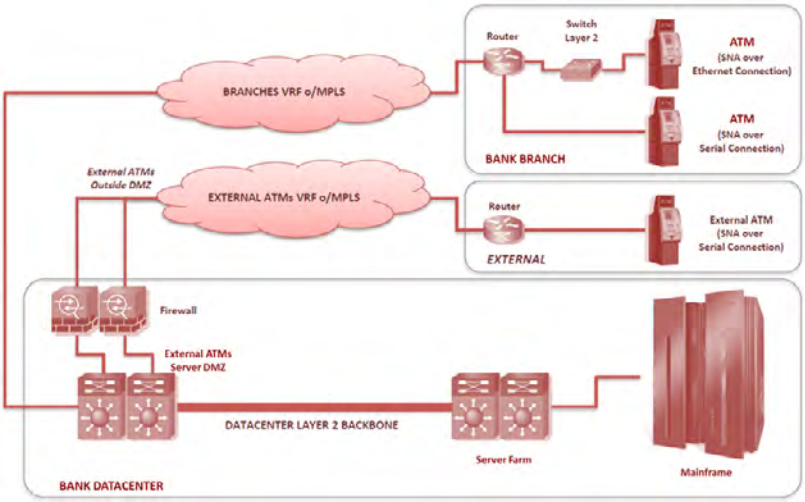


Figure 23: ATM connections

Without wishing to go into the technicalities of telematics transmission, it is important to clarify that both the ATM network of an individual party and the System that collects conversations between various entities, mainly banks, are closed Systems, not exposed to the Internet world, in proper terms.

Participating in the System requires membership of a convention – the SITRAD (interbank system of data transmission networks) convention – created for the performance of financial operations,

though which the participating parties commit to determined technical standards and rules of service.

The System participants are certified parties themselves who perform roles with defined responsibilities with regard to the standard flow of a withdrawal or payment transaction.

Low-level conversation is then covered by the applications protocols that are outlined below in the example of the conversation in a BANCOMAT transaction with the assumption that the chain of roles is the same for all types of operations

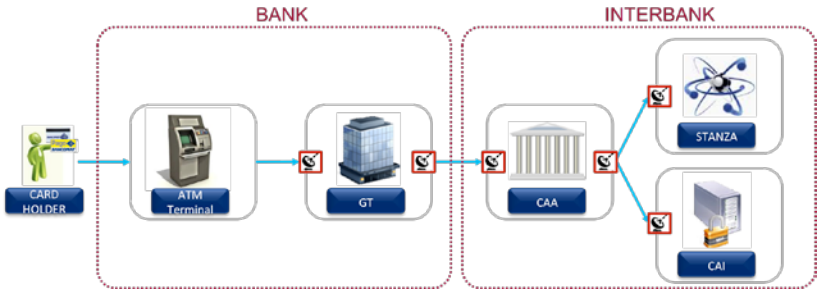


Figure 24: ATM conversation

The applications protocols, i.e. the languages that support the request messages and requests, can, in turn, be divided into subclasses:

- Interbank protocols
- Proprietary protocols

Interbank protocols are specific to the authentication/authorisation transactions sent to a credit/payment institution which holds the payment account belonging to the card holder.

Proprietary protocols are developed independently by agreement between the parties providing a service and supplying a series of information accompanying / integral to the interbank transaction.

Recently new generation ATMs offers services such as payment of utilities bills that pair standard payment transaction with information about debt owed, bill and creditor.

The advent of these new services has been made possible thanks to the potential of a multi-layered solution on which to trigger applications, software and diversified processes and thanks to a secure, protected, performance and multitasking network.

4.2 The development of services offered

Many latest generation ATM machines now often offer diversified services that are not limited to the traditional cash withdrawal operations: in fact, their functions are gradually including some activities that, until recently, were typically performed at the branch counter.

There are in fact many possibilities for operations that can be carried out at an ATM Machine, even if they are not always all present at the same time; some services – like withdrawals – are offered in circularity, others – for example account balance requests, list of transactions, payment requests – are mainly offered in companies, which means they are available only at a counter at the bank where the cardholder's payment account is held.

Any bank can make provisions for other services which are offered exclusively to its own customers and therefore do not comply with the standards acknowledged at System level but which are based on the proprietary protocols.

In general, the majority of ATMs now offer **advanced authentication services:** in these operations, the terminal is used to identify the natural/legal person based on the data held by the bank "hub" because the customer has opened a payment account there.

Once identified by authentication, the customer can carry out:

- **Information operations**: allow the customer to obtain registry certificates, information on account balance / transactions, card balance / transactions, summary documents relating for example to the management of payments / util-

ities or the management of securities deposits;
- **Withdrawal/payment operations:** allow the customer to perform withdrawals / payments via:
  - *Physical / virtual card*, to perform cash withdrawals / advances, telephone top-ups, prepaid card top-ups, utilities, tax, duty or fine payments,
  - *Other means*, such as direct debit, wire transfer, bank transfer, permanent provisions

These new services are possible thanks to the potential for a multilevel solution which makes it possible to trigger diversified processes, software and applications, but also thanks to a secure, protected, high-performance and multitasking network.

In recent years, we have seen increasing distribution – in particular abroad – of counters able to use new technologies such as, for example, converting local currency into virtual currency. These devices can actually be used to withdraw or pay virtual money into your account, and to make payments to parties that have an agreement.

All counters perform transactions known as "service" transactions, because they are not directed at the customer but required for the proper running of the device.

Service transactions are understood to mean a series of interface macro-activity between ATM and operator, such as the following examples:

- Operator action / end of operator action;
- Counter start-up;
- Accounting closing / opening;
- Printing Host information (on-line only);
- Selective printing;
  - Loading banknotes into the ATM;
  - Printing local information.

4.3 Terminal components

In parallel with the expansion of services provided by ATMs, we have also seen a dual tendency: firstly the essential components of the ATM have undergone gradual technological development

(for example, just think of the move from magnetic strip readers to chip readers, or the development to touch screen display monitors); secondly, there has been an improvement in the hardware and software components of the machines in order to accommodate the new services offered by the system.

Below is a list of some of the supplementary solutions that can now be found on ATM terminals.

4.4 Additional components

These are components that increase the speed, security and differentiation of the fundamental tools for identification or payment, so as not to paralyse the market by only card use; the latest trends are actually seeing an increase in cardless, or rather cashless solutions.

The following are specific examples of additional components:

- QR code readers
- Bar code readers
- NFC readers
- Cless readers
- Biometric authentication systems
- Recycling machines

The latter, for example, enable more secure management of the life cycle of the cash because they allow the transfer of money contained in the till of a point of sale (on the basis of a specific agreement between the bank and merchant) and the subsequent use of the transferred cash for withdrawals made from the same device.

Again, some QR code readers generate a code that represents credit usable at agreed points of sale.

The expanding range of technological hardware therefore sustains differentiation in the range of services, and at the same time promotes interaction between multiple parties (not only Acquirer and Issuer, but also new providers, merchants, GDO, etc.)

4.4.1 Components dedicated to accessibility

Many ATMs now installed in Italian territory are equipped with special components intended to facilitate and enable access to the functions of the terminal for disabled people.

- **Systems for the visually impaired:**
  - Hardware components: essential ATM components are made with strong colour contrast and the function of each element is made recognizable by specific signs in braille next to them.
  - Keyboard: operating commands are focused on the numeric keyboard, which must have specific features such as size, position and intensity of pressure on the keys.
  - Video: to make them more legible, text and commands given on screen are shown in a suitable size and in con-

trasting colours.
    - Timing: in the case of services for the disabled, for operations that must be performed within a specified time (e.g. card removal), the length of time is increased and the end of the period is signalled by an alert.
    - Operation receipt: receipts are printed in a larger size than the standard print to make them easier to read.
    - Audio: each ATM accessible to the visually impaired has an audio jack for headphones, to enable the use of a voice guide for carrying out operations. The operating instructions are simple, easy to hear and understandable; what is entered on the keyboard is confirmed by the voiceover of orders given and numbers entered, with the exception of PIN numbers.
- **Systems for the hearing impaired:** lights are used to indicate the main modules (e.g. card reader) or activities required (cash withdrawal, card withdrawal, etc.) both at the counter and in the surrounding environment (eg. reader to open doors)
- **Systems for the disabled**: to increase the accessibility of ATMs for people with motor or perception deficiencies, the access to the terminal must be free of obstacles, easy to use and free of any potential risk factors. There are rules governing other aspects such as, for example:
    - The height of the terminal and the depth required to enable use by a wheelchair user;
    - The minimum lighting levels to be guaranteed in the environment in which the terminal is installed;
    - The dimensions of access to the terminal;
    - Features of the flooring and the width of lobby doorways.

4.4.2 Security hardware components

With regard to security measures on ATM devices, to date there are no mandatory requirements but a series of national and international standards remain in place which recommend the presence of elements intended to prevent certain fraudulent activity. Of course, preventive measures are continuously developing as the known fraudulent activity could change with the distribution

of new "versions" of known phenomena or it may be necessary a development in security measures to face new types of attack.

On a national scale, there is an active collaboration, dating back many years, between banks, prefectures, law enforcement agencies, and the Italian Banking Association (ABI) to face brute attacks on bank branches, with particular focus on ATM terminals: the requirements considered most effective in terms of physical security are included in a protocol which is updated every year and signed by the stakeholders.

In particular, on the basis of the aforementioned protocol, the banks undertake to give each branch – within three months of the signing date – at least five of the security measures listed in the document. Some of these specifically refer to terminals, for example biometric detectors, video surveillance systems, anti-theft alarm systems, banknote dye-staining systems, banknote traceability systems.

Amongst the monitoring and contrast activities, Italian banks which are Members of the domestic Circuit manage a web platform for signalling and for sharing alerts and information which, over the years, has developed a standardisation of fraudulent events and the relevant preventive and contrasting measures.

In light of the above, the measures for the security of ATM terminals can be grouped together as follows:

- Measures for physical protection against attacks focussing on the card reader or cash dispensing unit (e.g. skimming, cash trapping, card trapping)
- Logical security measures to protect the cardholder's data
- Systems to protect the privacy of operations performed on the terminal by the card holder
- Security systems for the operating system and BIOS
- Security applications to identify and eliminate undesired applications / software
- Remote monitoring and surveillance system
- Alert systems and presence of sensors suited to the risks to which the terminal is most exposed
- Further deterrents and/or instruments to delay or block

physical attacks to terminals, for example locks / additional alarms, nebulisation systems, specific systems for anchoring to the floor, etc.

4.5 The transaction process

Below is an outline of the process that leads to the completion of an operation, composed of a flow of **requests**, which stems from the authentication of the parties involved, and an **authorisation** flow.

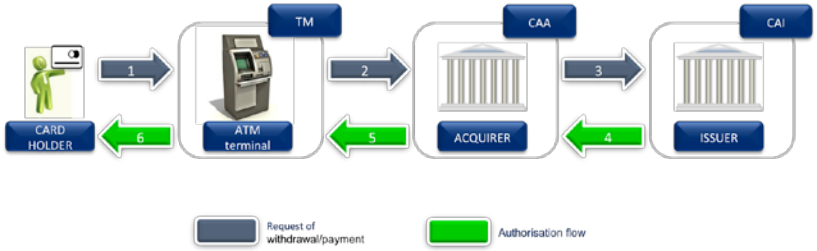


Figure 25: ATM transaction process

The initial start of the process consists of the recognition between the card and the terminal. In particular, entering the correct PIN ensures verification of the identity of the card holder and their intention to complete the transaction.

After this first step, the request moves on to the "recognition" stage between terminal and GT party, which – once the sender and recipient of the request have been identified – passes the operation to the authorised Acquirer or to the Applications Centre appointed by the latter.

The request can then go in two directions:

- To the party issuing the card, in the case of an OLI (On Line Issuer) authorisation process, in which the authorising par-

ty is the bank itself;
- To another party, in the case of an OLCA (On Line Applications Centre) authorisation process in which the authorising party is not the bank but a party appointed by the bank (typically an Applications Centre).

The authorising party, whoever this may be, carries out a series of preliminary and necessary checks in order to issue the authorisation to proceed with the completion of the operation:

- **Verification of technology**: the party verifies the technological means by which the operation is being performed (chip, bank, cless, etc.);
- **Verification of the availability of the card and current account**: the authorising party verifies that the request complies with the defined spending limits or card / account limits;
- **Verification of the conditions of the request**: the authorising party makes further checks, for example, the card's presence on a black list, the presence of anomalies previously included in monitoring, specific thresholds exceeded, etc.

Once all the verifications are completed, the authorising party sends the result – positive or negative – to the request: messages pass through all the hubs in the chain in reverse until they reach the initial hub, the cardholder, who is authorised, or not, for the transaction.

4.6 Back office processes

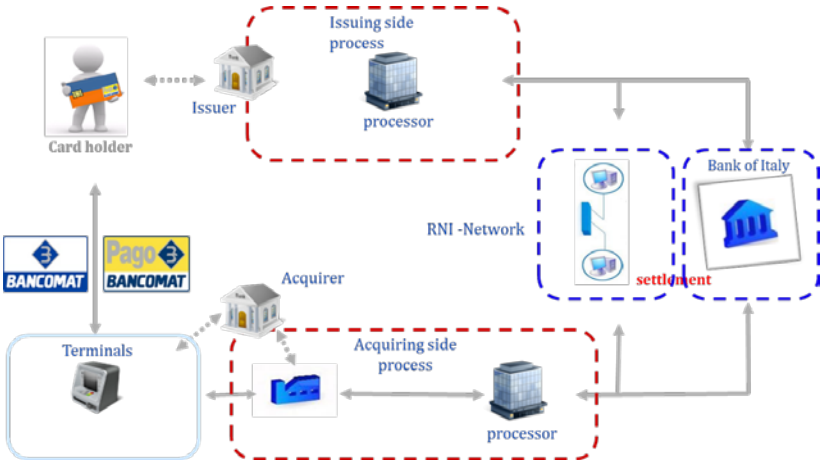
Any transaction processed in real time by the ATM is completed during a second phase of processing dedicated to settling the money.

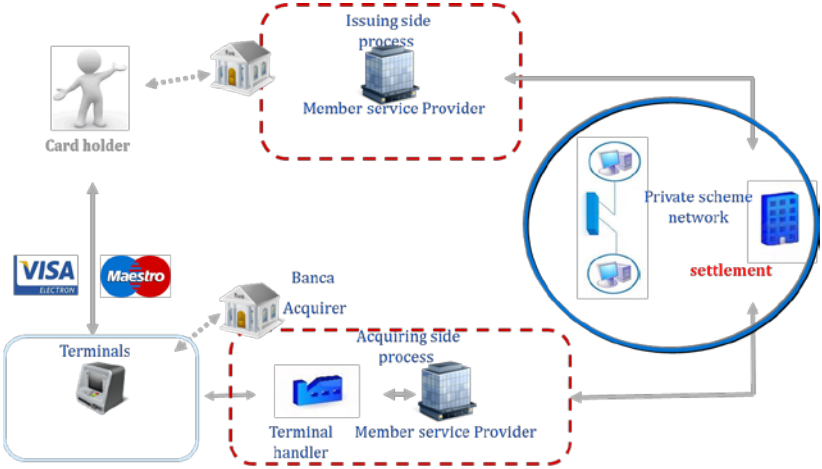
The settlement of money is carried out through a Clearing House, where Clearing & Settlement operations are performed.

Clearing regulates the give and take between banks on the basis of bilateral balances between two parties or multilateral balances between multiple parties at any given time. It consists, therefore, of providing and supplying the data required in the settlement phase.

Settlement consists of transferring cash flows within the System and of settling debit / credit positions against the Issuer and Acquirer.

Therefore only during the settlement process is money actually delivered via a telematic network between the different participants in the system (acquirer and issuer).





5 ATM authentication systems and cyber security challenges

ATMs have been under attack since at least 2008-2009, when the first malicious program targeting ATM Backdoor.Win32.Skimer was discovered.

The goal of every fraudster is to obtain money. When we talk about fraud related to ATMs we can generally divide it into two main categories:

1. **Direct losses**, when an attacker can obtain money from an ATM cash dispenser.
2. **Indirect losses**, when aim of the attacker is to obtain unique cardholder data from the ATM's users (including Track2 - the magnetic stripe data, the PIN – personal identification number used as a password, or newly appearing authentication methods – biometric data. Attacks of the latter type of authentication can increase risks of identity theft).

To achieve their goals, attackers must solve one of these key challenges – they must either bypass the customer authentication mechanisms, or bypass the ATM's security mechanisms. Criminals already use various methods to get profit from ATMs, such as ram-raiding and gas explosive attacks, or use skimmers and shimmers to attack customers. From our observations, criminal methods are shifting from physical attacks to so-called logical attacks. These can be described as non-destructive attacks on software or hardware implementations used in ATMs or their network. This provides fraudsters with more opportunities to leave their attack hidden for a longer time and thus increase the severity of the losses.

5.1 ATM authentication services

At the moment, the most commonly-used authentication method for an ATM cash withdrawal is a bankcard, usually protected with a four-digit PIN-code, although there are also other authentication methods available.

Bank card data (e.g. Track2) might be skimmed via various methods such as hardware skimmer, port sniffing or network attacks. A PIN is vulnerable to shoulder-surfing or fake-PINpad intercepting attacks. Attackers use skimmed data to clone bank cards and obtain fraudulent ATM transactions. Another method of ATM fraud is unauthorized access to an ATM cash dispenser, executed via attacks on ATM software or hardware components or via network attacks. A large number of ATM hacking incidents have occurred in the past three years, highlighting the weakness of these methods. One of these is malware Backdoor.MSIL.Tyupkin,[6] which affects ATMs from a major ATM manufacturer running Microsoft Windows 32-bit. In addition, the sensational Carbanak malware[7] makes ATMs dispense cash to attackers with no physical interaction.

Nowadays the term Strong Authentication (or Strong Customer Authentication) is widely used when talking about banking and financial services, where access to an account must be linked to an actual person, corporation or trust.

Strong authentication is often confused with two-factor authentication, or more generally, multi-factor authentication. The European Central Bank gives the following definition of strong customer authentication:

"A procedure based on the use of two or more of the following elements– categorised as knowledge, ownership and inherence: (i) something only the user knows, e.g. static password, code, personal identification number; (ii) something only the user possesses, e.g. token, smart card, mobile phone; (iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the Internet. The strong authentication procedure should be designed in such a way as

[6] Web-site: Kaspersky Lab's Global Research & Analysis Team, October 7, 2014. Tyupkin: manipulating ATM machines with malware. Available at: https://securelist.com/blog/research/66988/tyupkin-manipulating-atm-machines-with-malware/ (Accessed 29/06/2016)

[7] Web-site: Kaspersky Lab's Global Research & Analysis Team, February 16, 2015. The Great Bank Robbery: the Carbanak APT. Available at: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/ (Accessed 29/06/2016)

to protect the confidentiality of the authentication data."[8]

Contactless authentication

The most promising technology is NFC (Near Field Communication), which makes it possible to use radio frequency as an authentication method. NFC-chips are a form of passive data storage, which can be read, and under some circumstances written to, by an NFC-device. The chip can securely store personal data such as debit and credit card information, PINs and loyalty program data. NFC-chips can be fitted in smartphones to store bank card data, passports to store ID and biometric data, and watches or even the human body (in the hand, for example) to store various data. An NFC-device works in reader-writer mode, it is able to receive and transmit data at the same time. Thus, it can check for potential collisions if the received signal frequency does not match the transmitted signal's frequency.

NFC is fast and easy to use but insecure and vulnerable to various attacks, e.g. passive relay attack[9].

Biometric authentication

Biometric authentication technologies are being actively implemented in banking solutions, both on a commercial scale and at an early level of concept development. Biometrics refers to the automatic identification of clients based on their psychological, morphological or behavioural characteristics. Various types of biometric systems are being used for real time identification.

These may include:

- Iris recognition;
- Fingerprint recognition;

[8] Report: European Central Bank, January 2013. Recommendations for the security of internet payments, final version after public consultation. Available at: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf (Accessed 29/06/2016)

[9] Report: Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited. Available at: https://conference.hitb.org/hitbseccon-f2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMV-Contactless-Cards.pdf (Accessed 05/07/2016)

- Palm recognition;
- Vein recognition;
- Face recognition;
- Voice recognition;
- Other (for example, signature recognition).

Some ATMs (so-called Biometric ATMs) also use biometric data as multifactor authentication (in other words card + PIN + biometrics) or as combination of card or PIN. Some of these recognition methods might be used as single or multi factor biometric authentication. It could be used for online or offline authentication using smart cards or for cardless authentication.

Offline authentication using a smart card means the ability to authenticate the cardholder without connection to a backend biometric database. The template of biometric data is stored on the smart card chip according to so-called match-on-card technology.

The main reason for introducing biometric data recognition is to increase security and to achieve strong authentication. But various biometric security systems could be bypassed and sometimes in a simple way, for example, using images of the victims. One such example was delivered at the December 2014 Chaos Communication Congress, by security researcher Jan Krissler.[10]

The smart cards are sensitive to different types of attacks[11], even to man-in-the-middle attack[12].

Authentication with a one-time password

The theory behind using two-factor authentication is the need to en-

[10] Web-site: Swati Khandelwal, 2015, Hacker Finds a Simple Way to Fool IRIS Biometric Security Systems. Available at: http://thehackernews.com/2015/03/iris-biometric-security-bypass.html (Accessed 05/07/2016) The entire presentation in German, with Q&A, is available on web-site https://www.youtube.com/watch?v=pl-Y6k4gvQsY (Accessed 05/07/2016)

[11] Report: Benoit Vibert, Christophe Rosenberger, Alexandre Ninassi, 2013. Security and Performance Evaluation Platform of Biometric Match On Card. Available at: https://hal.archives-ouvertes.fr/hal-00848330/document (Accessed 05/07/2016)

[12] Report: Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson, 2014. Chip and Skim: cloning EMV cards with the pre-play attack. Available at: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland14chipandskim.pdf (Accessed 05/07/2016)

ter a one-time session key, also called a one-time password – an OTP, in addition to a user login and password.

An OTP can be used to withdraw money without a card – the password is delivered via SMS and should be used instead of a bankcard. This service is also known as Cellphone Banking. Various banks around the world, for example, Spain's Banco Sabadell[13] launched an ATM withdrawal service that allows clients to withdraw cash from their mobile phones. The client sends a request to the bank and receives a code via SMS. Then the client simply enters the code into an ATM to withdraw the cash, or sends the code to another person's phone, making it a person-to-person payment system. Now, the SMS-banking service is widely used for approving payments, or online transactions.

An OTP also can be used in mobile banking applications.

But delivering OTP via SMS is not so secure. Firstly, the OTP in the SMS might be obtained by an attacker via social engineering techniques, such as a fake call or SIM swap attack. Secondly, the SMS with the OTP might be extracted by an attacker via physical access to the phone, mobile phone Trojans or wireless interception.[14]

Another method is to use a personal electronic token with a cryptographic algorithm to generate an OTP. That password can be used to confirm banking transactions online and for the verification of 3D-secure technology transactions. MasterCard has launched a Chip Authentication Program (CAP) for using EMV banking smartcards for authenticating clients and transactions during online and telephone banking. In the future this will also be implemented in ATMs.

5.2 Infrastructures and attack targets

The ATM is the endpoint which the client regularly communicates with in everyday life. To carry out financial functions an ATM must

[13] Web-site: Vaseem Khan, October, 2013. 4 Cardless Ways of Withdrawing Cash from ATMs. Available at: https://letstalkpayments.com/4-cardless-ways-withdrawing-cash-atms/ (Accessed 29/06/2016)

[14] Report: Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, Jean-Pierre Seifert, 2014. Available at: https://www.eecs.tu-berlin.de/fileadmin/f4/TechReports/2014/tr_2014-02.pdf (Accessed 06/07/2016)

be connected by any available means to the processing center and control host, e.g. the ATM Active Directory. The bank's internal network includes a plurality of distributed components and servers, which handle services such as online-banking, as well as phone and SMS banking. Bank branch offices and employees are connected to this network. Biometric data for online authentication during ATM transactions or online/phone banking usage is contained in the database. A map of the banking network infrastructure is shown in the following figure.

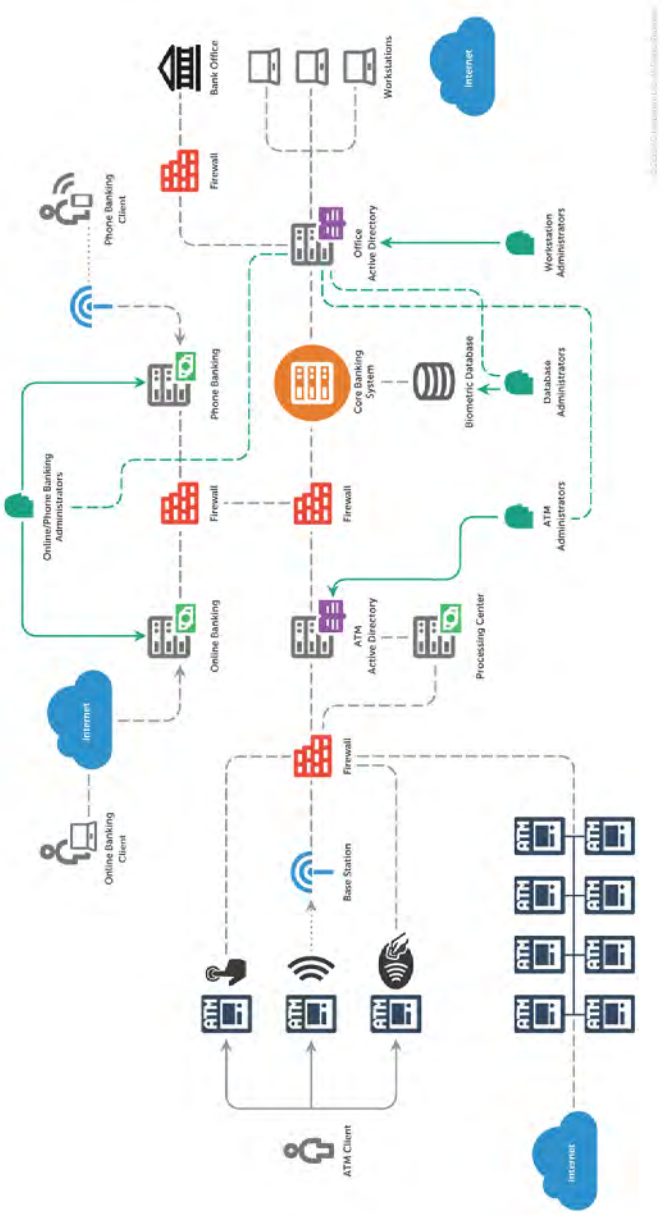


Figure 26:Simple diagram of bank network infrastructure

Almost any elements of the infrastructure are of interest to attackers. One of the points is biometric recognition bypassing.

We can find news about the successful implementation of biometric ATMs in various banks and countries. It is recognized that biometric authentication for accessing bank accounts (to perform financial transactions) is the most secure way to protect money.

However, biometric authentication is only one more target for criminals:

- Criminals sell specially crafted devices (such as skimmers) for intercepting biometric data on the black market,
- Criminals are testing these devices to be ready for ATM attacks when biometric authentication will be in place.

Criminals can prepare for two possible scenarios that use biometric authentication on ATMs.

1. **Biometric authentication is used with a card.** In this case criminals will use a device to intercept card data and biometric data. Fingerprints of all customers are stored in a biometric database. Two situations are possible: the finger is chosen statically (e.g. only the first finger is checked), or the finger to be checked is chosen at random. The first situation is easier for an attacker, because he only needs to skim the customer once. The latter situation is more difficult, because an attacker has to obtain all fingerprints for each customer for a successful attack
2. **Biometric authentication is used without a card**. Biometric data recognition is used for cash withdrawals with some ID (for example, as DCB Bank launched[15]) or without, in a cardless transaction.

Before using a biometric authentication service, the customer must go through the initial procedure of taking biometric data, when samples are collected via a special device (such as a scanner or reader) in the bank branch or office (simple scheme see on Figure 30). This biometric data must be placed in the biometric

[15] Report: DCB Bank, April 2, 2016. DCB Bank launches India's first 'Aadhaar Number' and 'Aadhar Biometric' enabled ATM. Available at: http://www.dcbbank.com/pdfs/India_s_first_Aadhaar_enabled_ATM_launched_by_DCB_Bank_Press_Release_3_April_2016.pdf (Accessed 29/06/2016)

database from which it will be requested by ATMs or other bank services that require customer biometric authentication.

In the case of cardless transactions criminals can create (or buy on the black market) fake biometric readers or scanners, and more globally they can use a fake ATM with a biometric device.

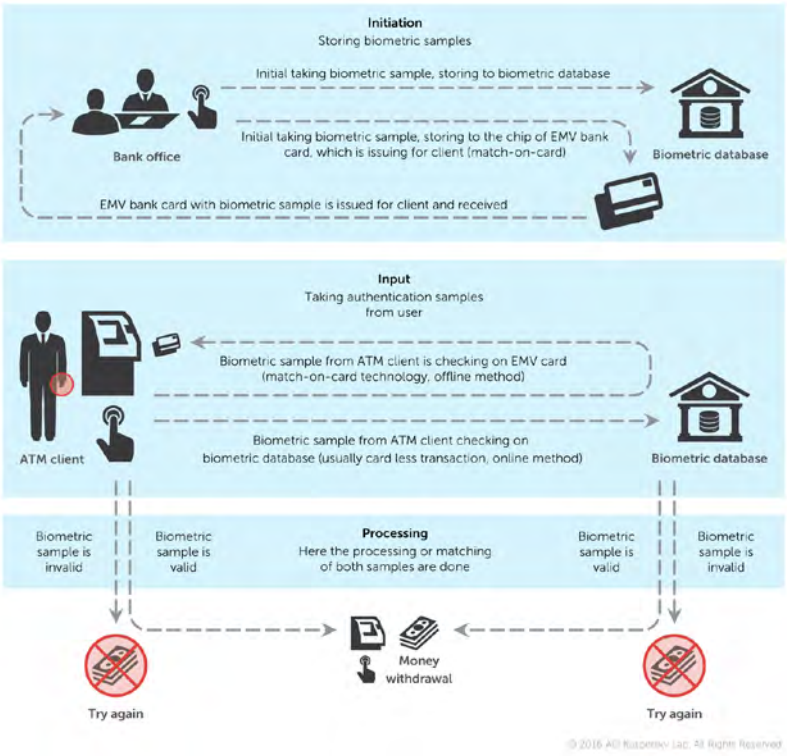


Figure 27 Simple scheme of biometric data flow

There are various malicious activities on underground forums to help attackers bypass biometric data recognition, according to the information from unofficial sources.

The creation of fake fingerprint readers is considered by malicious people to be more promising, because of its simplicity and low cost. Currently, there are about 12 manufacturers of fake fin-

gerprint readers. By comparison – the research and development of the palm vein and iris recognition systems involve about three companies due to the low popularity of those technologies, and the high cost of the equipment.

The first wave of presale testing of biometrical skimmers was in September 2015 and now the second is expected, in the EU. As a result of the first testing, developers discovered several bugs. However, the main problem was in using GSM modules for biometric data transfer, because obtained data was too large. New versions of skimmers use other data transferring technologies. Fraudsters started to create such devices after getting information on embedding biometrical scanners into ATMs.

Discussions are underway around the development of mobile applications based on the imposition of masks on the human face. An attacker can use a photo of a person posted on social networks in order to fool a facial recognition system.

So, what else have the criminals got via biometric data stealing?

The main properties of biometric data are its uniqueness, invariability and its non-repudiation. These properties make it possible to identify their owner uniquely and non-ambiguously. However, the more this data is used, the more likely it will be stolen. Thus, it is important to keep such data secure and transmit it in secure way. Biometric data is also recorded in modern passports – called e-passports, and visas. So, if an attacker steals an e-passport, he not only steals the document, but also that persons' biometric data. As a result he steals a person's identity.

5.3 Potential attacks techniques

Depending on the implemented logic for processing and transmission the authentication data potential attacker can use several attack vectors.

- Attacks on the Hardware components

- Attacks on the Software components
- Attacks on the Network layer

5.3.1 Attacks on the Hardware components

The general problem

ATM devices combine multiple units that are used to process the transaction and the money. Some of them are involved directly (e.g. a dispenser contains a money in cassettes) and indirectly (e.g. PC computer, that controls devices) with money. Such devices are interconnected with each other. Devices inside ATM box are considered trusted and it is supposed, that they can not be tampered or substituted with a rogue one. But often this practice is just a security through obscurity and devices doesn't have proper measures to identify the authenticity of unit endpoints (e.g. unprotected communication between the ATM core and ATM units.)

Black box attacks

1. An attacker may directly connect a malicious crafted device to the cash dispenser or the card reader.

All hardware units are connected to the ATM core (PC) through serial or USB ports, in rare cases SDC-bus. All the ATMs units and communication between them must be secure and authenticated. Such network of interconnected units is called trust zone. Entering trust zone should also be authenticated. If there a rogue device can enter trust zone, communication becomes unsecure, e.g. such device can bypass encryption and data is transmitted in plain text without circumventing protection mechanisms. In some ATM models those protection mechanisms are implemented, but not used by banks.

Black box attacks are popular methods of stealing money, and will be used more in the future. A black box attack is related to the direct manipulation of ATM devices, for example card readers (to obtain sensitive card information), or the cash dispenser (to jackpot money[16]). To per-

[16] Web-site: Olga Kochetova, February 26, 2016. Malware and non-malware ways for ATM jackpotting. Extended cut. Available at: https://securelist.com/analysis/publications/74533/malware-and-non-malware-ways-for-atm-jackpotting-extend-

form a black-box attack a criminal must disconnect the ATM's cash dispenser and attach it to an external electronic device - the so-called black box. The black box sends commands to the dispenser to eject cash, bypassing the need for a card or transaction authorization.

2. ATM manufacturers implement testing and debugging features which can be left in the production environment, and an attacker may use these to eject money.

As new devices are created, they are at first prone to different technical problems and issues. Thus, manufacturers often need to obtain technical information on the current state of hardware.

ATM vendors or third-party companies develop test or service tools for ATM hardware unit maintenance, making it possible to test cash withdrawals. This activity is protected by personalized token and cassette manipulation (service operators must open the safe door, using a safe key, and manipulate cassettes). Nevertheless, old or modified versions of these test tools can be installed onto a laptop or microcomputer, and this can be connected to the dispenser port or to the serial bus to eject cash. In some cases a specially crafted device can be connected to the serial bus via ports (e.g. EPP), which the attacker accesses through a hole made in the ATM's plastic cover.

Attacks on NFC devices

Newly installed in ATMs, NFC-readers or readers of biometric data with their proprietary drivers and programs will also require long-term testing before they are stable. This provides attackers with an excellent opportunity to explore the new device and assess how to take advantage of its vulnerabilities in the future.

Such attacks include gathering information from devices firmware, which can be downloaded from the device by using hardware debugging ports. Information gathered in such way can be later used to conduct attacks against devices with disabled debugging ports or even attack devices from similar family of devices.

The authentication data transmitted via NFC in plaintext may be intercepted by a rogue POS-terminal or a specially crafted smart-

ed-cut/ (Accessed 29/06/2016)

phone or device, which is then used for CNP-transactions. Stolen card data (stolen via skimming, for example) is then sold on underground forums.

For example, an attacker may prepare a specially crafted NFC-sniffer for biometric data sniffing from a customer bank card with an NFC-chip. He uses the NFC-sniffer in places with a huge amount of people, e.g. the metro. Approaching people closely, attacker collects card data from NFC-chip. Cards without NFC are protected by design against such attacks. NFC-card is protected if clients use physical protection against wireless communication (e.g. faraday cage). Then the attacker sells the card data on the black-market.

The attack scenario is shown in the figure below.

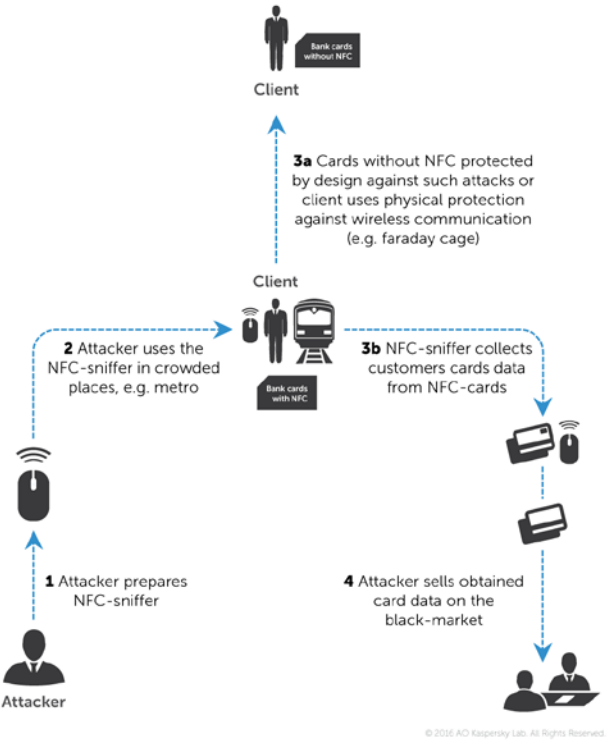


Figure 28: Scenario of attack “Stealing authentication data with NFC-sniffer”

Attacks on biometric data and devices

Biometric devices, which connect via USB/serial ports, might be hacked; and the data transmitted might be intercepted and stolen. There is identity theft, the sale of biometric data on the black market, and the use of stolen biometric data in other systems. It is a major problem for security: card information or PINs can be changed by customers after being compromised, but biometric authentication information is not modifiable and cannot be revoked after compromise.

An attacker can also use a biometric data skimmer to steal customers' authentication data. The attacker chooses the victim ATM and connects a specially crafted device which has been previously prepared for skimming biometric data. The attacker obtains biometric data (e.g., voice recordings) and can then use them in several ways:

- To authorize another bank service (online-banking, for example)
- To perform fraudulent online transactions and get money
- To sell biometric data on the black market.

Another attack technique is connected to stealing biometric data from EMV-cards using a special device.

The attacker prepares a specially crafted device for biometric data extraction from the customer's bank card with an EMV-chip. Using social engineering techniques he gets physical access to the customer bank card (or just steals it). The attacker then uses a malicious device to obtain the customer's card data, but if the card has implemented tamper-proof mechanisms attacker can only damage the chip biometric data during extraction, thus the data cannot be extracted. The attacker sells obtained biometric data on the black-market.

The attack scenario is shown in the figure below.

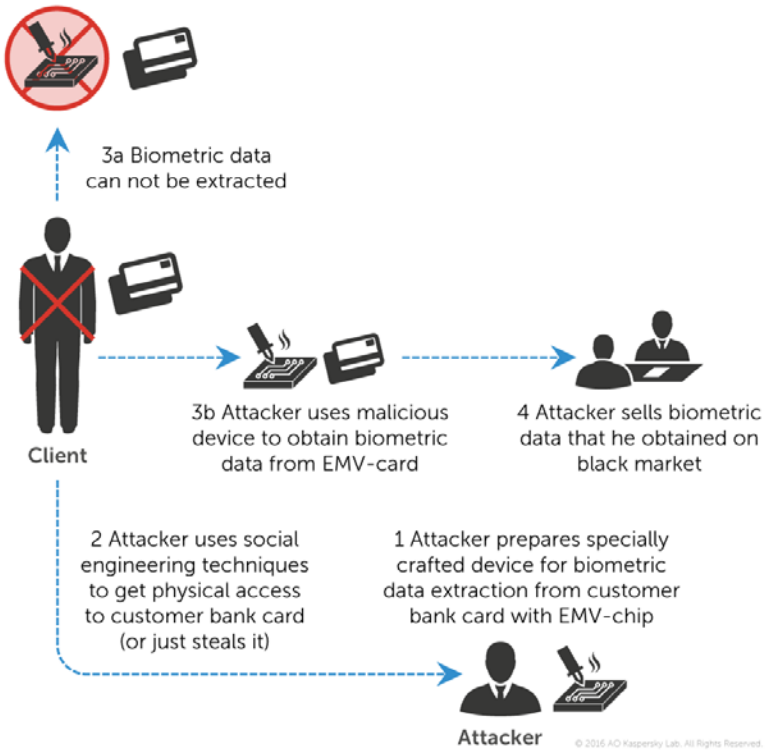


Figure 29: Scenario of attack "Stealing biometric data from EMV-card using special device"

5.3.2 Attacks on the Software components

The general problem

All information processing is based on software. When we talk about software, we should consider, that all problems that are

possible with attack on hardware components are possible by software means. Not to mention, that attack on software is much easier, because attacker has possibility to identify vulnerabilities by emulating all the necessary components by software means.

Malware attacks

The software is subject to zero-day vulnerabilities and may become easy prey for malware. Current state-of-the-art attacks in the malware world include several different approaches.

1. Memory scrappers

The main feature of these methods is memory scrapping/searching for sensitive customer information. This information includes Track2 data, personal information, and transaction history etc.

According to information provided by law enforcement agencies (LEAs), and the victims themselves, total financial losses from a Carbanak attack could be as a high as $1 billion[17] with more than 100 targets.

2. API-specific malware

The next generation of malware is leveraging the standard libraries and API of ATM vendors. The very same libraries that are used for legitimate interaction with an ATM can also be abused to obtain sensitive information about clients, or to interact with hardware to conduct fraud (including the unauthorized dispensing of money). It is safe to assume, that if a service engineer or authorized customer can do something with an ATM, an attacker can also do it without being checked if the software is not produced with security in mind.

XFS (CEN/XFS, and earlier WOSA/XFS), or the eXtensions for financial services, is a standard that provides client-server architecture for financial applications on the Microsoft Windows platform, especially peripheral devices such as ATMs. XFS is intended to standardize software so that it can work on any equipment regardless

[17] Web-site: Kaspersky Lab's Global Research & Analysis Team, Febraury 16, 2015. The Great Bank Robbery: the Carbanak APT. Available at: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/ (Accessed 29/06/2016)

of the manufacturer, and provides a common API for this purpose.

A simple scheme ATM infrastructure based on XFS is shown in the figure below.

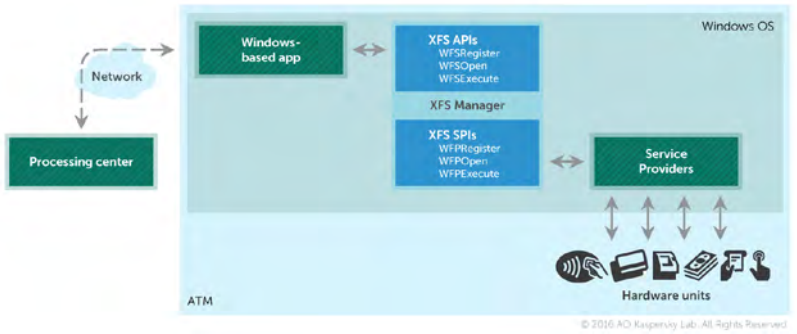


Figure 30 Simple scheme ATM infrastructure based on XFS

Thus, any application that is developed with the XFS standard in mind can control low-level objects by using only the logic described in this standard. And that application could well be any malicious program.

XFS provides attackers with the ability to manipulate:

1. Cash dispenser devices - an attacker can:
   - Perform cash withdrawals without authorization;
   - Obtain cassette and cash control;
   - Open the safe via software.
2. Identification card devices - an attacker can:
   - Control the processes that insert, eject and retain cards;
   - Read and write magnetic stripe card data;
   - Use the EMV-reader for accessing the payment history stored in chip.
3. PIN keypad devices - an attacker can:

Change secure mode to open mode for intercepting the PIN-code in clear text. To perform a PIN device man-in-the-middle attack, an attacker must request open mode from the PIN pad when the

client enters their PIN code. The attacker must acknowledge the button presses, but send an erroneous PIN block. The host will refuse the transaction, but now the attacker knows the client's PIN code (see pictures below).

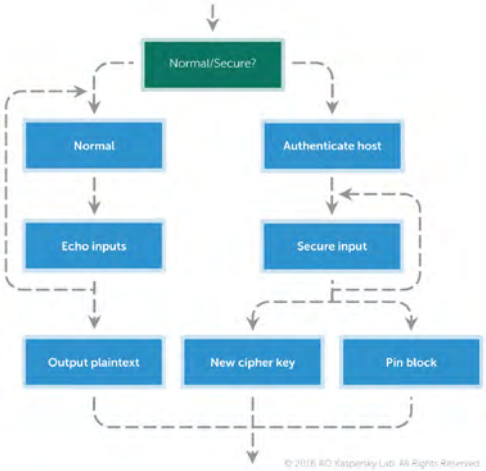


Figure 31 PIN device operation flow in open mode and secure mode

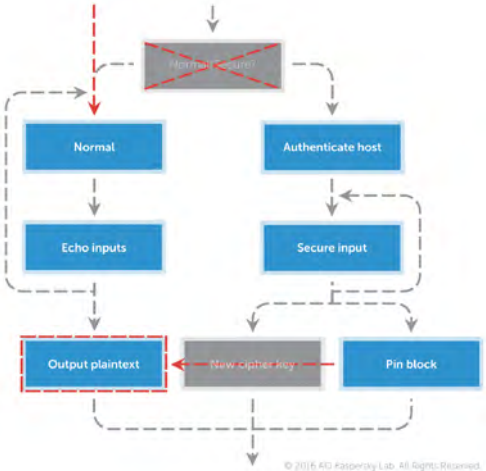


Figure 32 PIN device operation flow during Man-in-the-Middle attack

3. Skimmer – new generation malware

The latest generation of malware is more sophisticated. It employs a deep knowledge of ATM architecture and hardware. During an incident response investigation, Kaspersky Lab's expert team has found an improved version of a Skimmer malware on one bank's ATMs[18].

The Skimmer group starts its operations by getting access to the ATM system – either through physical access, or via the bank's internal network. After successfully installing Backdoor.Win32. Skimer into the system, it infects the core of an ATM – the executable responsible for the machine's interactions with the banking infrastructure, cash processing and credit cards.

Current functionalities of modified Skimmer malware include:

- **Directly commanding ATMs to dispense money** or covering interactions with malicious credit cards with special data
- **Interaction with smart cards** including receiving commands from smartcards, modifying itself from data on a card, sniffing sensitive information and conducting man-in-the-middle attacks
- **Gathering all information sent to the processing center,** because this information transfers in clear text, sending malicious data to the C&C centers or reverting SSL encryption

Skimer was distributed extensively between 2010 and 2013. Its appearance resulted in a drastic increase in the number of attacks against ATMs, with up to nine different malware families. This includes the Tyupkin family, discovered in March 2014, which became the most popular and widespread. Kaspersky Lab has now identified 49 modifications of this malware, with 37 of these modifications targeting ATMs by just one of the major manufacturers. The most recent version was discovered at the beginning of May 2016.

4. APT-attacks and implications on newer technologies

During spring 2016 it became widely known that the APT-group had kidnapped 81 million US dollars from a Bangladesh bank,

[18] Web-site: Kaspersky Lab's Global Research & Analysis Team, Olga Kochetova, Alexey Osipov, May 17, 2016. ATM Infector. Available at: https://securelist.com/blog/research/74772/atm-infector/ (Accessed 29/06/2016)

through its SWIFT system[19].

Attackers managed to get access to the Central Bank of Bangladesh, which holds an account in the Federal Reserve Bank of New York (part of the US Federal Reserve). The attack was implemented through the SWIFT system, and, as it became known later, the attackers used a custom malware of their own production.

The perfect example of the indirect attack on the ATM is the following incident. In August 2015 fraudsters using MasterCard payment cards issued by the bank "Kuznetsky" (Russia), dispensed 470 million rubles from the ATMs of other banks. The fraudsters used UCS processing system misconfiguration, which incorrectly handles rolled back transactions, and non-compliance on the international payments systems requirements.

This incident demonstrates the potential vector of attack for intruders, compromising banks and their components by defects and vulnerabilities in interbank exchange systems. This type of fraud chain is difficult to organize, but when successful, it is possible for attackers to compromise dozens of banking infrastructure components, including ATMs.

Another significant example of an APT-style campaign targeting (but not limited to) financial institutions is Carbanak. Carbanak attackers send phishing e-mails with a CPL attachment. After executing a shellcode, the backdoor is installed on the admin computer and, having gained access, it "jumps" through the network until finds a point of interest – ATMs.

ATMs have been instructed to dispense cash remotely without any interaction with the ATM itself, and with the cash being collected by straw men. With this method the SWIFT network was used to transfer money out of the organization and into the criminals' accounts; and databases with account information were altered so that fake accounts could be created with a relatively high balance, with straw men services being used to collect the money.

[19] Web-site: Mathew J. Schwartz, April 2016, Bangladesh Bank Attackers Hacked SWIFT Software. Available at: http://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061 (Accessed 08/07/2016)

Other kind of attacks via malware is interception card data in ATMs. Attacks that entail "Stealing authentication data using USB-port sniffer" are described in the document "Description of attacks and countermeasures".

5.3.3 Attacks on the Network layer

General problem

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

Man-in-the-middle attacks

As an entry point of attack intruders should use security or network misconfigurations on the ATM, or its externally available vulnerabilities, to conduct "man-in-the-middle" attacks.

There are several ways an attacker can compromise the network layer:

1. Lack of network segregation between ATMs

After getting ATM under their control, an attacker can gain access to other ATMs, which communicate with the compromised one. The attacker can then withdraw money from all hacked ATMs.

2. Lack of network protection between the ATM and the processing center

If the channel of interaction between the ATM and the processing center is not protected, and the processing of the server contains vulnerabilities, an attacker can gain access not only to a single ATM, but also to the processing center or other bank's services.

3. Lack of network segregation between an ATM and other parts of the bank's internal network

An attacker can gain access not only to the processing center, but also to the ATM's Active Directory host, to the ATM administrator host or even deeper – to bank office hosts or other bank's authen-

tication systems – because of network misconfigurations and segregation flaws.

The unsecure network's communications of ATMs with other banking components allows an attacker to intercept and modify the data being transmitted. This data may also be the authentication information that is unique to each client. If an ATM is under their control, an attacker can implement software interception, and if the ATM's casing is not hardened, physical interception with the devices is also possible.

The description of a "man-in-the-middle" network attack is provided in 6.1.

Network attacks on biometric database

An attacker can perform attack not on the ATM directly but on the biometric database, which contain the data of all clients. Attackers gather information about the maintenance supplier of the bank (i.e. from company/employee's profile on a website, social, ...), prepare malicious emails. Attacker uses social engineering tactics to send phishing e-mails to employees of ATM maintenance suppliers with malicious contents. The victim opens the e-mail with the malicious attachment, a malware with backdoor which allows the attacker to obtain AD administrator credentials. Not all the users open the email because they are aware or they have updates their antivirus software. Exploiting vulnerabilities, attackers escalate privileges and obtain database administrator credentials. Using uploaded malware attackers steal customer biometric data from the biometric database. Attacker sells the obtained data on the black-market or withdraws money via the straw man.

During the privileges escalation phase of attack, an attacker can find remote administration tools on the ATM administrator host, used for remote maintenance. Using installed remote administrative tools on the compromised ATM administrator host, the attacker can connect directly to the ATM. Then the attacker will easily upload malware on the ATM, affecting XFS manager and allowing malware to interact with the cash dispenser, withdrawing cash at the attacker's request.

5.4 Potential countermeasures

ATM security is a complex problem that should be addressed on different levels. Many problems can be fixed only by ATM manufacturers or vendors. Many countermeasures already exist and should be put to use by bank (or business structure which provide servicing of ATMs). Some can be mitigated by ordinary customers of ATMs.

The following lists include advices and possible countermeasures against attacks on ATM components (i.e. hardware, software and network). These countermeasures can effectively decrease risk of successful attacks and thus the fraud losses.

General recommendations

- Conduct regular ATM security assessments
- Monitor the situation on the black market (e.g. with Threat Intelligence reports)
- Conduct regular visual inspections of ATMs
- Mount video surveillance cameras inside and outside the ATM top box
- Enable all current security mechanisms implemented by manufacturers
- Use modern anti-fraud systems designed to prevent, detect and block fraudulent payment transactions
- Use additional authentication factors to confirm the financial transactions
- Use ATM monitoring systems
- Use Intrusion detection system/ intrusion prevention systems
- Implement organizational and technical measures to protect the ATM top box and external communication lines (including wireless)
- Implement organizational and technical measures to protect the ATM top box
- Encrypt data in-transit
- Use the technical means to protect the ATM - alarm system, vibration sensors, gas analysing system, drilling detection systems

- Use system to control unauthorized access to ATM units with possibility to break connection to unit (USB/SDC/COM connections)

Recommendations for preventing attacks on hardware components

- Implement authenticated dispense. Communications between the ATM core and ATM units, as well as communications between the ATMs and processing center must be encrypted (e.g. with TLS or VPN connections). The authenticity and integrity of these communications must be verified
- Use anti-skimming devices
- Implement cryptographic protection and integrity control over the data transmitted between all hardware units and PCs inside ATMs

Recommendations for preventing attacks on software components

- Implement the white-listing of software on ATMs
- Implement software integrity check mechanisms
- Implement a trust program zone on the ATM with secure means to authenticate such programs
- Use a strict access policy
- Use ATM malware protection systems
- Use strong encryption mechanisms for stored data
- Remove unused services and applications
- Establish a patching process and put upgrade procedures in place for the operating system and all software
- Conduct regular penetration tests on the infrastructure
- Use special sandbox tools to check the content of an unknown file

Recommendations for preventing attacks affecting the network communications

- Implement authenticated dispense. Network communica-

tions between the ATMs and the processing center, as well as communications between the ATM core and ATM units must be encrypted (e.g. with TLS or VPN connections). The authenticity and integrity of these communications must be verified
- Handle network segregation properly
- Eliminate network misconfigurations, and security flaws
- Use network access control mechanisms (e.g. 802.1x)
- Use antivirus and firewalls to protect against network attacks
- Remove excessive communication between ATMs, and between ATMs and the local network hosts (such as ATM administrator host, AD server etc.)
- Use a network security operation center (SOC) to monitor network activity
- Implement firewall protection in accordance with PCI DSS. All incoming and outgoing network connections for ATMs must be allowed only for a limited set of internal hosts and protocols. Restrict direct access to the ATMs from the Internet. Ensure that the ATM network is protected against man-in-the-middle attacks over protocols of data link and network layers.
- Monitor newly added devices and hosts

Recommendations for personnel

- Conduct regular security awareness trainings
  - Social media (including acceptable social media user policy)
  - Email anti-phishing trainings
- Inform employees about current information security measures
- Install anti-virus programs, with anti-spam systems on employees hosts

Recommendations for clients

- Inform clients about current information security measures
- Conduct an anti-phishing awareness campaign

- Increase customers awareness on secure usage of cards, ATM and necessity of authentication data secrecy

Recommendations in case of incident

- Implement a strategy for card data revocation in case of customer data leakage
- Conduct forensic investigations to obtain information on the scale of the attack

6 Attack scenarios against authentication systems communicating with ATM

In this section, are provided examples of attacks against authentication systems communicating with ATM.

6.1 Man in the middle attack

***Attack Description**:* Attackers connect the specially crafted device to the exposed Ethernet-cable or into the adjacent network socket, conduct man-in-the-middle attack and withdraws money from ATM
***Attack vector**: Network*
***Objectives**:* steal money
***Attack techniques**: attack on device, spoofing*

Attack Phase	Description	Countermeasures
1 Information gathering	Attacker gathers information about the maintenance supplier of the bank and prepares a specially crafted device which emulates the processing center	• Conduct security awareness trainings • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with Threat Intelligence reports)
2 Victim identification	Attacker chooses the victim ATM devices. These must have network equipment available on the outside, an exposed Ethernet-cable or insecure wireless communications (e.g. GSM)	• Conduct regular visual inspections of ATMs • Mount video surveillance cameras inside and outside the ATM top box • Use ATM monitoring systems • Implement organizational and technical measures to protect the ATM top box and external communication lines (including wireless) • Conduct regular ATM security assessments

Attack Phase	Description	Countermeasures
3 **Obtaining logical access to ATM network**	Attacker connects the specially crafted device to the exposed Ethernet-cable or into the adjacent network socket	• Remove unused services and applications • Handle network segregation properly • Eliminate network misconfigurations, and security flaws • Use network access control mechanisms (e.g. 802.1x) • Use a network security operation center (SOC) • Monitor newly added devices and hosts
4 **Network traffic manipulation**	Attacker conducts man-in-the-middle attack (e.g. ARP or DHCP spoofing) in order to connect other ATMs to the rogue processing center. Not all machines are susceptible to spoofing attacks, because of network segregation or implemented network security measures.	• Handle network segregation properly • Eliminate network misconfigurations, and security flaws • Use antivirus and firewalls to protect against network attacks • Remove excessive communication between ATMs, and between ATMs and the local network hosts (such as ATM administrator host, AD server etc.) • Establish a patching process and put upgrade procedures in place for the operating system and all software • Network communications between the ATMs and the processing center, as well as communications between the ATM core and ATM units must be encrypted (e.g. with TLS or VPN connections). The authenticity and integrity of these communications must be verified. • Enable all security measures implemented by manufacturers • Conduct regular penetration tests on the infrastructure
5 **Money withdrawal**	Attacker withdraws money from ATMs by issuing commands from the rogue processing center and emulating legitimate commands	• Use fraud monitoring systems • Implement authenticated dispense (network communications between the ATM processing center and ATM units must be encrypted. The authenticity and integrity of these communications must be verified) • Conduct forensic investigations to obtain information on the scale of attack

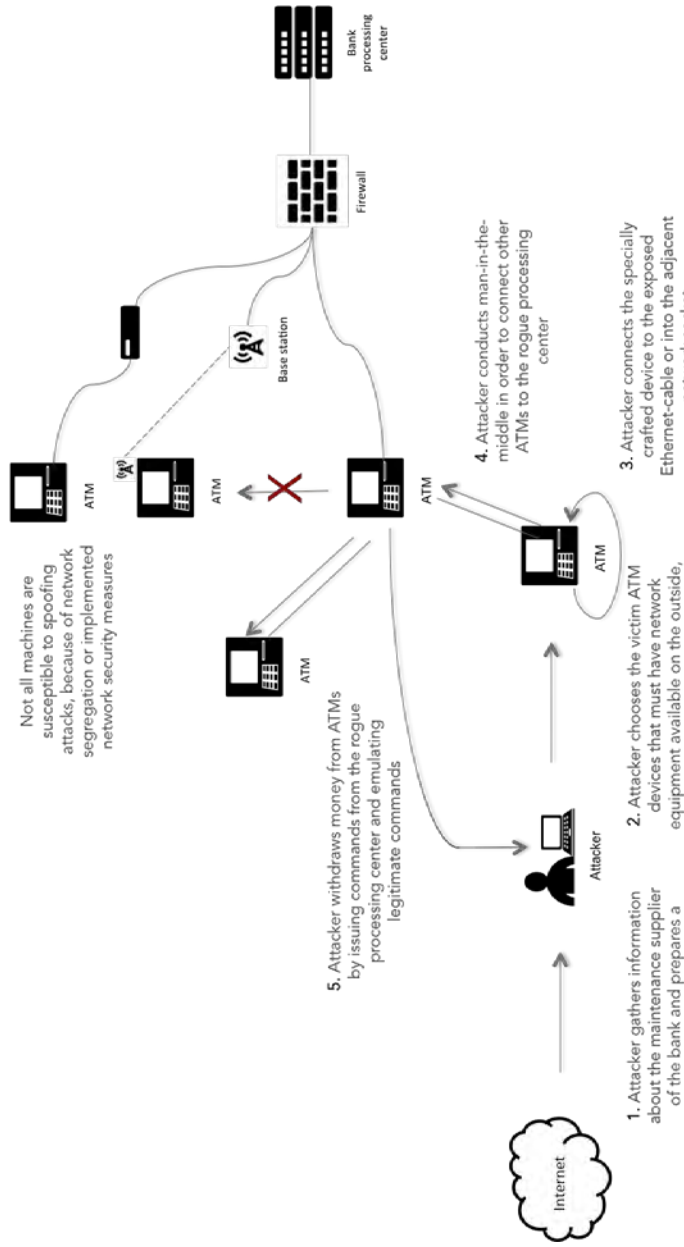


Figure 33: Man in the middle attack

6.2 Stealing authentication data using a USB-port sniffer

***Attack Description**:* attackers use a USB port sniffer to collect customer authentication data and card data, allowing him to perform fraud and sell it on the black-market
***Attack vector**: Software*
***Objectives**: steal customer data*
***Attack techniques**: malicious software, sniffing*

Attack Phase	Description	Countermeasures
1 Information gathering	Attackers gather information about the bank's maintenance supplier (i.e. from the company / employee profile on the bank's website, social media, etc.), and prepares malicious emails	• Social media acceptable user policy • Social media awareness campaign • Conduct security awareness trainings • Inform users and employees about information security measures
2 Victim identification	Attacker uses social engineering techniques to send phishing e-mails to employees of the ATM maintenance suppliers with malicious contents (such as the exploit code in an attachment)	• Use Intrusion detection system/ intrusion prevention systems • Run an anti-phishing awareness campaign, • Install anti-virus programs, with anti-spam systems on employees hosts
3 Spear-phishing attack	The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal network. Not all the users open the email because they are aware or they have updates their antivirus software.	• Behavioural monitoring system • Install anti-virus programs, and anti-spam systems on employee hosts • Use special sandbox tools to check the content of an unknown file • Monitor the situation on the black market (e.g. with threat intelligence reports)

4 **Privileges escalation**	Exploiting vulnerabilities, the attacker escalates privileges and obtains ATM administrator credentials. Using AD functionality for group policies, the attacker uses on ATM software USB-port sniffer.	• Implement software integrity check mechanisms • Implement a trust program zone on the ATM • Use a strict access policy
5 **ATM infections**	Using the installed sniffer, the attacker collects customer authentication data and card data, allowing him to perform fraud	• Use ATM malware protection systems • Use strong encryption mechanisms for stored data • Encrypt data in-transit • Implement the white-listing of software on ATMs
6 **Customer data leakage**	Attacker sells obtained data on the black-market	• Use fraud monitoring systems • Implement a strategy for card data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

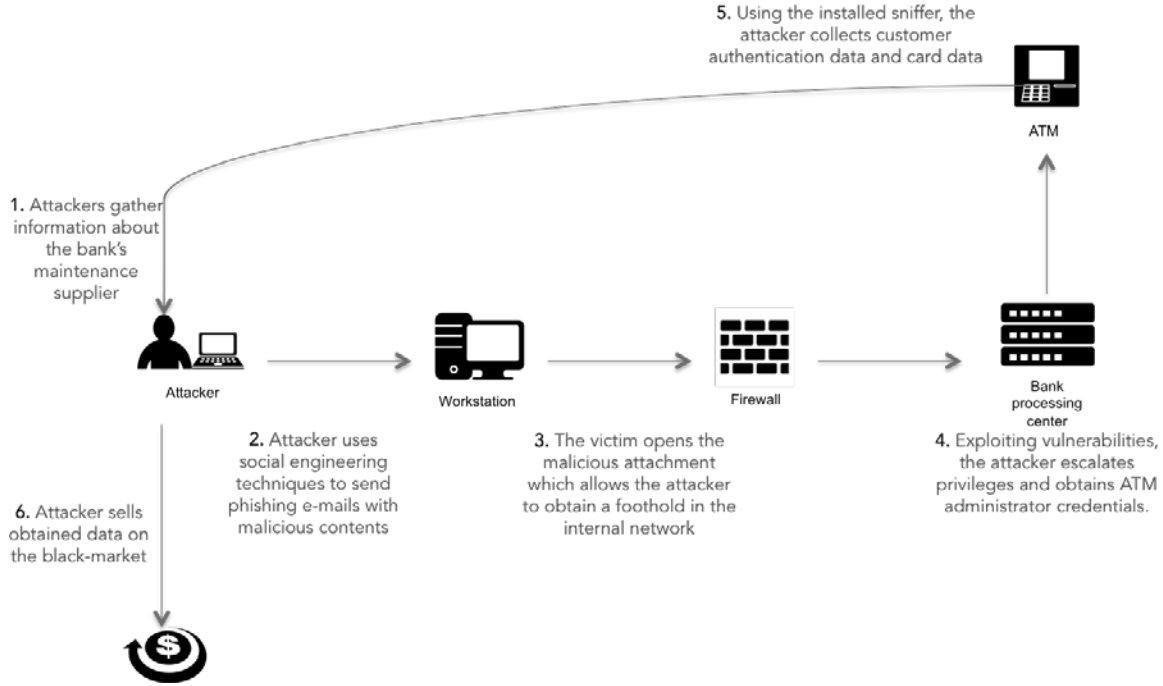


Figure 34: Stealing authentication data using a USB-port sniffer

6.3 Stealing biometric data using skimmer

***Attack Description**: attackers* use a biometric data skimmer to steal customers' authentication data and use it to authenticate and withdraw money or conduct fraudulent online transactions
***Attack vector**: hardware*
***Objectives**: steal money*
Attack te*chniques: Steal customer biometric data and money*

Attack Phase	Description	Countermeasures
1 Information gathering	Attacker gathers information about the maintenance supplier of the bank and prepares a specially crafted device for biometric data skimming	• Conduct security awareness training • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with threat intelligence reports)
2 ATM skimmer	Attacker chooses the victim ATM and connects to a specially crafted device for biometric data skimming	• Conduct regular visual inspections of ATMs • Mount video surveillance cameras inside and outside the ATM top box • Use ATM monitoring systems • Use anti-skimming devices • Implement organizational and technical measures to protect the ATM top box • Conduct regular ATM security assessments • Increase customers awareness on secure usage of cards, ATM and necessity of authentication data secrecy
3 Biometric data interception	Attacker obtains clients' biometric data (e.g. voice record)	• Conduct regular ATM security assessment • Enable all current security mechanisms implemented by manufacturers

Attack Phase	Description	Countermeasures
4.a Biometric data interception	Attacker uses stolen biometric data to authorization in another bank service (e.g. online-banking)	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack
4.b Selling in the black market	Attacker sells stolen biometric data in the black market	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack
5 Fraudulent online transaction	Attacker conducts fraudulent online transactions and gets money	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

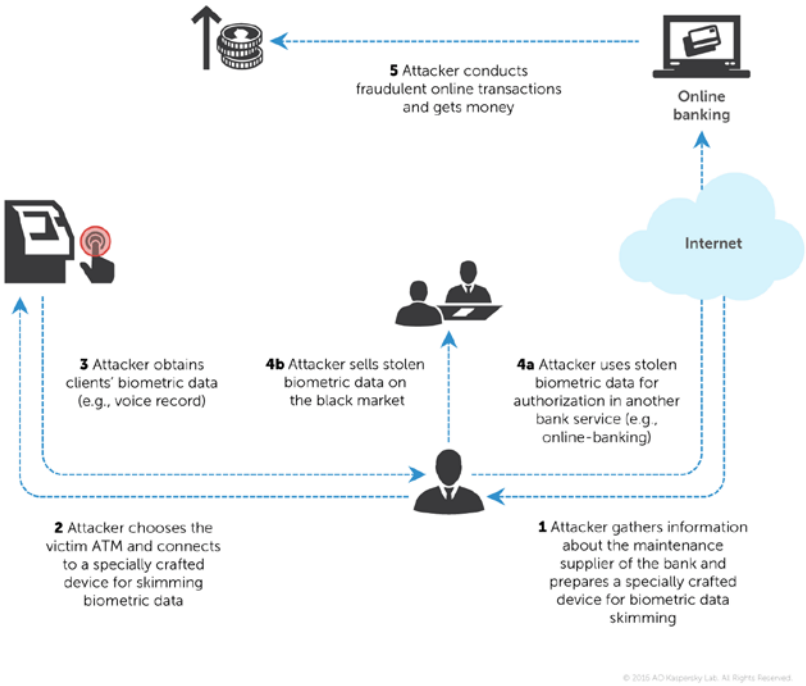


Figure 35: Scenario of attack "Stealing authentication data using biometric data skimming"

6.4 Stealing biometric data from the biometric database

Attack Description: Attackers perform attack not on the ATM directly but on the biometric database, which contain the data of all clients. They infect ATM maintenance suppliers workstations sending phishing e-mails with malicious contents, exploiting vulnerabilities, escalate privileges and obtain database administrator credentials and using uploaded malware steal customer biometric data from the biometric database.
Attack vector: network
Objectives: steal biometric data
Attack techniques: malicious software and APT techniques

Attack Phase	Description	Countermeasures
1 Information gathering	Attacker gathers information about the maintenance supplier of the bank, prepares email list of the bank employees and prepares malicious emails	• Conduct security awareness trainings • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with Threat Intelligence reports)
2 Victim identification	Attacker uses social engineering techniques to send malicious email (with exploit code in attachment)	• Use Intrusion detection system/ intrusion prevention systems • Run an anti-phishing awareness campaign, • Install anti-virus programs, with anti-spam systems on employees hosts
3 Spear-phishing attack	The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal network Not all the users open the email because they are aware or they have updates their antivirus software	• Behavioural monitoring system • Install anti-virus programs, and anti-spam systems on employee hosts • Use special sandbox tools to check the content of an unknown file • Monitor the situation on the black market (e.g. with threat intelligence reports)

Attack Phase	Description	Countermeasures
4 Privileges escalation	Attacker conduct lateral movement in the network by exploiting vulnerabilities to escalate privileges and obtain database administration credentials	• Implement software integrity check mechanisms • Implement a trust program zone on the ATM • Use a strict access policy
5 Biometric data stealing	Attacker steals customers biometric data from the biometric database	• Use strong encryption mechanisms for stored data • Encrypt data in-transit • Use tokenization for data security
6 Selling on the black market	Attacker sells obtained biometric data on the black market	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack
7 Money withdrawal	Attacker uses obtained biometric data to withdraw money using straw man	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

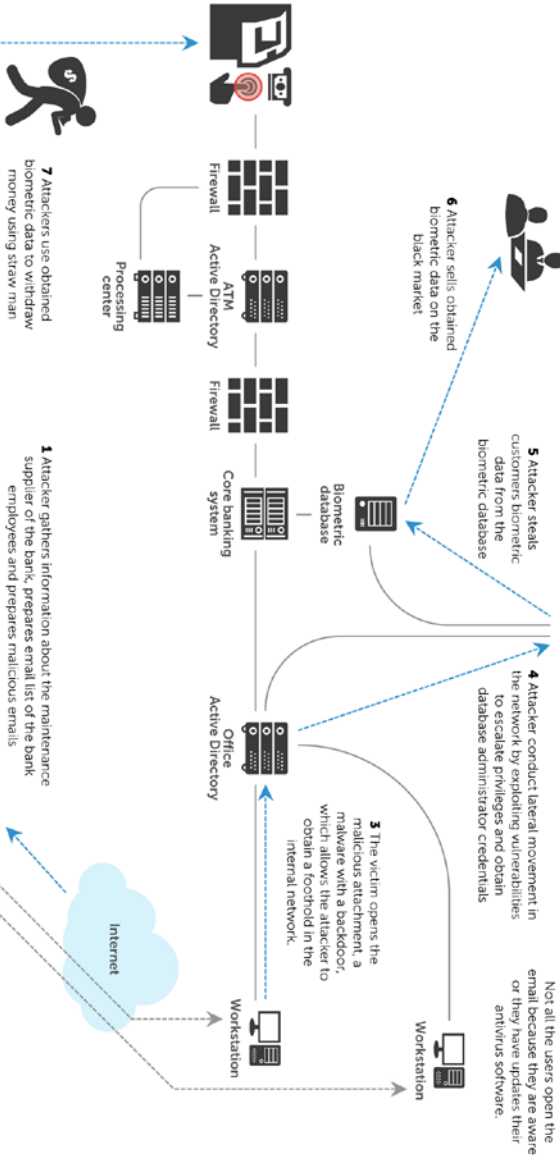


Figure 36 Scenario of attack "Stealing biometric data from the biometric database"

6.5 Stealing authentication data via remote administration tools

Attack Description: Attackers perform attack directly on the ATM. They infect ATM maintenance suppliers workstations sending phishing e-mails with malicious contents, exploiting vulnerabilities escalate privileges and obtain database administrator credentials, connect and compromise ATM with a malware and withdraws money.
Attack vector*: Network*
Objectives*: steal money*
Attack techniques*: malicious software and APT techniques*

Attack Phase	Description	Countermeasures
1 Information gathering	Attacker gathers information about the maintenance supplier of the bank, prepares email list of the bank employees and prepares malicious media	• Conduct security awareness trainings • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with Threat Intelligence reports)
2 Victim identification	Attacker uses social engineering techniques to send malicious email (with exploit code in attachment)	• Use Intrusion detection system/ intrusion prevention systems • Run an anti-phishing awareness campaign, • Install anti-virus programs, with anti-spam systems on employees hosts
3 Spear-phishing attack	The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal bank	• Behavioural monitoring system • Install anti-virus programs, and anti-spam systems on employee hosts • Use special sandbox tools to check the content of an unknown file • Monitor the situation on the black market (e.g. with threat intelligence reports)

Attack Phase	Description	Countermeasures
4 Privileges escalation	Attacker conduct lateral movement in the network by exploiting vulnerabilities to escalate privileges and obtain database administration credentials	• Implement software integrity check mechanisms • Implement a trust program zone on the ATM • Use a strict access policy
5 ATM connection	Using the installed remote administrative tools on the compromised host, attackers connects to the ATM	• Implement software integrity check mechanisms • Implement a trust program zone on the ATM • Use a strict access policy
6 ATM infections	Using remote access, the attacker uploads malware, which affects XFS manager, on the ATM	• Use ATM malware protection systems • Use strong encryption mechanisms for stored data • Encrypt data in-transit • Implement the white-listing of software on ATMs
7 Money withdrawal	Malware interacts with cash dispenser and withdraws money	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

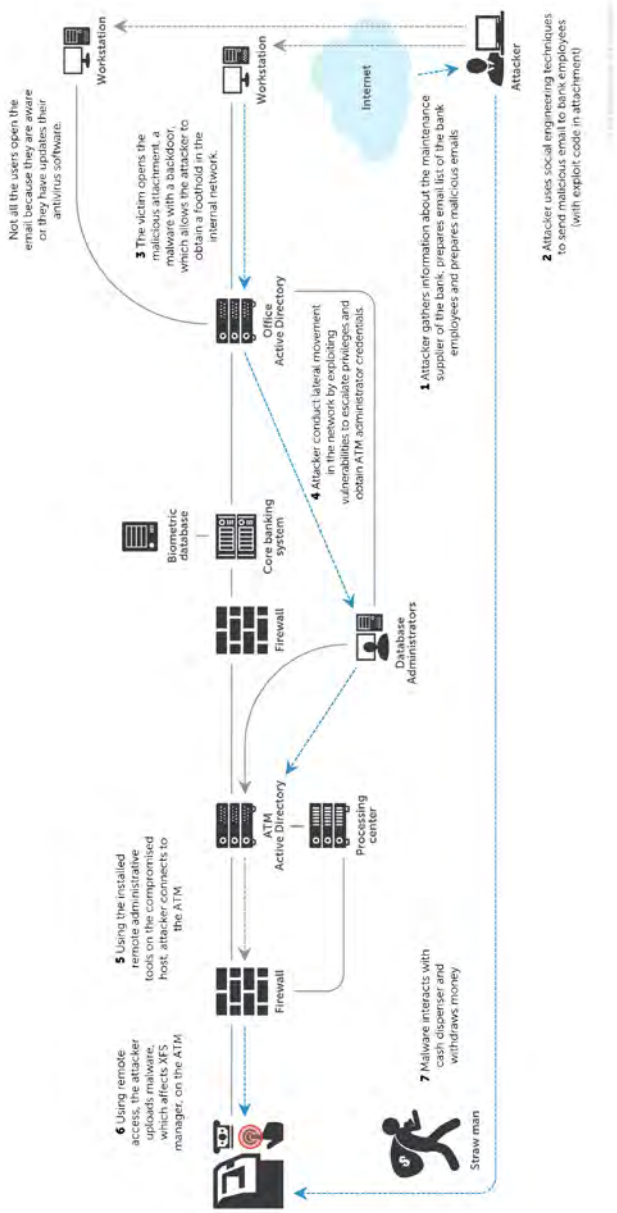


Figure 41 Scenario of attack "Stealing authentication data via remote administration tools"

7 Attack scenarios against ATM system: a point of view of an ATM operator

Each day we hear of new reports of attacks on ATMs from around the world. More and more frequently we hear of ways that the criminals continue to vary and modify their attack to attempt to bypass the protections in place. The sophistication of the criminal's tools and methods have also increased.

Understanding each of the crimes can become complicated and seem overwhelming. As we look at the landscape we are able to look at the broader picture. This view shows that the types of crimes fall into three general categories.

- Identity Theft
- Logical Theft of valuable media
- Physical Theft of valuable media

In this section, we will describe the available attack techniques that are used, and illustrate how the attacks evolve as an 'arms race' develops between the defenders and the attackers.

NCR will also describe effective strategies for each category that can be used to win the war in each case.

7.1 Identity Theft

Identity Theft refers to the category of crimes that are used to capture the data used by a consumer to authenticate themselves at a Self Service Terminal to enable financial services.

The most frequent attack vectors in this category include Card Skimming, Card Trapping, and Card "Sniffing".

A card skimming attack is defined as 'the unauthorized capture of magnetic stripe information by modifying the hardware or software of a payment device, or through the use of a separate card reader'. Skimming is often accompanied with the covert capture

of customer PIN data. Armed with this information, the fraudsters create dummy cards and raid the customer's account.

The devices used in Card Skimming Attacks fall into a variety of categories. However, they all have in common that they are foreign devices that contain some form of electronic device that is used to read and capture data from the magnetic stripe from the card being used to activate the ATM transaction.

The most common forms of Card Skimmers are:

- Bezel Mounted Card Skimmers: These are devices that are made to fit over the existing bezel of the ATM. They appear to look like the authorized bezel.
- Insert Skimmers: Are small electronic devices, designed to fit inside the card reader. Due to the nature of their size Insert Skimmers are nearly impossible for the layman to detect.

Card Skimming remains, by far the most frequent form of ATM attack, and currently represents nearly 95% of all losses from ATM attacks. Card skimming frequency remains high even in markets where EMV has been fully deployed and Chip cards are used. This is the case since the vulnerability here lies with the magnetic strip that is on the card. As long as the magnetic stripe remains on the card and the card is passed through any device that reads the magnetic stripe data there will be the risk of card skimming.

These forms of card Skimming can be effectively prevented thought the deployment of comprehensive anti-skimming solutions. Card Skimming has become something akin to an arms race. Historically there has been a vicious cycle between the criminals and the ATM manufacturers and companies who sell card skimming device. A solution is developed in response to a form factor of the skimmer. The criminals then go back and vary the skimmer to bypass the solution, making the current solution vulnerable, the ATM deployers then is forced to by new solutions. The pattern then repeats itself.

A different approach is needed for the strategy to protect from card skimming solutions.

Effective anti-skimming must contain the ability to both detect the presence of a skimmer, attempt to disable the skimmer and provide notification to the ATM operator that skimming is occurring at that ATM.

All of these components are included in best in class anti-skimming solutions

Eavesdropping Attacks: In this attack, a hole is made in the ATM or access gained to the top box of the ATM. Electronic hook ups are attached directly to the card reader to attempt to capture the information.

Eavesdropping attacks can be prevented by retrofitting existing ATMs with physical barriers around the internal card reader.

Network sniffing attack: With this approach the criminals attempt to capture the cardholder information as it is being sent from the ATM to the ATM switch or host. This is done by attaching a device onto the network connection cables. There are several layers to the defence strategy to protect against network sniffing attacks.

The easiest and immediate defence would be to add a physical barrier to prevent any unauthorized access to the network cables. This can be by shielding the wires in a conduit, or behind the wall. More sophisticated solutions would be to deploy secure communication connections. Implementation to TLS encryption is recommended. Encrypted wireless communication can also be deployed in addition to the TLS to provide additional protection against this form of attack.

The following table represents a summary of the attack threats in this area, and the recommended solutions to protect ATMs.

Skimming Category	Description	Recommended Solutions
Bezel Overlay	Manufactured overlay containing a skimmer which fits a specific ATM model	Anti-skimming solutions with Skimmer Detect and Alert Monitoring
Bezel Insert	Manufactured insert containing a skimmer which fits a specific ATM model	Anti-skimming solutions with Skimmer Detect and Alert Monitoring
Card Read Tap – Destructive (Eavesdropping)	Attacks that penetrate the ATM fascia or cabinet with the intention of providing direct access to the card reader	Anti-skimming solutions with SPS with Skimmer Detect and Alert Monitoring, plus Anti-Eavesdropping protection
Card Read Tap - Non-Destructive	Attacks that involve opening the ATM cabinet with the intention of providing direct access to the card reader	ATM location security, appropriate cabinet locks, encrypted USB
Differential Skimming (Stereo Skimming)	Using twin read heads connected in differential mode to negate the effects of a jamming signal	Anti-skimming solutions with SPS with Skimmer Detect and Alert Monitoring
Deep Insert Skimmer	A device placed inside the card reader using the card slot as the entry point	Card reader device detection firmware, Third party anti-insert kits
Sabotage	Any attempt to disable any anti-skimming technology	Anti-skimming solutions with SPS with Skimmer Detect and Alert Monitoring
Shimming	Capture of chip card data with the intent to produce a cloned mag strip card	Transaction Authorisation as per EMV
Network Sniffing	Capture of card data via sniffing of network communications to the host	Communications Encryption TLS 1.2
Malware Sniffing	Capture of card data via malicious software installed on the ATM Hard Disk	See controls for Offline and Online Malware in the following section

7.2 Logical Theft of Valuable Media

Logical theft of valuable media refers to the category of crimes that are used to steal cash or other valuable media, from the ATM using methods which do not physically breach the cash enclosure. This category is the one where we are experiencing to greatest rise in number and variety of attacks. This category is also the one which makes use of modern technology to exploit features of ATMs which would not have been considered vulnerable at the time of the original ATM design. Since 2012 there has been an alarming increase in the frequency of these forms of attacks. We have now seen successful logical attacks occur in all global regions. The nature of these crimes allow the attack to occur on a large number of ATMs at once. The outcome of the crime could be the theft of all of the cash in the ATM. This can lead to very significant financial losses in a very short period of time.

Typically, these attacks fall into three major categories:

- Black box attacks
- Malware in the Network
- Malware installed on the ATM

In a Black Box Attack, the criminal gains access to the dispenser cable inside the ATM. They then bypass the ATM's core processor and connect an electronic device to the cash dispenser. The criminal is then able to send unauthorized commands to dispense cash from the ATM. ATMs should have high levels of internal dispenser encryption to provide protection from these forms of attack. This protection requires the ATM operator setting the Dispenser Security Setting at Level 3 (Physical) as well as running current versions of platform software and device firmware.

The second category is where Malware in the Network allows the criminal to intercept the communications between the ATM and host. With this they are able to capture information or cause unauthorized dispense of cash from the ATM amongst other things. Encrypting the communications channel between the ATM and the host, along with good network security controls can prevent these network based attacks.

Another type of attack is when malware is installed on the ATM hard drive. This software is often designed to allow the criminal to send commands to the ATM that cause an unauthorized dispenses of cash from the ATM.

There are two major variations of these malware attacks.

One where the attack is done while the ATM Hard disk in online (with its operating system up and running in its normal state). This is typically done using USB devices with Auto play enabled or using a known Windows Administrator password.

The other variation, which is the most common logical attack against ATMs, is an offline attack. An offline attack is when an attacker inserts removable media (for example, DVD, CD or USB) into an ATM core and reboots the ATM. The ATM will then boot to the removable media. Malware is then copied from the removable media onto the ATM hard disk. The ATM is rebooted again with the removable media detached allowing the ATM to start up as normal. However, now the ATM has malware running on its hard disk.

These forms of attacks can be prevented by:

- Deployment of Whitelisting solutions tools that are designed to protect the software that is installed on the ATM. This is done by ensuring that Only authorized code can run. That authorized code or memory cannot be tampered with. That authorized code or memory cannot be hijacked.
- Encrypting the ATM hard disk. This makes the hard disk unreadable when offline. When it is unreadable, attackers cannot copy malware onto the hard disk.
- In addition to preventing offline attacks, Hard Disk Encryption also prevents reverse engineering of the deployed software stack. The solution prevents dispenser encryption keys being copied from the hard drive when it is offline. This will provide an additional layer of protection from black box attacks.
- Locking down the BIOS. This prevents the ATM from booting to removable media. When an attacker inserts removable media into the ATM core and restarts the ATM, the ATM will not boot to that device. The ATM will start as normal.

- Encrypting the ATM hard disk. Hard Disk Encryption is the most comprehensive protection against offline attacks on ATMs.
- Protects against offline malware attacks Prevents malware being copied onto the hard disk when the ATM is booted from removable media
- Prevents malware being copied onto the hard disk when the ATM hard disk is removed and mounted as a secondary drive
- Ensures the contents of the hard disk is encrypted and unreadable when it is removed from the ATM core, when the core is removed from the ATM, when network connectivity is compromised

Protection from logical attacks is only possible through the complete deployment of a layered and comprehensive deployment of security guidelines. These include:

- Secure the ATM BIOS to only allow boot from the primary hard disk. BIOS editing must be password protected.
- Establish an adequate operational password policy for all passwords. A single password for every ATM is not secure.
- Implement communications encryption (TLS encryption or VPN). This should be considered as mandatory if you are using public wide area networks.
- Establish a firewall. This also should be considered as mandatory if the ATMs are on a public wide area network.
- Remove unused services and applications. Any code is a source of vulnerability, so minimize it.
- Deploy an effective whitelisting applications.
- Establish a patching process for Operating System Patches.
- Establish a regular patching process for ALL software installed.
- Disable Windows Auto-Play.
- Ensure the application runs in a locked down account with minimum privileges required.
- Define different accounts for different user privileges.
- Remotely & securely control passwords with enhanced permissions.
- Deploy a network authentication based Hard Disk Encryption Solution

- Ensure there is protected communications to the dispenser of the ATM.
- Perform a Penetration Test of your ATM production environment annually
- Use Remote Software Distribution. This helps enable some of the earlier security requirements.
- Consider the physical environment of ATM deployment

An additional, but critical layer of the solution strategy comes with the deployment of Enterprise Fraud detection solutions. This layer provides the financial institution with the ability to track and monitor transactions throughout all of their channels. The Fraud detection solution will provide the ability to note abnormal transaction patters. This can include frequency of transactions, location of transactions by geography and by merchant.

7.3 Physical theft

Physical theft of valuable media - the category of crimes that are used to steal cash or other valuable media, from the ATM using methods which physically breach the cash enclosure. This category includes all of the traditional robbery techniques that can be used to open a safe, and includes emerging trends of using explosives.

These crimes continue to be major problems for ATM operators. According to data provided by the European ATM Security Team, nearly 50 million Euro were lost from physical attacks on ATMs in 2015.

The main categories of these physical attacks are:

- Explosions to physically breach the safe. Traditionally this was done in certain regions where there was easy access to solid explosives, such as dynamite. More recently we have seen a scary increase in the use of gas explosives. This has led to these forms of attacks occurring in more areas of the world.
- Cutting the safe by some means of brute force. This can be done using torches or grinders.
- Ram Raid – instances where the ATM is physically removed from its installation environment.

Key protective strategies here center around ensuring that ATM op-

erators choose the correct safe based on the threat environment.

These solutions include:

- Cash degradation solutions such as Ink Staining or Glue solutions that will make the cash unusable if the ATM cassette is breached.
- Gas Detection / Neutralization solutions can be installed to detect the presence of gas used as part of an explosive attack. These devices can be configured to trigger alarms, smoke, sirens, or other notifications. Gas neutralization will counteract the presence of an explosive gas to prevent an explosion from occurring.
- GPS devices and ATM trackers can be installed to both notify when motion is detected on an ATM, and the location of the ATM can be monitored.

8 Attack scenario when ATM is a bridge for attacks

8.1 GENERAL DESCRIPTION OF ATTACKS

With the increasing use of plastic money the spread of Mobile Payments and micropayment systems, the use of cash will become more and more a residual ability to perform transactions on ATM terminals. At the same time the capillary diffusion of terminals, which is developing also in emerging countries, represents an opportunity to provide access to the most various services, in particular for those poor technological penetration reality or where this is geographically concentrated.

The ability to access money services growths with the availability of access to computer networks in an increasing number of people.

The same types of money services are evolving in a manner often released with each other, just think of the introduction of cryptocurrency and the use of complementary currencies, still confined in small market niches, but exposed to the pressures of globalization.

Regarding cryptocurrency, for example, you can find now terminals can process Bitcoin transactions already in various parts of the world ATM.

These terminals, called BTM, are an example of a response to a specific need of technologically advanced users.

In addition to advanced money services, the ATM terminals will have the possibility to become the access point for a whole series of additional services not directly related to the banking and financial world.

Figure 38: Bitcoin ATM Map (source Coin ATM Radar)

Gradually we will see the transformation of ATM terminals from simple dispensers of cash and delivery of services related to money, to advanced terminals offering worldwide new features to citizens and businesses.

Even now it is possible use ATM terminals, known as totems or kiosks, which provide a range of services not directly related to banking, such as ticketing and booking, e-commerce, and specific e-government services.

Natural evolution will be the integration of the functionality of these kiosks in ATM terminals, mainly to take advantage of diffusion and User Base.

The ATM terminals still maintain long-features relating to the provision and management of money but as a further evolution, they will bind more usage to the mobile world, especially in countries where the use of terminals and mobile networks is more widespread. The User Interface already is moving inside mobile terminals and in apps. The users will use more and more mobile terminals to interface to the ATM and get access to the different services offered, until the payment of the money in CNP manner.

All these innovations and developments open new opportunities and new attack scenarios for both petty crime, more and more aligned with technological evolution, both the organized crime that might be interested in the new possibilities of money launder-

ing provided by the new technologies.

From all the news foregoing, but also from the evolution of the personal authentication systems, for example biometrics, it derives the extension of what in Information Security is defined as "Attack Surface".

This term refers to the set of possible vectors exploitable by an attacker with intent of interacting fraudulently or not with a system or application.

Typically the attack surface increases as the interconnections with other systems, the various points of interaction, by the number of features offered and then, as you might guess, with the generic system complexity.

The attack surface of the existing ATM systems is quite delineated and over the years has been defined in a more and more detailed and a series of countermeasures have been developed to prevent or mitigate a series of identified threats.

The developments outlined above will considerably change the technological and business environment and introduce new challenges to be faced to allow a sufficiently secure service delivery, banking and non.

8.2 Attack Scenarios using ATM as a bridge for attack

This section describes possible scenarios and related countermeasures that we can imagine today. These scenarios are derived in part from the evolution of the well-known attack patterns, in part have been hypothesized analysing the possibilities arising from:

- The introduction of new authentication mode
- The interconnection of devices in systems other than banking
- The ability to manage users' personal information
- The ability to manage the identity, digital or not, of users
- The introduction of new features

- A general increase in the complexity of the systems and infrastructure
- Use in conjunction with systems and infrastructures characterised by low technological maturity and security

ATM proxy attack

This attack is inspired on an investigation of Security Brokers conducted during a test of a e-government services infrastructure in a state of Southeast Asia. During the Penetration Testing, on a kiosk were found signs of hacking that would suggest an attempt to unauthorized access to e-government systems.

The assumption on the base of this scenario is that security requirements implemented for heterogeneous services are rarely aligned to the level of the most critical one.

Consider an ATM terminal able to provide not strictly financial or banking services. In this case, usually the ATM terminal is connected to an external service provider and dialogues with the various systems that compose the infrastructure. In fact, normally these services are not delivered through the banking systems and infrastructure.

In this case, the ATM terminal is as a point of contact between two realities with different criticality and applied countermeasures.

For an attacker, the external service provider represents a easier attack vector to access to the ATM terminals or to the interconnection network. Compromising any of these systems presumably requires a less effort than required to directly violate the terminal or the banking network.

Once obtained the access to the Service Provider network, the attacker have to deal with the different countermeasures, if present, up to reach a login, more or less privileged to a system that interacts with the ATM terminal. For example, the threat agent may be able to compromise the system that deploys the updates of one of the non-banking applications running on the ATM terminal.

In absence of mechanisms to verify the legitimacy update sent and a good management of segregation between applications it is plausible to expect that the updated application with the malicious code can be executed with sufficient privileges to allow direct access to the ATM terminal, for example with a reverse shell.

The ATM terminal becomes a bridgehead for the execution of direct attacks on banking systems, because it is authorized to communicate with the various networks creating in fact an Advanced Persistent Threat.

In the event that inspired this scenario, the attack had been carried in a more simplified way, exploiting a remote vulnerability in the Windows XP operating system, still widely used in ATM kiosks and terminals, gaining complete control of the system.

Only a change of addressing plan in the compromised system network was able to block the attack preventing the implementation of tools for the persistence and extent of control to the e-government systems, which were subject of activity of information Gathering.

Man in the ATM

In recent times, the ATM banking service is becoming increasingly popular to meet the user's need to reduce the time necessary for carrying out simple operations in a self-service mode, but also to meet the banking world, interested in reducing the costs arising from the presence of the tellers.

Today at the ATM terminal, it is now possible execute the most common banking transactions, such as paying bills, carrying out transfers or prepaid credit recharge.

These type of operations are performed more often using ATMs as a point of access to the same online banking services accessible via Internet.

After user authentication by card and pin, the terminal proposes

the execution of transactional operations, generally with a simplified interface.

The online banking services have been the subject of several malware distribution campaigns with the intent to capture the customer access data and then perform fraudulent operations

To contain the effects of these cyber-crime campaigns, over time a series of countermeasures have been implemented. They vary from the use of one-time password systems for the confirmation of order transactions to real-time reporting of transactions.

By accessing the Online banking services from ATM terminals typically, these additional countermeasures are implemented in a more bland, even for usability issue,. These are usually limited to the notification of the transaction. This stems from the belief that the user is better protected authenticating to a system (ATM) considered inherently more secure compared to a Personal Computer and therefore it is possible to decrease any precautions normally implemented.

The Online banking services might become particularly attractive, in case of ATM compromised by malware. Today the banking malware can be considered a enough mature “technology”, thanks to the widespread availability of Exploit Kit and even banking-Trojan-as-a-Service.

It is very easy to imagine a future union of the know-how of malware for ATM and Banking to steal large amounts of money, more than currently obtainable before the block of a card for suspicious movements. Imagine for example a scenario in which an agent of threat is able to infect some ATM terminals with a malware able to interact with the online banking application. It may happen with the complicity of the maintenance staff (as often happens in some countries) or with an APT attack.

This malware could resemble the recently discovered malware, such as Mangit or the new Skimmer, but offer fraudulent features related to bank accounts and not directly to cash cards.

It is easy to assume that these malware are able to intercept, in a

silent way, all need to perform transactional operations, perhaps in a massive and coordinated way, activated via the ATM interface. They can remain silent for all the time needed to identify, for example through analysis techniques of memory or traffic interception, transactions to change real time recipient information before the execution of required transaction or of recurrent payments to hide unsolicited transactions among those legitimate.

These malicious codes can implement techniques to by-pass one-time password systems or benefit from their absence if not implemented.

Particularly attractive could be transforming an ATM compromised with a malware in a system for the execution of money laundering operations, using the authentication information captured to perform the Money Laundering techniques, such as the Smurfing.

8.3 Examples of Attack patterns

In this section, are described possible attack patterns applied in the scenarios presented in the previous section

8.3.1 ATM proxy attack

Attack Description: Through the compromise of a non-bank, service provider is conceivable to obtain the installation of malicious software that allow direct access to the ATM and after use that device as a bridge to access the other interconnected networks available
Attack vector: software & network
Objectives: use the ATM as a proxy between networks with different security levels
Attack techniques: malicious software & APT techniques

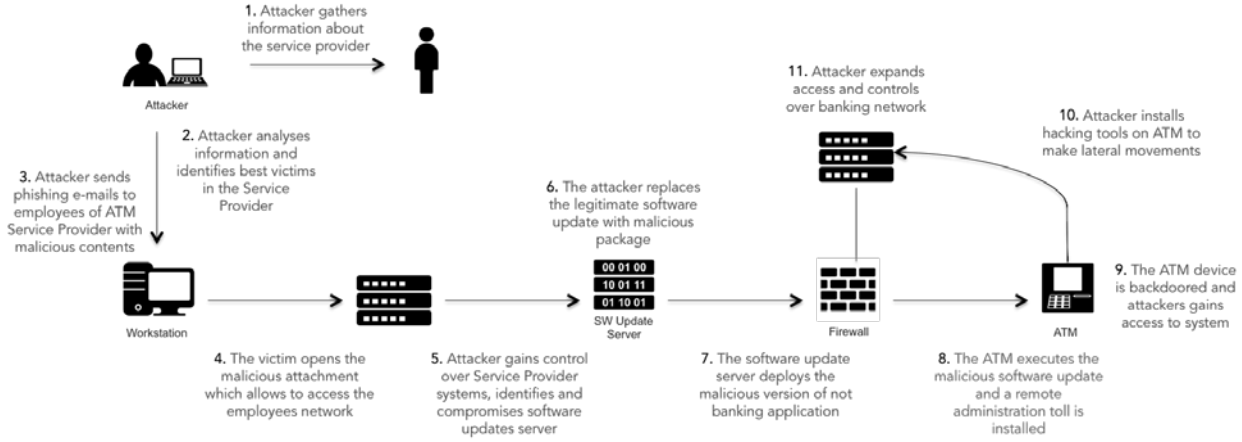


Figure 39: ATM proxy attack

Attack Phase	Description	Countermeasures
1 Information gathering	Attacker gathers information about the service provider	• Social Media Acceptable User Policy • Social Media awareness campaign
2 Victims identification	Attacker analyses information gathered and identifies best victims in the Service Provider	• OSINT Analysis & Countermeasures
3 Spear-phishing attack	Attacker sends phishing e-mails to employees of ATM Service Provider with malicious contents	• Intrusion Detection System/ Intrusion Prevention System • Anti-phishing awareness campaign • Anti-spam systems
4 Remote access to the network	The victim opens the malicious attachment, a backdoor, the attacker installs a remote administration tool and accesses the employees network via a reverse shell	• Executable sandboxing • Intrusion Detection Systems • Correct firewall policies • Log analysis and Correlation
5 Update server compromise	Through the reverse shell attacker gains control over Service Provider systems and identifies and compromises the server that handles software updates	• Intrusion Detection Systems • Host Intrusion Detection Systems • Correct firewall policies • Log analysis and Correlation
6 Malicious software update	The attacker replaces a legitimate software update with malicious software update package that allows attackers to gain access on ATM device (e.g. a reverse shell)	• Integrity check on software deployed
7 Malicious software update deploy	The update server deploys the malicious version of not banking application	• Secure software update best practices

Attack Phase	Description	Countermeasures
8 Malicious software update execution and ATM device	The ATM device executes the malicious software update and a RAT is installed	• Secure software update best practices • Executable sandboxing • Virtualization for application isolation
9 ATM Device backdooring	The ATM device is backdoored and attackers gain access to system through a reverse shell	• Executable sandboxing • Intrusion Detection Systems • Correct firewall policies • Log analysis and Correlation
10 Tools install	Attacker installs some hacking tools on ATM to perform discovery, maps adjacent networks, escalates privileges and accesses and makes lateral movements from the entry point	• Executable sandboxing • Host Intrusion Detection System • Intrusion Detection Systems
11 APT on banking network	Through the reverse shell attacker expand access and control over banking network	• Intrusion Detection Systems • Correct firewall policies • Log analysis and Correlation

8.3.2 Man in the ATM

Attack Description*:* use a hacked/infected ATM to attack banking service and execute unauthorized transactions, with the intent of stealing customers ' money by bank wire or using bank accounts for money laundering
Attack vector*: software*
Objectives*: use the compromised ATM to steal money or make money laundering*
Attack techniques*: malicious software*

Figure 40: Man in the ATM attack

Attack Phase	Description	Countermeasures
1 **ATM compromise**	The ATM is compromised by using any technique known and gets infected by a malware	Executable sandboxing Virtualization for application isolation[20]
2 **Malware memory analysis**	Malware analyses ATM memory and acquires IBAN, login information or identify applicative operation	Executable sandboxing Virtualization for application isolation
3 **Malware modify applicative operation**	Malware modifies on the fly the recipient IBAN for wire transfer and transaction is made by user	Time OTP Mobile OTP2 Executable sandboxing Virtualization for application isolation
3bis **Malware inject applicative operation**	Malware injects other applicative operations after transaction made by user	Time OTP Mobile OTP[21] Anti-fraud system with behavioural analysis and frequency and small threshold Cyber intelligence on compromised IBAN or bank account used by money mules
3ter **Malware execute applicative operation**	Malware executes smaller wire transfer from many customer bank account to many other bank account to	Anti-fraud system with behavioural analysis and frequency and small threshold Cyber intelligence on compromised IBAN or bank account used by money mules

[20] In some cases, the use of virtualization technologies is itself a bulwark to the spread of malware, because several malicious codes contain in them routines that will stop the execution in the presence of clues of a virtualized environment. The malware deeming to be running on a virtualized system used for sandboxing and analysis will turn off for protection from reverse engineering.

[21] The use of SMS as One Time Password must be considered insecure because of the many attack vectors available (i.e. SS7 signalling technology vulnerabilities)

9 Standard and Regulation

9.1 Standard list

This article describes the current existing set of Security Standards, Guidelines, Regulations, Sets of Requirements, Laws etc. involved (at different grades and levels) with ATMs.

The image below addresses ATM components that, under attack, may lead to the compromise of sensitive data (PIN, sensitive/account data or keys); components of an ATM, such as the cash dispenser or the safe, that are not directly related to compromise of PIN or sensitive/account data, are not within the scope of this article.

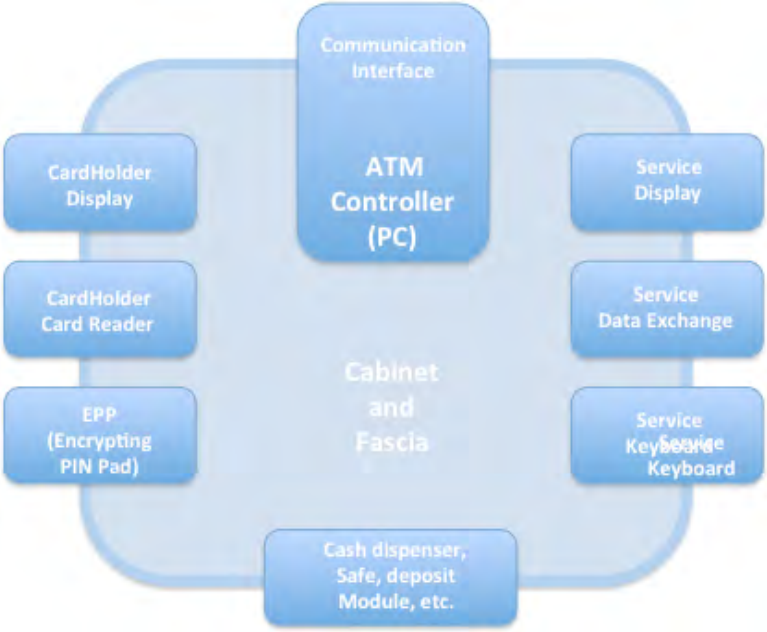


Figure 41: ATM components that may lead to compromise of sensitive data

Let's start with a first important note: ATMs (as a whole) are not covered by any existing Security Standards.

Many technical IT security standards have been produced about ATMs. They address their operation, cryptographic key management, wireless connectivity, operating system hardening, physical security, skimming, etc. They also address different stages of the ATM security life, from configuration to deployment and initialization. These standards and guidelines are originated at ISO, ANSI, PCI SSC, EPC, and ATMIA or issued by vendors themselves. The most relevant implementation and usage guidelines are listed below.

As organized global crime targets ATMs, the financial industry needs a global ATM security standard to promote the availability of secure ATMs. The main characteristics of this standard would be:

- Focus on mitigating the effects of skimming and PIN-stealing/data-stealing attacks
- Primarily targeted at products from ATM vendors and deployers
- Provide a complementary framework for device approval (evaluation methodology, evaluation facilities, and approval management)

The current versions of PCI PTS POI Security Requirements and PCI PIN Security Requirements (see below) are excellent starting points for these needed standards. However they are currently defined for POS terminals and their adjustment to ATMs is currently under consideration at the PCI Council.

Until there is an effective PCI ATM standard, the perceived current guidance gaps:

- ATM vendors need direction to develop the next generation of ATMs.
- PCI Payment Brand acquirers need support for their procurement processes and to educate their deployers and customers

are addressed in the "Information Supplement: ATM Security Guidelines" document by the PCI Council, attached to the "PCI PIN

Transaction Security Point of Interaction Security Requirements (PCI PTS POI)" Standard, also by the PCI Council.

Here is a list of the Standards, Guidelines, Regulations, Sets of Requirements etc. involved (at different grades and levels) with ATMs, starting with the above mentioned supplement by the PCI Council:

1. Information Supplement: ATM Security Guidelines
2. PCI Data Security Standard (PCI DSS)
3. PIN Transaction Security (PTS) requirements
4. Payment Application Data Security Standard (PA-DSS)
5. P2PE
6. PCI-PIN
7. VISA Operating Regulations
8. Consorzio Bancomat
9. EMV
10. ISO
11. NIST
12. ATMIA
13. EPC/SEPA includes PCI-PIN and PCI-DSS
14. Italian Law

9.2 In-Depth List Analysis

PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. The Scope is very simple. Assets dealing with PAN are in scope, assets not dealing with PAN are not. Subjects involved are:

- Banks
- Merchants
- Service Providers (subjects dealing with PAN and not in the other three categories)
- Payment Applications Developers

It is important to point out that Banks must be PCI DSS compliant, although they do not need a formal validation by a PCI Assessor (known as a QSA – Qualified Security Assessor) and by a PCI ASV (Approved Scanning Vendor).

Payment Applications Developers actually must be compliant to PA DSS (see below).

Merchants and Service Providers are organized in Levels, depending on the number of transactions per year or the number of managed PANs per year.

The main points to be mentioned about Levels are the following:

- Level1 subjects must undergo an On-Site Audit performed by a QSA
- Non-Level1 subjects should compile a Self-Assessment Questionnaire (known also as SAQ)
- All subjects must undergo 4 External Scans per year performed by an ASV

The 6 topics and the12 Macro-Requirements of PCI DSS are:

- Build and Maintain a Secure Network
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  - *Requirement 2*: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data

- Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security

As is easily seen, PCI DSS is both a technical-oriented and a process-oriented (very good) Set of Requirements. PCI DSS can be seen as the main reference point when it comes to secure a set of assets (a CDE) dealing with CHD, which includes ATMs Infrastructures and related processes.

In general, the PCI Council approach and vision can be depicted by the following Image, which includes all the Standards mentioned in this study.

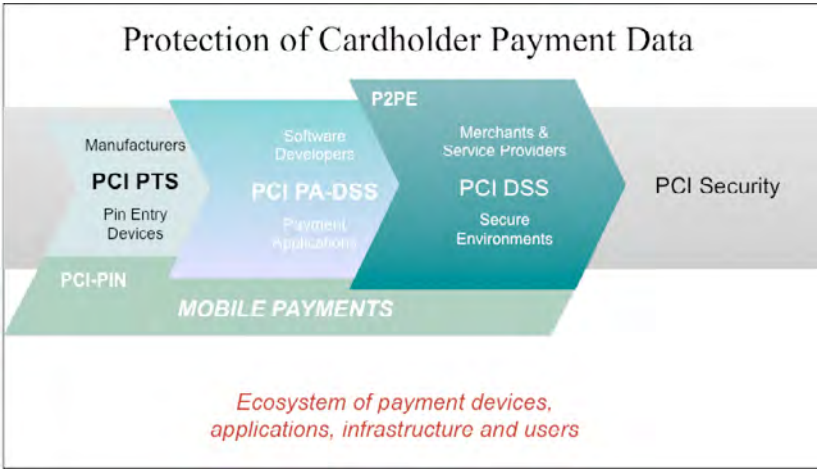


Figure 42: PCI Council approach and vision

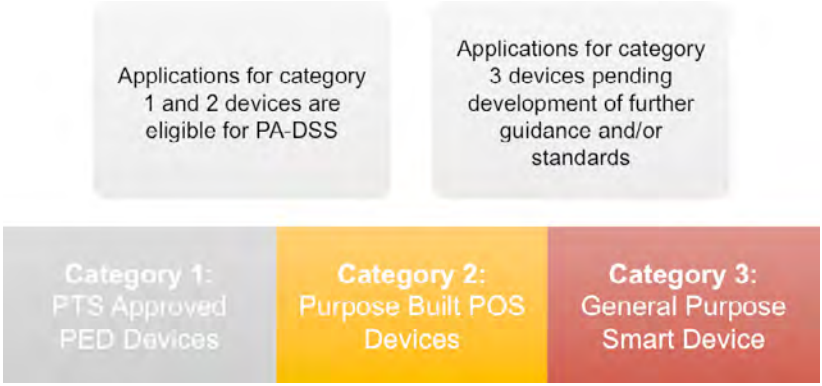
All the Security Standards in the Payment market are moving under the PCI Council management.

PIN Transaction Security (PTS) requirements

PIN Transaction Security (PTS) requirements, which contains a single set of requirements for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads and unattended payment terminals. A list of approved PIN transaction devices is maintained by the Council and can be accessed on-line.

Payment Application Data Security Standard (PA-DSS)

Payment Application Data Security Standard (PA-DSS) aims to help software vendors and others develop secure payment applications. The Council maintains a list of Validated Payment Applications.



PA-DSS is the best candidate for covering "new solutions", but this Image summarizes a very important fact: the whole emerging world of new General Purpose Mobile Devices - based

Solutions are far from being covered by PA-DSS or by any similar Security Standard.

In other words, an "official" Security Standards coverage (at the present time) cannot cope with the time-to-market of the new emerging Payment Solutions.

It is interesting to point out that a long-time existing Security Standard (ISO15408, also known as "Common Criteria") could cover also Payment Solutions, being a general-purpose (although very heavy) set of requirements for building Secure Systems at various levels of acceptance (up-to military ones and/or mission-critical levels).

P2PE

P2PE is a set of validation requirements for point-to-point encryption solutions, and provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE

solution for account data acceptance and processing.

PCI-PIN

PCI-PIN - The Visa PIN Security Programme is a global programme designed to ensure all participants in the acquiring transaction processing chain maintain the highest level of Personal Identification Number (PIN) security. The confidentiality of cardholder PINs used in CC transactions depends on all payment system participants complying with the following applicable requirements:

- Payment Card Industry PCI PIN Security Requirements
- PCI PIN-Entry Device Security Requirements
- PCI Encrypting PIN Pad Security Requirements
- PCI Point of Interaction Requirements
- Visa Requirements.

These requirements are designed to ensure the secure transmission of cardholder PINs from the point of entry. The PCI PIN Security Requirements complement the PCI Data Security Standards (DSS) for entities that accept or process PIN-verified transactions. PIN-accepting entities must be fully compliant with the PCI PIN and PIN Transaction Security (PTS) Requirements.

PCI-PIN covers the PIN production and management processes from the Back-Office point of view. It is directly managed by VISA itself, so it does not have a third-party-based certification approach. Many PCI-PIN Audits (performed by VISA personnel) had taken place in Italy in the last few years, involving major Banks and Service Providers.

VISA Operating Regulations

VISA Operating Regulations are series of tomes existing in three

versions: domestic, European and global. They contain the rules governing VISA's operations, including those applying to PCI Standards and the related fees.

Consorzio Bancomat

Quoting the official description: "Consorzio BANCOMAT® is the owner of the BANCOMAT® and PagoBANCOMAT® brands, and the Governance Authority of the related Circuits. Banks and Payment Institutions willing to offer BANCOMAT® and PagoBANCOMAT® capabilities to their customers (meaning POS or ATMs able to accept such Cards) can adhere. Subjects adhering to BANCOMAT® and PagoBANCOMAT® Circuits must be compliant to the Security Rules given by the Consorzio and make sure that the Cards and the Terminals supplied to their customers comply with the Security Standards given by the Consorzio itself".

As can be easily seen, the above mentioned Standards are Italian-only, and they must be included in the compliance management processes together with all the others, dealing with the unavoidable overlap issues.

Recent publications:

- Circolare n. 2 /2016 – 2 Maggio 2016 –BANCOMAT Security Verification Framework
- BANCOMAT Security Verification Standard
- Best practice per la gestione sicura delle transazioni a marchio BANCOMAT e PagoBANCOMAT

EMV

EMV is a technical standard for smart payment cards and for payment terminals and ATMs that can accept them. EMV is an acronym for Europay, Mastercard and Visa, the three organizations that developed the initial specifications. EMV is an open-standard set of specifications for smart card payments and acceptance devices. The EMV specifications were developed to define a set of

requirements to ensure interoperability between chip-based payment cards and terminals.

ISO

ISO 15408 (Common Criteria)
ISO 11568: Banking – Key Management (Retail)
ISO 27XXX (up to ISO/IEC 27002:2015)

Common Criteria (CC) is a Standard (born after ITSEC) aimed to certify secure-built systems, where a "system" could be a piece of software, a piece of hardware/firmware, or some IT assets too. It can go up to military-grade certifications. It is very interesting because it can be applied to almost everything, and its guidelines about building a secure system are amazingly applicable. It is also very interesting because it contains several formal definitions of terms widely (and wrongly) used nowadays, including "Vulnerability Assessment" and "Penetration Test", and most of all because it introduces the concepts of "Effectiveness Analysis" and "Correctness Analysis". Truly secure systems can be built ONLY after a Correctness Analysis, which is something similar to the more-commonly known "White-Box Analysis".

ISO27XXX is a Standard dealing with IT Security Management. It can be considered having a "Quality management" approach. For the purpose of this article, it is interesting that it contains requirements covering the compliance issues, which leads to an "othogonal" approach through Requirement 15 of ISO27001-2 (or Requirement 18 of ISO/IEC 27002:2015), with huge potential of implementing synergies with PCI DSS and related Security Standards.

NIST

Quoting the official description: "From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterial, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology. Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce."

NIST Standards and Guidelines are often used as de-facto references in many IT Security matters. Examples:

- Guidance for securing Microsoft Windows XP systems for IT Professionals
- Wireless Management and Security — Part 1: General Requirements
- Wireless Management and Security — Part 2: ATM and POS

EPC/SEPA

- SEPA
- Guidelines for ATM Security European Payment - Council DTR 413
- Recommended ATM anti-skimming solutions within SEPA European Payment - Council Doc115-8

The Single Euro Payments Area (SEPA) stands for a European Union (EU) payments integration initiative. It focuses on the integration of the euro payments market. Since the introduction of the Euro currency, the political drivers have called upon the payments industry to bolster the common currency, by developing a set of harmonised payment schemes and frameworks for electronic euro payments.

SEPA cites to PCI-PIN and PCI-DSS as the Security Standards to be followed.

Italian Law

Italian Law should be always taken into consideration when dealing with IT Security matters, not only for (obviously) being compliant with the Privacy issues, but also for being ready to apply the right legal procedures when a compromise event occurs. Taking the wrong actions when such an incident occurs leads to non-legally-usable compromised assets, meaning that they can not be used as legal proofs.

9.3 Possible contents of a future ATM dedicated security standard

As can be easily seen, ATMs as a whole are not covered by any single Security Standard. ATMs are directly (and partially) covered only by PCI-PTS for the PIN Pad and (for Italy only) by the Consorzio Bancomat requirements.

Banks, financial entities, manufacturers, developers etc. must try to comply with all the above in the best way possible.

The PCI Council, however, has already listed the possible contents of a future ATM-dedicated Security Standard, which is summarized here:

Integration of Hardware Components
Objective: Avert magnetic-stripe and other account data compromise and PIN stealing
Security targets:

- EPP, readers, cabinet, privacy shields, anti-skimming devices
- The ATM cabinet and the ATM controller
- Guidelines for further integrators and software developers

Intended audience: ATM manufacturers/deployers/operators, ATM integrators, repairing organizations, refurbishers

Security of Basic Software
Objective: Avert magnetic-stripe skimming and PIN stealing
Security targets:

- Operating System, BIOS
- Middleware (XFS, CEN XFS, CEN J/XFS, multivendor software, Open Protocols)

Intended audience: Software integrators, application developers, ATM manufacturers/deployers/operators

Device Management/Operation
Objective: Ensure adequate management of:

- ATM during manufacturing
- ATM in storage of deployed ATM estates
- ATM individual security configuration (hardware and software)

Security targets:

- Cryptographic/key management, from initialization/distribution to decommissioning
- Manufacturing management system
- Estate management process and tools
- Environmental security

Intended audience: ATM manufacturers/deployers/operators and supporting organizations/service providers

ATM Application Management
Objective: Address security aspects of the ATM application. **Security targets**: Security functions driven by the ATM application and application management
Intended audience: Application developers, software integrators, ATM operators

10 Conclusions

Although it is highly challenging for the different types of organisations (such as Banks, Terminal Managers, Application and Authorisation Centres, etc.) involved in the management of ATM solutions and support systems to "keep up" with the technological developments that make it possible to perpetrate often effective fraudulent attacks, a structured model for security management continues to represent one of the most effective strategies to prevent and counter increasingly complex criminal activities.

But, essentially, what does it mean to build a well-structured security management system?

There is definitely no "one size fits all" approach, since it would not be productive to define a universal method without clearly taking into consideration the many organisational, technological, and contextual features that characterise the various actors operating in payment systems.

However, it is at least possible to track down the drivers that may accompany organisations in the design and consequent implementation and monitoring of their security management systems, outlining a truly structured organisational model.

A suitable security model should in fact be rooted in constantly updated risk analysis, in order to focus and maximise resources and energies on the areas most exposed to risk without wasting efforts on events that – at present – are unlikely to occur and/or have a low impact.

For this purpose, it is necessary to:

1. **Automate the detection of known phenomena,** by creating a record of incidents ("event collection") and successful resolutions in order to implement effective and "proven" strategies in the shortest time possible;
2. **Identify unknown phenomena,** by discarding known events

and allowing, by exclusion, the early detection of unknown phenomena that have circumvented preventive controls;

3. **Channel information in the right direction,** by having full knowledge of the expertise and internal processes of the organisations in order to direct information to "strategic" nodes of the service delivery chain;
4. **Prioritise interventions,** by focusing efforts where vulnerabilities with the greatest impact are detected, avoiding the dispersion of resources and at the same time facilitating monitoring activities.

However, the strength of security models also depends on the availability and quality of information: organisations should, in fact, maintain a dynamic classification of terminal attacks, countering solutions, and preventive approaches to fraudulent activities. By drawing from this wealth of information, they would be able to enrich their models and continuously update the same in order to keep pace with the increasingly advanced techniques used by criminal teams.

In light of this, it becomes necessary to establish and maintain relations based on the sharing of information between System actors, local governance authorities, and anti-fraud institutions and structures present in Europe, implementing alerting and monitoring systems while remaining aware and careful in keeping information confidential and protecting it from indiscriminate disclosure.

When applying these principles to ATM terminal fraud prevention, organisations should first of all perform vulnerability assessment activities on a regular basis, so as to identify and isolate any technical, procedural, and organisational weaknesses that could become a security hazard if exploited to perpetrate attacks.

Once the areas of greatest risk exposure are identified, organisations should implement a series of organisational, procedural, and technological security measures in order to mitigate the emerging vulnerabilities and limit the impact of possible attacks.

An **organisational measure** is a rule, a contextual dimension that an organisation decides to assert and enforce for the more effective functioning of the system, through the definition of clear roles and responsibilities for the efficient execution of activities and the simplification of internal communication flows.

A **procedural measure** is a rule that influences the definition, standardisation, and performance of one or more activities to clearly identify the process owners, establish execution times and procedures, and define the expected performance levels.

A **technological measure** is a rule expressed through the implementation of new applicative and/or infrastructural solutions or through the custom configuration of solutions that the organisation has already implemented for the ongoing supervision of its terminal fleet, maintaining and – if possible – strengthening the associated security level.

In the context of the national Network, Consorzio BANCOMAT has developed a framework to support Authorised Parties through an assessment activity for the continuous improvement of a security management model.

Consorzio Bancomat Security Framewok

The framework is based on internationally recognised standards and regulations for the significant and effective identification and measurement of core areas and processes to identify vulnerabilities that the service delivery chain, for example accessible through ATMs, is exposed to.

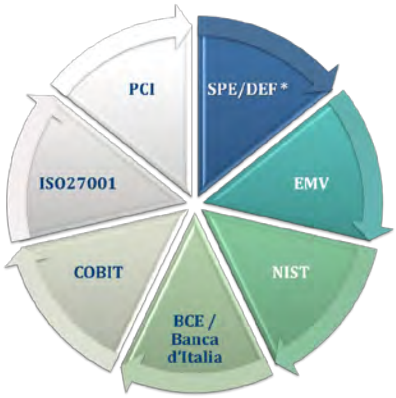


Figure 43: Standards reference of Consorzio bancomat Security Framework

To take a concrete example, the framework incorporates the requirements issued by CIPA (the *Interbank Convention* on Automation *Problems)* in relation to electronic systems and the recommendations of supranational standardisation bodies, consisting of:

- **Mandatory requirements** (organisational, technological and procedural) that Authorised Parties in national payment networks must implement for secure transaction management, also through payment and withdrawal solutions as well as infrastructural components involved in processing branded transactions.
- **Best practices**, understood as excellent references identified for the execution of requirements stipulated in the Standard.
- A periodic **assessment tool** for the adoption of such requirements/best practices and the related supporting process.

This process includes the execution of different stages:

- Start of the Self-assessment Process – periodic launch of the process through the sending of detection checklists;
- Compilation of the checklists;
- Analysis of the results - Consorzio BANCOMAT® analyses the results, identifying the areas of greatest risk exposure, the risk level of each subject and of the entire acceptance network of branded transactions;
- Execution of the Action Plan – the results obtained from the checklist analysis enable the definition of any countermeasures to mitigate and manage the level of risk, since actions aimed at mitigating individual vulnerabilities also benefit the entire ecosystem. These actions may involve the adoption of specific technological or procedural measures, whose implementation plan requires an integrated approach managed through the coordination of specialist groups, the review of the documentary system of the framework, and the adaptation of legal provisions;
- Monitoring – on a continuous basis and according to specific needs, Consorzio BANCOMAT® implements the constant monitoring of the execution of the action plan and its results.

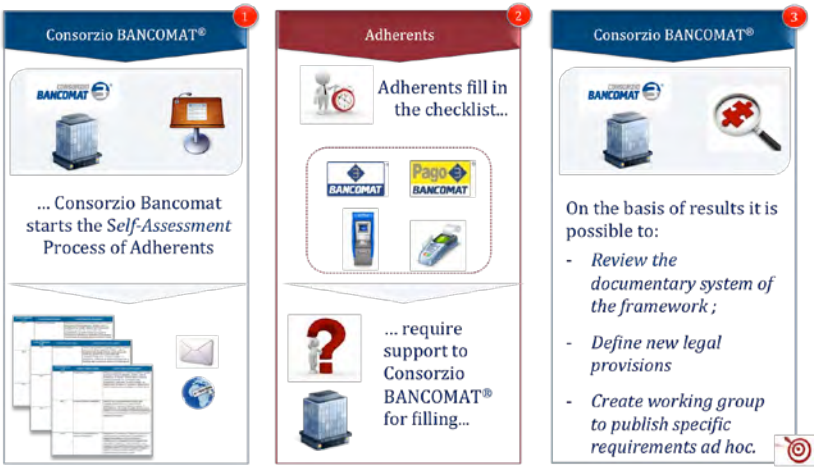


Figure 44: Consorzio Bancomat Security Framework process

The framework is structured in a number of areas for the identification, design, development, and assessment of organisational, technological, and procedural measures:

- **Organisation governance:** this involves the definition, documentation and implementation of a security governance system for ATM terminals and related systems, performing, for example, risk assessment and management activities, analysis/regulatory compliance activities, asset management activities, periodic reviews (e.g. audits, vulnerability assessments and penetration tests), management of regular internal and external awareness and training activities, etc.
- **Third party security management:** this includes activities for the secure management of relations with Third Parties such as, for example, the definition of specific security clauses to be included in agreements and contracts, the evaluation of the suppliers, and the periodic testing of compliance with security clauses.
- **Security measures for ATM hardware/software components:** these include activities for the analysis, definition, implementation, and periodic review of security measures related to ATM hardware (physical) and software (logical)

components, aimed at preventing fraudulent attacks on terminals.

- **ATM environmental security management:** this includes all activities necessary to manage the security of the various environments where ATM terminals and/or their related infrastructural components are present, transported, stored, or installed, namely: warehouses, laboratories for testing, data centres, etc.
- **ATM logical security management:** this involves the definition, documentation and implementation of logical security measures for ATM terminals and/or their related systems (management of user identification, as operators and system administrators, device management, etc.).
- **Infrastructural security management:** this includes the definition and implementation of processes, procedures, and operational measures for the infrastructure security management (connection systems, security functions for infrastructural components, etc.).
- **Data processing security management:** this includes the definition and implementation of processes, procedures, and operational measures for the secure management of cardholder data or other personal/sensitive data.
- **Secure management of cryptographic keys:** this includes the definition and implementation of processes, procedures, and operational measures for the management of protocols and cryptographic keys used to guarantee the security of data processed by the infrastructure and systems.
- **Monitoring of ATM security aspects:** this involves the definition and implementation of processes, procedures, and operational measures for logging and for monitoring ATM transactions, security components, and related systems.
- **Product installation, operation and maintenance:** this includes the governance and coordination of installation, operational management, and maintenance of ATMs and related systems: e.g. management of onsite/remote interventions for repairs, replacement of hardware and/or software components, secure disposal.

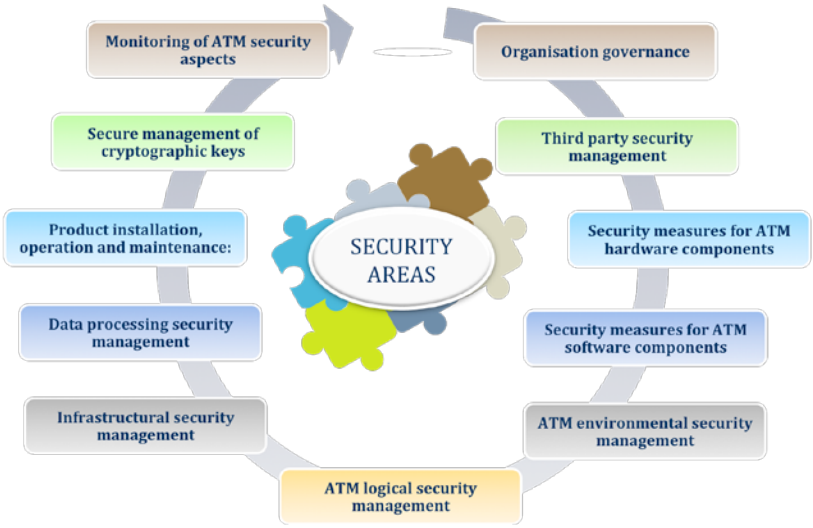


Figure 45: Security areas of Consorzio Bancomat Security Framework

In conclusion, the framework embodies an integrated approach to security, which goes from the design and management of a precise model for analysing the scope of intervention, classifying criticality, managing information, identifying vulnerability and countermeasures, all the way to testing the resilience of the entire System and therefore the residual risk.

Case study of Consorzio Bancomat Security Framewok application

In the previous chapters, both known attacks, more or less widespread, and attacks – for the time being only hypothetical – based on possible system developments were examined.

As already said, it is impossible to define prevention strategies that are both valid a priori for any type of organisation and effective in

any context, since the ATM acceptance network is now subject to relentless and rapid developments that are changing the reference scenario and are requiring organisations to reason dynamically on matters of security, taking into account an increasingly broad view.

However, it is possible to reasonably envisage the development of a security model that considers all aspects that are a part of the framework in order to address any vulnerability that could expose the system to the risks described.

Clearly, countermeasures must necessarily be the result of combined assessments that take into consideration all aspects that affect the probability of the occurrence and the potential impact of the attacks.

Take, for example, the case of the man in the ATM: the attack, which is not focused so much on the appropriation of cash as the interception of account information, is able to exploit both the vulnerabilities of ATM terminals and those of services offered through online banking channels (see chapter 8.3.2).

In order to prevent patterns of this type, a good security model must include, among **technological** measures, the implementation of an effective segregation of network segments, in order to contain the exchange of information between the different areas of the corporate network.

Moreover, it is important to maintain updated antivirus systems able to detect and remove any unwanted applications installed on the ATM software, and develop advanced systems of recognition and notification of transactions to account holders.

The integrated security model must take account of all **organisational** preventive and countering measures; according to the provisions of the BANCOMAT Security Verification Framework, organisations should clearly define responsibilities with regard to the analysis and updating of security systems, and establish regular reviews of the measures adopted in order to promptly respond to changes in the operational context of the ATM network.

Finally, in the context of **procedural** measures, the current focus

is on "intelligent" anti-fraud systems capable of studying the behavioural patterns of cardholders and recognising in real time any deviations or anomalies that could be a symptom of fraudulent events taking place.

By applying the framework to specific cases, lastly, it is possible to identify certain best practices – purely illustrative – relating to the different areas in question that could help organisations to build a comprehensive security model.

ORGANISATION GOVERNANCE: it is recommended to document and implement a process to:

- Identify the security risks and related vulnerabilities associated with terminals;
- Assess the implementation of additional security checks based on the results obtained from analysis activities;
- Verify the countermeasures in place to mitigate security risks related to terminals;
- Define and implement mitigation, control, and monitoring measures for security risks related to terminals and relative systems.

CUSTOMER GOVERNANCE: it is recommended to define and periodically provide cardholders with:

- General instructions on the secure use of cards;
- Information on main fraud scenarios (e.g. card or cash capture);
- Information on measures to adopt in order to prevent and/or manage the same effectively (e.g. activation of alert systems, systematic control of account statements, procedure for blocking cards, PIN shielding practices).

HW/SW COMPONENT SECURITY: it is recommended to:

- Protect the upper part of ATMs where the computer is gen-

erally located with adequate security measures;
- Define and implement security procedures for the operating system and BIOS;
- Define and implement protection measures aimed at preventing the installation of unauthorised and/or irrelevant software for the functioning of the ATM.

ENVIRONMENTAL SECURITY: it is recommended to:

- Document and perform vulnerability assessments and penetration tests (VAPT) on terminals, at least annually, during the installation of the terminal, and after any significant changes that may impact the physical characteristics of the terminal;
- Adopt procedures to clearly distinguish between the staff of Authorised Parties and any external visitors (e.g. maintenance workers) requiring access to the data centre;
- In case of ATMs located inside branches, provide for controlled access systems to access the area hosting the terminal.

LOGICAL SECURITY: it is recommended to:

- Document, implement and update policies and procedures for the management of security applications for the identification and elimination of unwanted applications, malwares, etc. (such as antivirus and antimalware programs) on infrastructural components;
- Provide for controls on ATM devices able to detect behaviours or series of events that may indicate the presence of malwares (e.g. sudden restarts, unexpected cash-outs, anomalies in log verification and transaction recording activities, presence of legitimate files in incorrect positions, etc.).

INFRASTRUCTURAL SECURITY: it is recommended to:

- Define and implement processes and procedures that seg-

regate different network partitions to allow operations only by operators authorised for activities in the area;
- Define and implement processes and procedures that provide for the adequate management, registration and monitoring of accesses and connections, in order to track actions relevant for security purposes.

DATA PROCESSING SECURITY: it is recommended to define a list of all the positions where applications memorise cardholder data and other sensitive data and to implement procedures for the protection of the same in order to ensure their non-readability, with the sole exception of specifically authorised processes or staff.

SECURE MANAGEMENT OF CRYPTOGRAPHIC KEYS: it is recommended to adopt secure procedures for the generation, review, management, replacement and monitoring of the validity of algorithms and cryptographic keys.

MONITORING OF SECURITY ASPECTS: it is recommended to document and implement a reliable logging system for transactions performed on ATMs that includes at least the recording of:

- Logs of the activation of service interfaces;
- Logs of all maintenance and system operations;
- Logs of all service operations;
- Logs of all user transactions performed on the terminals;
- Logs indicating any opening of the ATM terminal.

INSTALLATION, OPERATION AND MAINTENANCE: it is recommended to:

- Provide for and implement a structured process to manage the repair and replacement of hardware and software components of the terminals and related systems;
- Define and implement a process for the overall control of

the terminal and related systems and supporting infrastructure (e.g. periodic scan), in order to verify that the terminal and/or environment it is operating in have not been subject to unauthorised changes such as to compromise its functioning and/or pre-existing security features.

As described in this document, ATM security is a complex issue that could not be faced only at a technical level. Often, the ATM is seen just as a box to withdraw money, to recharge mobile credits or to look at bank account. The functions and services that an ATM could provide are heterogeneous and could also be functional to reach areas with a low density of population. The role of ATM will be still prominent in the future. Most consumers seem to wish to interact with ATM through mobile app instead of bank card and Public Administration could rely more and more on ATMs to deliver public services and documents.

Institutions, providing ATMs services should think about ATM security as a continuous activity because the threat evolves and security managers shall be aware about that.

The basic principles to protect ATM services are the same; a security manager has to provide for other services.

First of all, it is necessary to have a clear map of the perimeter to protect, in terms of people involved, processes put in place, technology and interdependencies. The map is also preparatory to perform an activity of rationalization, reducing the complexity of the networks and the surface of attack too.

The collaboration internally and externally between departments and Institutions should be strengthen, avoiding conflicts and joining skills and capabilities. Some attacks have been perpetrated with the same system on ATMs of different Institutions. The information sharing is vital to prevent a spreading of attacks.

The knowledge of enemies Techniques, Tactics and Procedures of attack shall also be deeper. Information security managers should know the "enemy", monitoring blog/forum, media, chat, black market to learn potential model of attacks or the release of new vulnerabilities or attack tools. Thinking and acting as an attacker allow testing the protection layer and increasing the countermeasures.

The security is not something to delegate totally to vendors or advisors. It is a capability that should be developed inside the company. It is a process that involves all the stakeholders, including the business owner and clients too.

Security Managers have to consider several aspects and approach the security also as a business. They have to collaborate with business owner to determine the budget needed to protect ATMs; with Customer Manager to disseminate awareness campaigns; with IT department to understand the technology chain and the implications; with Marketing for the future applications they want to release and so on.

The security should become a driver for doing business, creating trust and confidence in the services delivered.

11 Authors

11.1 Braintech

Founded in 2008 is specialized in security infrastructure management, single sign-on systems integration and provides specialized consultancy services. The company provides to its customers a reliable support in the field of Information & Communication Technologies and Business Application. In order to provide a global and high quality service, it has partnerships with other companies that have complementary characteristics, but guaranteeing a single interlocutor to the end user. Braintech is continually looking for products and innovative solutions to offer to its own clients to improve their efficiency and operations. In this regard, Braintech resells products in the following areas: security, networking, infrastructure anagement, monitoring, certified data erasure, financial risk, and data quality analysis..

Carlo De Luca

With thirty years of experience in field of ICT; Carlo was first in Telecom Italy, after in American Express becoming IT Manager where he increased its past international experience, then in Primeur, an integration and security company, where he held various managerial positions for ten years. In 2008, along with other professionals, he founded Braintech of which is currently CEO and sole shareholder.

Nicola De Bello

Degree in Engineering in Padua, after almost ten years in software development of mission-critical systems for the Telco market (Necsy), in 1994 he founded his first company (Atman), which carried out the first medial catalogue on Italian CD-ROM (for Nordica / Rollerblade). In 1996 Nicola founded ISYI, one of the first Italian companies of Cyber Security acquired in 2000 by the American multinational ISS (now IBM). In 2003 he founded Sirion, immediately acquired by Primeur Group. In 2004 he founded Kima (since 2009

part of the IKS Group), the first Italian company accredited by the PCI Standards in the field of Electronic Money. In 2010 he founded WARE'S ME. Nicola boasts in the ICT sector the most important national and international references. From 2014 is responsible of Braintech security team.

11.2 Consorzio Bancomat

Consorzio BANCOMAT® is the owner of the BANCOMAT® and PagoBANCOMAT® trademarks and the Governance Authority of the related circuits, in which Specialized parties can participate. These are Banks, Financial Intermediaries, Payment Institutions, E-money Institutions wishing to offer to their customers BANCOMAT® e PagoBANCOMAT® branded cards or ATM and POS terminals enabled to acquire said cards.

In line with its mission, the Consortium undertakes, in particular, the following activities:

- Approval of the admission to the BANCOMAT® and PagoBANCOMAT® circuits of Banks and other Authorised Parties which can operate in the payment services area;
- Definition of rules for the use of the BANCOMAT® and PagoBANCOMAT® Trademarks and for the operation of the relevant Circuits;
- Definition of Technical and Security Standards for BANCOMAT® and PagoBANCOMAT® branded products (e.g. Cards, POS/ATM Terminals);
- Validation of Products and Processes operating on the Circuits;
- Monitoring of the Authorised Parties' operations for compliance with the Circuit rules;
- Realization of market analysis for the development of its systems
- Control of frauds and risks to guarantee the highest security on BANCOMAT® and PagoBANCOMAT® branded products, also by participating in the main international round tables;
- Definition of interchange-fees related to its Circuits.

Veronica Borgogna

Veronica is Head of Processes & Controls Area in Consorzio BANCOMAT. The Processes & Controls Area includes Audit, Risk Management e Fraud Management units. She is responsible of monitoring and controls of delivery of the services related to the use of the BANCOMAT and PagoBANCOMAT brand, the riskiness of the processes and products of the entire System and the trend of fraudulent phenomena. Through the Anti-Fraud Centre coordinates the activities of analysis, prevention and contrast and participates in national and international working group on the issue of combating fraud as GIPAF, Osservatorio Sicurezza e Frodi informatiche, Security Working Group EPCA, EC3 Europol and she is a EAST (European ATM Security Team) board member. She is also external auditor for Licensee, Adherents, suppliers and stakeholders of the System.

Claudia Talone

In Consorzio BANCOMAT from 2012, Claudia inside the Processes & Controls Area manages the Anti-fraud center, competence center set up to analyse, prevent and contrast frauds within the domestic payment scheme. She is also engaged in the activities of the risk management function that works to the identification, measurement and management of risk categories related to the business and operational model of Circuits. Degree in Business Administration, she gained several years of experience in payment systems; she has also held positions in administration and management control for leading Italian companies.

11.3 Diebold Nixdorf

Diebold Nixdorf is the world's leading provider of self service solutions and services to Retail Banks, Postal Organizations and Retail Industry, born from the business combination between Diebold Inc. and Wincor Nixdorf GmbH

The main focus of the group's comprehensive portfolio lies on business process optimization, especially in the branch operations of three sectors. Diebold Nixdorf has established a presence in

more than 130 countries around the globe, giving it an outstanding profile when it comes to customer proximity. The company also places great importance on building close relationships with sales partners that have an excellent knowledge of the local requirements and conditions on the customer side.

Diebold Nixdorf has a total workforce of around 25,000 people, over half of those are Service members and about 1,700 are Software professionals. With more than 3,000 patents Diebold Nixdorf is a technology leader based with two corporate offices in North Canton Ohio (US) and in Paderborn (Germany).

Christian Beine

After joining Wincor Nixdorf Christian worked for the Platform Software Development for security components for 8 years. Since 3 years he is appointed as a Security Consultant within the department Corporate Security and Fraud Management focusing on different aspects of Product and Solution Security within Wincor Nixdorf. This includes incident response as well as intelligence gathering and security related internal consultancy during the development of future products.

He is a certified CISSP also representing Wincor Nixdorf at EAST or other security related initiatives.

11.4 GCSEC

The Global Cyber Security Center (GCSEC) is a newly established not-for-profit organization created to advance cyber security in Italy, the region, and around the world. The Center, funded by Poste Italiane, is based in Rome with a strong collaboration with Italian and International government institutions, private bodies, research institutions and international bodies. The mission of the center is to develop and disseminate knowledge and awareness on Cyber Security, creating the conditions for improving capabilities, skills, cooperation and communication between the different stakeholders involved in the use and protection of Internet. In order to achieve these objectives, the Global Cyber Security Center will be a hub of cooperation and innovation where people of every

country could meet and work together, sharing their knowledge and experience.

Elena Mena Agresti

Elena is a senior expert in information security and international standards. She participated in technical committee responsible for reviewing and developing standards or guidelines for ISO and OECD. Elena was the Scientific Direct of Master in Cyber Security organized under the Cyber Security District of Poste Italiane and is Professor in several university masters dedicated to cyber security. She worked in Booz & Company in the Global Resilience practice and has competences in security governance, training and awareness, critical infrastructure protection, risk management, security auditing, policy development, privacy, process analysis and compliance.

Massimo Cappelli

Massimo is Planning Operations Manager in GCSEC. He coordinates, as PMO, research and education activities of the foundation. After economic studies, he obtained PhD in "Geoeconomics, Geopolitics and Geohistory of border regions" focus on Critical Infrastructure Protection Programme and a Master in "Intelligence and Security Studies". In the previous experience, he assumed the role of Associate Expert in Risk Resilience and Assurance in Booz & Company (previous Booz Allen Hamilton). He participated as Advisor in NATO Industrial Advisory Group 179. He is PMO of several GCSEC projects.

Nicola Sotira

Nicola is the Director General of GCSEC and Information Security Manager in Poste Italiane. He works in the field of information security for over 20 years with experience in different international companies. Professor at the Master in Network Security of La Sapienza University of Rome, is Member of the Association for Computing Machinery. He is a promoter of technological innovation and was member of several startups in Italy and abroad.

11.5 Kaspersky Lab

Kaspersky Lab is a global cyber security company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Olga Kochetova

Olga is interested in how various devices interact with cash or plastic cards. She is a senior specialist for the penetration testing team at Kaspersky Lab, providing security services, such as threat intelligence, penetration testing, ATM/POS security assessments, application security assessments and more. She has more than five years' experience in information security and more than four years' experience in practical security assessment. Olga has authored multiple articles and webinars about ATM security. She is also the author of advisories about various vulnerabilities for major ATM vendors and has been a speaker at international conferences, including Black Hat Europe, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack and others.

Yuliya Novikova

Yuliya is an analyst for the security services analysis team at Kaspersky Lab, providing security services, such as threat intelligence, penetration testing, ATM/POS security assessments, application security assessment and more. Yulia's areas of interest are mobile application security assessment, threat modelling, and OSINT practices.

Alexey Osipov

Alexey is a lead expert on the penetration testing team at Kaspersky Lab, providing security services such as threat intelligence,

penetration testing, ATM/POS security assessments, application security assessment and more. He has more than five years' of experience in information security and more than four years' experience in practical security assessment. He is the author of a variety of techniques and utilities exploiting vulnerabilities in XML protocols, telecom networking and ATM security, as well as advisories about various vulnerabilities for major ATM vendors. He has been a speaker at international security conferences, including Black Hat Europe and Hack in Paris (presenting the paper on ATM vulnerabilities), Black Hat USA, NoSuchCon Paris, Positive Hack Days, Chaos Communication Congress, and Nuit Du Hack.

Fabio Sammartino

Fabio Sammartino, 36 years old, keen on technological innovations, thanks to the years of experience he has gained strong experience in sales of security software and excellent ability to technical support and diagnosis through a systematic methodology for the analysis of technical problems. From January 2013, he is Pre-Sales Manager and Technical Trainer for Kaspersky Lab Italia managing all pre-sale operations and training activities for partners and customers including demonstrations, customer presentations, creation of proof-of-concept, reporting and analysis of client infrastructure. From 2009 to 2013, always in Kaspersky, he was Technical Trainer & Pre-sales Engineer and dealt after-sales support, product analysis, and management training.

Gianfranco Vinucci

Gianfranco Vinucci, Head of Pre-Sales Kaspersky Lab Italia, coordinates the Italian team dedicated to presales and training activities to partners and clients. In Kaspersky Lab from October 2008, he was Head of Support & Services Manager as responsible of technical support activities in Online, Retail and Corporate markets in Italy and Israel. In the last years, he has successfully coordinated cyber security consultancy and training activities in national and international organizations. Gianfranco, was born in August 1977 in Rome, has always been keen on informatics has acquired technical and managerial competences collaborating with relevant system integrator companies and a roman ICT distribution company.

11.6 NCR

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, GA, USA, with over 30,000 employees and does business in 180 countries.

Owen Wild

Owen Wild is a Global Marketing Director for NCR financial services line of business. In his role he is responsible for the global development and execution of NCR's marketing strategy and programs for NCR's Enterprise Fraud and Security solution portfolio.

Owen had previous experience leading the global marketing activities for NCR's Travel and Gaming Division focused on the development and adoption of self-service solutions throughout all segments of the travel industry

Prior to joining NCR, Mr. Wild was Director of Marketing for Amadeus North America, where he was responsible for the implementation of all marketing programs and communications activities in the US and Canada.

11.7 Security Brokers

Established in 2012 with the mission to develop innovative solution for ICT security and Cyber Defence issues, Security Brokers is a boutique of advisory and Information Security solutions, composed of an élite team of ethical hackers, ICT security researchers, top-class information security, ICT law and GRC experts that gather the know-how and specialization in each project; all freelance and individual companies acting as an unique entity sharing

values, objectives and mutual respect. Security Brokers, with an innovative corporate form, proposes an model able to address the issue of Cyber Defense from all points of view and develop ad hoc security services for different needs through an international network of professionals with a strong multidisciplinary and thanks to a model, open, transparent and informal organizational model which facilitates relationships both internally and externally.

Raoul Chiesa

Raoul Chiesa has been among the first Italian hackers back in the 90's (1986-1995). Then, he decided to move to professional InfoSec. Since 2003 he started its cooperation with the United Nations Interregional Crime and Justice Research Institute, working on "HPP", the Hackers Profiling Project run by ISECOM and UNICRI; in 2005 he has been officially recognized as a cybercrime advisor. Nowadays his role at UNICRI is that of "Independent Senior Advisor on Cybercrime".

Since February 2010, Raoul Chiesa is a Member of the European Network & Information Security Agency (ENISA) Permanent Stakeholders' Group (PSG) covering the previous two mandates, 2010-2012 and 2012-2015. He is regular key speaker at official security events such as National Security Observatory at the Italian MoD, Security Summit, CCDCoE/NATO in Estonia, World Institute for Nuclear Security (WINS), Italian Senate, HackCon Norway, RACVIAC Croatia, Swiss Cyber Storm, Secure Poland by CERT-PL, GOV. CERT-NL, SANS, ESA (European Space Agency), ISF China (Internet Security Forum), IDC China (Internet Data Centers Conference) 8.8 (Chile) and many more.

Matteo Benedetti

With over 20 years of "hands-on" experience in the field of Cyber Security, Matteo was an Ethical Hacker and Security Advisor, conducting and coordinating hundreds of penetration testing and security audit on varied infrastructure, platforms, devices, mobile and web applications. He investigated frauds and cyber attacks for TELCO and large enterprises and was the leader of an incident re-

sponse team for many years. He was threat analyst fraud specialist and contributed to design, build and launch several Security Operation Centers. His background includes all domains of information security, with particular reference to mobile security, payment systems, IoT and BYOD, Automotive, SCADA. His motto is “think evil”.

CONSORZIO BANCOMAT

Braintech

DIEBOLD NIXDORF

KASPERSKY lab

NCR

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

GLOBAL CYBER SECURITY CENTER

GCSEC - Global Cyber Security Center – Viale Europa, 175 00144 Rome, Italy – www.gcsec.org