FUTURE ATTACK SCENARIOS AGAINST AUTHENTICATION SYSTEMS, COMMUNICATING WITH ATMS

CONTENT

INTRODUCTION

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, directly or indirectly. When we talk about fraud in relation to ATMs we can generally divide it into two main categories:

1. **Direct losses**, when an attacker obtains money from an ATM cash dispenser.

2. **Indirect losses**, when the 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.

DESCRIPTION OF THE CURRENT AND FUTURE 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[1], which affects ATMs from a major ATM manufacturer running Microsoft Windows 32-bit. In addition, the sensational Carbanak malware [2] 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),*

[1] 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)

[2] 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)

> *and not capable of being surreptitiously stolen via the Internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data."*[3]

The high rate of development of new technologies, and the development of new information security mechanisms, is leading to the evolution and expansion of the following authentication methods for ATMs:

1. 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.[4]

2. 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 behavioral characteristics. Various types of biometric systems are being used for real time identification.

These may include:

- Iris recognition;
- Fingerprint recognition;
- Palm recognition;
- Vein recognition;
- Face recognition;

[3] 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)

[4] Report: Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited. Available at: https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMV-Contactless-Cards.pdf (Accessed 05/07/2016)

- 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.[5]

The smart cards are sensitive to different types of attacks[6], even to man-in-the-middle attack.[7]

3. Authentication with a one-time password

The theory behind using two-factor authentication is the need to enter 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[8] launched an ATM withdrawal service that allows clients to withdraw cash from their mobile phones. The client sends

[5] 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=plY6k4gvQsY (Accessed 05/07/2016)

[6] 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)

[7] 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)

[8] 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)

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.[9]

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.

[9] 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)

DESCRIPTION AND DIAGRAMS OF 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 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 Figure 1

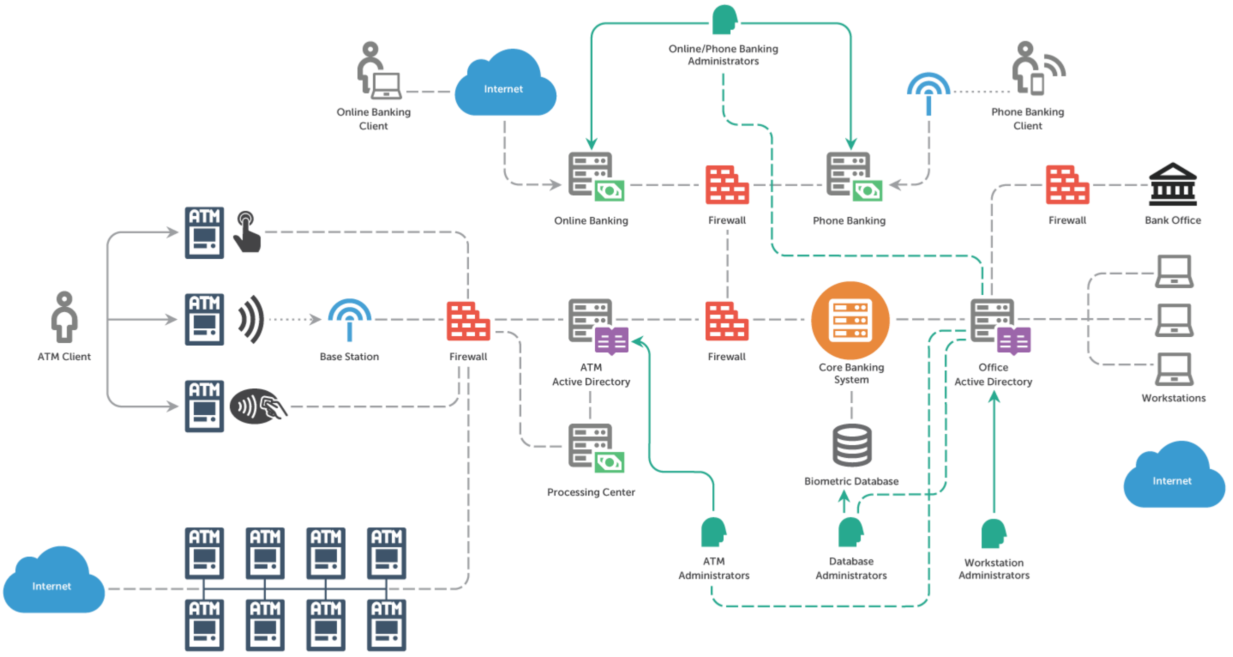


Figure 1 Simple diagram of bank network infrastructure

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) or without, in a cardless transaction.[10]

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 2). This biometric data must be placed in the biometric 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.

[10] 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)

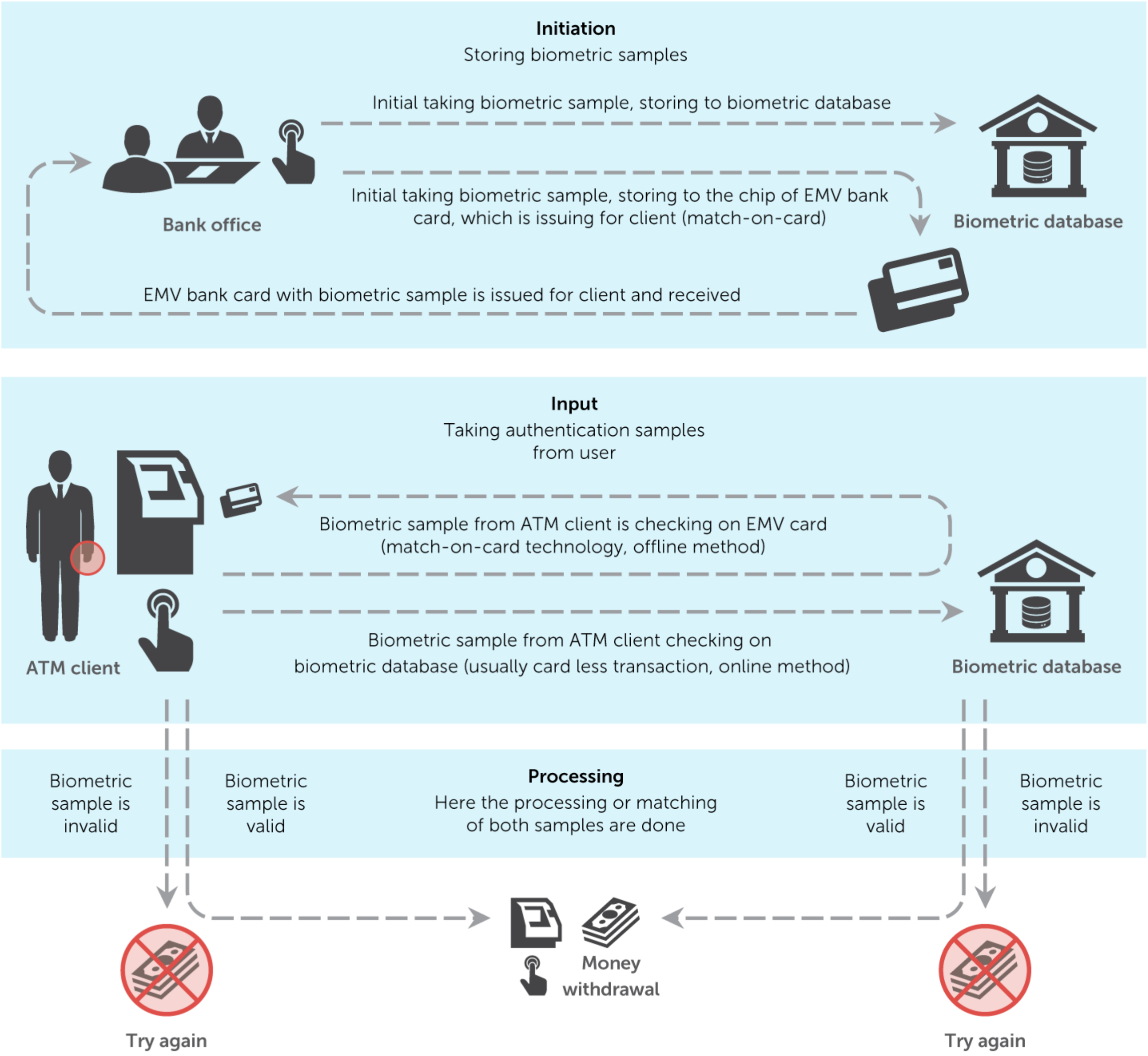

Initiation
Storing biometric samples
Initial taking biometric sample, storing to biometric database
Bank office
Initial taking biometric sample, storing to the chip of EMV bank card, which is issuing for client (match-on-card)
Biometric database
EMV bank card with biometric sample is issued for client and received
Input
Taking authentication samples from user
Biometric sample from ATM client is checking on EMV card (match-on-card technology, offline method)
Biometric sample from ATM client checking on biometric database (usually card less transaction, online method)
ATM client
Biometric database
Biometric sample is invalid
Biometric sample is valid
Processing
Here the processing or matching of both samples are done
Biometric sample is valid
Biometric sample is invalid
Money withdrawal
Try again
Try again

Figure 2 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 fingerprint 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.

POTENTIAL ATTACKS TECHNIQUES

Attacks on 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[11]). To perform 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.

[11] 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-extended-cut/ (Accessed 29/06/2016)

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 smartphone 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.

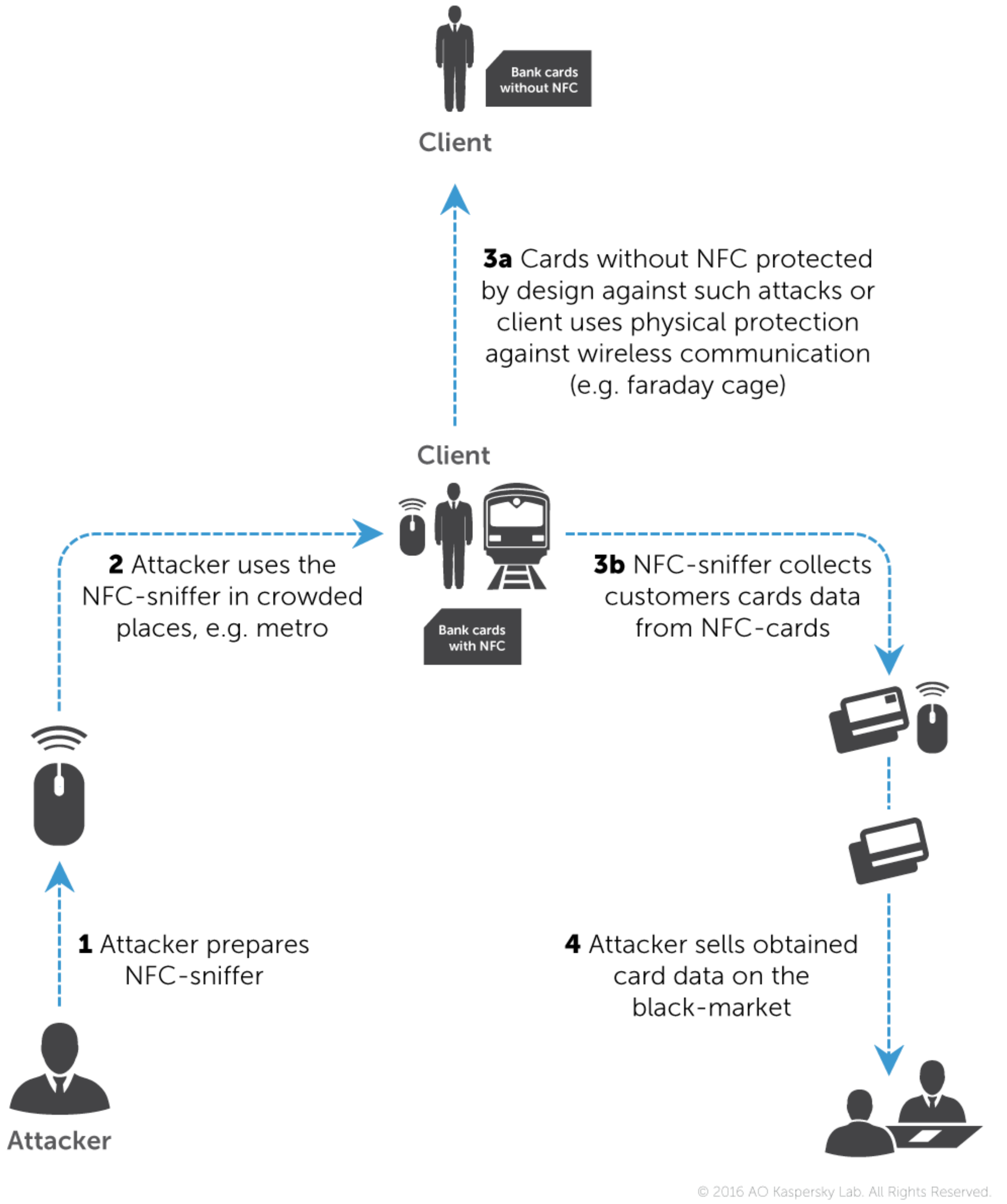

Bank cards without NFC
Client
3a Cards without NFC protected by design against such attacks or client uses physical protection against wireless communication (e.g. faraday cage)
Client
2 Attacker uses the NFC-sniffer in crowded places, e.g. metro
Bank cards with NFC
3b NFC-sniffer collects customers cards data from NFC-cards
1 Attacker prepares NFC-sniffer
4 Attacker sells obtained card data on the black-market
Attacker
© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 3 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.

The attack scenario is shown below.

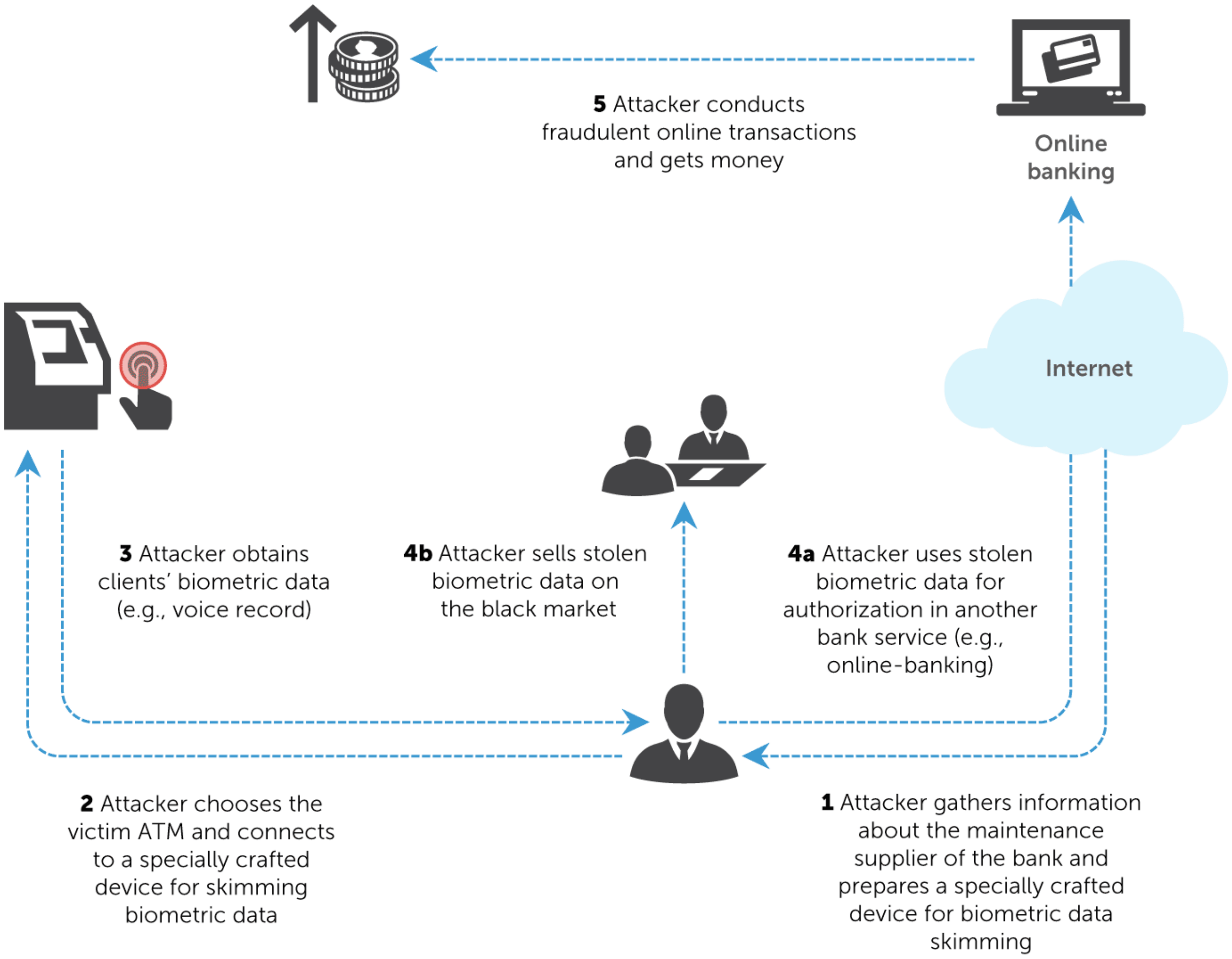

5 Attacker conducts fraudulent online transactions and gets money
Online banking
Internet
3 Attacker obtains clients' biometric data (e.g., voice record)
4b Attacker sells stolen biometric data on the black market
4a Attacker uses stolen biometric data for authorization in another bank service (e.g., online-banking)
2 Attacker chooses the victim ATM and connects to a specially crafted device for skimming biometric data
1 Attacker gathers information about the maintenance supplier of the bank and prepares a specially crafted device for biometric data skimming

Figure 4 Scenario of attack "Stealing authentication data using biometric data skimming

The "stealing biometric data using skimmer" attack is described in the document "Description of attacks and countermeasures".

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.

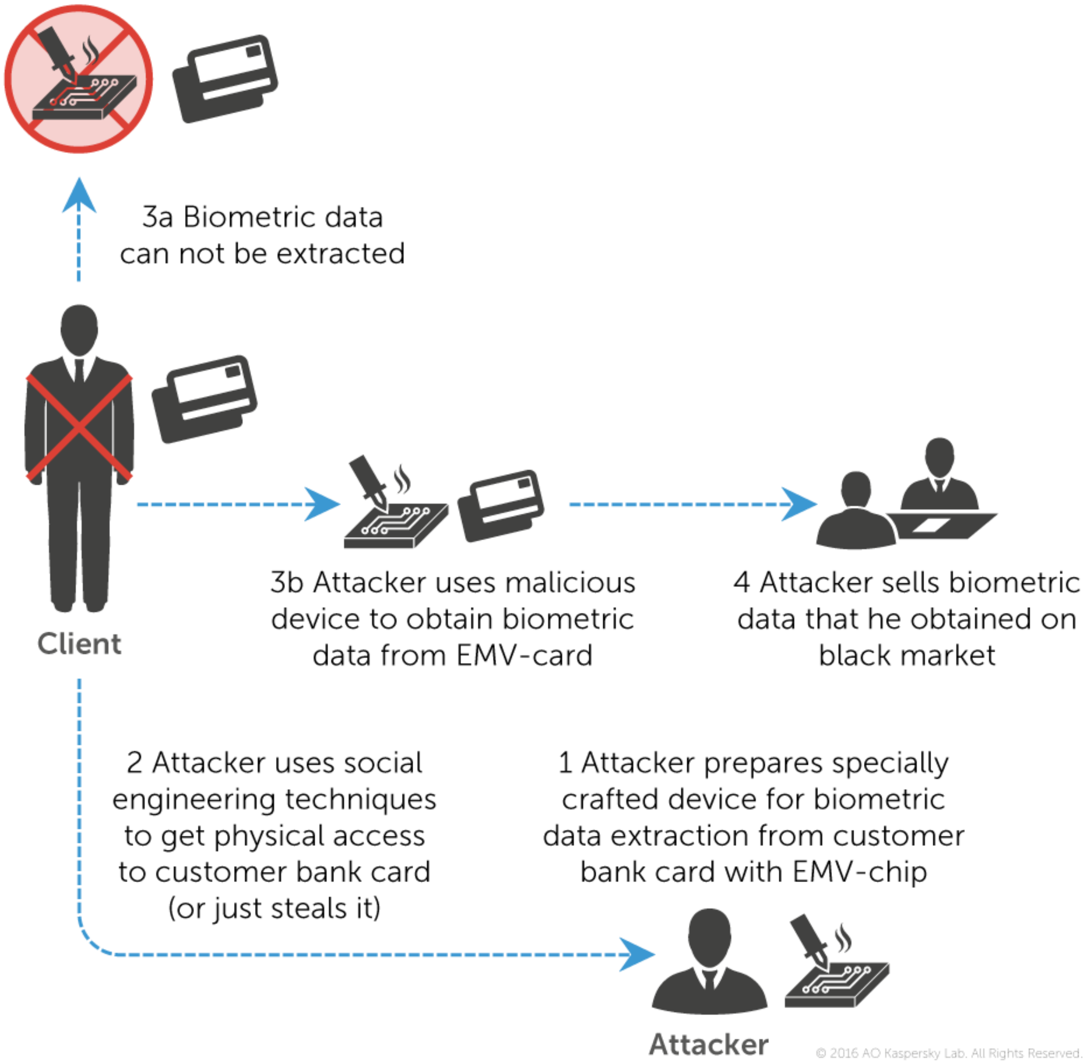

3a Biometric data can not be extracted
Client
3b Attacker uses malicious device to obtain biometric data from EMV-card
4 Attacker sells biometric data that he obtained on black market
2 Attacker uses social engineering techniques to get physical access to customer bank card (or just steals it)
1 Attacker prepares specially crafted device for biometric data extraction from customer bank card with EMV-chip
Attacker
© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 5 Scenario of attack "Stealing biometric data from EMV-card using special device"

Attacks on 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[12] with more than 100 targets.

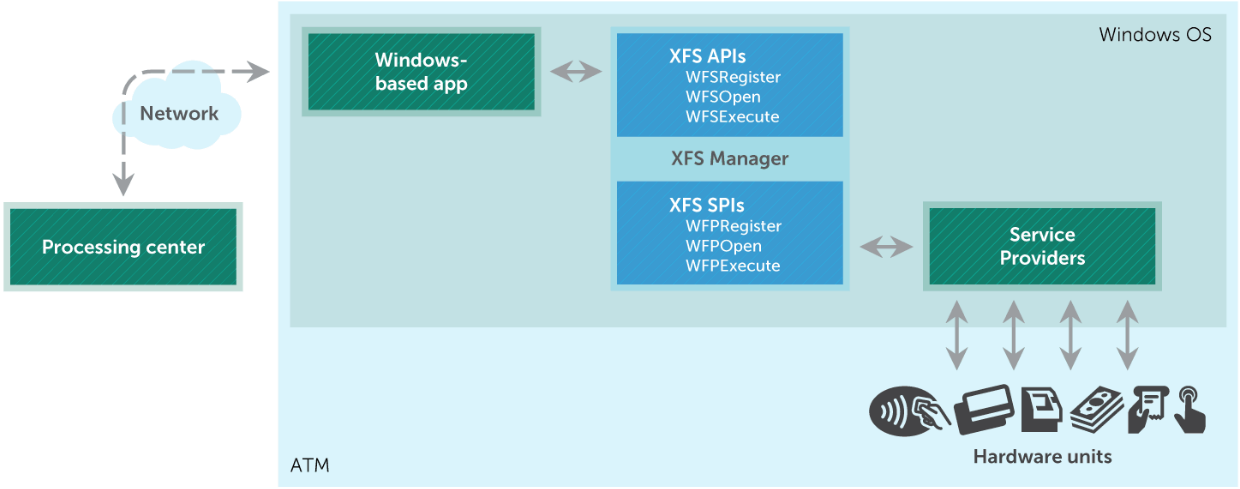
2. API-specific malware

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

[12] 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)

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



© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 6 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. dentification card devices - an attacker can:
   - Control the processes that insert, eject and retain cards;
   - Read and write magstripe 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).

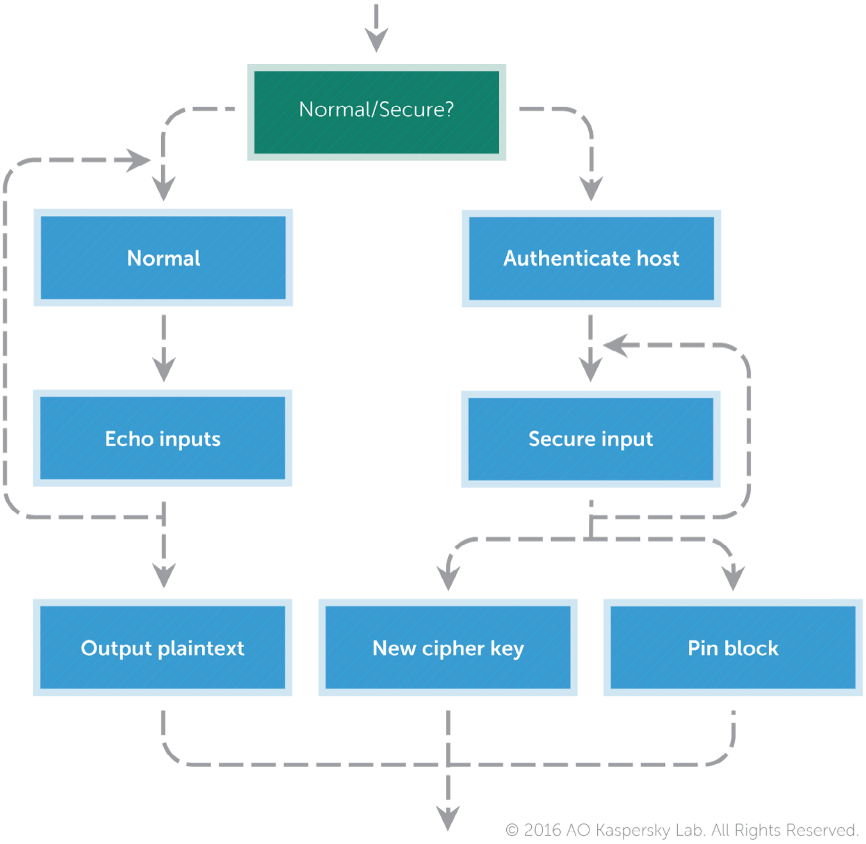


Figure 7 PIN device operation flow in open mode and secure mode

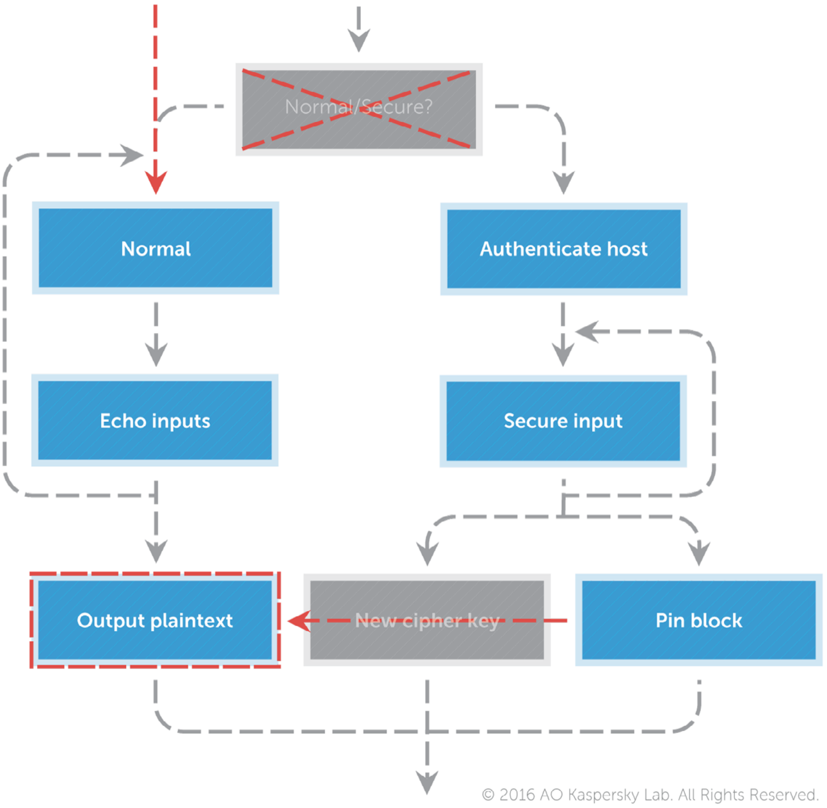


Figure 8 PIN device operation flow during Man-in-the-Middle attack

3. Skimer – 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 Skimer malware on one bank's ATMs.[13]

The Skimer 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 Skimer 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, through its SWIFT system.[14]

[13] 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)

[14] 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)

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.

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".

Attacks on the network layer

The general problem:

All ATMs should be connected to banking network to provide services, so 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 authentication 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 the document "Description of attacks and countermeasures".

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.

The attack scenario is shown below.

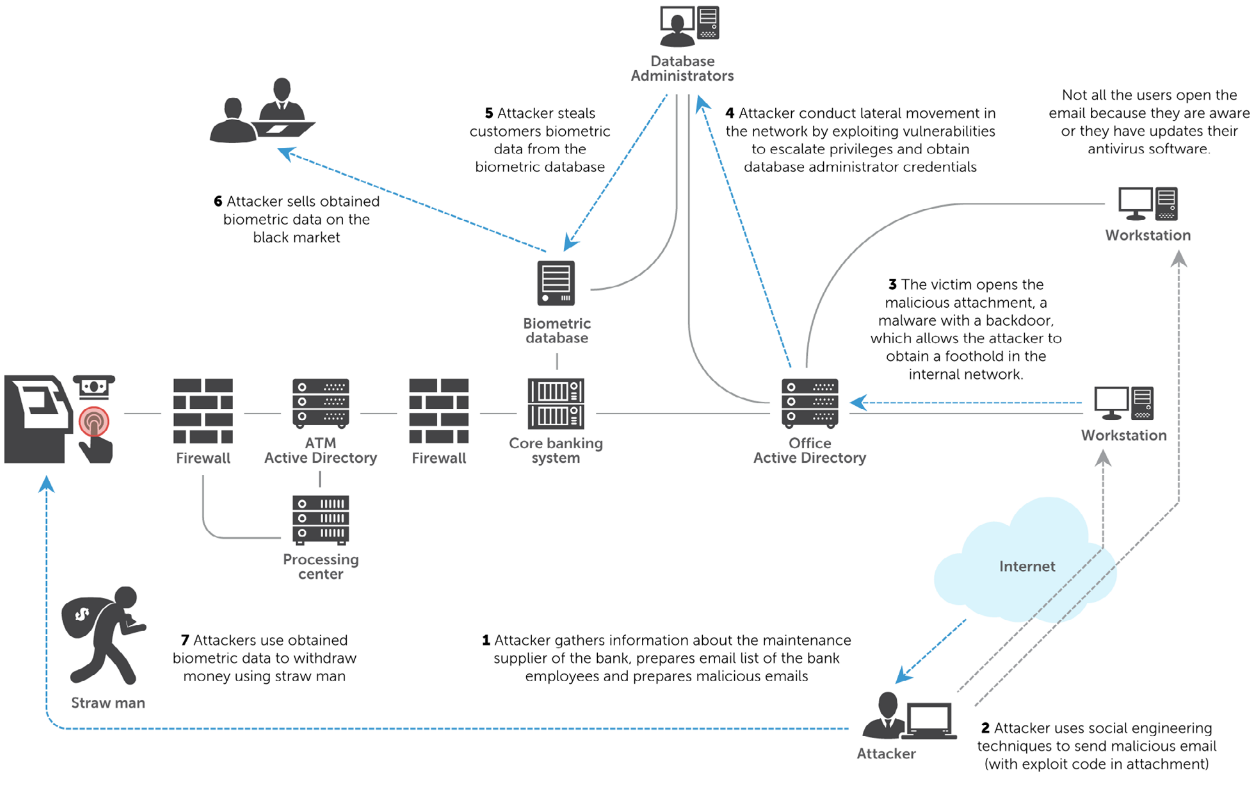
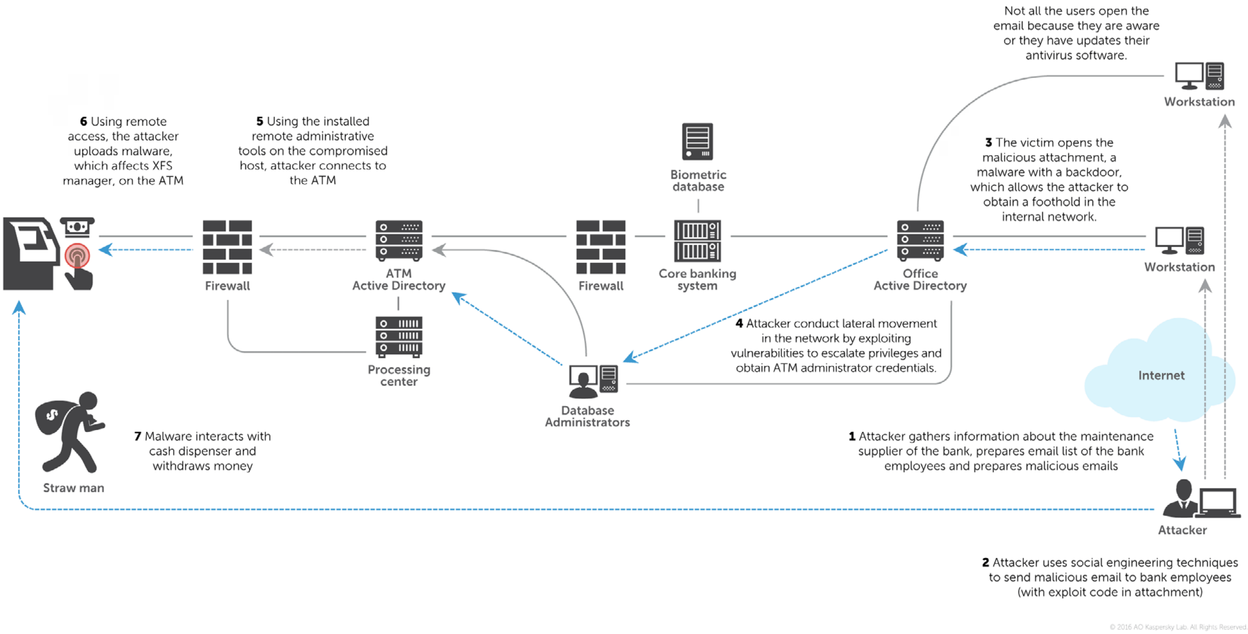

Database Administrators
5 Attacker steals customers biometric data from the biometric database
4 Attacker conduct lateral movement in the network by exploiting vulnerabilities to escalate privileges and obtain database administrator credentials
Not all the users open the email because they are aware or they have updates their antivirus software.
6 Attacker sells obtained biometric data on the black market
Workstation
Biometric database
3 The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal network.
Firewall
ATM Active Directory
Firewall
Core banking system
Office Active Directory
Workstation
Processing center
Internet
7 Attackers use obtained biometric data to withdraw money using straw man
1 Attacker gathers information about the maintenance supplier of the bank, prepares email list of the bank employees and prepares malicious emails
Straw man
Attacker
2 Attacker uses social engineering techniques to send malicious email (with exploit code in attachment)

Figure 9 Scenario of attack "Stealing biometric data from the biometric database"

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.

The attack scenario is shown below.



Not all the users open the email because they are aware or they have updates their antivirus software.

1 Attacker gathers information about the maintenance supplier of the bank, prepares email list of the bank employees and prepares malicious emails

2 Attacker uses social engineering techniques to send malicious email to bank employees (with exploit code in attachment)

3 The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal network.

4 Attacker conduct lateral movement in the network by exploiting vulnerabilities to escalate privileges and obtain ATM administrator credentials.

5 Using the installed remote administrative tools on the compromised host, attacker connects to the ATM

6 Using remote access, the attacker uploads malware, which affects XFS manager, on the ATM

7 Malware interacts with cash dispenser and withdraws money

Figure 10 Scenario of attack "Stealing authentication data via remote administration tools"

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 exists 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 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
- 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

ABOUT AUTHORS

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.

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.

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 modeling, and OSINT practices.

ABOUT COMPANY

Kaspersky Lab is a global cybersecurity 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

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy