Journal of Mechatronics, Automation and Identification Technology
Vol. 1, No.4. pp. 11 - 15

Security Aspects of Banking Kiosks in Serbia's Payment System

Miroslav CVETANOVSKI, Petar BJELJAC, Igor ZEČEVIĆ, Sabolč HORVAT, Miroslav NIĆIN

Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
Credit Agricole Bank, Braće Ribnikar 4 - 6, 21000 Novi Sad, Serbia
Institute for Public Health of Vojvodina, University of Novi Sad, Futoška 12, 21000 Novi Sad, Serbia
miroslav.cvetanovski@gmail.com, pbjeljac@uns.ac.rs, igor.zecevic@uns.ac.rs, horvatsz@gmail.com, miroslav.nicin@creditagricole.rs

***Abstract*— The purpose of this article is to give an overview of principals, technologies and aspects used in building the security around Banking kiosks services. The study is based on ATM banking kiosk built and deployed in Serbia's payment system. The evermore use of information technologies and automated teller machines (ATMs), that are located on remote and not so physically secure locations, require additional levels of security. Linking physical, networking, procedural, surveillance, logging, testing, integration with third party services, debugging, encryption and infrastructure redundancy is essential in today's secure payment process.**

***Keywords*— ATM security, Network security, ATM surveillance, Bank procedures, ATM procedures, ATM testing, ATM integration, Payment system, Transactions logging, Security Aspects, Server redundancy, IT Infrastructure redundancy, Backup Solutions**

I. INTRODUCTION

Microorganisms, According to the ATM Industry Association (ATMIA), there are now close to 3 million ATMs installed worldwide. This number is rising steadily and there are no indicators that would suggest otherwise [1]. The use of electronic payment systems like mobile banking, Internet banking and similar electronic payment processes has not made significant impact on this trend. The evermore use of ATMs in everyday life requires additional levels of security to be taken into account [2].

The risk of potential loss from ATM abuses should be technically and technologically reduced up to the point where it meets the investment on the security (Figure 1) [3].

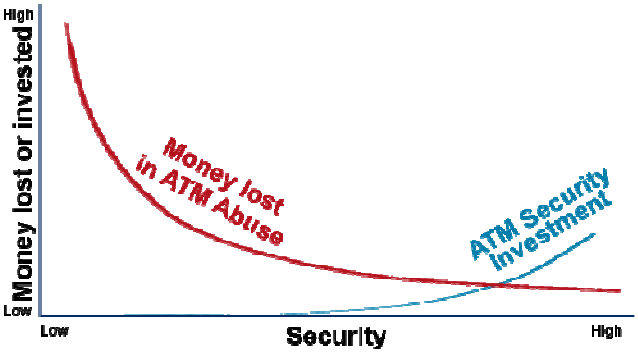

Fig. 1. Optimal level of investment in security

A. Automated Teller Machine

An automated teller machine (ATM), also known as an automated banking machine (ABM), cash machine, cashpoint, cashline, minibank or bankomat, is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller.

B. Banking kiosk

Banking kiosk has another and/or additional functionality from the standard ATM machine. It has the ability to make credit card or paper money payments directly from the client, exactly as it would be possible in direct interaction with a human representative in the bank. It has the ability to print transaction slips with the official bank stamp that is pressed on to the printed paper, to give or print the summary of client bank accounts, make transactions from one bank account to another, to electronically convert funds from one currency to another, etc.

C. Banking system in Serbia

The Republic of Serbia banking system consists of the central bank (National Bank of Serbia) and commercial banks. There are already predefined communication

channels which banks use in their transactional communication. Therefore, the security of the Bank kiosk is based on the Bank kiosk itself and on its ability to communicate with transactional servers of commercial banks.

II. Bank Kiosk System Architecture Integration in Serbia's Payment Process

The Every bank has its own information system and its own predefined transactional communication methods. Because of that, as a model of the Bank kiosk infrastructure, the broker model is selected (Figure 2)[4]. It consists of three parts:

- Banking kiosk
- Central kiosk broker server
- Bank server

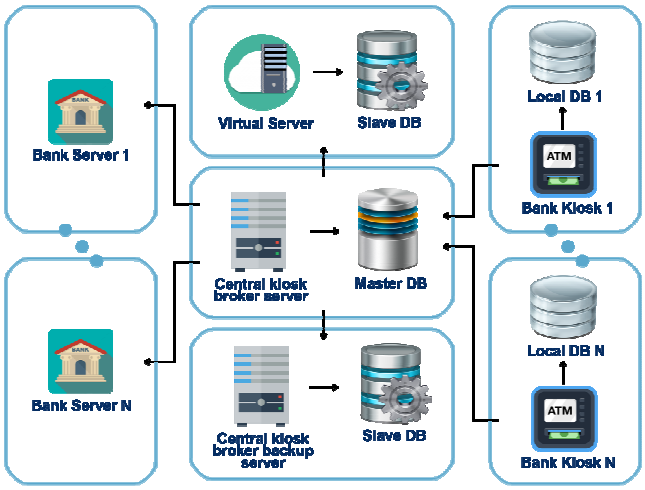

Fig. 2 Banking kiosk system integration

A. *Banking kiosk*

123 Banking kiosk is the physical ATM machine located on a remote site. It is constantly communicating with the Central kiosk broker server, and its communication has the goals:

- To accept or decline transactions made by the client, in communication with the Bank server
- To keep the transaction logs and record all changes locally
- Keep a local copy of the information critical for that ATM
- To alarm the Central kiosk broker server if potential problems occur

B. *Central kiosk broker server*

Central kiosk broker server is used as a communication intermediary in communication between Banking kiosks and the Bank server. It can modify the format of messages sent and received from both Bank kiosk and Bank server, and enables flexibility, monitoring and tracking of transactions.

C. *Bank server*

Bank server is the authorized transaction server in the bank's headquarters and it is directly linked and integrated into the banks information system. The Bank servers are the warranty for transaction completion and are responsible for making calculations of transactional fees.

III. ATM Abuses and Attacks

There are a number of ways an attacker can exploit the ATM machine, and therefore the Bank kiosk. The themes of this article are not exploits on the Bank server side in order to use the ATM only as a money withdrawal system. The article focuses on physical and software manipulations an attacker can commit on the ATM itself. Most used exploit techniques can be categorized as:

A. *ATM Take Away*

Lifting and taking away the whole ATM machine. Usually requires the use of heavy machinery and driving it to a remote location.

B. *ATM Burglary*

Stealing paper money assets from the ATM by breaking into its safe.

C. *ATM Forking*

Attaching a mechanical jammer in the money input and/or output mechanism that is used to confuse the ATM software to record a false positive, or a false negative transaction completion.

D. *PIN Scraping*

PIN scraping is usually done using three different techniques.

- Hidden camera that is focused on the keyboard part of the ATM;
- Fake PIN keyboard that is placed above the real one;
- Watching across the shoulder of the victim and/or looking from a distance using optical enhancement equipment. Also known as "shoulder surfing".

E. *Credit card magnet strip copying – Skimming*

Attackers "fake" the credit card reader that is used to clone the credit card information [5]. Usually is done by adding additional device over/between the existing hardware.

F. *Touch screen scraper*

Using a touch screen foil placed over the ATM touch screen, to track the payment details and/or authentication information.

G. *Network sniffing and man in the middle attacks*

Intercepting, and/or modifying the messages sent/received from/to ATM machine. In case the ATM software is updated or remotely controlled over the network, the network sniffing is used to record the information flow over the network, or load attacker software on to the ATM machine.

IV. Security Principals

Security principals are the main ideas used in designing the ATM machine, and should achieve the listed goals:

- Make ATM mechanically secure
- Detect any mechanical and/or software anomalies

- Validate the devices used in the payment process before the transaction is made
- Identify the client
- Encrypt data
- Monitor and log
- Be redundant, highly available and resistant to failures Sections V and VI describe the way in which security principals have been implemented in one of the Banking kiosk services in Serbia's payment system.

V. Mechanical and Physical Security

Mechanical security is essential in preventing the attacks and exploits on ATM machines. Without it, any other software, procedural or technological protection can be manipulated in thinking that all conditions are met to successfully complete the transaction. Physical security should also be met for the Central kiosk broker server and Bank server, but this is not the theme of this article.

The ATM should be designed more like a safe, rather than a device that is used to complete the banking transaction inside of the bank waiting room. It is not considered a good practice, to use the same design of ATM machines for use inside and outside of a safe location.

A. Mechanical protection

1) Thick – walls: A thin sheet of aluminum is not enough to stop the violent attacker from breaking into the paper money cases that are inside of the ATM. The aluminum should be thick enough to withstand the attack performed using human held tools.

2) Double locks: The locks should be vandal proof and hard to pick. It is a good practice to have a different key for every ATM and to have a separate compartment inside of the ATM where the money cases are stored.

3) *Smart money cases:* Smart money cases that support the electronics tracking of its current content should be used. Some money cases are also equipped with the ability to mark or destroy the paper money inside of them; and/or with the ability to mark the attacker with visible or invisible paint, so the potential suspect could be identified without any doubt.

4) *Weight of ATM:* The ATM should be bolted on to a solid structural part of the floor or the wall. It should be immobile and, if possible, should weigh more than 500 kilograms (the weight considered to be impractical for lifting with human strength).

5) No protruding parts: To avoid potential injury of clients, protruding parts should be avoided at all costs. They could also be used by burglars to hook their pulling devices and try to carry the whole ATM machine.

B. Location protection

Location is important as any other factor in designing and deploying the secure and safe ATM. The location should be as public as possible, well lighted and impractical to approach the ATM on its sides and back.

C. Security team authorized by local police station

When a group of alarms are triggered, the human operators located at the monitoring center of the ATM service headquarters, have the ability to manually re-check alerts and directly dispatch the nearest security team, and/or alert the local police station.

VI. IT Security

The IT security is the most flexible and most cost effective. With minimal additional hardware or by modifying the existing one, banks and ATM service providers can make their ATMs safer. The software is used to detect any anomalies and alert and/or block the ATM service at any time.

1) *Camera surveillance:* IP cameras are used in the ATMs and the ATMs surroundings because of the flexible communication options they provide. Every ATM has the minimum of 3 cameras:

- Camera facing the client of the ATM – with face recognition software that can detect if the clients face is covered; and pause and/or refuse the transaction until the face is recorded from the "en face" (fr.). The same camera is used to record the persons that are authorized to manipulate with the money cases and do maintenance on the ATM itself.

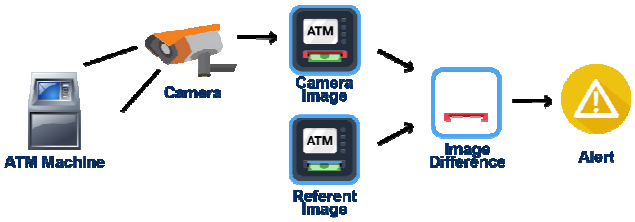

Fig. 3 Referent imaging alert procedure [6]

- Camera facing directly toward the ATM machine that is used to detect attached devices used in skimming attacks (Figure 3) – with software that can detect any difference in comparison to a referent image of the ATM machines in its original form[6].
- Cameras in the vicinity of the ATM that cover the surroundings.

Live camera surveillance should be simultaneously recorded locally inside of the ATM and on Central camera server. It should have a redundant Internet connection, usually available with the use of GSM or WiFi networks.

2) *Encryption:* Each entry to the database should be encrypted, as well as all communication in relation ATM <-> Bank kiosk central server <-> Bank Server.

3) *Data validation:* The communication layer used in the transaction, in this scenario, is the SOAP protocol[7]. To ensure that the messages have not been modified using a man in the middle attack, the validation XML fields are added and used with hashed values of private and public keys.

4) *Network protection:* Sniffing the communication is prevented with additional layer of security via Site-to-Site VPN ESP-3DES-SHA IPsec encryption pre-shared key

tunneling [8][9]. One static-static IP VPN tunnel is used to connect Bank kiosk central server with Bank Server, and another dynamical-static IP VPN is used to connect all ATMs with the Bank kiosk central server. Each ATM should have its own VPN group on the firewall that is protecting the Bank kiosk broker server. The same VPN connection should also be used to transfer camera surveillance and monitoring features.

5) Monitoring: Monitoring is used in 3 different ways:

- Network PING monitoring – is responsible to detect the heart beat of the connections with ATM networks inside of the physical ATM machine. It monitors every IP capable device.
- Remote application monitoring – is used to test the applications engines that are used in the payment process
- Synchronization consistency from ATM and Central server – that periodically test the database values and entries.

6) *GPS locators:* GPS module is used to record the location of the ATM at any time and alert if any unauthorized location changes have been made.

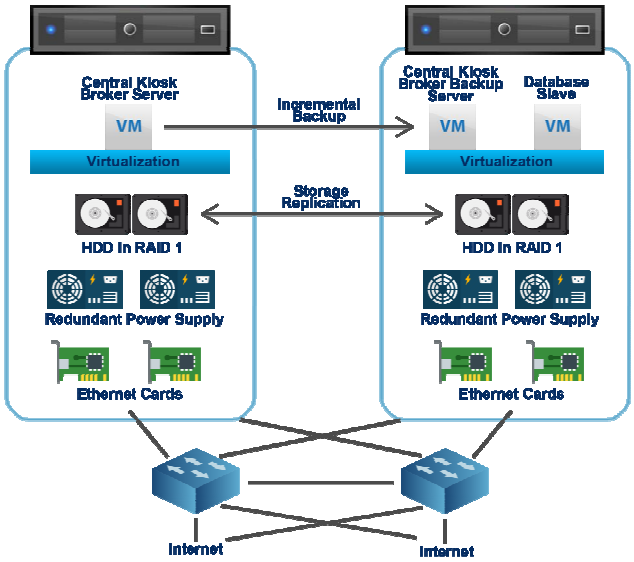

Fig. 4 Central kiosk broker server schema

7) *Temperature and water detection:* ATM machines are equipped with temperature and liquid sensors, to be able to detect burglary attempts and soaking of the equipment (short circuit attacks).

8) *Uninterruptible power supply:* ATM machines are equipped with UPS solutions, so they can detect and correct small power anomalies, live through the short period power outages and, if necessary, perform graceful shutdown of the operational systems.

9) Central kiosk broker server redundancy: The infrastructure around Central kiosk broker server and the hardware used are all in redundant active-active mode (Figure 4). Bare metal virtualization platform[10] is used for easier move, backup and redundancy, as well as to make a:

- Highly available logical storage across both servers, with redundant copies of both hard drive RAID 1 pair;
- Highly available LAN connections on each physical servers;
- Highly available virtual machine (VM) in a failover mode is used, so if one physical server goes offline, or is broken, the Bank kiosk service will not suffer.

The pair of hard drives used in the physical servers are in a RAID 1 (mirror mode) and the servers have two power supplies, each capable of normal power sustainability.

Stable and redundant network flow is achieved by using two active-active and interconnected Internet connections, in conjunction with paired network routing and communication equipment.

10) Central kiosk broker server backup: The virtualization platform is very flexible and can perform backup on the fly, without performance loss or need to shut down the Central kiosk broker server. Backup is performed on a separate machine and the backup process can:

- Make a complete backup of the VM
- Verify the data consistency and recoverability after it was backed up
- Manage data compression of backed up data
- Create incremental backup that save storage space and enables the backup to be made every few minutes
- Support VM backup recoverability in under 5 minutes

11) Database backups: The local database of the ATM machine is used as a transactional backup of the payments made on that machine, while the complete database is stored on the Central kiosk broker server. For the purposes of live backup, the Central kiosk broker server database is a master in a master-slave replication process that is used (Figure 2). One slave database is stored on a separate machine located in the same datacenter (on a backup machine), while the second slave database is stored on a virtual private server (VPS) in a distant datacenter. VPS server and a master database server are connected via Site-toSite static-static IP VPN ESP-3DES-SHA IPsec encryption pre-shared key tunnel.

12) *Integration with third party services:* The use of Central kiosk broker server enables easy (one point) integration with all third party services. One of potential services is an automated SMS alerting service with an independent SMS provider.

13) *Live Monitoring:* It is crucial to have a live monitoring system that can alert human operators in the Management center. From there, the operator can invoke actions like rebooting of the ATM systems, manual checkup of the ATM, direct contact with the local police stations, etc.

14) Procedural: Implementing the ISO 27001 in the formal and/or non formal way is considered good practice

in data protection [11][12]. Procedures should include details about:

- ATM use and maintenance
- ATM database debugging
- Testing patches and monitoring
- Logging and backup

VII. Non Standard Security

There are multiple ways researchers and ATM service developers try to make ATMs more secure[13]. They all have a positive and a negative side attached to it.

1. Biometric data - Biometric data can provide an additional layer of security. However the biggest issue is collection and storing of sensitive data. There are privacy issues connected with the use of biometric data, and many countries, including Serbia, have strict laws that prevents it.
2. Two step authentication - The use of mobile phones or additional hardware to help authenticate the user (contact, or contactless short wave technologies) may make it harder to perform identity theft attacks. However, this adds additional complexity to the system, raises costs and adds a single point of failure.
3. Software defined authentication - Live camera identification and similar technologies can be implemented with the existing hardware, but at the cost of network bandwidth and CPU processing costs. The non 100% accuracy of the software defined authentication can potentially make the service unavailable for the user.

VIII. Conclusion

If the trend of using paper money assets continues, or if the trend starts to favor virtual payment processors, Banking kiosk, in its current form (with touch screen input device), has the ability to almost completely replace the need for counter workers on bank premises and make regular ATM machines obsolete. Therefore, investments in Bank kiosks services will not be lost.

The use of Central kiosk broker server enables easy (one point) integration with numerous third party services. This potentially means that the same ATM infrastructure can be used with multiple commercial banks, or multiple additional service providers simultaneously. It can make the services available with the lowest price and/or fees, by sending request across multiple providers, and choosing the best one.

The Bank kiosk has a limited number of vulnerabilities that are mentioned in this and referenced articles, and security measures that have been taken to develop a new Bank kiosk in Serbia's payment process are well above the industry standard. With minimum investment increase per unit, in comparison to the regular ATM, it can withstand most of the attacks and reduce losses to a minimum, while providing more flexibility and features.

Using a highly available infrastructure for the Central kiosk broker server, as well as using 3 database backup instances in 2 separate data centers, adds redundancy to the system, that can backtrack every single transactions if needed.

The biggest vulnerability in using the Bank kiosk system is still the identity theft that cannot be stopped by modifying the Bank kiosk itself. The use of old security features (magnetic strip) on credit cards is still the single most exploited vulnerability. While the use of biometric data, software authentication and two step verification can provide additional layers of security, it is considered costly, not 100% reliable and has the problem with privacy related issues.

The future researchers should be focused on developing a smarter payment hardware and process that could prevent identity theft.

References

[1] L. Bielski, "Beyond Cash: Self-Service: Will a Concept with Epic Potential Get a Platform-And Some Respect-In US Banks?."ABA Banking Journal99.11 (2007): 33.

[2] Marie A. Wright, “Computer Fraud & Security Bulletin”, Volume 1991, Issue 9, September 1991, Pages 11-14

[3] Marie A. Wright, “Computer Fraud & Security Bulletin”, Volume 1991, Issue 9, September 1991, Pages 11-14

[4] Petar Bjeljac, Igor Zečević, Jelena Stankovski, Srđan Tegeltija, Miroslav Nićin, “Arhitektura povezivanja bankarskih kioska na sistem platnog prometa Republike Srbije”, Infoteh Jahorina 2015, ISBN 978-99955-763-6-3, 2015

[5] Nattakant Utakrit, "The Phantasm of ATM Withdrawal.", 5th Australian Information Security Managmen Conference, December 2007, Pages 207-215

[6] Flook, Ronald Arthur, Steven Barnett Rakoff, and Marcin Parkitny. "ATM security system." U.S. Patent 7,995,791, issued August 9, 2011.

[7] D. Linthicum, "B2B application integration" Boston, San Francisco, Addison (2001).

[8] Frankel, Sheila, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey, and Steven R. Sharma. "Guide to IPsec VPNs." NIST Special Publication (2005): 800-77.

[9] Navneet Sharma, Vijay Singh Rathore, "Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions.", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 –8958, Volume 1, Issue 4, April 2012

[10] Haletky, Edward, “VMware ESX and ESXi in the Enterprise: Planning Deployment of Virtualization Servers.” Pearson Education, 2011.

[11] Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.

[12] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five.", International Journal of Electrical & Computer Sciences IJECS-IJENS, Volume 11, no. 05, October 2011, Pages 23-29

[13] Srivatsan Sridharan, Gorthy Ravi Kiran, Sridhar Jammalamadaka, "Improvising Authenticity and Security of Automated Teller Machine Services.", JCSMC, Volume 3, Issue 2, February 2014, Pages 666–674