EVALUATING THE PERFORMANCE OF TWO-FACTOR AUTHENTICATION SOLUTION IN THE BANKING SECTOR

Olufemi Sunday Adeoye
Department of Computer Science
University of Uyo, Nigeria

ABSTRACT

Two-factor authentication delivers authentication through devices the customers have and the information (PIN) they already known. In today's corporate environment, the need exists to ensure that only authorized individuals or customers gain access to critical devices or services offered. This paper looks more closely at the banking industry by reviewing trends in transactions, infrastructures and consolidation using Two-factor authentication (2FA) with respect to Automated Teller Machine (ATM) and also examines the performance of the ATM.

Keywords: PIN, ATM card, Performance, Two-factor authentication, authentication factor, strong authentication.

1. INTRODUCTION

An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints.

Multifactor authentication (MFA) is a system where in two or more different factors are used in conjunction to authenticate. Using more than one factor is sometimes called "strong authentication". The process that solicits multiple answers to challenge questions as well as retrieves 'something you have' or 'something you are' is considered multifactor.

True multifactor authentication requires the use of solution from two or more of the three categories of factors. Using multiple solutions from the same category would not constitute multifactor authentication [12].

Two-factors or multi-factor authentication is exactly what it sounds like. Instead of using only one type of authentication factor, such as only things a user KNOWS (Login Ids, passwords, secret images, shared secrets, solicited personnel information, etc), two-factor authentication requires the addition of a second factor, the addition of something the user HAS or something the user IS.

Two-factor authentication is not a new concept especially in the banking industry. Two-factor authentication is used every time a bank customer visits their local ATM. One authentication factor is the physical ATM cards the customer slides into the machine. The second factor is the PIN they enter. Without both, authentication cannot take place.

Mathematically,

$$\mathbf{MFA = SYH + SYK}$$

or $$\mathbf{MFA = SYH + SYA}$$

or $$\mathbf{MFA = SYK + SYA}$$

or $$\mathbf{MFA = SYH + SYK + SYA}$$

Where,
MFA = Multi-factor Authentication.
SYH = something you HAVE.
SYK = something you KNOW.
SYA = something you ARE.

The thing you have can be anything from a smart card to a USB key-fob to your fingerprint. The thing you know is usually a conventional password. There are dozens of methods of two-factor authentication and they vary enormously in their sophistication, security, and cost. In general, you have to spend more to get higher levels of security. Logging into a workstation on a secretary's desk typically doesn't require the same level of security as a transaction moving a couple of million Naira half way around the planet.

However, the need for different levels of security poses an additional complication for any one who has to evaluate two-factor authentication products. You have to decide whether the proposed method is appropriate for the specific application.

Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In two-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

Factors are generally classified into three classes:

i. The ownership factors – something the user has (e.g. wrist band, ID cards, security token, phone, library card, photo card, ATM card, smart card, etc). From the examples, security token or software token, this is also referred to as TOKEN-BASED.
ii. The knowledge factor – something the user KNOWS (e.g., a password, pass phrase, personnel identification number (PIN))
iii. The inherence factors – something the user is or does (e.g., fingerprint, retinal pattern, facial image, DNA sequence, signature or voice recognition, unique bio-electric signals, or any biometric characteristic)

According to proponents, two-factor Authentication (T-FA) could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief access to their information [6], [8], [9].

2. THEORETICAL BACKGROUND
2.1 BRIEF HISTORY OF ATM

ATMs of course, are an establishment part of the payment landscape. But ATMs do not represent a payments type per se; rather, they are an electronic means of dispensing cash. They offer a convenient alternative to more traditional dispensers, such as bank tellers and automatic drive- through facilities [7].

Significant, even dramatic, changes are reshaping the ATM industry, including heavy consolidation and a decline in the number of ATM networks. Yet, the industry remains diverse. ATM in recent years has not only improved consumer convenience, but has expanded business opportunities for non bank ATM operators as well as for ATM networks.

The late 1960s marked the beginning of modern ATM and point of sales systems, although the concept of ATMs and debit cards existed prior to this. It might be argued that the first ATMs were cash dispensing machines. England Barclays Bank, near London for example, installed the first cash dispenser in 1967. The first cash dispenser was made by De La Rue Instruments. It uses paper vouchers bought from tellers. The machine is called the De La Rue Automatic Cash System, or DACS. Donald C. Wetzel has being credited with developing the first modern ATM, which is initially met with résistance from bankers. The idea came to him in 1968 while waiting in line at a Dallas bank, after which he proposed a project to develop an ATM to his employer [11]. A major part of the development process involved adding a magnetic stripe to a plastic card and developing standards to encode and encrypt information on the stripe. A working version of the Docutel ATM was sold to New York's Chemical Bank in 1969. The installation marks the first use of magnetically encoded plastic. Although the Docutel ATM did use the modern magnetic stripe access card, the technology remain primitive compared with today's. The Docutel ATM only dispensed cash and was an offline machine. To enable payment processing, the machine printed a transaction record that was MICR encoded.

By the early 1970s, ATM technology advanced to the system we know today. ATMs were first accessed primarily with credit cards, but in 1972, City National Bank of Cleveland successfully introduced a card with an ATM but not a credit function [4]. ATMs were developed that could take deposits, transfer from cheque to savings or savings to cheque, provide cash advances from a credit card, and take payments. ATMs also were connected to computers, allowing real-time access to information about cardholders account balances and activity. By connecting a string of ATMs to a centralized computer, banks established ATM networks.

Although many ATM networks were proprietary (single bank) networks, a major development was the emergence of shared networks. In a shared network, ATMs owned by a variety of banks would connect to a single network. Rather than be limited to using ATMs owned by the card-issuing bank, shared networks allowed cardholders to use all ATMs in the network. Shared network not only enhanced consumer convenience but also extended the geographic service areas of banks at a manageable cost. The early 1970s saw establishment of shared ATM networks, and the growth of shared networks accelerated in the mid-1970s. Shared networks represented 18 percent of all ATM networks in 1980, but the mix of shared/proprietary networks changed dramatically during the 1980s until 94 per cent of ATM networks were shared in 1990. Today, almost all ATM networks are shared [9], [11].

At first, ATMs were located on the premises of bank offices, but off-premise ATMs soon followed. Grocery stores, convenience stores and hospital quickly recognized the benefits of installing ATMs on their premises. By providing convenient access to cash, ATMs increased customer traffic as well as the amount of purchases per customer.

2.2 ATM USAGE

An Automated Teller Machine or ATM is basically a computer with a built in telecommunication access facility device. An ATM mainly does the work of providing access to your bank account and thus allowing you to withdraw cash without a cashier or a bank teller. To use an ATM, you will need a bank account, and you will also need an ATM card. With this card you will get a code, also known as a PIN. It is important that you keep the pin secret; otherwise someone else could potentially access your account.

An automated teller machine remains in passive stand-by mode until someone inserts his ATM card. The magnetic strip on the back of the card includes the bank's routing number, the user's bank account and their password. Once the card is entered, the machine reads the information on the magnetic strip and prompts the user to enter his password or PIN. If the PIN entered matches the PIN stored on the card, the user then gains access to the ATM's other functions.

Using the bank's routing number, the ATM connects to the main computer of the bank that issued the card via telephone line. Once connected, the ATM allows the user the option of receiving money, depositing money or checking his balance (some ATMs do more, but these are the three basic functions of all ATMs). If, for example, the user wants to withdraw money, the request for the amount is sent to the bank that checks the amount against the amount in the account. If the amount requested is the same as or less than the amount in the bank, the withdrawal is approved, and the bank deducts the amount from the account. If the amount requested is more, the withdrawal is denied.

Once the ATM receives approval, it dispenses the specified amount of money through a slot in the machine. The money is held in a sealed container with a spring-loaded bottom to maintain pressure. Rubber wheels in contact with the top bill roll, causing the money to be dispensed into a holding area until the correct amount is reached. Once the correct amount is counted out, the bills exit via the external slot to the user. The ATM then returns the card, prints a receipt and returns to stand-by mode.

To use the ATM, you will first place your card into the machine, and enter your PIN. Then you will be able to do your banking. Available transactions include money, depositing money or checking your account balance, or transferring money. With this ATM facility, funds are made available to you even when you are situated in another country. This cash is from your available bank balance. So if you don't have the required amount of cash available in your bank balance, the automated teller machine will prompt you saying "no sufficient balance."

2.3 TRENDS IN THE BANKING TRANSACTION

Technology has brought about a complete paradigm shift in the functioning of banks and delivery of banking services. Gone are the days when every banking transaction required a visit to the bank branch. Today, most of the transactions can be done from the comforts of one's home and customers need not visit the bank branch for anything. Technology is no longer an enabler, but a business driver. The growth of the internet, mobiles and communication technology has added a different dimension to banking. The information technology (IT) available today is being leveraged in customer acquisitions, driving automation and process efficiency, delivering ease and effieciency to customers.

2.4 ATM SAFETY

Safety is important when using the ATM. Keep your PIN number secret, and do not disclose it to anyone. Do not write your PIN on a piece of paper in the same location as your ATM card. Do not keep this number in your wallet. For added security, change your PIN number periodically. If your ATM card is ever lost or stolen, report it immediately to your bank. If you are going to do a deposit, try to have all the necessary paperwork ready. In fact, try to keep some deposit envelopes with you so that you minimize the time spent at the ATM. Make sure the ATM location is well lit. Do not approach or use the ATM if the area looks unsafe. Look for the suspicious people around the ATM. Use the machine that is visible to nearby traffic. If possible, bring a friend along to stand nearby when using an ATM. Avoid talking to strangers when using the ATM.

When entering your PIN, be sure no one is looking over your shoulder, and position yourself to block anyone from seeing your PIN code. When your transaction is complete, be sure to take your money and place it immediately in your wallet or purse. Also, don't forget to take your ATM card before leaving. Do not stand around and count your money at the ATM. If there is a discrepancy between the amount withdrawn, and the cash received, then notify your bank immediately (be sure to identify the machine that you used). Moreover, don't leave your bank receipt or trash at the machine.

2.5 ATM Hardware Components

An ATM is typically made up of the following devices:

i) CPU (to control the user interface and transaction devices)
ii) Magnetic and / or Chip Card Reader (to identify the customer)
iii) PIN pad (similar in layout to a touch tone or calculator keypad), often manufactured as part of a secure enclosure.
iv) Secure cryptoprocessor, generally within a secure enclosure.
v) Display (used by the customer for performing the transaction)
vi) Function key buttons (usually close to the display) or a touchscreen (used to select the various aspects of the transaction).
vii) Record Printer (to provide the customer with a record of their transaction)
viii) Vault (to store the parts of the machinery requiring restricted access)
ix) Housing (for aesthetics and to attach signage to)

Recently, due to heavier computing demands and the falling price of computer-like architectures, ATM have moved away from custom hardware architectures using microcontrollers and / or application-specific integrated circuits, most of which are based on Intel 8086 architecture, to adopting a hardware architecture that is very similar to a personal computer. Many ATMs are now able to use commercial operating systems such as Microsoft Windows and Linux. Although it is undoubtedly cheaper to use commercial off – the – shelf hardware, it does make ATMs vulnerable to the same sort of problems exhibited by conventional computers.

Mechanism found inside the vault may include:

a) Dispensing mechanism (to provide cash or other items of value)
b) Deposit mechanism, including a cheque processing module and batch note acceptor (to allow the customer to make deposits)
c) Security Sensors (Magnetic, Thermal, Seismic)
d) Locks (to ensure controlled access to the contents of the vault)

3.0 EVALUATING TWO-FACTOR AUTHENTICATION IN THE BANKING SECTOR

Generally, two-factor authentication systems are secure because it is very difficult to obtain both factors. Even if an attacker manages to learn the user's password, it is useless without also having physical possession of the device. Conversely, if the user happens to loose the physical device, the finder of that device would not be able to use it unless he or she also knows the user's password.
Two-factor authentication solutions can be evaluated by looking at three critical areas.

- The security and scalability of the technology.
- User adoption
- Total cost to deploy and support the system.

3.1 SECURITY AND SCALABILITY

The underlying security of the authentication method is the most critical factor. If the second factor of authentication is not protected your network, data, and users, then it is not worth implementing at any cost. ATM security had been questioned by many users whose money have been withdrawn without their consent even when they are still holding the ATM card in their hands. The major problem

here is that ATM card can be cloned very easily but the new verve card is difficult and cannot easily be cloned. Another security problem with Two-Factor authentication is that it may not be feasible to carry and keep track of multiple security tokens (e.g., ATM cards) especially for people who have accounts with three or more banks.
Early ATM security focused on making the ATMs invulnerable to physical attack; they were effectively safes with dispenser mechanisms. A number of attacks on ATMs resulted, with thieves attempting to steal the entire ATMs by ram raiding.

Modern ATM physical security concentrates on denying the use of the money inside the machine to a thief, by means of techniques such as dye markers and smoke canisters. This change in emphasis has meant that ATMs are now frequently found free-standing in places like shops, rather than mounted into walls. Another trend in ATM security leverages the existing security of a retail establishment. This is a situation in which a fortified cash dispenser is replaced with nothing more than a paper-tape printer. The customer requests a withdrawal from the machine, which dispenses no money, but merely prints a receipt. The customer then takes this receipt to a nearby sales clerk, who then exchanges it for cash from the till. Moreover, ATM transactions are usually encrypted with DES but most transaction processors will require the use of the more secure triple DES [13].

3.2 USER ADOPTION

Globally, ATMs have been adopted and are still being adopted by banks. They offer considerable benefits to both banks and their depositors. The machines can enable depositors to withdraw cash at more convenient times and places than during banking hours at branches. In addition, by automating services that were previously completed manually, ATMs reduce the cost of servicing some depositor demands [13].

3.3 TOTAL COST OF OWNERSHIP

ATMs cost involves significant upfront authentication hardware/software investment plus cost for initial and replacement devices. It also includes high internal deployment and ongoing support costs [13].

4. ATM RELIABILITY

ATMs are generally reliable, but if they do go wrong customers will be left without cash until the following morning or whenever they can get to the bank during opening hours. Of course, not all errors are to the detriment of customers; there have been cases of machines giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. On the part of customers there have also been cases of shortage of money dispensed from the machine. Errors that can occur may be mechanical (such as card transport mechanisms, keypads, hard disk failures); software (such as operating system, device driver, application); communications; or purely down to operator error.

5. ASSESSMENT OF ATM IN BANKS

5.1 Strengths

i) Customers can make cash withdrawals at any time and without the need for a human teller, i.e. no closing hour.
ii) Can check their account balances at any time.
iii) Allows people to deposit cash or cheques.
iv) Allows for money transfer between customers bank accounts
v) Provides customers with access to financial transactions in a public space.
vi) ATM’s card of a customer hanging inside the machine does not disturb other customers from their transactions.
vii) It is a convenient way to get fast access to cash.

5.2 Weaknesses

i) The card and the PIN number can be stolen and intruders have access to your account.
ii) ATM can go out of service thereby denying customers of opportunity to make transactions.
iii) ATM cards can be cloned and used to have access to customers’ accounts.
iv) The entire ATM can be stolen by ram-raiding.
v) The environment where ATM is installed may not be secured, especially off-premise ATMs.
vi) Free standing ATMs located in places like shops, rather than mounted into walls can be stolen by thieves.
vii) Money dispensed may not be complete.
viii) There may be cases of “phantom withdrawals” from ATMs.
ix) ATM card may hang inside the ATM.
x) There can be cases of the machine giving out money without debiting the account or giving out a higher denomination of note by mistake.
xi) Sometimes, customers account is debited without the machine dispensing money.
xii) Finally, there have been cases of incidents of fraud where criminals have used fake machines or have installed fake keypads or card readers to existing machines. These have been used to record customer’s pin number and bank accounts and have then used this information to create fake accounts and steal money from customers.
xiii) ATMs located in busy locations may not have adequate funds for busy holiday weekends when large numbers of people are taking out cash.
xiv) ATM does not prevent identity theft and fraud.

6.0 ATM PERFORMANCE MEASUREMENT

Marwedel identified five metrics for the evaluation of the efficiency of an embedded system. Three of these and additional three provided by the researcher are used in this paper to evaluate the performance of an Automated Teller Machines [14].

i) **Power Consumption:** The energy consumption of a small bank machine for one day can be calculated as illustrated below.
Power consumption of ATM (when it is in use)

2.0A @ 115 VAC at 60Hz
1.0A @ 230 VAC at 50Hz
Power = Amps * Voltage
= 2.0 * 115
= 230W or 0.23kW
Energy Consumption = Power used * Time
The above will give answer in kilowatt hours (kWh), which is the same unit as electric bill.

∴ The energy consumed by a small ATM in one day is:
Energy = Power * Time
= 0.23kWh * 24h
= 5.52kWh
The above is the average energy consumption per ay when the machine (ATM) is in use.

Power consumption when the machine is idle:
0.6A @ 115VAC at 60Hz
0.3A @ 230VAC at 50Hz
Power = Amps * Voltage
= 0.6 * 115
= 69W or 0.069kW
Energy consumption = Power used * Time
= 0.069kWh * 24h
= 1.656kWh

Besides the low power consumption, most of the embedded systems also make use of a battery. ATM is not an exception. To reduce the battery drain and void frequency recharging of the battery, the power consumption of an embedded system has to be very low.

ii) **Run-Time Efficiency:** Automation makes the banking processes to be more efficient in processing transactions. There are benefits because you experience fast and efficient transactions and compliance besides reduced risks of human error. For instance, you can make cash deposits and withdrawals using ATM fast and efficiently.

iii) **Lower Operation Costs:** Bank automations could help reduce costs in the area of hiring staff, training employees, purchasing office equipment, as well as physical office overheads. This is because automation offers strong payment systems enabled by e-commerce and information systems. Without automation, banks would be made to hire many employees whose duties would be efficiently done a single automation process. Also, without an established automation system, banks would be made to regularly invest funds in hiring and training new and old staff.

iv) **Increase Productivity:** Automation of banking business has helped increase productivity. This is because it eliminates the tedious, repetitive, and cumbersome tasks such as paper work often associated with the banking process. In a mid-to-large banking business environment, automated business strategy would assist in simplifying processes, which could in turn increase productivity of each employee. For instance, withdrawals and deposits by 10 bank tellers at the counter could be simplified by having one ATM machine.

v) **Availability:** ATM is not like human cashier that may go on break within the office hours or get engaged in other activities that may took him/her away from his/her duty post. Besides, human cashier also have a closing hour as determined by the bank he/she is working for. ATM is available round the clock without any closing hour or official engagement. It can be accessed 24/7.

vi) **Speed:** In a society where speed and convenience matter more and more make sure your customers can access their money fast and easily with an ATM. Using a CASHPOINT ATM, customers can access their bank accounts to make cash withdrawals, credit card, cash advances, and check their account balances.

7.0. RECOMMENDATION

From the discussion in this paper, it is clear that two-factor authentication in banks through the use of ATM card is porous. Therefore, customers must be protected from ATM fraud; financial institutions should educate customers about typical skimming techniques and offer zero-liability protection that includes PIN credit and debit card losses.

Moreover, ATM vendors should use “anti-skimm” designs for their ATM surface and keyboards. Also ATM vendors should use payment card industry (PCI) - certified components to guard against common software vulnerabilities that can be exploited. The introduction of verve cards that cannot easily be cloned is a step in the right direction to stop or reduce ATM fraud to the barest minimum.

8.0 CONCLUSION

Two-factor authentication solution equips customers with a cost effective means of providing flexible and strong authentication to very large scale, diverse audiences both inside and outside of your infrastructure. ATM has helped the banking sector to offer security and privacy to all their customers. It is reliable, available, and efficient with low power consumption. However, since fraud is still being reported with Two-Factor authentication, it shows that it is not totally secured, only that the fraud rate is reduced as compared to that of One-Factor authentication.

9. REFERENCES

[1] A-Ma, ATM Fraud. A Growing Threat to Banks, Africa News, Business, World News, June 29, 2009.
[2] Amit Bhawani. (2010). What is an Automated Teller Machine? Available: ezinearticles.com/?
[3] Avivah Litan. Criminals Exploit Consumer Bank Account and ATM System Weaknesses, Gartner Research Publication, USA. 2005.
[4] Billings Farnsworth. (2009, May). The History of Automated Machine. Available: http://EzineArticles.com/?

[5] Bob Sullivan. (2006, Nov. 30). ATM System Called Unsafe – The Red Tape Chronicles. Available: redtape.msnbc.com/2006/11/researchers_who.html.
[6] Christopher Hockings. (2005). Two-Factor Authentication using Tivoli Access Manager WebSEAL. Available: PDWeb/www/lib/html/C/tokenlogin.html.
[7] Fumiko Hayashi, Richard Sullivan, Stuart Welner (2003), A Guide to the ATM and Debit Card Industry, Federal Reserve bank of Kansas city, Kansas City, Missouri, USA.
[8] Paul Roberts. Multi-Factor Authentication, IEEE. 2004.
[9] Roel Schouwenberg. (2010). Here’s How to Fix Online Banking Fraud. Available: http://threatpost.com/en-us/30T.
[10] Srikrishnan H. Two-Factor Authentication for Online Banking, Portwise, Yes Bank, Portwise. 2006.
[11] Tom Harper. (2004). Timeline: The ATM’s History. Available: www.thocp.net/hardware/atm.htm

[12] Federal Financial Institutions Examination Council. (2006). Available: www.ffiec.gov/

[13] Guide to Evaluating Two-Factor Authentication Solutions. www.phoneFactor.com

[14] Peter Marwedel (2003): Embedded System Design, KluwerAcademic Publishers.

[15] The Advantages of Automating a Banking Businessǀ eHow.com.http://www.ehow.com/info_8445168_advantages -banking-business. Html#ixzz1umLztUbj

Author's Profile.

Olufemi Sunday Adeoye is currently a PhD student in Information Management Technology Department, Federal University of Technology, Owerri, Nigeria. He did M. Tech. in Computer Science from the Federal University of Technology, Akure, Nigeria. His field of interest is Theoretical Computing, Computer Performance and Security.