Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 6 No. 2. June, 2015 – www.cisdijournal.net

Improving The Security of Point of Sale Terminal Transactions Using Mobile Phone Embedded Authentication

Adedayo, O.S. & Bolaji, A.A.
Department of Computer Science and Mathematics
Adeleke University
Ede, Osun State, Nigeria
State of Osun, Nigeria
E-mails: olatunjisamuel01@yahoo.com, badefola@gmail.com

ABSTRACT

Emerging technologies has cut across both human and business activities and in the same vein revolutionised banking, online payment, automated-tellering, mobile payment as well as payment on the point of sale terminal. These technological innovations has simplified commercial activities and encouraged cashless transactions in the twenty first century. The point of sale terminal is a mobile payment gateway that has become very popular with most financial institutions and business owners across the world. Consequently, card usage on a point of sale terminal can be considered vulnerable, secured and more secured by the way of card swiping only, swiping and using a PIN and also swiping, using a PIN and concluding the transaction with an automated token number sent to a pre-registered mobile phone linked with your account. This paper focuses on introducing a multi factor authentication by improving the security on the point of sale terminal through the introduction of a security procedure which links a pre-registered mobile phone and a card account in order to conclude a payment on the POS terminal.

Keyword: Personal Identification Number (PIN); Automated Teller Machine (ATM); Multi Factor Authentication (MFA); Point Of Sale (POS);

1. INTRODUCTION

Banking majorly revolves around cash deposit and withdrawal, but in recent times a lot of products and services have been added to banking services especially from the late nineties. The introduction of the different products and services has grown so rapidly such that a bank account holder may not necessarily need to transact with the branch the account was opened initially. The technology that has eliminated residential access to banking is known as Electronic banking otherwise called online transactions which has made it possible to do banking and other merchandise online (Shim, 2000). Electronic banking in simpler terms is a fusion of banking and electronics which means accessing banking electronically. Electronic access to banking comes easily with the aid of telecommunication devices and of course computer networks such as using the automated teller machine, internet/mobile banking, point of sale terminal and telephone banking.

As earlier mentioned, eliminating distance constraints and allowing remote access to banking services has been enhanced by telecommunications. Telecommunications refers to communications over a distance (Shim, 2000) and this technology has made the payment of goods and services possible using a point of sale terminal. The introduction of POS terminal has given significant rise to the use of electronic mode of payment (Olutayo et al, 2014) such that cashless transactions can be consummated using a verifiable bank card over the terminal. A successful authentication and authorization of a bank card over the terminal allows a bank service request to be granted. The authentication and authorization takes place using telecommunication channels. Authentication can be single, double or triple, when an authentication process is more than one, it is considered multi and it increases the level of security on the object.

1.1 What is a PoS?

According to GTBank (2015); A Point of Sale terminal is a portable device that allows local debit cardholders make payment for goods and services in a retail environment. The point of sale terminal includes a computer, a cash register and other hardware and software that work together for the transmission of sales data to the merchant and customer's accounts. A typical wireless PoS terminal is as shown in Figure 1.

Figure 1: A Typical Wireless Point-of-Sale Terminal

1.2 How a PoS works

A point of sale (PoS) system is used by businesses as a way to make transactions, record sales, and track inventory. Based on the type of system in use, there are a variety of other functions it can perform to accommodate the specific needs of a business.These were predominately used by larger companies and especially retail chains in the past, they are now used by many small to mid-sized businesses as well (Nick, 2013).

The beauty of a PoS system is that all the information is contained in one database, making it easy to search for any nugget of information and connect it to others through reports to keep business running smoothly (Munroe, 2015). The usual setup of a PoS system includes a computer server with one or more terminals that serves as workstations, depending on how many checkout stations there are. There is usually a keyboard for data entering, credit/debit card swiper, a receipt printer, pin pad, and a cash drawer. Utilization of some type of barcode scanner to input information quicker is common to many companies. There may also be a checkout scale, card reader, and customer display. Some more recent systems offer touchscreens for a more streamlined experience. Mobile and wireless technology is a fairly new addition to PoS systems and mobile devices such as iPads, android and window-based tablets and iPhones are starting to be used by more companies. This option is known to be cost-effective for small to mid-sized businesses with limited needs and can also be quite efficient (Nick, 2013).

1,3 POS Components

According to Small Business Depot (2005), computer-based PoS system is made up of computer platforms, special peripheral devices and a PoS software. They are as identified as follow:

i. **Software**: It coordinates and controls the behavior of a PoS. It is broadly categorized into: a. Operating System,
   b. PoS Application Software,
   c. Credit card authorization software and
   d. the accounting software

ii. **Hardware**: Computer-based POS makes use of the common desktop peripherals like keyboard and mouse but it also has some peripherals that are specific to retail PoS. They are:
   a. Cash Drawer (Receipt printer driven or direct connect)
   b. Receipt printer
   c. Barcode Scanner (Attached or Portable)
   d. Label/Report Printer
   e. Pole Display
   f. Magnetic Stripe Reader
   g. PoS Keyboard
   h. Touch Screen/Display Terminals
   i. Personal Data Assistant
   j. Scales
   k. Wireless Payment System

2. OPERATIONS OF POS

A PoS, or point of sale, system can help reduce paperwork, track inventory and market to customers through one easy-to-use process, making more time to manage business rather than staying bogged down in details. According to Munroe (2015), many PoS systems are geared toward small businesses, and some are industry-specific; their operations include:

i. ***Data Entry***
POS systems are designed to minimize the time spent on data entering of customers' details and their purchases. Modern PoS systems allow for the pulling up of customers data by name, phone number or customer number once they've been entered, saving a considerable time in the long run. Industry-specific POS software has time-saving inventory management features, such as customizable list of existing available parts in a sales shop of a mechanic or a searchable database of books in a small bookstore which allows for entering new inventory with a single click instead of tracking the items by hand.

ii. ***Inventory Management***
The inventory management systems can be as general or specific as the need may be in order to keep the business running smoothly. Stock taking must first be done in a store in order to be able to keep the track record of how parts or items are sold. Most PoS systems make this process simple; for example, if you list a part on a customer's invoice, it is subtracted automatically from your inventory. Some systems provide alerts when certain inventory items get low.

iii. ***Customer Marketing***
By tracking the purchases of customers along with their contact information, simple marketing strategies can be designed to help gain more business. Most systems allow for email marketing as well as direct mail reports, this makes allowance to compose and send email directly from PoS system. It's also helpful in face-to-face communication with customers. A customer past transactions can be seen immediately and ask if he was satisfied with his most recent transaction, using his specific information. Notes can as well be entered on most systems, such as a spouse's name or the customer's birthday.

iv. ***Reporting***
A major feature of PoS systems is the ability to run reports. Financial reports typically can be transferred automatically to the accountant or separate financial tracking software, this eliminates the need to enter every paper transaction at the end of the day or add up employees' hours; most PoS systems have a feature that allows staff to clock in and out each day. PoS systems typically come with standard reports such as cost of goods sold, gross sales, low inventory, existing inventory, customer purchase history and item-specific sales reports.

3. AUTHENTICATING A BANK CARD OVER A POS TERMINAL

Using a bank card over a PoS terminal requires a form of authentication. Authentication is a mechanism designed to verify the identity of an agent, human, or system before access is granted (Raggad, 2010). Authentication is very necessary for security management and thus it is implemented in bank cards. During authentication of a bank card on a terminal, the card details and digital identity are verified to ensure that the card has not been fraudulently reproduced and the information on the card matches the identity that has been previously stored. It is debatable to say that a fraudulently reproduced card will equally pass the authentication test since it is likely to have all the information and features. In as much as this claim is very uncertain, there are some authenticating techniques that can allow or disallow the authentication of a fraudulently reproduced bank card.

According to Patel (2010), there are three major types of entity authentication techniques which are:

i. Something the user knows (type 1): something the user knows as related to using a bank card on a PoS terminal is a PIN or password which are expected and believed to be known only to the authorised carrier/owner of the card.

ii. Something the user is (type 2): this is something inherent to a human individual e.g. biometric feature.

iii. Something the user has (type 3): a physical material or handy hardware are considered to be something the user has such as cell phone, bank card, security token etc.

Bank card authentication often passes through two out of the three aforementioned authentication factors and but since security cannot be overemphasised the combination of all the types would go a long way to secure PoS transactions.

3.1 Security Vulnerability of Each Authentication

The use of a bank card over the POS terminal has come with some vulnerability. The security vulnerability is mostly attributed to the fact that type 1 and 3 are the commonest form of authentication that is useable on a POS terminal and sequel to this, some of the security vulnerability has been stated as follow:

i. Type 1 and 3 authentication methods: this multifactor authentication is a combination of what you know and have which literarily means the PIN and the bank card. Shoulder surfing and cloning of cards are the threats to these types.

ii. Type 3 authentications only: using this type means swiping your bank card against the chip reader of the POS terminal. Swiping alone is a single factor authentication which does not require the use of a PIN and this is highly risky due to the fact that a fraudulently reproduced card can be used to consummate a transaction online and against a pos terminal.

iii. Cost of token acquisition: a token hardware can attract a charge which may discourage a bank account owner. The implication of this is that the higher security that should have been ordinarily enjoyed becomes unknowingly evaded.

3.2 Token-Based Authentication.

Token-based authentication is a process that relies on information or substance that the user possesses that other user of the identifier is not supposed to possess or have access to. According to Bosworth, Kabay and Whyne (2014), Token authentication achievement is possible in many ways, including:

i. **Access Card Entry Systems:** The means of encoding identification data on the cards include optical bar code, magnetic stripe, smart cards with embedded chips that store biometric data, and cards with embedded bits of metal. Most bar codes are not secure; the cards are easily duplicated. Although the newer, two-dimensional bar codes are nearly tamperproof but they cannot store much information.

ii. **Proximity and Touch Cards**: The best of the new card access control systems use proximity or touch cards. These cards communicate with readers using infrared or microwave transmissions. The reading device powers some types of cards, while others contain miniature batteries. Physically, the cards and card readers are weatherproof, vandal resistant, and do not wear out. Proximity card readers can be surface mounted, recessed flush into a wall, or entirely concealed within a partition so that they do not call attention to a security door.

iii. **Smart cards and dongles**: Another form of token is a smart card. These cards can go into a PC card reader or can be read by a specialized reader. *Dongles* are smart cards that fit into input-output ports such as Universal Serial Bus (USB). A smart card has its own processing capability and typically stores a private key associated with the user. Often, a password or PIN is required to access the card, thereby providing two-factor authentication capability. The smart card enables user authentication by signing some challenge presented to it with the user's private key. The signature is verified by means of the user's public key.

iv. **One-time password generators:** A popular form of token, from vendors such as RSA Data Security Inc. and CryptoCard, displays a one-time password, typically a six- or eight-digit numeral, which changes each time an access button is pushed or when a given time has elapsed since the password was last used. The user authenticates by entering the user ID and current value displayed by the token. The password is called one-time because it expires at the end of its allowable period for use. The token is typically contactless, in that it does not need electrical contact with the computer where the user is presenting authentication data. The user transfers the necessary information from the token via a keyboard or other input device. To make this a two-factor authentication, a fixed user password is also required in addition to the changing one-time password displayed by the token. These tokens are based on shared secret keys, so both the token and the server have a shared secret. The server and the token need to be initialized and then kept synchronized for this scheme to work.

v. **Soft tokens**: The idea of *soft tokens,* or *software tokens,* has been proposed as a low-cost alternative to hardware tokens. Early soft tokens consisted of a user's private key encrypted with a password and stored on some transportable medium, such as a floppy disk. Such a scheme is extremely vulnerable to dictionary attacks because a guessed password can be verified easily (by testing a putative private key to see if it decrypts a message encrypted using the user's known public key). An alternative scheme would be to store the user's entire private key on an online server and make its use contingent on a secure password-based protocol.

.

3.2 Authentication Using Mobile Devices

The use of mobile devices is another form of token based authentication increasingly available for access to restricted Websites such as bank account pages registers a mobile device such as a cell phone or a tablet that is capable of receiving Short Message Service (SMS) text messages. During login, the authorized user receives a one-time code to enter in the Web page. This approach puts additional value on security measures to protect the mobile device; for example, short timeouts requiring entry of a PIN, encryption of data in the device's memory, and methods for remotely inactivating or wiping the device if it is lost or stolen (Bosworth *et al*., 2014).

4. USING MOBILE PHONE AS A TOKEN HARDWARE

A mobile phone can perform the function of a token device and provided a multi factor authentication for a PoS transaction. Table 1 shows a sequential procedure of allowing mobile phone to serve as a token device.

Table 1: Sequential step on making a mobile phone a token

TASK	KEY FACTOR
Bank account	Bank card
Register mobile phone with card account	Use IMEI
Register SIM number	Unique mobile number
Receives credentials for a requested service	SMS authentication
Sends received credentials	SMS authorization

.

4.1 Mobile Phone Authentication Infrastructure

A mobile phone and SIM card registered with the bank account can only receive the one time password as an SMS. This is achieved using the unique identification of the mobile device such as the IMEI and also the SIM number which is equally the mobile number that were previously registered with the card account. After authenticating the bank card using the PIN on the PoS terminal, the supplicant receives an SMS containing the information of the requested service on the registered mobile phone and will respond back to confirm the authorization request. The device responds by forwarding the received credentials which are checked against an identity provider or domain server (Buchanan, 2011). This process ensures that the mobile phone and SIM card that are registered with the bank card receives and sends the authorised credentials.

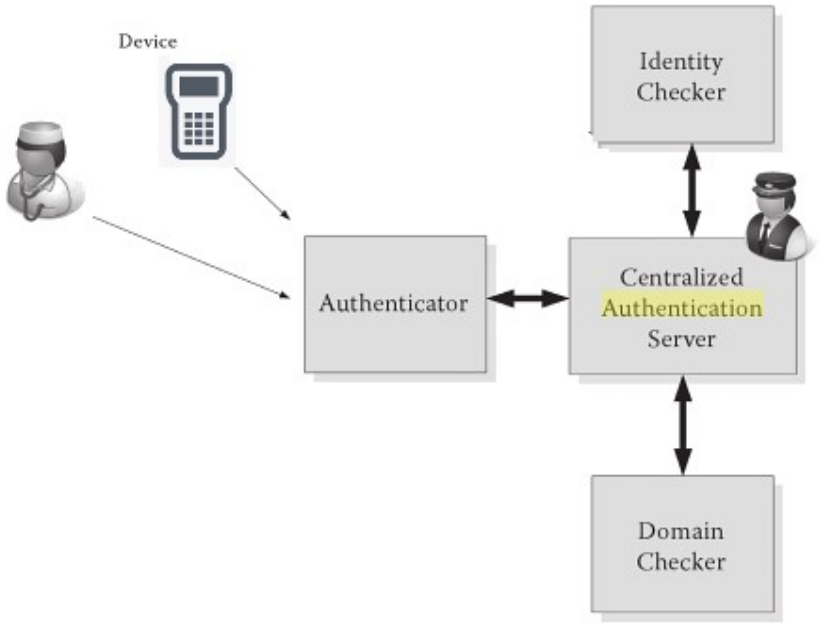

Figure 2: Mobile phone authentication infrastructure

It has been evidently shown that the use of short message service for authentication requires a second registered physical device: a cellular phone. At the time of authentication, a computer-generated code is sent to the user's mobile phone and entering the code proves that the device is present and authenticates the user (Patel, 2010).

4.2. Benefit of this Model

i. Provides security during PoS transactions

ii. Cloned cards cannot be successfully used without access to the registered mobile phone

iii. Cost of token acquisition has been eliminated.

iv. Gives ease of use without having to use an extra device

5. CONCLUSION

The need to improve the security provisions on PoS transactions is inevitable due to the fact that transaction performed on a PoS terminal uses either a single or double factor authentication. Using a mobile phone to provide another level of authentication will increase the security on PoS transactions whereby making same more secured and giving a higher level of convenience and comfort to a card user. The use of a mobile phone complements banking services thus the ease of use and improved security will still be achieved.

REFERENCES

1. Shim, J.K. (2000). Information systems and technology for the non-information systems executives. CRC Press LLC,Florida, Pp 89 - 91.

2. Raggad. B.G., (2010). Information Security Management concepts and practise. CRC Press Taylor & Francis Group,Florida, Pp 22.

3. Patel. D.R., (2010). Information Security Theory and Practice. PHI Learning Private Limited, New Delhi-110001, Pp 147 – 159.

4. Buchanan. W.J., (2011). Introduction to Security and Network Foensics. CRC Press Taylor & Francis Group,Florida, Pp 404.
5. Olutayo V.A., & Olakunle A.S., (2014). Improving the service quality in the Nigeria banking industry. International Conference on Science, Technology, Education, Arts, Management and Social Sciences, iSTEAMS Research Nexus Conference, Afe Babalola University, Ado-Ekiti.
6. GTBank, 2015. Available at: http://www.gtbank.com/personalbanking/ways-to-bank/point-of-sale. Accessed 5th June, 2015
7. Bosworth Seymour, Kabay Michel E. and Whyne Eric (2014). Computer Security Handbook. Sixth Edition Volume 1. John Wiley & Sons, Inc., Hoboken, New Jersey.
8. Nick Mann (2015). How does a POS works? Available at: http://www.businessbee.com/resources/profitability/pos-system-work/ Accessed 10th July, 2015.
9. Munroe Shala (2015). How Do POS Systems Work? Available at: http://smallbusiness.chron.com/pos-systems-work-41627.html. Accessed 10th July, 2015.
10. Small Business Depot (2005). A Beginners guide to Computerized POS Software. Available at: www.barsnstripes.com/docs/**pos**4beginners.**pdf** . Accessed 10th July, 2015