International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:8, No:6, 2014

A Proposal to Mobile Payment Implementing 2AF+

Nael Hirzallah, Sana Nseir

***Abstract*—**Merchants are competing to offer the use of mobile payment to encourage shopping. many mobile payment systems were made available in various locations worldwide; however, they have various drawbacks. This paper proposes a new mobile payment system that discusses the main drawbacks of these systems, namely security and speed of transaction. The proposal is featured by being simple to use by customers and merchants. Furthermore, the proposed system depends on a new authentication factor that is introduced in this paper and called by Two-Factors Authentication Plus, (2FA+).

***Keywords*—**Electronic Commerce, Payment schemes, Mobile Payment, Authentication Factors, Mobile Applications.

I. Introduction

THE number of mobile phones, mainly smart phones, being sold has increased dramatically in recent years. They are becoming more preferred companions to users than desktops or notebooks, [1]. Thus they are serving much more than just communication tools. This has led to more and more sensitive data being stored on these mobile devices. Furthermore, in developing countries, the number of mobile phone users exceeds the number of those having bank accounts. Thus, the low banking service penetration and the large migrant communities are other factors to utilize mobile phones for payment purposes, [2]. There are many variables that are involved in mobile payments. While discussing some of these variables, this paper proposes a new scenario for mobile payments that tackles the main concerns related to mobile payments, namely security and speed of transaction; yet without complicating the process or making it undesirable to users. The issue of securing the mobile phone and the content it contains have exceeded beyond just securing the device from a virus attack. There are hard threats that affect the physical device itself such as theft, illegal access, and getting the possession of its MicroSD memory card. Such threats should be considered when implementing a mobile payment method. For that, the proposed scenario depends on a new Authentication Factor that is defined and explained in this paper. It is called the Two-Factors Authentication Plus or 2FA+.

In the next section, this paper discusses where Mobile Payment is currently standing. This is done by listing a number of deployed systems worldwide and then discussing how a number of these systems work. The section ends by listing a number of drawbacks that most of the current system suffers from. The section that follows this, talks about the well-defined authentication factors: the two and the multiple. It then proposes a new terminology called the Two-Authentication Factor Plus that will be used in the proposed system which is discussed in detailed in the section the follows. Finally, the paper ends with the conclusion.

Nael Hirzallah is with the Department of Computer Science, Applied Science University, Amman, Jordan (e-mail: hirzallah@asu.edu.jo).
Sana Nseir was with the Department of Computer Science at Zarqa University, Zarqa, Jordan (e-mail: sananseir@gmail.com).

II. Related Work

A. Current Deployed Systems

There have been a number of deployments of mobile payments worldwide across the spectrum of proximity and remote payment. The following is a list of some deployments, [3]:

- Google Checkout™: Google partnership with Sprint®, Citi®, MasterCard, and FirstData® in US.
- PayPal Mobile™. It provides mobile PIN-based web and SMS capabilities for PayPal account payments in US. As well as modified eWallet from Paypal.
- Handy-Ticket, A ticket stamping machine of the Austrian Federal Railways that can be used to purchase mobile tickets ("Handy-Ticket"), [4].
- NCR in US, [5],
- etc…

Expresspay ™ from American Express, [6] is based on an encrypted computer chip that is built into some American Express® Cards. It is not really a mobile payment system, but the fact that the chip could also be located in the mobile phone instead makes it considered as one. It enables the buyer to make purchases without having to swipe the card. Expresspay purchases are faster than cash and standard magnetic stripe transactions, and best of all, the expresspay-enabled card never needs to leave the holder possession. The payer needs just to hold his expresspay-enabled card or the phone to the specially marked reader at the register, collect the receipt, and leave. The expresspay chip transfers payment information wirelessly when one holds the card or the phone to the contactless reader.

B. Mobile Payments Drawbacks

There are many challenges associated with mobile payments systems. However, among these challenges the following are what this paper will focus on and attempt to resolve in its proposal:

- Fast process at cashier: Customers usually avoid long queue at check out which may be caused by bank approval request issued to customers on the mobile phone to confirm a payment.
- Secure against theft: Customers would like to be assured that no payment can be done via the phone by unauthorized users.

- The need for extra HW: Merchants usually prefer to avoid purchasing new hardware if the added value is not worth it.
- Fixed prices: Mobile payment stakeholders usually require a share from each transactions. The more parties involved in the process the more expensive the item may get.

III. Multi-Factor Authentication

A. Two-Factor and Three-Factor Authentication

Many people are highly familiar with the importance of online security, logins, usernames and passwords due to increasing digital crime and internet fraud, [7]. Standard security procedures require a simple username and password. Such information is called “something you know” or “what you know”. Thus it is easy for criminals to gain access to a user’s private data such as personal and financial details and then use that information to commit fraudulent acts, generally of a financial nature.

Two Factor Authentication, also known as 2FA, is an extra layer of security that requires not only a password and username but also something that only the users have on them such as a physical token, thus, called as “something you have” or “what you have”.

Historically, two-factor authentication is not a new concept but its use has become far more prevalent with the digital age we now live in. Recently on February 2011, [8] Google announced two factor authentication, online for their users, followed by MSN and Yahoo.

Many people probably do not know that this type of security process is called Two-Factor Authentication and likely do not even think about it when using hardware tokens, issued by their banks to use with their card and a personal identification number when looking to complete internet banking transactions. Simply they are utilizing the benefits of this type of multi factor authentication.

In fact, the concept of multi-factor authentication is usually explained in terms of requiring not only "something you know” and “something you have” but also it is extended to “something you are" to be authenticated. Simply, “something you are” is just like requiring a voice biometric to gain access to account balances or a quick automated call back to the account owner to verify a large online payment which is a practical way to protect against fraud.

The downside to the second factor of authentication is that new hardware tokens need to be ordered, then issued and this can cause slowdowns and problems for a company’s customers wanting and waiting to gain access to their own private data via this authentication procedure. The tokens are also usually small and easily lost so causing more problems for everyone when customers call in requesting new ones. With over 5 billion mobile phones in use, turning a phone into an authentication device quickly solves the need and additional cost and delays sending out hardware tokens.

B. The Proposed 2FA+

In this paper, the third factor is left out from the discussion because it already exists on smartphones as an optional tool to unlock the phone. This would add another level of security to accessing the mobile application made for payment. An example on such a tool is facial recognition or voice recognition that could easily be applied at any time.

Two Factor Authentication process is believed sufficient to help lower the number of cases of identity theft on the internet, as well as phishing via email, because the criminal would need more than just the users name and password details. However, if the mobile phone is the token for the second factor of authentication, then unfortunately, theft of mobile devices has been and still is a significant concern to customers. For that, the proposed mobile payment scenario will consider using two tokens instead of one in order to yet add another level of security. The information that the smart phone supposed to hold, will be split and stored on two different locations: one on the mobile and another in the wallet on a traditional external card. This will be called as Two-Factors of Authentication Plus (2FA+) due to splitting “something you have” to more than one token.

To recall how authentication is carried out in the traditional credit card payment process, the customer is expected to offer 2FA. These two factors are the signature or the PIN number and the existence of the card itself or its details.

The proposed mobile payment scenario, on the other hand, requires two tokens to verify identity for the second factor: i.e. “what you have”. One is the mobile phone itself, while the other is the card, which is probably placed in the customer wallet. This of course, besides the PIN code that is required by the payment service, which could be the same or a different one to that used to unlock the Mobile phone, or to access the mobile payment application, if the former is not implemented.

IV. Proposed Mobile Payment

This section introduced an innovative mobile payment system, which supports and delivers secure and easy operating mobile payment transactions based on 2D barcodes. Unlike other mobile payment systems and solutions, the proposed system has several features.

- Supports 2D barcode-based solutions for mobile payment.
- Improves mobile user experience by reducing user inputs in mobile payment.
- Considered a fast process since it does not need a remote user confirmation.
- Secure as authentication is split into three parts: PIN, separate card, and the existence of a MobPayApp on a mobile device.

The proposed mobile payment solution depicted in Fig. 1 and discussed in this section could be considered to belong to the Peer-to-Peer Payment model, [9]. Yet, this scenario could be modified a little to suit any other mobile payment model such as Bank-centric or Operator Centric model.

The scenario depicted in Fig. 1 is a merge between the traditional credit card payment process and the mobile

payment methods. The solution depends mainly on a Line-of-Sight between the merchant and the user. Thus, although encryption to QR Barcodes could be easily implemented as in [10] [11]; however, since the communication media between the merchant and the customer is considered optical and needs a Line-of-sight, such extra security measures may not be needed.

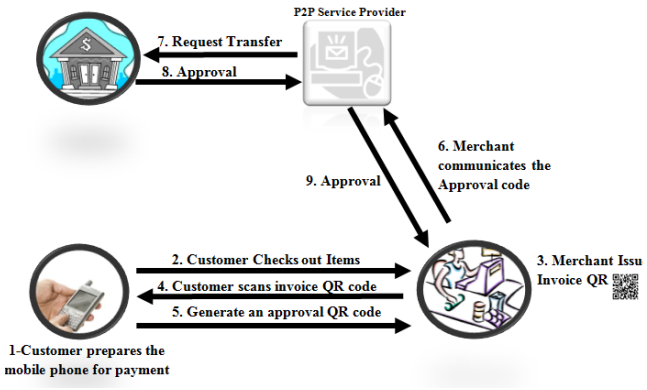

Fig. 1 The proposed solution Model

In other words, the steps are as follows. The process starts while the customer is waiting in line to check out his basket. The customer may choose to prepare the mobile phone for payment before arriving at the cashier or once arrived. To do that, he/she pulls out a card that has a private QR code. The private code contains the Mobile Identification Number (MIN) -a 10-digit number derived from your phone's number, and half of the account number to which the transaction will be associated with. This account number is for mobile payment transactions that are opened at either the MNO or a Bank.

Once the customer scans the code, the system will prompt the user to enter a maximum amount that is expected to be paid (in case of wrong expectation, the customer rescans the external card to confirm amount, this will be discussed later). The time the QR code is scanned is essential to the transaction to prevent fraud. The above mentioned scanning process assures the identity of the customer and sets a limit to the amount to be paid.

Once the cashier checks out all the items, his/her screen will display the invoice QR code. In other words, it generates an Invoice as a 2D Barcode. This code includes the following information:

- Amount to be paid.
- Transaction ID and Date.
- Merchant Public ID.

The mobile application will then scan this invoice QR code and prompt the user to enter the account number PIN while displaying the amount to be paid. It will then generate a QR code called the approval QR code.

If the merchant and customer are equipped with NFC, Near Field Communication, [12], hardware, then the customer sends the approval code to the merchant via NFC, otherwise the merchant scans the Approval QR code.

In turn the merchant communicates the approval code to the third party payment service provider, mobile network operator, or the merchant bank depending on the model used. Finally, a payment approval is received from them to the merchant to settle down the transaction. If approved, the payment service providers may send an SMS to the customer for the record.

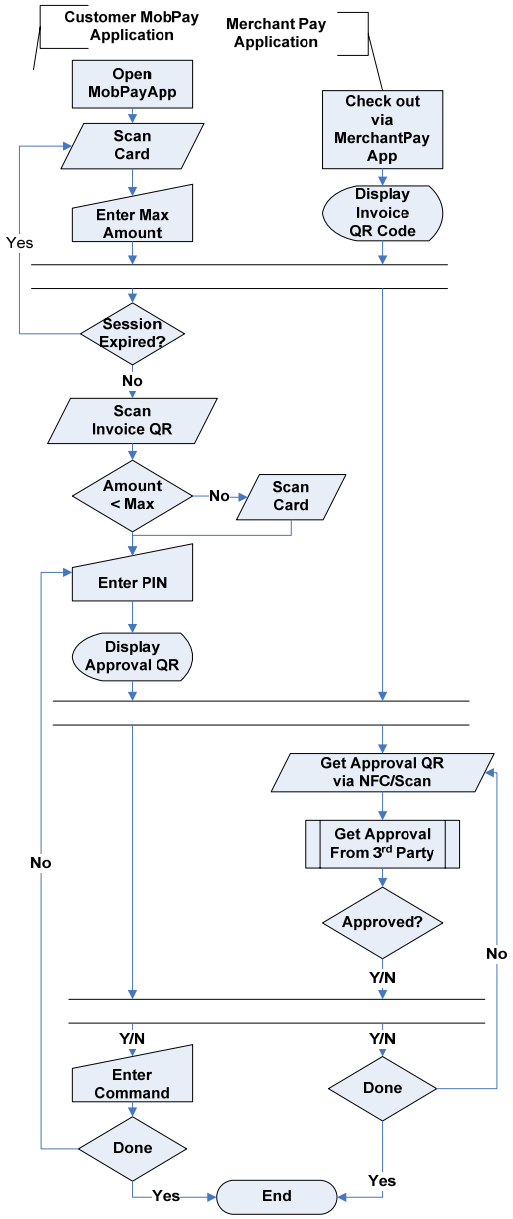

Fig. 2 Flow chart of Mobile application payment

Depending on the Payment model used, the approval code may contain:

- Customer Bank PIN code.
- Amount to be paid.
- Customer account information.
- Merchant ID.
- Transaction ID.

Since there is no handshaking step for the transaction confirmation between the third party and the customer, but between the third party and the merchant, the processing time is expected to be faster than that which requires an online approval from the customer.

A. The Application

The solution will require two modules: a mobile module running on the customer mobile phone, called as MobPay Application (or MobPayApp), and a Merchant Module (or MerchantPayApp). The flow chart of both applications is depicted in Fig. 2.

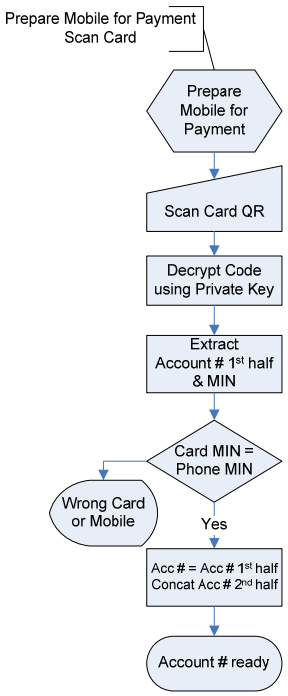

Fig. 3 Scan Card and Generate Approval Code flow chart

As discussed in the previous section, the process starts in pre-checkout phase with the customer preparing the mobile phone for payment. This process flow chart is depicted in Fig. 3. Using the MobPay Application, the customer scans a private QR code available in his/her wallet. The application will request the customer to set a maximum value to pay. Once the items are checked out, the merchant displays the Invoice QR code. The customer then via the MobPayApp scans the Invoice QR code. The application will then request a PIN code from the customer, in order to generate an Approval QR code to be transmitted to the Merchant via either the merchant scanner or NFC

In turn, the Merchant will communicate the Approval Code that includes the customer account details as well as the transaction details to the third part via the regular secured link between the Merchant and the third party. Once the transaction approval is received by the merchant, the process is declared completed.

B. Scenario Example

Assume the following example. The information associated with the customer is as follows:

- Account # 12345678,
- Mobile Phone MIN: 0787746000
- PIN number for the account: 1111

The external card QR code will then include:

- MIN: 0787746000 (encrypted using customer public key)
- Account # (1st half): 1234 (encrypted using customer public key)

In this case, the phone will store the following data (data is recommended to be encrypted using encryption password offered by the Mobile device):

- Account # (part 2): 5678,
- Private key

At the time of shopping, the user scans the external card. MobPayApp will read and decrypt the card. It then makes sure that the MIN matches occurs before composing the Full Account number by concatenating both halves, the first half from the card and the second from the phone. The system will then request the user to set a maximum limit to the value expected to pay.

After the check-out counter scans the items, the user scans the invoice QR code. The MobPayApp system displays the amount to be paid to the user, requests the user to enter the account PIN, and then forms the Approval QR Code which will be transferred to the merchant through either NCF or merchant system scanner camera.

The invoice QR code contains:

- Transaction ID.
- Amount to be paid.
- Merchant ID.

While the approval code contains:

- Customer account information.
- Customer Account PIN code (Encrypted using the Customer Account Issuer Public Key).
- Amount to be paid.
- Merchant ID.
- Transaction ID.

Finally, the merchant in turn sends the information to the MNO/Bank requesting an approval over SSL connection.

C. The Main Features

Among the features that this proposed mobile payment system has are fast processing speed and increased level of Security. These two features will be discussed in the following two sections.

1. Speed Feature

To speed up the payment process, the scenario requires only the merchant to confirm the transaction with the third party payment service provider, whether it was the MNO, a Bank, or a financial institution. Therefore, it does not require the involvement of the customer to confirm the transaction via for example the MNO. Therefore, this will result in a faster transaction because the merchant usually has a more reliable

and faster connection with the third party involved in the transaction (usually via ISP or a dedicated link). On the other hand, the customer connection speed with the third party (usually via the MNO) may differ from one customer to another, and thus the speed and reliability will vary from one customer to another. Another advantage is that there will be less number of stakeholders requesting a share of these transactions. Thus, investing in such a link between the merchant and the third party will be cost effective.

In other words, we believe that getting a confirmation from the customer on a transaction by the third party may slow down the transaction process and increase the number of stakeholders. If the merchant acts as the mediator between the Customer MNO or Bank to send the necessary customer verification information, such as a PIN number, will speed up the process. Such information will be passed from the customer to the merchant via NFC or a scanning camera, which is considered much faster than the Mobile operator network or a Wi-Fi Network.

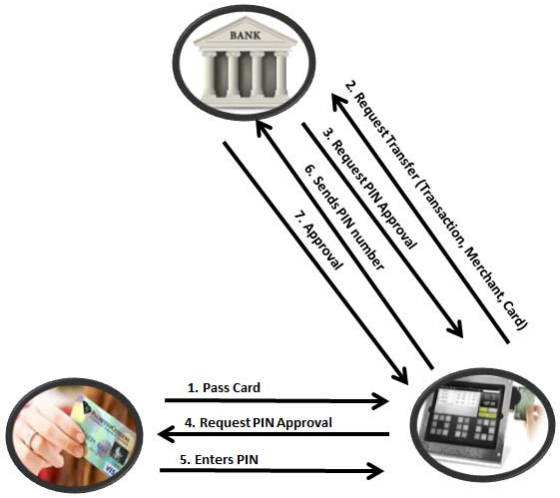

Fig. 4 Paying via VISA card scenario

2. Security Feature

The proposed system is also featured by being more secured than, say, a credit card (CC) payment. To understand this, let's look at the way the payment through VISA card is performed. Fig. 4 depicts one example of a VISA Card payment scenario. One can see that the existence of a card and a PIN number are enough to carry out a transaction verification. Besides, there are seven separate sequence steps in this scenario.

These steps start when the customer passes the CC to the cashier POS. The POS issues a request to transfer the funds and sends it to the payment service (PS). The PS requests back a verification code to confirm identity. The customer enters the code and sends it to the PS, which consequently will approve the transaction if the information received is correct.

In the proposed system on the other hand, we will need a PIN and the mobile phone, which represent a physical token similar to the VISA card. However, not all the information should exist on the phone. Thus, there will be another physical token to complete the information. This is similar to splitting the VISA card into two parts as depicted in Fig. 5. The needed information will be split between the phone and an external card read by the phone. While, of course, the PIN still exists. Once the information is complete, it will be transferred by the mobile phone to the merchant POS.

Fig. 5 Splitting the Information

In brief, the advantages of the proposal could be summarized in Table I. Under all three criteria, the proposal shows that it needs almost no extra hardware, there won't be long queues at cashiers waiting for payment confirmation, and it is more secure due to the need to a second physical token.

TABLE I
SUMMARY OF ADVANTAGES OF PROPOSED SOLUTION OVER RELATED WORK

	Insecure Against Theft	Waiting Time at Cashier	Need Extra HW
MobPay-App	Low 2FA+	Low Confirmation via Merchant	Low Built-in Camera

V. CONCLUSION

Mobile payments are becoming a feature that more and more people are using. This has resulted in more sensitive financial data are being stored on these mobile devices. This paper proposed a scenario for mobile payments that focuses on two of mobile payment concerns. These concerns are the processing speed and security. The steps of this proposal could suit any of the four known mobile payments models. The processing speed, due to the absence of a handshaking confirmation between the customer and the payment service, is said to be faster than many current mobile payment systems. Yet, such a confirmation still exists but through the Merchant application. The security steps considered in this work are based on a new terminology that is defined in this paper, namely 2AF+. It is shown to introduce a less threat than when paying via a credit card. Thus, among the features of the proposal are:

- It increases the security for mobile payment transactions.
- It is faster than other mobile payment systems.
- It is simple.
- It adds no extra cost on either merchant or customer as far as hardware is concerned.
- It improves mobile user experience by reducing user inputs and waiting time.

ACKNOWLEDGMENT

The author would like to acknowledge the financial support received from Applied Science University that helped in

accomplishing the work of this article.

REFERENCES

[1] Reinhardt A. Bothaa, Steven M. Furnellb, Nathan L. Clarkeb "From desktop to mobile: Examining the security experience" Computers & Security Volume 28, Issues 3–4, May–June 2009, Pages 130–137
[2] Stuart J. Barnes, Brian Corbitt "Mobile banking: concept and potential" International Journal of Mobile Communications Volume 1, Number 3/2003, pp 273-288
[3] Bailly, Laurent, and Bernard Van der Lande. "Breakthroughs in the european MoBilepayMent Market." White paper, Atos Oringin (2007).
[4] Widmann, Rainer, et al. "System Integration of NFC Ticketing into an Existing Public Transport Infrastructure." Near Field Communication (NFC), 2012 4th International Workshop on. IEEE, 2012.
[5] Retail Customer Experience, "http://www.retailcustomerexperience. com/video/3402/ncr-at-nrf-presenting-the-mobile-shopper" , NCR at NRF, visited on = 2013-08-7
[6] Jones, David. "Thai e-purse ready to roll out", Card Technology Today Volume 17, Issue 6, June 2005, Pages 16
[7] Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. "Multi-Factor Authentication." U.S. Patent No. 20,130,055,368. 28 Feb. 2013.
[8] Info Security Island, "http://www.infosecisland.com "Google Offers Two-Factor Authentication Option" Article on Thursday, February 10, 2011 visited on = 2013-08-7.
[9] Technomobs, "http://technomobs.blogspot.com/" Mobile and Wireless - Emerging Business Models, visited on = 2013-08-7.
[10] Vibha Kaw Raina and Pandey MunishMakkad "Barcode Payment System in Trusted Mobile Devices" in International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012 (ISSN: 2278-7720).
[11] A. Sankara Narayanan, "QR Codes and Security Solutions" in International Journal of Computer Science and Telecommunications, Volume 3, Issue 7, July 2012.
[12] Standard ISO/IEC number 18092, "Information Technology - Telecommunications and Information Exchange between Systems -- Near Field Communication - Interface and Protocol (NFCIP-1)", 2013, 44 pages.