A Secure Mobile Payment System using QR Code

Sana Nseir
Faculty of Science and IT
Zarqa University,
Zarqa – Jordan
sananseir@gmail.com

Nael Hirzallah
Faculty of Science and IT
Applied Science University
Amman, Jordan
Hirzallah@asu.edu.jo

Musbah Aqel
Faculty of Science and IT
Zarqa University,
Zarqa – Jordan
musbahaqel@yahoo.com

***Abstract*—Mobile phones have become an inseparable companion for many users, serving much more than just communication tools. In developing countries, the number of mobile phone users exceeds the number of those having bank accounts. Besides, the low banking service penetration and the large migrant communities are another factor to utilize mobile phones for payment purposes. Therefore, mobile payment may find the success it is targeting easily and much faster than in developed countries. There are a lot of variables involved related to Mobile Payments. In this paper, the various models used for Mobile payments are first discussed. Then, the paper will propose a scenario for mobile payment that tackles both concerns of the process, namely: speed of transaction and security, without complicating the process or making it undesirable to users.**

Keywords—Security; Mobile phones; Smart phone; QR Code, Payments.

I. INTRODUCTION

The usage of Mobile phones, mainly smart phones, has been dramatically increased in recent years. Moreover, Mobile phones are becoming very small in sizes that are used as general purpose computers. They have become an inseparable companion for many users, serving much more than just communication tools. Users are storing more and more sensitive data on these mobile devices, and they are already paying for some of the mobile content such as games and other applications. This indicates that users are willing to utilize mobile phones for payment purposes.

Thus, 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. This paper presents the various Mobile Payment methods or model in the following section, before proposing one that considers such theft threat in section 3. Finally, the paper concludes in Section 4.

II. VARIOUSE MOBILE PAYMNET MODELS AND DEPLOYMENTS

Mobile payment is defined as a payment for products or services between two parties, consumers and merchants, for which a mobile phones are involved in direct purchase of goods and services as plays as the medium of accomplishing the transaction. It can be categorized based on the technology used as either one of two types—proximity or remote.

Proximity payment generally refers to contactless payments where Near Field Communication (NFC) technology is involved. Examples of this type are: Installations of this type are: ExpressPay™ from American Express, Discover® Network ZipSM, MasterCard® PayPass™, and Visa® payWave™ and Speedpass™. In July 2011 PayPal™ introduced a new payment model using NFC. It is a variant on the eWallet® model in which PayPal acts as a transparent intermediary for payment person-to-person (P2P) allowing Android™ users to pay one another by tapping two NFC-enabled devices together.

Remote payment is a payment via a mobile web browser or a smartphone application, in which the mobile phone is used as a device to authenticate personal information stored remotely. It uses services such as Short Message Service (SMS) to initiate or authorize payment. For low-value transactions (micropayments) billing may be via the user's phone bill based on the mobile subscriber identification number (MSIDN). While Higher-value transactions payments are made via credit card, or eWallet, or also phone bill. However, user card and bank account information should be stored on the user's mobile device. Therefore, PIN-based authentication should be used to verify the transaction through say interactive voice response (IVR), WAP, SMS or USSD (Unstructured Supplementary Service Data) channels.

On the other hand, Mobile Payments methods usually belong to one of three models based on the entities that are involved in the process. The four potential mobile payments business model scenarios are as follows:

A. Operator centric model

Many examples of Operator Centric Models are already available and operational. In this case, the mobile operator provides the technology, process the transactions and compensates the system. In this model, it is necessary to connect the mobile-payment system and banking accounts or cash deposits. The applications may support a prepaid stored value model or the charges may be integrated into the customer's mobile bill. The mobile operator usually provides the merchant with a wireless POS system. Another method is to have the operator enables the proximity payment application on the merchant's NFC mobile device.

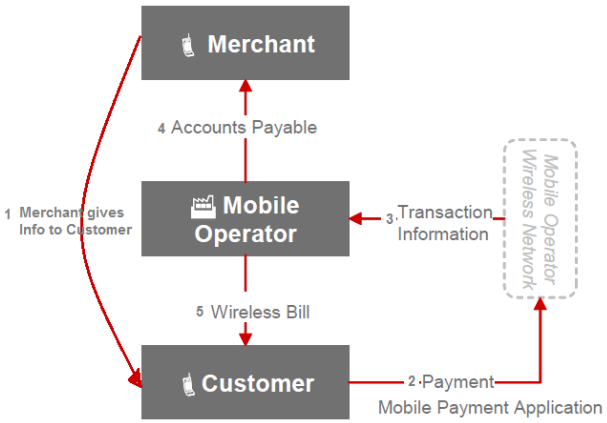

Figure 1 Operator Centric Model

One of the scenarios of this model, as depicted in Figure 1, is when a customer wants to pay for his purchase at a department store. Through NFC, the customer gets the merchant info as well as the amount to be paid. The customer then sends a payment request to his Mobile Operator through the MON using Mobile Payment Application. The MO confirms the payment to the merchant after which the merchant settles the purchase. In step 5, the MO bills the customer.

B. The Bank Centric Model

In this model a bank is involved in the process. The customer gives the needed info (using NFC) in order to make the payment for the merchant. The merchant bank will contact the customer bank to get the payment transaction done. Note that the customer bank might need the customer approval for the payment. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods.

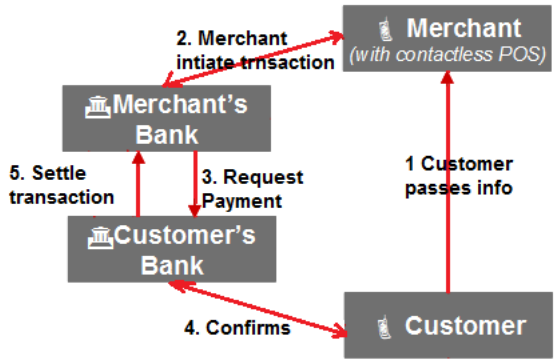

Figure 2 Bank Centric Model

This model, as shown in Figure 2, is not as frequent as the operator model. This is because operators hold the technology. Banks face generally a very different environment. They have many competitors and do not hold the technology. They must compete or more successfully cooperate with other financial partners and collaborate with mobile operators without any substantial bargaining advantage. The Bank Centric Model can be considered as an evolution of the credit card model. The users receiving the payments are not generally clients of the same bank than the payer. A general compensation system must then operate between banks with or without connections with the classic inter-bank flows. The partner's banks of this compensation system must also pay fees to one or many mobile operators associated to the operation.

C. Peer-to-Peer Model

In this model, an independent peer-to-peer service provider provides secure mobile payments between customers or between customers and merchants, where both merchant and customer should have accounts with the service provider. Via the established accounts, the service provider will be able to charge the needed payment to the customer and transfer it to the merchant. The service provider could be either a financial instate, such as a credit card issuer, or just a trusted mediator among banks that hold the real customers and merchant accounts.

It is the job of the independent peer-to-peer service provider to provide secure mobile payments between customers or between customers and merchants. The Peer-to-Peer Model is an innovation created by payments industry newcomers who are trying to find ways to process payments without using existing wire transfer and bank card processing networks.

The ability to send money from one person to another, even across great distances, has existed for many years through providers such as Western Union. While the Internet has made this service even more convenient, the high fees associated with the transfers can make them cost prohibitive and not for everyday use. Internet bill payment services provided by most banks have made remote payments to merchants convenient, but cannot be used for real-time purchases. Mobile phones with peer-to-peer capabilities overcome these obstacles. One of the scenarios that can exist in this model is when the service provider uses an existing online application (e.g., PayPal Mobile). Otherwise, POS for NFC or contactless service equipment will be required.

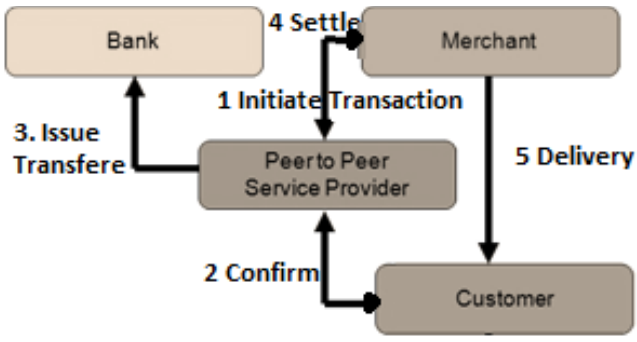

Figure 3 Peer-to-Peer Model

Figure 3 depict one scenario to peer-to-peer model. Once the transaction started, the merchant communicates to the service provider the information needed, such as the transaction ID and amount, as well as the customer ID. The

Service provider requests confirmation from the customer if the customer's information was sent within the merchant message; otherwise, the service provider waits for a request-to-pay message from the customer that carries the same transaction ID and amount. Once the service provider verifies the information to pay, the Banks of both the customer and merchants will be contacted to perform the transfer. At the same time, a message will be sent to the merchant to confirm the completeness of the transaction who will in turn deliver the products.

D. The Collaboration Model

The Collaboration Model involves collaboration among banks, mobile operators and other stakeholders in the mobile payments value chain, including a potential new stakeholder, a trusted third Party to manage the deployment of mobile applications. This model includes two possible scenarios:

Scenario 1: A mobile operator partners with one bank to offer a bank-specific mobile payments service.

Scenario 2: Industry associations representing mobile operators and financial institutions negotiate and set standards for applications that reside on secure elements in mobile devices, allowing multiple card types from different banks to be used.

In both scenarios, NFC-enabled mobile devices and compatible POS devices are deployed that meet the standards set by the Partner bank or industry associations. The amount paid and collected by each stakeholder is the source of considerable contention. Generally it is expected that merchant fees are split between banks, mobile operators, and perhaps third party trusted service managers (TSMs). Comparable models exist in the credit card industry for customer acquisition and marketing fees between partners.

III. VARIOUSE MOBILE PAYMNET DEPLOYMENTS

Worldwide there have been a number of deployments of mobile payments across the spectrum of proximity and remote payment and for both bank-centric and nonbank-centric transaction models. For instance, Safaricom and Vodafone (Africa) have launched M-PESA (an SMS-based payment service targeting the unbanked, prepaid mobile subscribers in Kenya), Google Checkout™ (Google partnership with Sprint®, Citi®, MasterCard, and FirstData® in US), Paybox by Mobilkom (an SMS-based system that also has an NFC system for mobile ticketing for mobile transport in Austria), NTT DoCoMo, Inc. (Osaifu-Keitai® mobile wallet service in Japan), Obopay™, Inc. (A P2P mobile payment company enabling mobile phone users to send and receive money through their phones via a mobile web browser or SMS in US), PayPal Mobile™ (Provides mobile PIN-based web and SMS capabilities for PayPal account payments in US), Western Union® (Mobile application provides P2P money transfers from the sender's bank account to the recipient's Western Union cash card), and e-Transfer by Interac, Inc. (Provides the ability to send and receive money directly from one bank account to another using online or "mobile banking" through a participating financial institution without sharing any personal or financial information, in Canada).

IV. THE PROPOSAL

As discussed in the previous section, there are four different models for mobile payments. Each model may offer one or more scenarios for implementation. In almost all these scenarios, the issue of security and transaction speed is of a main concern.

Rather than proposing a new model, this paper will propose a scenario that will address both concerns. This scenario will belong to no specific model, but could be slightly modified to suit whichever model of the four discussed above.

For the issue of speed of settling a transaction, the transaction initiator must be the merchant. This is because the merchant usually have a more reliable and continuous connection with the third party involved in the transaction, who could be either the bank, service provider, or the mobile operator. We avoid relying on the customer to initiate the transaction for two folds. One is the connection between the third party and the customer may differ from one customer to another. Two is because that the Merchant needs continuously to do transactions. Thus, investing in such a link between the merchant and the third party is cost effective.

For the same reason, we believe that getting a confirmation from the customer on a transaction by the third party may be slow down the transaction completion. Thus, if the information needed from the customer is sent via the merchant, this will speed up the process. Such information could be passed from the customer to the merchant via NFC, which is considered much faster than the Mobile operator network or ISP Wi-Fi Network. However, the issue of security becomes of a concern to the customer should the mobile phone be stolen. Besides, we cannot rely on the merchant to verify the customer ID.

This paper proposes yet another way to eliminate fraud transactions caused by device theft. Recalling the traditional payments via Credit Card, at least two tokens are expected from the customers to prove an authenticated transaction. These two could be the existence of the card itself, and the signature or the PIN number which is getting more popular in POS's than signatures.

Both tokens exist in different places with the customer. The credit card is placed in the customer's wallet, while the signature or the PIN number usually exists in the customer's brain. Following the same concept, this paper requires two tokens to verify identity. One is the mobile phone which is placed in the customer's pocket (away from the wallet), while the other token is proposed to be a QR code, which will exist in the customer wallet, or simply a PIN number.

Having both basis implemented, we could describe the following scenario. While the customer waits in line for the cashier or is about to perform a transaction, the customer scans a QR code placed in his wallet and specifies a ceiling limit to the amount to be paid at the cashier. The time the QR code is scanned is also essential to the transaction to prevent fraud. The purpose of this action is to acknowledge the identity of the mobile phone holder. Once the merchant is ready to initiate the transaction, the Merchant displays a QR code that includes information on the transaction. Upon scanning this QR code, a one way private key gets generated once mixed with the owner

QR code and transferred to the Merchant through NFC. This information gets in turn transferred to the third party, which should be enough to carry on the transaction without further confirmation. Depending on the model used, the mobile operator will bill the customer, the customer's bank will transfer the amount of money, or the service provider will carry on the money transfer from the customer's to the merchant's banks.

A further security step could be added when scanning the customer QR code. This step is to enter a PIN number. However, we believe that this is not necessary especially that mobile phones are usually locked. The above mentioned scanning process assures the identity of the customer and sets a limit to the amount to be paid. Furthermore, since there is no handshaking for transaction confirmation between the third party and the customer, the processing time is expected to be faster than a credit card payment process.

CONCLUSION

This paper has proposed a scenario for mobile payments that focus on two of the main mobile payment concerns. These concerns are processing speed and security. The steps that this paper is proposing could suit any of the four mobile payments models. The processing speed, due to the lack of handshaking payment confirmations, is expected to be faster than a credit card payment process. Yet, the security steps considered in this proposal is no less secure than when paying via a credit card.

In future, we will be working on private and public key security to generate encrypted code that could be used to authenticate customers, as well as planning to implement a prototype of this proposed scenario.

REFERENCES

[1] Clarke, N., and Furnell, S.: Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security, 24(7):519–527, 2005.

[2] Bluetooth Security by Stephen Walsh, Jun Wan, and Arran Sadlier http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group15/index.html. Retrieved 2012-11-30

[3] - https://www.bluetooth.org/foundry/sitecontent/document/security_ whitepaper_v1. Retrieved 2012-11-30

[4] - http://news.zdnet.co.uk/0,39020330,39145886,00.htm. Retrieved 2012-11-30

[5] - http://www.thebunker.net/security/bluetooth.htm. Retrieved 2012-11-30

[6] - http://www.bluejackq.com/what-is-bluejacking.shtml. Retrieved 2012-11-30

[7] - http://securityresponse.symantec.com/avcenter/venc/data/ epoc.cabir.html. Retrieved 2012-11-30

[8] http://en.wikipedia.org/wiki/Mobile_operating_system . Retrieved 2012-11-30

[9] www.gartner.com/it/page.jsp?id=1466313 Retrieved 2011-02-21.

[10] ICS is coming to AOSP – Android Building. Groups.google.com (2011-11-14). Retrieved on 2012-07-03.

[11] http://www.canalys.com/newsroom/64-million-smart-phones-shipped-worldwide-2006 Retrieved 2012-01-13.

[12] "Gartner Smart Phone Marketshare 2011 Q3". Gartner, Inc. Retrieved 2012-05-26.

[13] "Nokia has sold over 1.5 billion Series 40 phones". http://press.nokia.com Retrieved 2012-01-25.

[14] Tognazzini, B.: Design for Usability. Cranor, L.F., Garfinkel, S. (eds.): Security and Usability. Designing Secure Systems That People Can Use. O'Reilly (2005)

[15] Botha, R., Furnell, S., and Clarke, N.: From desktop to mobile: Examining the security experience. Computers & Security, 28(3-4):130–137, 2009.

[16] IDC: IDC press release from 28 Jan 2010 at www.idc.com/getdoc.jsp?containerId=prUS22186410 . Retrieved 2012-11-30

[17] Jain, A.K., Flynn, P., Ross, A.A. (eds.): Handbook of Biometrics. Springer (2008)

[18] Clarke, N., Furnell, S., Rodwell, P., and Reynolds P.: Acceptance of subscriber authentication methods for mobile telephony devices. Computers & Security, 21(3):220–228, 2002.

[19] Noam Ben-AsherOn et al, "the need for different security methods on mobile phones", MobileHCI '11 Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services