popular TomTom GO 910 GPS device was found to have a virus late in 2006, which, although low risk, had the potential to spread onto a corporate network upon being connected to an attached PC via a USB port. Such attachment might be effected periodically to back up the device's content, and in some cases to download software upgrades. Yet many enterprises are unaware that such devices are potential sources of peril. Indeed the lesson is that plug-and-play devices constitute a new category of attack vector that needs to be considered.

## Categorisation

An important step in determining mobile security policy therefore is to categorise the various devices that could access the network, then define what privileges they will have. At this stage, existing policies, relating users to the servers they can access depending on where they are, can be applied. Just as users may be allowed greater access rights when at their desks than when in a hotel room, so they may have fewer privileges when on a mobile device. Similarly, rights can be assigned to devices such as the mobile GPS, defining what they can do when attached to the system. Some of the answers may lie in the technical realm, for example in making it possible to define clear pathways for specific plug-and-play devices. Similarly it will be down to vendors of authentication and encryption to work with silicon providers to develop robust hardware-based security. But technology will not deliver security without considering the user. Security should after all be as transparent as possible, and this should be considered in defining how devices should comply with the policy. For example it is not necessary to require passwords just to access basic telephony functions. Having to enter a password just to take an incoming call would be an unacceptable and unnecessary imposition. Yet if the same device can access customer data subject to privacy laws, then clearly strong authentication is then required, with additional security checks on top of basic passwords or PINs.

## Get ahead

There is no doubt that mobility brings an extra dimension of complexity to IT security. Unfortunately this does require a major revision of security policies. But nothing fundamentally changes, and at a deeper technical level no new threats are introduced. Existing methods can still be used, enabling vendors such as Symantec to offer protection against threats that have yet to manifest themselves. There is an opportunity unique in IT security history to be one step ahead of the game.

# Analysis of mobile payment security measures and different standards

**Saleem Kadhiwal and Muhammad Anwar Usman Shaheed Zulfiquar, Ali Bhutto Institute of Science and Technology, Karachi, Pakistan**

**If mobile technology fulfils its possibilities, then users could be making payments with their mobile phones. Researchers in Pakistan look at the technologies and security concepts.**

As mobile technologies are becoming more advanced and mobile devices are making a big impact on daily life, a new type of payment system named mobile payment (m-payment) has emerged, enabling users to pay from their wireless devices especially mobile phones wherever they go. Mobile payment is predicted to have a bright future. Mobile Network Operators (MNOs), banks and other institutions such as financial service providers, payment service providers etc. are playing a big role in the development of mobile payment systems. In this paper we discuss the characteristics of mobile payment systems and the issues regarding security and standards, which need to be addressed in order to make a secure m-payment. We will also give an overview of technologies, devices, protocols and their security concepts.

## Introduction

The term e-commerce is shorthand English for electronic commerce. It is a realisation of doing business using Internet technology but generally E-commerce does not say anything about the kind of device that the end user employs to gain access to the Internet[1]. With the growing prevalence of electronic commerce and the widespread use of mobile devices, a new type of channel has emerged, called mobile commerce. Furthermore, since Mobile Network Operators (MNOs) are heavily in debt due to massive investments in 3G licenses, designing an application so as to generate substantial revenues rapidly is becoming a priority and it has already been predicted that mobile payment (m-payment) will become a successful mobile service[2]. *M-payment can be defined as any payment transaction which involves a mobile device*[3]. Although there are numerous types of Internet-based payment systems, we are still facing many problems in mobile payment systems. In recent years many papers were published discussing business models for m-payment but very few including protocols, design issues and security of the mobile payment system[4].

## Mobile payment

M-payment is already in use in many parts of the world, including Europe and Asia. There are several Payment Service Providers (PSP), but Telco and financial institutions are playing prominent roles in offering the m-payment

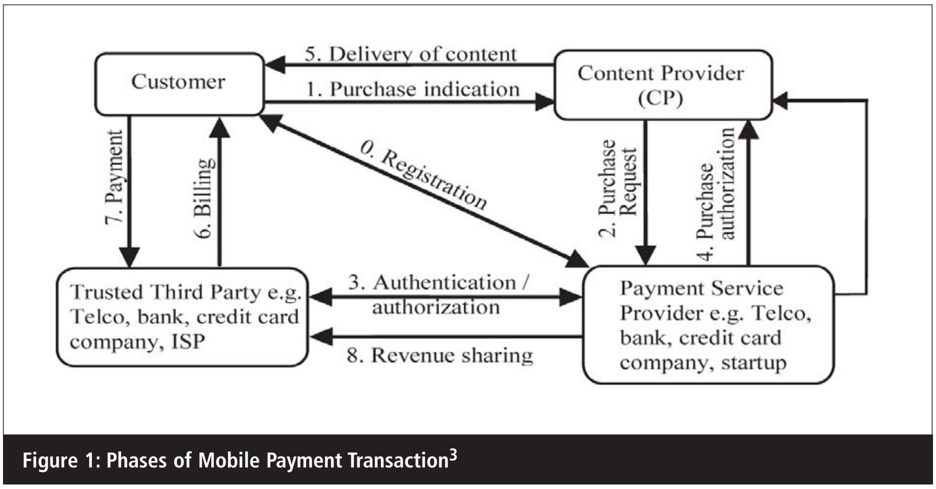
Customer
5. Delivery of content
1. Purchase indication
Content Provider (CP)
0. Registration
7. Payment
6. Billing
2. Purchase Request
4. Purchase authorization
Trusted Third Party e.g. Telco, bank, credit card company, ISP
3. Authentication / authorization
8. Revenue sharing
Payment Service Provider e.g. Telco, bank, credit card company, startup

Figure 1: Phases of Mobile Payment Transaction[3]

services[3]. Little (2004) estimated in his global study that m-payment transaction revenues would increase from US$3.2 billion in 2003, to US$11.7 billion in 2005, and to US$37.1 billion in 2008 worldwide[5].

Payment amount has an influence on the design of electronic payment protocols. For example, payments in the order of €1 are only viable if the incurred computational and communication overheads are kept small[1]. Accordingly, there is a distinction between:

- Micropayments (up to about €2).
- Small payments (up to about €20).
- Macropayments (more than about €20)[5].

According to recent studies SMS has been the common payment mechanism and obtains the highest revenue potential between m-payment applications. Thus far, more sophisticated technologies like IVR, WAP, Java and RFID will play a more important role in offering more convenience to the customers[3]. M-payment systems can be used in multiple conditions and scenarios. The simplest scenario involves the user, the device and a single payment process like mobile operators, banks etc. The complex scenario involves at least one additional third party, the merchant[5].

### Types of M-payment:

The existing m-payment systems can be classified as:

**Account-based payment systems**

- Mobile phone based payment systems.
- Smart card payment systems.
- Credit-card payment systems.

**POS payment systems**

- Automated POS payments.
- Attended POS payments.

**Mobile wallets[4]**

## Mobile payment delivery value chain

Different players are performing non-traditional roles in the m-payment delivery chain, which determines their abilities in offering m-payment services. A well-defined delivery chain can be categorised as:

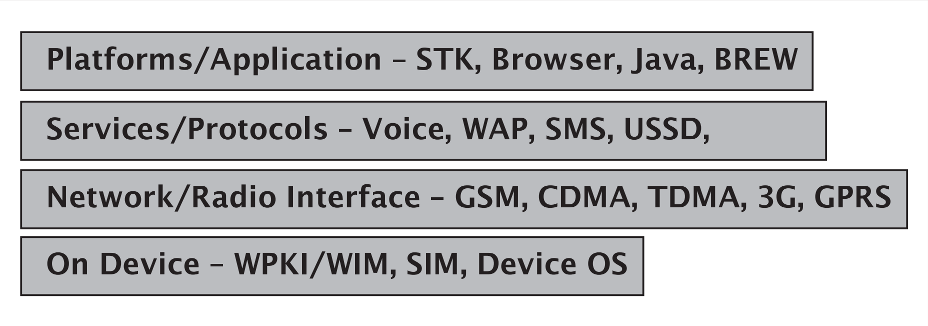
Platforms/Application – STK, Browser, Java, BREW
Services/Protocols – Voice, WAP, SMS, USSD,
Network/Radio Interface – GSM, CDMA, TDMA, 3G, GPRS
On Device – WPKI/WIM, SIM, Device OS

Figure 2: The required security levels for m-payment

- Financial service providers (FSP).
- Payment service providers (PSP).
- Merchants (m-service providers).
- End-users.
- Network service provider (NSP).
- Device manufacturers[6].

## Enabling technologies

Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing. The key technologies are:

- WAP, including WAP Identity module (WIM) for additional security.
- Bluetooth.
- Network, including GSM, GPRS, 3G.
- Mobile payment software.
- Smart card and SIMs[7].

These technologies are needed to address various payment industry needs, which include:

- Secure authentication infrastructure on mobile devices.
- Secure transmission infrastructure for wireless payment.
- Trust/validation directories – i.e. buyer and seller authentication information validated along with payment transactions by validation services and directories that trust each other.
- Virtual "wallets" stored on a mobile device or accessible over a network that users fill with information on their financial accounts and their payment preferences[7].

## Mobile payment transaction

There are many phases involved in an m-payment transaction. The transport of payment details will involve a mobile network operator and use either a browser-based protocol such as WAP or HTML, or a messaging system, such as SMS or Unstructured Supplementary Service Data (USSD). Alternatively the transport of payment details could be via Bluetooth, infrared, RFID or contactless chip in the case of proximity payments. Trusted Third Party (TTP) and Payment Service Providers (PSP) also play a key role in an m-payment transaction[3].

## M-Payment issues

There are various issues in the area of m-payment that are classified under two headings: security and standardization.

## Security

Security is the biggest issue in the field of m-commerce because without secure commercial information exchange and safe electronic financial transactions over mobile networks, no one will trust m-commerce. Therefore, various mobile security procedures and payment methods have been proposed and applied to mobile commerce. The following diagram shows the levels of security required for m-payment.

## Security properties

A secure mobile payment system must have the following properties:

### Confidentiality

The confidential information must be secured from an unauthorized person, process or device.

### Authentication

Ensures parties with access to a transaction are not impostors and are trusted.

### Integrity

The information and systems have not been altered or corrupted by outside parties.

### Authorization

Verify that the user is allowed to make the requested transaction.

### Availability

The system must be accessible for authorized users at any time.

### Non-repudiation

Ensures that the user must not deny that he/she has performed a transaction and must provide proof if such a situation occurs[8].

## Security challenges

M-commerce without a secure environment is not acceptable, especially for those transactions involving monetary value. Therefore there are different security challenges of m-commerce related to:

### Security of mobile devices

As the mobile devices contain confidential user date and are more prone to theft and destruction they need to be protected accordingly. Security from unauthorized use can be achieved by user authentication mechanisms (e.g. Personal Identification Number (PIN), Personal Unblocking Key (PUK) or passwords) and secure storage of data and security of the operating system[1]. Additional smartcards employed in mobile phones (dual chip and dual slot) considered as WIM (Wireless Identification Module) for storing information that require extra protection, including the terminal information needed during communication, the electronic authentication certificates etc. are considered to be more secure then single SIM, therefore the concept of smart phones is growing rapidly. The security level provided by devices needs to be continuously upgraded and device-manufacturing companies are playing a major role in this area[3].

### Security of network technologies

The user confidential information must be protected from eavesdropping in a radio environment in order to promote m-commerce.

GSM provides a basic security mechanism for m-commerce transactions by customer authentication and encrypted links with a secure symmetric key, which is never sent over the network. But there are weaknesses: there is no network authentication mechanism included in the mobile station; and a false base station can perform a 'man-in-the-middle' attack. UMTS on the other hand is carefully designed to fix the security problems of GSM by mutual authentication and the encryption, which is optional in GSM is made mandatory[1].

### WLAN

WLAN operating in the unlicensed 2.4 GHz and 5 GHz band does not provide any security allowing mobile attackers to eavesdrop and manipulate all the wireless traffic with standard tools.

### WEP

In order to provide a certain level of security, the IEEE defined WEP (Wired Equivalent Policy) is available, but unfortunately, some compromises that were made in developing WEP have resulted in it being much less secured than intended. VPN technology is another approach employing IPSec in order to establish network layer security but the link layer specific information (like MAC addresses) are still unprotected. Also, a VPN solution on its own does not address the requirement for QoS and seamless roaming between subnets[1,9].

### Bluetooth

Bluetooth also operates in the unlicensed 2.4 GHz band. The security mechanisms provided by bluetooth are still not significant. The security problems with Bluetooth are: the E0 encryption scheme employed by Bluetooth could be cracked under certain circumstances. The Bluetooth Device Address, an address unique to every Bluetooth device introduces yet another problem allowing the tracing of personal devices. So, Bluetooth in its current form is unsuitable for the transfer of sensitive data[10].

Despite the above discussed, there are other technologies e.g. Infrared is also available but a lot more work is required to provide a secure radio interface for m-commerce.

### Service security

The service level security is also important for secure m-commerce applications, especially those involving monetary transactions.

SMS (Short Message Service) is a most popular data service offered by MNOs and most widely used for m-payment. By using SMS to initiate or authorize payments the SMS can be then used as the unit of currency itself. The device can exchange data via a SMSC by sending and receiving standard SMS messages identified by IMSI (International Mobile Subscriber Identity), which an attacker cannot forge without breaking the GSM/UMTS security. However, the protection ends in the radio interface. There is no end-to-end security, the network operator and its infrastructure must be trusted for transactions[1, 6].

### USSD

USSD (Unstructured Supplementary Service Data) unlike the asynchronous SMS service opens a session, which may induce other network operators or an USSD response before releasing the connection. But unfortunately USSD also possesses no security properties and relies on the GSM/UMTS security mechanism[1].

### SAT

SIM Application Toolkit (SAT) is a technology that allows configuration and programming of the SIM card. The SIM card contains simple application logic that is able to exchange data with the SMSC, to carry out m-payment transactions. The specific mobile operator provides the application logic and is responsible for providing the SIM card. However, the security depends on the application whether the security mechanisms are implemented or not[6].

### Voice-based payment transaction

Voice-based payment transaction can be done by calling a special number and providing the credit card number. Voice recognition techniques can be used but they also contain security loopholes[6].

### I-mode

I-mode is another technology where the content can be placed on the content server without the domain of the gateway because the user has i-mode subscription; the telephone number is identified by the caller ID and linked directly to the bank account[11].

### Transport Layer Security Mechanisms

Along with the service there are also transport layer security mechanisms like SSL/TLS (Internet Secure Socket Layer) protocols. KSSL (Kilobyte SSL) implemented by SUN does not offer client side authentication. WTLS (Wireless Transport Layer Protocol) is standardized by WAP forum as part of the WAP 1 stack. WTLS provides transport security between a WAP device and WAP gateway, which perform the protocol transformation to SSL/TLS. Hence, no real end-to-end security is provided and the WAP gateway needs to be trusted[1].

## Standardization

There is widespread heterogeneity of technologies for mobile devices and as there are many MNOs working in the area of m-commerce in order to generate revenues against heavy investments they have made. Therefore there exists lots of standards and approaches for m-payment, which are running independently. Therefore, issues arise in the adoption of the standard as these independent systems do not address integration with other systems developed by any other vender. Therefore, a standard interface is necessary because ease of use and commonality of experience is key to driving adoption of new technology. The m-payment is still being held back due to lack of common standards and disparity of systems that do not necessarily work together. It is essential to find common approaches, both at national and international level. In recent years we have witnessed the rise and fall of several mobile payment efforts. The World Wide Web features a great number of companies that have introduced or planned to introduce m-payment services or working of m-payment standards[3].

Some of them are:

- NTT DoCoMo.
- PayCircle.
- MoSign.
- Mobile Payment Forum.
- Mwif.
- Radicchio.
- Encorus.
- SmartPAY.
- EMPS (Electronic Mobile Payment Service).
- Fastpay.
- M-pay.
- Mobipay
- Paypal.
- PayBox.
- SecurePay.
- SEMOPS (Secure Mobile Payment System).
- SmartMoney.
- Sonera.
- TELEPAY.
- ZOOP.
- ExpressPay and many many more.

The new payment standard only has a chance to be accepted on the market if it makes good economic sense for the key players to promote the service. All the features offered to the end users - the security, the comfort, the wide reach may be in vain if there are no economic incentives for the service providers. However it is obvious that the service providers alone cannot make a success story of the service if the users are dissatisfied with either the service or the terms of the usage. The flexibility of the model and its capability of integrating new payment processors quickly is critical for its survival. The customers of any new financial provider that connects to the infrastructure can immediately transact with all other customers of the other providers in a transparent way. That will lead to a rapid expansion of the service that can establish it as a global payment service[5].

## M-Payment Systems

Mobile payment is considered by many experts as the next 'big thing' that will empower existing e- and m-commerce efforts and unleash the true potential of mobile business. Different approaches have come to the market and tried to address existing needs, but up to now no global solution exists. Existing electronic payment solutions are not secure enough, too difficult and slow to use, or available only for a limited variety of goods or a small selected clientele. Some of the systems are described below:

### PayPal

PayPal is a popular online payment service that was recently acquired by eBay. Via WAP-enabled phones the customer can use PayPal's wireless interface to accommodate MP. With PayPal Mobile, users can send money, purchase items or donate to charities from their mobile devices. PayPal Mobile users make payments by sending a text message to PayPal. PayPal calls the user back to confirm the mobile payment, and then sends the money to the recipient. In the case of a Text to Buy purchase, after the merchant receives the payment, the item is shipped to the address already saved in the user's PayPal account[12].

### PayCircle

PayCircle is a vendor-independent, computer-company dominated (Hewlett Packard, Lucent, Oracle, Siemens, and Sun Microsystems) organization that was founded in January 2002. Its main focus is to accelerate the use of payment technology and to develop or adopt open payment APIs based on XML, SOAP, and Java. In 2003, Paycircle released the ParlayX Web Service Specification that has integrated the Paycircle API, as well as a reference implementation and sample software. Paycircle focuses on a mobile payment infrastructure based on mobile Web services. In order to also tackle more effectively authentication and identity management, Paycircle teamed up in Jan 2004 with the Liberty Alliance Project[13].

### MobiPay

MobiPay is an easy system that activates existing payment means (normal or virtual credit, debit or pre-paid cards) and that allows to carry out a variety of transactions transforming your mobile phone into your day-to-day payment means[14].

### SEMOPS

SEMOPS (Secure Mobile Payment System) is a complex, universal, user friendly payment system. The possible transactions include POS payments, in band purchases – Internet and WAP, P2P transfers, purchases made at vending machines and also bill payments. The payments are not limited by values either, as both micro and macro transactions can be performed. The service facilitates not only retail but also B2B transactions. For the customers and merchants, the payment service is provided by their own banks or mobile operators. As no intermediaries are involved in this relationship the whole payment transaction is based on trust between known partners. In SEMOPS customers do not provide any sensitive data to the merchant during the payment process therefore they can practically remain anonymous during the payment process. Having received the necessary transaction details, the customer prepares and signs a payment request and forwards it to its own payment processor. If the necessary funds are available the merchant receives a payment notification, a kind of guarantee from its own payment processor[15].

Beside these systems there are many m-payment systems currently providing services to customers in many parts of the world, especially in the US, Canada, European countries and Asia Pacific region.

## Future trends

As mobile communication continues to evolve and new technologies emerge, m-payment vendors will be compelled to evolve their solutions continually to support increasingly sophisticated client applications for mobile handsets. The need for secure, reliable payment methods to be made available to customers cannot be understated and therefore, it is crucial to define standards so as to guarantee real mobility, enabling seamless m-payment. In addition, there are necessary amendments to be made in other areas such as banking laws and retail traditions. Partnerships among mobile operators, financial institutions and other businesses continue to emerge to provide dynamic, secure mobile payment solutions[3].

## Conclusions

M-payments have a glorious future because m-payments can be used for all types of payments - anywhere and any time. However, there are still security issues like authentication and authorization for mobile payment transactions and fraud management which have to be resolved in order to make m-payment an alternative of cash and many other payment types. On the other hand lack of standards within devices as well as networks may be pertinent issues for the future of m-payment. There are many companies working in this regard but one of the main challenges is to unify payment solution, providing the highest possible level of security.

### REFERENCES

[1] Scarlet Schwiderski-Grosche & Heiko Knospe, 2002, Secure M-Commerce

[2] Jan Ondrus, Yves Pigneur, 2005, A Disruptive Analysis in the Mobile Payment Market

[3] P. Candace Deans, 2004, E-commerce and M-Commerce Technologies, USA

[4] Jerry Gao, Jacky Cai, Kiran Patel, and Simon Shim, 2005, A Wireless Payment System, USA

[5] Mehdi Khosrow, 2006, Encyclopedia of E-commerce, E-Government, and Mobile Commerce, USA

[6] Anders Cervera, 2002, Analysis of J2ME™ for developing Mobile Payment Systems

[7] XingJiang Song, 2001, Mobile payment and security

[8] Wen-Chen Hu, Chung-wei Lee, Weidong Kou, 2005, Advances in security and payment method in mobile commerce

[9] http://www.wi-fiplanet.com/tutorials/article.php/953561

10 http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group3/security.html

[11] J. Jonker, 2003, M-Commerce and M-Payment

[12] http://www.shareholder.com/paypal/releaseDetail.cfm?ReleaseID=192226&Category=US

[13] www.paycircle.org

[14] http://www.mobipay.com

[15] http://www.semops.com