M – COMMERCE AS A SHAPE OF E-COMMERCE AND ITS SECURITY ASPECTS

A. Sarajlić MSc EE, E. Kadušić BSc EE
BH Telecom/ID of Mobile network, Sarajevo, B&H

INTRODUCTION

M-commerce is process of purchasing physical and nonphysical goods and services by mobile phone, using wireless technology. Today, a considerable proportion of mobile commerce consists of the purchase of different types of digital content that in most cases is utilized in the mobile phone. Symbian OS and Java technology offer new possibilities for application developers, while users are able to easily configure and personalize the functionality of the mobile device to match their needs and preferences. Consumers increasingly personalize their mobile phones with ring tones, screen savers, and wallpapers. Games, downloadable phone applications, as well as music and video clips are also becoming more and more popular. Also, mobile recharging, mobile shopping and mobile banking are getting more and more popular and attractive for mobile users.

As more digital content and services as well as physical goods become available for purchase with mobile devices, there is a growing need for different mobile charging and payment methods. Content and service providers will require secure, versatile, and cost-efficient transaction capabilities, and consumers will require convenient user experiences. Up until now, the most common means of payment in the mobile environment has been the phone bill, but there is a rising need for other micro-payment and macro-payment methods as well as credit and debit card payments.

As the main precondition that impose for m-commerce deployment is, mobile operator’s ability to collect payment for mobile contents, applications, informations and different business models, including revenue sharing. M-commerce and its success enables to mobile operator to create a new revenues and develop the ways for acquiring the new users and retaining the old users, by breach in the new segments of business, out of the currently field of mobile operator.

Technology which enabling these services in the most cases is SMS, USSD, WAP over GSM or GPRS mobile infrastructure.

In order to m-commerce has a success, it is necessary to achieve a right balance of technology, strategy, content and marketing.

SUBJECTS AND VALUES OF M-COMMERCE

M-commerce includes a various subjects with different and often opposite motivations. The subjects that M-commerce value chain consists of are: mobile network operator, users, merchants/content providers and financial institutions.

From user’s aspect, the very service must be suitable and easy to handle. Also, the service must be secure and respect a privacy, and as such, perceived by user. The values and key questions are different for content providers and merchants. Content providers haven’t ability to collect payment for their content, because they haven’t business relation with users, what restrict their market. Merchants observe m-commerce as another way for extension of sale channels, which complete existing payment methods (cash, credit/debit cards).

Mobile network operators have the most motivation for m-commerce, because it is source of additional revenues, through increased traffic in the own network and provisions of achieved transactions. For some mobile operators, the most value laying in the fact that mobile gets on its usable value, becoming a new means of payment, and as that take more important place in regulary life of users.

Financial institution observe m-commerce as another way of payment for its existing users, in addition to supplementary earning through transaction management and a solution for financial questions.

As M-commerce service provider, the most often appear mobile network operators and financial institutions.

On the Figure 1, mobile operator is showed as m-commerce service provider, that is as micro and macro payment service provider.

Figure 1: Mobile operator as m-commerce service provider

On a base of transaction values and charging place we can talk about next classification:

- micropayment or payment of little value – typical limited on values of a few Euro. In mobile environment those are the most often some digital contents, as ring tones, video downloads, games etc. Micropayment is related to little amounts which are charging from subscribers postpaid ore prepaid account. That...
means, this charging is carry out on prepaid or postapaid billing using appropriated mediations.

- Macropayment or payment of great value – which enable the simillar limits as credit/debit cards, in size of order of couple of hundred Euros. Macropayment is related to greater amounts which are charging from subscribers banking account. In mobile environment, those are the most often mobile shopping, POS shopping, …

**CONCEPT SOLUTION FOR M-COMMERCE MOBILE PAYMENT PLATFORM**

The next figure shows the layered block structure of m-commerce platform:

![Figure 2: Block structure of m-commerce platform](image)

As we can see, there are three lyers on the drawing:

- A layer for requests acquiring which assembly users requests to specifical applications, over different access channels, for example: SMS, USSD, WAP
- A layer for requests processing, coordination, processing and routing of transactions, realization settlement and clearing among partners in m-commerce chain.
- A layer for charging in the micro and macro payment.

Here is quoted only short description of every layer, because detailed consideration would request much more papers.

**SECURITY ASPECTS**

During the financial transactions, security is one of the key problems. In many cases, the strong security is increasing of the transaction costs and complexity of usage of service. However, varied m-commerce services, special in macro payment sphere, request a high level of security.

**Security Threats**

We will look at three common security threats: spoofing, sniffing and tampering. When data is being transferred, whether over a wireless or wired network, we need to take precautions against these risks.

**Spoofing**

Spoofing is the attempt by a party to gain unauthorized access to an application or system by pretending to be someone he or she is not. If the spoofer gains access, he can then create fake responses to messages in an attempt to gain further knowledge and access to other parts of the system. Spoofing is a major problem for Internet security, because a spoofer can make application users believe that they are communicating with a trusted source, such as their bank, when in reality they are communicating with an attacker machine. Unknowingly, users often provide additional information that is useful to the attacker to gain access to other parts and other users of the system.

The process of sniffing is often used in conjunction with spoofing to get enough information to access the system in the first place. For this reason, implementing both authentication and encryption is required to combat spoofing.

**Sniffing**

Sniffing is a technique used to monitor data flow on a network. While sniffing can be used for proper purposes, it is more commonly associated with the unauthorized copying of network data. In this sense, sniffing is essentially electronic eavesdropping. By "listening" to network data, unauthorized parties are able to obtain sensitive information that will allow them to do further damage to the application users, the enterprise systems, or both.

Sniffing is dangerous because it is both simple to do and difficult to detect. Moreover, sniffing tools are easy to obtain and configure. In fact, Ethernet sniffing tools come with the Microsoft Windows NT and 2000 installs; fortunately, these tools are simple to detect. To combat the more sophisticated sniffing tools, data encryption is the best defense. If an unauthorized user is able to access encrypted data, he or she will lack a way to decrypt it, essentially making it useless.

**Tampering**

Data tampering, also called an integrity threat, involves the malicious modification of data from its original form. Very often this involves intercepting a data transmission, although it also can happen to data stored on a server or client device. The modified data is then passed off as the original. Employing data encryption, authentication, and authorization are ways to combat data tampering.

**SECURITY ENVIRONMENT**

Requests acquiring from the two aspects: user access side and technical side. From user access side, security can be considered in five points:

- **Confidentiality**
  Confidentiality is one of the most important aspects of security, and certainly the most talked about concerning issues about maintaining data privacy, making sure it cannot be viewed by unwanted parties. Most often, when people are worried about the security of a system, they are concerned that sensitive information, like a credit card number or health records, can be used by parties with malicious intent.

- **Authentication**
  Authentication is the process of proving that the people or organizations are who or what they claim to be.
At the application layer, authentication is important at two levels: the client and the enterprise server. To gain access to enterprise data, the client has to prove to the server that it is what it says it is. At the same time, before a client allows an outside server to connect to it—for example, to push some content—the server has to authenticate itself to the client application. The simplest, and probably least secure, method of authentication is a username/password combination. More advanced methods include digital certificates or digital signatures.

- **Data Integrity**
  Data integrity is assurance that the data in question has not been altered or corrupted in any way during the transmission from the sender to the receiver. This can be accomplished by using data encryption in combination with a cryptographic checksum or Message Authentication Code (MAC). This information is encoded into the message itself by applying an algorithm to the message. When recipients receive the message, they compute the MAC and compare it with the MAC encoded in the message to see if the codes are the same. If they are, recipients can be confident that the message has not been tampered with. If the codes are different, recipients can discard the data as inaccurate.

- **Authorization**
  Authorization is the process of determining the user’s level of access—whether a user has the right to perform certain actions. Authorization is often closely tied to authentication. Once a user is authenticated, the system can determine what that party is permitted to do.

- **Nonrepudiation**
  Nonrepudiation is about making parties accountable for transactions in which they have participated. It involves identifying the parties in such a way that they cannot at a later time deny their involvement in the transaction. In essence, it means that both the sender and the recipient of a message can prove to a third party that the sender did indeed send the message and the recipient received the identical message.

The next three factors:

- User’s agreement;
- User’s MSISDN in User Directory, where is mapped one or more banking accounts, access rights as well as security polices;
- mPIN for confirmation of transactions;

are the most important in order to user has passed through a mobile network infrastructure and a m-commerce platform and arrived to interface toward financial institution, following a Financial institution tests (type accounts and balance…).

From technical side, security of payment system can be considered in relation to security of access channels, that is, as security of mobile network infrastructure, where m-commerce platform is implemented as set of applications.

**SECURITY TECHNOLOGIES**

**Cryptography**

The basic objective of cryptography is to allow two parties to communicate over an insecure channel without a third party being able to understand what is being transmitted. This capability is one of the core requirements of a secure environment, as it deals with all aspects of secure data transfer, including authentication, digital signatures, and encryption.

**Algorithms and Protocols**

Cryptography works on many levels. At the lowest level are cryptographic algorithms. These algorithms describe the steps required to perform a particular computation, typically based around the transformation of data from one format to another. Building on these algorithms, is a protocol.

The protocol describes the complete process of executing a cryptographic activity, including explicit information on how to handle any contingency that might arise. Making this distinction is important, because an excellent cryptographic algorithm does not necessarily translate into a strong protocol.

The protocol is responsible for more than just the encoding of data; data transmission and key exchange are also properties of a protocol.

Finally, on top of the protocol are the applications. Once again, a strong protocol does not guarantee strong security, as the application itself may lead to further problems. Thus, in order to create a secure solution, a strong protocol is required, as well as a good, robust application implementation.

**Data Encryption**

The core of any cryptographic system is encryption, the process of taking a regular set of data, called plaintext, and converting it into an unreadable form, called cipher text. Encryption allows you to maintain the privacy of sensitive data, even when accessed by unauthorized users. The only way the data can be read is by transforming it back to its original form using a process called decryption. The method of encryption and decryption is called an algorithm or cipher.

Figure 3 demonstrates the concept of encryption. As the message is transported over an insecure public channel, it is encrypted, preventing anyone eavesdropping on the line from being able to understand the data being sent.

![Figure 3: Sending a message using encryption](Image 492x165 to 501x185)

Modern algorithms use keys to control the encryption and decryption of data. Once a message has been encrypted, it can only be decrypted by users who have the corresponding
key. Key-based algorithms come in two classes: symmetric and asymmetric.

Symmetric algorithms are efficient: They use a single key to encrypt and decrypt all messages. The sender uses the key to encrypt the message and then sends the message to the intended recipient. Once the message is received, the recipient uses the same key to decrypt the message. This type of algorithm works well when there is a safe way to transmit the key between users, such as by meeting before the transmission takes place. Unfortunately a substantial problem arises when exchanging data between loosely related parties, such as an e-commerce Web site and a customer. Exchanging the key is a problem that symmetric encryption itself is incapable of solving; and without a secure method of exchange keys, this method is only useful between private parties.

Symmetric encryption is also referred to as secret-key encryption. The most popular form of this method is the Data Encryption Standard (DES), which was developed in the 1970s. Since then more secure forms of symmetric encryption have been developed; leaders among them include the Advanced Encryption Standard (AES), which is based on the Rijndael algorithm; Triple DES; International Data Encryption Algorithm (IDEA); Blowfish; and the Rivest family of algorithms, RC2, RC4, RC5, and RC6.

Asymmetric encryption addresses the main problem that has plagued symmetric key systems: the use of a single key. Diffie and Hellman developed a solution using two separate but related keys: one to encrypt the data and another to decrypt it. The key used to encrypt the data is called the public key. This key can be widely distributed over insecure lines, for general public use. The key used to decrypt the corresponding data is called the private key. This key is never transmitted, as it is only required by the party that needs to decrypt the data. These keys are related in an obscure way using extremely large prime numbers and one-way functions. This technique makes it computationally infeasible to calculate the private key based on the public key. The larger the key is, the more difficult it becomes to break the system. Sixty-four-bit key systems, such as DES, are capable of being attacked by brute force—that is, trying every single key combination until the attacker finds the correct one. The more common 128-bit systems, such as ECC, so far have proven invulnerable to brute-force attacks.

Here is an example of how asymmetric, or public key, cryptography works. Suppose a person A wants to send a secure message to the person B. A can use B's public key to encrypt the message, since it is publicly available. It then sends the message to B. When he receives the message, he uses his private key, to which only he has access, to decrypt the message. Now A is able to send a secure message to B without having to do a key exchange. If information is to be exchanged in both directions using asymmetric encryption, each party must have his or her own public key and private key combination.

Encrypting a message with the private key and decrypting it with the public key is possible as well, but this has a different objective. It can be used on non-sensitive data simply to prove that the party who encrypted it actually has access to the private key.

The first, and best-known, asymmetric key algorithm was released in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman; who are commonly known as RSA. Other popular algorithms include Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH). RSA is being challenged in the mobile space by ECC, which is much less expensive in terms of processing power and key size, which are essential attributes in mobile computing.

Asymmetric ciphers are not, however, a perfect solution. Choosing a private key is not trivial, as a poor choice can lead to an easily broken scheme. Also, asymmetric ciphers provide a solution to the key distribution problem by using a public key and a private key, but they also are much more complicated, and therefore computationally slower than symmetric ciphers. For large sets of data, this can be problematic.

In these cases, a combination of symmetric and asymmetric systems is an ideal solution. This allows you to take advantage of the higher performance of symmetric algorithms, by sending the secret key over insecure channels using public key systems. Once all parties have the secret key, the remainder of the data for that session can be encrypted and decrypted using symmetric algorithms. This is the basis for public key cryptography as used by many of today's leading protocols.

References


Letter of thanks: (The work on this project is whole financed by means of BH Telecom, Sarajevo)

Abstract: In the future, it is expected to m-commerce becomes one of the predominant ways to payment for services and goods in the mobile environment. In this work are presented the main characteristics of m-commerce, platform for purchasing and payment of digital contents, applications and informations as well as nondigital goods. There have been explained security aspects, through threats and environment. Also, have been quoted in brief the main security technologies.

M – COMMERCE AS A SHAPE OF E-COMMERCE AND ITS SECURITY ASPECTS, A.Sarajlić MSc EE, E.Kadušić BSc EE.