Mobile Commerce and Related Mobile Security Issues

Ashish Wadhaval¹, Rugved Mehta², Ashlesha Gawade³

¹ Information Technology, Mumbai University

Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering, Sion, Mumbai.

Abstract: This article will discuss how m-commerce conducts transactions of the mobile device through Internet and how these technologies are developed throughout the years. The article will also judge the security and privacy levels when dealing with mobile commerce and what kind of issues are encountered when using mobile commerce systems. The article will also evaluate the solutions on how m-commerce issues are avoided and how they are tackled by the technology evolution.

Keywords: M-commerce, security and privacy issues, mobile devices, network.

1. INTRODUCTION

M-commerce is a term that is used to refer to the growing practice of conducting financial and promotional activities with the use of a wireless handheld device. The term m-commerce is short for mobile commerce, and recognizes that the transactions may be conducted using cell phones, personal digital assistants and other hand held devices that have operate with Internet access. While still in its infancy, the concept of m-commerce has been refined in recent years and is beginning to become more popular.

One of the basic examples of m-commerce has to do with receiving sales promotions via the hand held device. The most common application would involve the service provider sending text messages to the subscriber that promote new product offerings, free trials on additional services, or other types of promotional campaigns. The subscriber is not charged a fee for the text message, and often can respond with a return text message without incurring any type of fee. Several major cellular services off subscribers to opt into this type of m-commerce, or be excluded from receiving the messages.

Benefits of mobile commerce:

According to some market research institutes, by 2004 at least 40 % of customer-to-business e-commerce will come from smart phones using the WAP. Many new applications are becoming possible, and many existing e-commerce applications can be modified for a mobile environment. To illustrate the great potential of the m-commerce, we just mention some potential applications: selling and buying of different goods, mobile inventory management (tracking the location of goods and services), proactive service management (transmitting information about aging components, such as automobile parts, to the vendors), wireless reengineering (Improving business services), mobile auction and reverse Auction, mobile entertainment services, mobile office (services for business people, such as traffic jam reports, airport and flight information, procurement of products and services), mobile distance education (offering classes using streaming audio and video), wireless data centre (providing downloadable information from data warehouses), and others.

2. ISSUES THAT CONCERN M-COMMERCE IN TERMS OF SECURITY AND PRIVACY.

Security threats in mobile commerce can range from passively eavesdropping into others' message to actively stealing user's data. In a radio frequency operated mobile commerce, with minimum difficulty it is possible to listen to one's conversation. This has an impact for consumers because they are concerned about their data and voice messages from unauthorised access. On the other end of the problem is the inherent security risk involved in transferring information over the networks. This problem consists of two components: identification integrity and message integrity. The identification integrity refers to the signature elements found in the messages in order to establish where the message is originating. The message integrity refers to details to establish that the message is received as sent and no third party has attempted to open, modify or alter the contents. According to Zhang and Lee, these two items appear to cause a lot of concern to both sender and receiver.6

While the sender risks theft or misuse of their personnel information such as account and bank details, the receiver (usually a merchant) risks repudiation of the transaction and resultant non-payment.
Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common. Increasing online transactions personal and sensitive information shared over network. Confidentiality to MAC frames.

Authentication
Process of verifying identity of a user

Integrity
Data that arrives is the same as that is sent

Confidentiality
Sensitive information should not be visible to eavesdropper - use

Encryption

Non-repudiation
Assurance that any transaction that takes place can subsequently be proved to have taken place

Authorization
Assigning access rights to users

3. SOLUTIONS ON HOW TO SOLVE THE MAIN ISSUES OF MOBILE COMMERCE:

Mobile payments is one of the most dynamic sectors in the global economy, with disparate technologies and business models targeting various markets depending on how mobile users choose to transact. As new mobile payment networks emerge, consumers' payment options for virtual and actual goods will expand. Notwithstanding the challenges of increased merchant competition, high deployment costs and consumer confusion, there is a market need for a true end-to-end m-payment solution that merchants can immediately use to drive consumer behaviour and additional revenues.

The m-payment opportunity
Consumers have an immense appetite for transacting on mobile devices. A recent Forrester report pegs U.S. m-commerce revenues at $6 billion for 2011, with expected growth to $31 billion by 2016. However, for the market to accept a ubiquitous mobile payment model and embrace a new era where consumer engagement unites with commerce, solution providers have a lot of work ahead.

4. DISCUSSION:

Mobile commerce is an emerging market. As with any emerging market there are significant opportunities and significant risks. The temptation at this stage is for key players to impose their own rules based on their own business models. Although this can be beneficial for a few in the short-term and in some markets may be the only way to start doing mobile commerce, in the long-term this will have a negative impact on business because lack of interoperability and higher operating costs will create barriers to growth and adoption. However a dynamic market needs an environment that favours innovation and a diversity of stakeholders.

5. CONCLUSION:

In conclusion, the article has looked at some of the most sensitive areas of the new mobile commerce such as, bank transaction systems, online shopping because it engages with large amounts of money every day. Therefore the system used for transactions has to absolutely secure and to be free of corruption as mentioned earlier in the article; business will lose customers if the mobile security system is not secure enough. On the other hand the article also discussed the variety of ways of how our mobile commerce works and how it is been improved through the years. It also showed the protocols that have been developed in order to make our mobile commerce safe and secure from fraud.

6. REFERENCES:

(MOBILE COMMERCE APPLICATIONS AND SERVICES: A DESIGN AND DEVELOPMENT APPROACH),
(2003).
[12] Shintaro Okazaki College of Economics and Business Administration Autonomous University of Madrid, Spain,
(NEW PERSPECTIVES ON M-COMMERCE RESEARCH), (2005).
[14] Scarlet Schwiderski-Grosche, Heiko Knospe. (secure M-commerce),
(2000).
[15] Suresh Chari, Parviz Kermani, Sean Smith, and Leandros Tassiulas,
(Special Issue on M-Commerce), AUGUST (2007).