Chapter 7.6
Security Issues Concerning Mobile Commerce

Samuel Pierre
École Polytechnique de Montréal, Canada

INTRODUCTION

Electronic commerce or e-commerce can be briefly defined as a financial transaction or commercial information between two parties based on data transmitted over communication networks (Soriano & Ponce, 2002). It relies upon users' interventions to initiate a transaction and select the main steps of the process. Users' actions stem from a succession of virtual decisions. Indeed, when shopping with a virtual catalog, customers can select products which meet their needs, tastes, and respect their price range. Such decisions consistently require the users' input, thus costing them both time and money. These costs are even more exorbitant when a search is launched for an order that includes a variety of products from different sources which have different characteristics (price range, delivery dates, etc.). When transactions involve users who are moving or take place over mobile networks, this is referred to as *mobile electronic commerce*, a specific type of e-commerce.

Mobile electronic commerce (or m-commerce) refers to an ability to carry out wireless commercial transactions using mobile applications within mobile devices, such as mobile phones and personal digital assistants (PDAs). It is generally defined as the set of transactions or processes which can be carried out over a wireless mobile network. According to this definition, m-commerce constitutes a subset of all electronic commercial transactions (electronic commerce or e-commerce) from business to consumer (B2C) or business to business (B2B). Thus, short personal messages such as those from SMS (short messaging system) sent between two individuals do not fall into the category of m-commerce, whereas messages from a service provider to a salesperson or a consumer, or vice versa, do fit this very definition. M-commerce appears as an emerging manifestation of Internet electronic commerce which meshes together concepts such as the Internet, mobile computing, and wireless telecommunications in order to provide an array of sophisticated services (m-services) to mobile users (Varshney, Vetter, & Kalakota, 2000; Veijalainen, Terziyan, & Tirri, 2003).

E-commerce includes an initial step where consumers search for a product they wish to purchase by virtually visiting several merchants. Once the product is found, negotiations can take place between the customer and the merchant (electronic negotiation or e-negotiation) (Paurobally, Turner, & Jennings, 2003). If an agreement is reached, the next step is the payment phase. At each step of the process, some problems arise, such as transaction security, confidence in the payment protocol, bandwidth limitations, quality of service, shipping delays, and so forth (Younas, Chao, & Anane, 2003; Zhang, Yuan, & Archer, 2002). The peak withdrawal periods have always presented a major challenge for certain types of distributed applications. The advent of m-commerce further highlights this problem. Indeed, in spite of rather optimistic predictions, m-commerce is plagued by several handicaps which hinder its commercial development, security being the main one.

Many market research studies, like those carried out by Strategy Analytics and the Gartner Group, predicted that by 2004 there would be over one billion wireless device users, some 600 million wireless Internet subscribers, a $200 billion m-commerce market, and 40% of consumer-to-business e-commerce will take place over Web-enabled phones (Gosh & Swaminatha, 2004). However, these business opportunities could be compromised by new security risks specific to the wireless medium and devices. As a result, the potential boom in the number of new m-commerce applications and markets can be achieved if and only if security and privacy can be integrated into online m-commerce applications.

This article analyzes some major security issues concerning mobile commerce. The next section presents background and related work, followed by a summary of some security issues and challenges. Future and emerging trends in secure m-commerce are then outlined, and the article is concluded.

BACKGROUND

While e-commerce systems are designed for purchases conducted on the wired Internet, m-commerce is extended to handle the mobility aspects related to the user equipment such as a mobile phone or a PDA. One of the main characteristics of an m-commerce system is the use of the Internet as the backbone and e-commerce with mobile terminals as user equipment. M-commerce applications can be as simple as a system to synchronize an address book or as complex as the system used to enable credit card transactions. They are deployed using mobile middleware which can be defined as a functional layer of software provided by application developers to link their e-commerce applications to an operating system and various mobile networks to allow their applications to bypass certain mobility issues.

Any party engaging in business needs a certain level of security. Security relies on a set of basic concepts and requirements such as: confidentiality, authentication, integrity, non-repudiation, and authorization. Confidentiality assures that the exchange of messages between parties over wireless access networks or global networks is not being monitored by non-authorized parties. Authentication ensures that the parties engaging in business are who they claim to be. Integrity allows users to verify whether modifications have occurred; however, it does not guarantee that information has not been altered. Non-repudiation certifies that the business transactions the parties engage in are legally binding. Authorization refers to a set of access rights assigned to an entity by a certification authority (CA). It does not guarantee that messages received do really come from a given counterpart; that is the task

Related Content