Category: Concepts, Trends, and Challenges

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

Copyright © 2006, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

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 of authentication.

In a wired network, the secure socket layer (SSL) protocol and the transport layer security (TLS) protocol, which are well-established security protocols, provide privacy and data integrity between two communicating applications. In fact, HTTP over TLS-SSL is used to secure transactions for security-sensitive applications like m-commerce. It is generally known that these protocols do not adapt well to wireless environments with reduced processing capability and low-bandwidth links. Indeed, wireless devices such as cellular phones and PDAs have limited storage and minimal computational capacity. As a result, security issues were not taken into account when they were designed.

The scheme devised during the wireless application protocol (WAP) forum, which has defined an entirely new suite of protocols, uses a WAP gateway or proxy between the wireless and wireline environments to ensure connection and security. The SSL and TLS ensure security within the Internet, while the wireless transport layer security (WTLS) protocol ensures secure channels between the client and the WAP gateway. Transactions between WTLS and TLS are executed by the WAP gateway. However, the use of the WAP proxy, which is also a point of failure, does not allow for end-to-end security. As a matter of fact, because there are storage and translation operations at the WAP proxy, it becomes a point of entry for attacks. A solution to strengthen this weakness was provided by Soriano and Ponce (2002). They suggested providing a secure end-to-end tunnel between an Internet server and a mobile user by implementing a TLS compatible security layer at the wireless application environment (WAE) layer on the client side, named WAE-Sec. WAE-Sec therefore prohibits translations by the WAP gateway and permits compatibility with the TLS protocol. Note, however, that this solution resembles the one proposed by Gupta et al. (2001).

On the other hand, Tang, Terziyan, and Veijalainen (2003) have defined other related security issues to m-commerce, namely hostility, information security, and vulnerability. Hostility means that dishonest customers who get fraudulent identities by stealing mobile devices can make illegal operations and, thus, should be quickly identifiable. Information is more vulnerable in wireless networks since other parties can easily intercept it. The solution is to encrypt data with adequate keys. Vulnerability arises from a malfunctioning of the mobile device itself or from the physical access of malicious persons to the terminals. To remedy these additional problems, Tang et al. (2003) suggested the use of a mixed personal identification number (PIN) storage scheme which let the PIN be partially stored on the mobile device while the remainder of the PIN is stored on the network. Researchers assume that the probability of discovering the PIN located at two different places does not depend on the length of the PIN nor on the fact that a single part was discovered. Thus, discovering the whole PIN will require digging and/or guessing for twice as long than if the PIN was located at a single place. The improvements brought about by this strategy have been shown using a probabilistic model, but its implementation has yet to be investigated.

A new protocol for m-commerce was proposed by Katsaros and Honary (2003). Fully applicable to third-generation mobile networks, this protocol is characterized by three novel properties, as opposed to the existing methods of m-commerce. In fact, it provides a simplified and secure transaction method, minimizes the number of entities involved in the transaction, and finally reduces the probability of security threats, thus reducing the risk of fraud. Unfortunately, this protocol does not solve certain security issues related to m-commerce.

SECURITY ISSUES AND CHALLENGES

Mobile commerce provides an exciting new set of capabilities which can lead to new services that enhance the end-user's experience. With these new business opportunities, the risk of new security threats also arises. New mobile devices such as PDAs and mobile phones enable easy access to the Internet and strongly contribute to the development of m-commerce services, while Smartcard

3 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-issues-concerning-mobile-commerce/12659

Related Content

Mobile Handheld Devices for Mobile Commerce
Wen-Chen Hu, Jyh-haw Yeh, Hung-Jen Yangand Chung-wei Lee (2008). *Electronic Commerce: Concepts, Methodologies, Tools, and Applications (pp. 152-162).*
www.irma-international.org/chapter/mobile-handheld-devices-mobile-commerce/9461

Relational Benefits as Predictors of Relationship Quality Outcomes in Online Retailing
Daniel K. Madukuand Ryan L. Mathaba (2022). *Journal of Electronic Commerce in Organizations (pp. 1-34).*
www.irma-international.org/article/relational-benefits-as-predictors-of-relationship-quality-outcomes-in-online-retailing/305737

An Examination of Consumers' High and Low Trust as Constructs for Predicting Online Shopping Behavior
Donald L. Amorosoand Tsuneki Mukahi (2013). *Journal of Electronic Commerce in Organizations (pp. 1-17).*
www.irma-international.org/article/examination-consumers-high-low-trust/78554

A Behavioral Beliefs Model of Trustworthiness in Consumer-Oriented E-Commerce
Craig Van Slyke, France Belangerand Christie L. Comunale (2009). *Journal of Electronic Commerce in Organizations (pp. 22-43).*
www.irma-international.org/article/behavioral-beliefs-model-trustworthiness-consumer/3529

Developing Mobile Commerce Applications
Nikolaos Folinas, Panos Vassiliadis, Evaggelia Pitoura, Evangelos Papapetrouand Apostolos Zarras (2008). *Journal of Electronic Commerce in Organizations (pp. 63-78).*
www.irma-international.org/article/developing-mobile-commerce-applications/3506