Chapter 4.12
Secure Multicast for Mobile Commerce Applications: Issues and Challenges

Mohamed Eltoweissy
Virginia Tech, USA

Sushil Jajodia
George Mason University, USA

Ravi Mukkamala
Old Dominion University, USA

ABSTRACT

With the rapid growth in mobile commerce (m-commerce) applications, the need for providing suitable infrastructure to support these applications has become critical. Secure multicast is a key element of this infrastructure, in particular, to support group m-commerce applications such as mobile auctions, product recommendation systems, and financial services. Despite considerable attention to m-commerce security, most existing security solutions focus on unicast communications. On the other hand, numerous solutions for secure multicast exist that are not specifically designed with m-commerce as a target environment. Clearly, to address secure multicast in m-commerce, we must start by forming a comprehensive picture of the different facets of the problem and its solutions. In this chapter, we identify system parameters and subsequent security requirements for secure multicast in m-commerce. Attacks on m-commerce environments may undermine satisfying these security requirements resulting, at most times, in major losses. We present a taxonomy of common attacks and identify core services needed to mitigate these attacks and provide efficient solutions for secure multicast in m-commerce. Among these services, authentication and key management play a major role. Given the varying requirements of m-commerce applications and the large number of current key management schemes, we provide a taxonomy and a set of performance metrics to aid m-commerce system designers in the evaluation and selection of key management schemes.

INTRODUCTION

The exponential growth of the Internet, wireless communications, and electronic commerce, coupled with the recent advances in mobile Web services and pervasive computing, are transforming mobile commerce (m-commerce) from an idea to reality. However, for m-commerce to realize its potential, there is a critical need for providing suitable service environments where numerous mobile, context-aware, smart services will interact among themselves, and consumers and suppliers to accomplish commercial transactions. Secure group communications is, therefore, one of the key elements of this service environment. M-commerce applications such as mobile auctions, product recommendation systems, and financial services require secure and reliable group communications services (Varshney & Vetter, 2002). In addition to being secure, group communications services underlying such applications also need to be efficient in terms of the computing and communications overhead that they impose on the mobile devices. While real-time response is of concern in some applications (e.g., stock trading transactions), dynamic joins/leaves of group members is of concern in other applications (e.g., online video games). Unlike e-commerce applications that run on fixed networking infrastructures with fairly high reliability and bandwidths, m-commerce applications have to depend (at least partly) on wireless infrastructure. Typically, wireless infrastructure has low bandwidths, is power constrained, and is often not so dependable. These requirements, as well as others to be discussed shortly in this chapter, call for secure multicast communications services supporting m-commerce applications.

In order to further illustrate the need for secure multicast communications in m-commerce, let us consider two scenarios, one involving mobile auctions and the other a collaborative investigation team.

- **Mobile auctions:** Consider an auctioning system where both sellers and buyers can participate in an auction involving both stationary and mobile users. For example, an antique collector on travel may want to be alerted about online auctions even when on travel. Since some of these auctions may have only short durations for the sale of the items, it is important that the mobile user be able to participate in the process while on the move. For example, let us assume that a firm XYZ specializes in online antique auctions. All potential customers must subscribe to this firm's services. Whenever a seller (not necessarily a subscriber) intends to auction an item, he/she informs the XYZ firm, providing a minimum price. The firm sends this information to all its subscribers through a secure multicast. While the users on the Internet with fixed IP addresses can be reached via the IP Multicast protocols, the coverage of mobile subscribers calls for a mobile multicast protocol. One of the challenges in achieving this coverage is the ability to locate the mobile users and efficiently multicast the messages to them. Obviously, they would be geographically distributed in different regions. Another challenge is timely delivery. Since most auctions are time-sensitive, it is important that all subscribers receive the information in a timely manner, and their responses (or bids) also reach the destination in a timely manner. In addition, it may be important to guarantee delivery to all subscribers. In other words, each auction message should reach its subscribers (mobile or stationary) with a very high probability. If XYZ firm cannot offer such guarantees, then it will soon lose its clients. Similarly, it is most important that the messages received by the subscribers be genuine. This can be enforced by some security authentication measures. In summary, this scenario illustrates the