Mobile Commerce Security and Payment

Chung-wei Lee
Auburn University, USA

Weidong Kou
Xidian University, PR China

Wen-Chen Hu
University of North Dakota, USA

INTRODUCTION

With the introduction of the World Wide Web (WWW), electronic commerce has revolutionized traditional commerce and boosted sales and exchanges of merchandise and information. Recently, the emergence of wireless and mobile networks has made possible the extension of electronic commerce to a new application and research area: mobile commerce, which is defined as the exchange or buying and selling of commodities, services or information on the Internet through the use of mobile handheld devices. In just a few years, mobile commerce has emerged from nowhere to become the hottest new trend in business transactions. Mobile commerce is an effective and convenient way of delivering electronic commerce to consumers from anywhere and at any time. Realizing the advantages to be gained from mobile commerce, companies have begun to offer mobile commerce options for their customers in addition to the electronic commerce they already provide (The Yankee Group, 2002).

Regardless of the bright future of mobile commerce, its prosperity and popularity will be brought to a higher level only if information can be securely and safely exchanged among end systems (mobile users and content providers). Applying the security and payment technologies for electronic commerce to mobile commerce has been proven a futile effort because electronic commerce and mobile commerce are based on different infrastructures (wired vs. wireless). A wide variety of security procedures and payment methods, therefore, have been developed and applied to mobile commerce. These technologies are extremely diverse and complicated. This article provides a comprehensive overview of mobile commerce security and payment methods.

BACKGROUND

Mobile security is a crucial issue for mobile commerce. Without secure commercial information exchange and safe electronic financial transactions over mobile networks, neither service providers nor potential customers will trust mobile commerce systems. From a technical point of view, mobile commerce over wireless networks is inherently insecure compared to electronic commerce over the Internet (Pahlavan & Krishnamurthy, 2002). The reasons are as follows:

- Reliability and integrity: Interference and fading make the wireless channel error-prone. Frequent handoffs and disconnections also degrade the security services.
- Confidentiality/privacy: The broadcast nature of the radio channel makes it easier to tap. Thus, communication can be intercepted and interpreted without difficulty if no security mechanisms such as cryptographic encryption are employed.
- Identification and authentication: The mobility of wireless devices introduces an additional difficulty in identifying and authenticating mobile terminals.
- Capability: Wireless devices usually have limited computation capability, memory size, com-

munication bandwidth and battery power. This will make it difficult to utilize high-level security schemes such as 256-bit encryption.

Mobile commerce security is tightly coupled with network security. The security issues span the whole mobile commerce system, from one end to the other, from the top to the bottom network protocol stack, from machines to humans. Therefore, many security mechanisms and systems used in the Internet may be involved. In this article we focus only on issues exclusively related to mobile/wireless technologies. On a secure mobile commerce platform, mobile payment methods enable the transfer of financial value and corresponding services or items between different participators without factual contract. According to the amount of transaction value, mobile payment can be divided into two categories. One is micro-payment, which defines a mobile payment of approximately $10 or less (ComputerWorld, 2000), often for mobile content such as video downloads or gaming. The other is macro-payment, which refers to larger-value payments.

MOBILE COMMERCE SECURITY

Mobile commerce transactions can be conducted on the infrastructure of wireless cellular networks as well as wireless local area networks. Lacking a unified wireless security standard, different wireless networking technologies support different aspects and levels of security features. We thus discuss some popular wireless network standards and their corresponding security issues.

Wireless Cellular Network and Security

In addition to voice communication, cellular network users can conduct mobile commerce transactions through their well-equipped cellular phones. Currently, most of the cellular wireless networks in the world follow second-generation (2G, 2.5G) standards. Examples are the global system for mobile communications (GSM) and its enhancement, general packet radio service (GPRS). GPRS can support data rates of only about 100 kbps, and its upgraded version – enhanced data for global evolution (EDGE) – is capable of supporting 384 kbps. It is expected that third-generation (3G) systems will dominate wireless cellular services in the near future. The two main standards for 3G are Wideband CDMA (WCDMA), proposed by Ericsson, and CDMA2000, proposed by Qualcomm. The WCDMA system can inter-network with GSM networks and has been strongly supported by the European Union, which calls it the Universal Mobile Telecommunications System (UMTS). CDMA2000 is backward-compatible with IS-95, which is widely deployed in the United States.

GSM Security

The Subscriber Identity Module (SIM) in the GSM contains the subscriber's authentication information, such as cryptographic keys, and a unique identifier called international mobile subscriber identity (IMSI). The SIM is usually implemented as a smart card consisting of microprocessors and memory chips. The same authentication key and IMSI are stored on GSM's network side in the authentication center (AuC) and home location register (HLR), respectively. In GSM, short messages are stored in the SIM and calls are directed to the SIM rather than the mobile terminal. This feature allows GSM subscribers to share a terminal with different SIM cards. The security features provided between the GSM network and mobile station include IMSI confidentiality and authentication, user data confidentiality and signaling information element confidentiality. One of the security weaknesses identified in GSM is the one-way authentication. That is, only the mobile station is authenticated; the network is not. This can pose a security threat, as a compromised base station can launch a "man-in-the-middle" attack without being detected by mobile stations.

UMTS Security

UMTS is designed to reuse and evolve from existing core network components of the GSM/GPRS and fix known GSM security weaknesses such as the one-way authentication scheme and optional encryption. Authentication in UMTS is mutual and encryption is mandatory (unless specified otherwise) to prevent message replay and modification. In addition, UMTS employs longer cryptographic keys and newer cipher algorithms that make it more secure than GSM/GPRS.