Preface

Introduction

With the introduction of the World Wide Web, 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 admission of electronic commerce to a new application and research subject: 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. In fact, the growth of mobile handheld devices has been more rapid than the growth in any previous technology.

Yet, one of the biggest impediments to the growth of mobile commerce has been a lack of consistency in security and payment methods and an absence of consensus on technology standards. Various wired or electronic commerce security and payment methods have been modified and applied to mobile commerce, but experience shows that simply adapting those solutions to mobile commerce is not feasible. Different methods and approaches must be taken to enforce mobile commerce security and secure payment methods. Many novel security and payment technologies, therefore, have been proposed and applied to mobile commerce and they are highly diverse and broad in application. This book attempts to provide a comprehensive study of mobile commerce security and payment methods and address the complex challenges facing the mobile commerce industry.

This book contains high-quality research, and industrial and practical articles in the areas of mobile commerce security and payment methods from both academics and industrialists. It includes research and development results of lasting significance in the theory, design, implementation, analysis, and application of mobile commerce security and payment methods. It could be used for a textbook of an advanced computer science (or related disciplines) course and would be a highly useful reference book for IT professionals.

Organization

The issues related to mobile commerce security and payment methods are wide and varied, and this book has benefited from contributions by authors with a range of backgrounds. To help readers better understand this book, it is divided into four major sections and a brief overview of each chapter is given below.

Section I

This section describes the fundamentals of mobile commerce security and payment methods and includes four chapters on the general concepts, reputation and trust, intrusion detection, and a secure authentication infrastructure.

Chapter I, *Mobile Commerce Security and Payment Methods*, is by Chung-wei Lee, Weidong Kou, and Wen-Chen Hu. This chapter provides a comprehensive overview of mobile commerce security and payment methods. A secure mobile commerce system must have the following properties: (i) confidentiality, (ii) authentication, (iii) integrity, (iv) authorization, (v) availability, and (vi) non-repudiation. It discusses the security issues related to the following three network infrastructures: (i) wireless local area networks, (ii) wireless wide area networks, and (iii) WAP. Among the many themes of mobile commerce security, mobile payment methods are probably the most important. A typical mobile payment process includes: (i) registration, (ii) payment submission, (iii) authentication and authorization by a content provider, and (iv) confirmation. This chapter also describes a set of standards for mobile payments.

Chapter II, *Reputation and Trust*, is authored by Li Xiong and Ling Liu. The authors introduce reputation systems as a means of facilitating trust and minimizing risks in m-commerce and e-commerce in general. They presents PeerTrust, an adaptive and dynamic reputation based trust model that helps participants or peers to evaluate the trustworthiness of each other based on the community feedback about participants' past behavior.

Chapter III, *Intrusion Detection and Vulnerability Analysis of Mobile Commerce Platform*, is authored by Changhua Zhu and Changxing Pei. Intrusion detection and vulnerability analysis play the same important roles in wireless infrastructure as in wired infrastructure. This chapter first gives the methods and technologies of intrusion detection and vulnerability analysis. It then gives the security issues in various wireless networking technologies, analyzes the vulnerability of the enabling technologies for the mobile commerce platform, and proposes a distributed wireless intrusion detection & vulnerability analysis (WID&VA) system that can help to address the identified security issues.

Chapter IV, *A Secure Authentication Infrastructure for Mobile Users*, is authored by Gregor v. Bochmann and Eric Zhen Zhang. This chapter first explains the requirements for an authentication infrastructure for electronic commerce, identifying the partners involved in e-commerce transactions and the trust relationships required. An improved authentication protocol, which provides trust relationships for mobile e-commerce users, is then presented. Its analysis and comparison with other proposed authentication protocols indicate that it is a good candidate for use in the context of mobile e-commerce.

Section II

This section discusses issues related to mobile commerce security and includes four chapters on policy-based access control, XML-based trust negotiations, mobile agents, and secure multicast.

Chapter V, *Policy-Based Access Control for Context-Aware Services over the Wireless Internet*, is authored by Paolo Bellavista, Antonio Corradi, and Cesare Stefanelli. The spreading wireless accessibility to the Internet stimulates the provisioning of mobile commercial services to a wide set of heterogeneous and limited client terminals. This requires novel programming methodologies to support and simplify the development of innovative service classes. In these novel services, results and offered quality levels should depend on both client location and locally available resources (context). Within this perspective, this chapter motivates the need for novel access control solutions to flexibly control the resource access of mobile clients depending on the currently applicable context. In particular, it discusses and exemplifies how innovative middlewares for access control should support the determination of the client context on the basis of high-level declarative directives (profiles and policies) and distributed online monitoring.

Chapter VI, *A Comprehensive XML Based Approach to Trust Negotiations*, is authored by Elisa Bertino, Elena Ferrari, and Anna Cinzia Squicciarini. Trust negotiation is a promising approach for establishing trust in open systems like the Internet, where sensitive interactions may often occur between entities at first contact, with no prior knowledge of each other. This chapter presents Trust-X, a comprehensive XML-based XML framework for trust negotiations, specifically conceived for a peer-to-peer environment. It also discusses the applicability of trust negotiation principles to mobile commerce, and introduces a variety of possible approaches to extend and improve Trust-X in order to fully support mobile commerce transactions and payments.

Chapter VII, *Security Issues and Possible Countermeasures for a Mobile Agent Based M-Commerce Application*, is authored by Jyh-haw Yeh, Wen-Chen Hu, and Chung-wei Lee. With the advent of wireless and mobile networks, the Internet is rapidly evolving from a set of connected stationary machines to include mobile handheld devices. This creates new opportunities for customers to conduct business from any location at any time. However, the electronic commerce technologies currently used cannot be applied directly since most were developed based on fixed, wired networks. As a result, a new research area, mobile commerce, is now being developed to supplement existing electronic commerce capabilities. This chapter discusses the security issues related to this new field, along with possible countermeasures, and introduces a mobile agent based solution for mobile commerce.

Chapter VIII, *Secure Multicast for Mobile Commerce Applications: Issues and Challenges*, is authored by Mohamed Eltoweissy, Sushil Jajodia, and Ravi Mukkamala. This chapter identifies 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. A set of common attacks and the core services needed to mitigate these attacks are discussed first. It then provides 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, it also provides a set of performance metrics to aid m-commerce system designers in the evaluation and selection of key management schemes.

Section III

Section III covers the issues related to mobile commerce payment methods and includes three chapters on the subjects of mobile payment introduction and overview, micro-payments, and a mobile payment service SeMoPS, respectively.

Chapter IX, *M-Payment Solutions and M-Commerce Fraud Management*, is by Seema Nambiar and Chang-Tien Lu. The shift from physical to virtual payments has brought enormous benefits to consumers and merchants. For consumers it means ease of use. For mobile operators, mobile payment presents a unique opportunity to consolidate their central role in the m-commerce value chain. Financial organizations view mobile payment and mobile banking as a way of providing added convenience to their customers along with an opportunity to reduce their operating costs. This chapter starts by giving a general introduction to m-payment by providing an overview of the m-payment value chain, life cycle and characteristics. The second section reviews competing mobile payment solutions that are found in the marketplace. Different types of mobile frauds in the m-commerce environment and solutions to prevent such frauds are discussed in the last section.

Chapter X, *Multi-Party Micro-Payment for Mobile Commerce*, is authored by Jianming Zhu and Jianfeng Ma. This chapter introduces a new micro-payment scheme that is able to apply to multi-party for mobile commerce, which allows a mobile user to pay every party involved in providing services. The micro-payment, which refers to low-value financial transactions ranging from several cents to a few dollars, is an important technique in m-commerce. Their scheme is based on the hash function and without any additional communication and expensive public key cryptography in order to achieve good efficiency and low transaction costs. In the scheme, the mobile user releases an ongoing stream of low-valued micro-payment tokens into the network in exchange for the requested services.

Chapter XI, *SeMoPS: A Global Secure Mobile Payment Service*, is authored by Stamatis Karnouskos, András Vilmos, Antonis Ramfos, Balázs Csik, and Petra Hoepner. Many experts consider that efficient and effective mobile payment solutions will empower existing e- and m-commerce efforts and unleash the true potential of mobile business. Recently, different mobile payment approaches appear to the market addressing particular needs, but up to now no global mobile payment solution exists. SEMOPS is a secure mobile payment service with an innovative technology and business concept that aims to fully address the challenges the mobile payment domain poses and become a global mobile payment service. They present a detailed description of the approach, its implementation, and features that diversify it from other systems. They also discuss on its business model and try to predict its future impact.

Section IV

The issues related to mobile commerce security and payment methods are wide and disparate. This section consists of three chapters on digital signatures and smart cards.

Chapter XII, *Remote Digital Signing for Mobile Commerce*, is authored by Oguz Kaan Onbilger, Randy Chow, and Richard Newman. Mobile agents (MAs) are a promising technology, which directly address physical limitations of mobile devices such as limited battery life, intermittent and low-bandwidth connections, with their capability of providing disconnected operation. This chapter addresses the problem of digital contract signing with MAs, which is an important part of any mobile commerce activity and one special challenging case of computing with secrets remotely in public. The authors use a multi-agent model together with simple secret splitting schemes for signing with shares of a secret key carried by MAs, cooperating to accomplish a trading task.

Chapter XIII, *A Mobile Coalition Key-Evolving Digital Signature Scheme for Wireless/Mobile Networks*, is authored by Quanxing Zhang, Chwan-Hwa "John" Wu, and J. David Irwin. A scheme is proposed in this chapter to apply a secure digital signature scheme in a mobile-IP environment and treats the three entities in a dynamic path as either foreign agents (FA), home agents (HA) or mobile agents (MA), such that a coalition is formed containing each of the individual agents. Each agent has a pair of keys: one private and one public. The private key is evolving with time, and the public key is signed by a certification authority (CA). All the private keys of the three agents in the coalition are needed to sign a signature. Furthermore, all the messages are signed and verified. The signature is verified against a public key, computed as the product of the public keys of all three agents, and readily generated when a new dynamic path is formed.

Chapter XIV, *Smart Card Based Protocol for Secure and Controlled Access of Mobile Host in IPv6 Compatible Foreign Network*, is authored by R.K. Ghosh, Abhinav Arora, and Gautam Barua. This chapter presents a proposal to combine the advantages of IPSec and smart cards in order to design a new protocol for secure bi-directional access of mobile hosts in an IPv6 foreign network using smart cards. The protocol, called mobile authentication protocol (MAP), builds a security association needed for IPsec. An access router in a foreign network contacts an AAA (authentication, authorization and accounting) server in order to authenticate and authorize a mobile host that approaches the router to access services. The access router then acts as a gateway for all subsequent service requirements of the mobile host.