Computer Communications and Networks

Series editor
A.J. Sammes
Centre for Forensic Computing
Cranfield University, Shrivenham Campus
Swindon, UK

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Jesús Téllez • Sherali Zeadally

Mobile Payment Systems

Secure Network Architectures and Protocols

Springer

Jesús Téllez
University of Carabobo
Valencia, Carabobo, Venezuela

Sherali Zeadally
University of Kentucky
Lexington, KY, USA

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-23032-0 ISBN 978-3-319-23033-7 (eBook)
DOI 10.1007/978-3-319-23033-7

Library of Congress Control Number: 2017948868

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To the most important persons in my life, my wife, Raiza, and my daughter, Alexandra, whose sacrifice was essential to allow me to finish this work. I also dedicate this book to my parents who are no longer physically in this world but will live in my mind and heart until my last breath. Finally, but no less important, I cannot forget my friends, brothers and sisters, students, and coworkers who have supported me in my professional career.

Jesús Téllez

*To my wife, Borrara; my daughters, Zobia
and Zofia; and my parents.*

Sherali Zeadally

Preface

In the last two decades, we have seen significant technological advances in computing, networking, storage, and processing technologies. All these advances have led to the emergence of various types of networks, all kinds of user applications, and a wide range of computing devices whose costs keep decreasing while their performance keeps improving. These new capabilities have paved the way for users to have the ability to access information anywhere, anytime from any personal computing device. Additionally, we have also witnessed the rapid development of mobile networking technologies and communication protocols that have accelerated the design and deployment of mobile payment systems (MPSs) which enable payments for services and goods from mobile devices using different methods, such as credit card payments, micro-payments, and digital coins. Security issues in these payment systems have become increasingly important for all parties involved (customers, merchants, banks, etc.) during their interactions. Security is one of the most important aspects that must be taken into consideration when designing, implementing, and deploying secure payment systems. It is essential to mitigate threats, vulnerabilities, and risks that affect such systems. While supporting secure payment transactions, high performance is also another major objective that must be met by any MPS even in the presence of constraints of portable devices, limited communication capabilities, and other limitations.

The main aim of this book is to present state-of-the-art research achievements and results in the field of MPSs. We expect this book to be a valuable and an authoritative reference for designers, developers, engineers, students, faculty members, and researchers who have a strong interest in mobile commerce and in particular mobile payment systems. We have organized this book into five chapters: “(1) Introduction”; (2) “Mobile Device Security”; (3) “Architectures and Models for Mobile Payment Systems”; (4) “Security in Mobile Payment Systems”; and (5) “Future Challenges and Opportunities.”

Mobile Payment Systems: Secure Network Architectures and Protocols is an in-depth literature review of recent research results obtained by experts and researchers around the world, along with the authors’ results in the area of MPSs. We present here a summary of the chapters in this book.

Chapter 1, “Introduction”, presents the basic and fundamental concepts related to MPSs. In this chapter, we give an overview of mobile commerce, mobile payment characteristics, existing mobile payment methods, mobile payment stakeholders, and technologies for mobile payments. The chapter further discusses the benefits and disadvantages of MPSs and the general entities that underpin such systems.

In Chap. 2, “Mobile Device Security”, we review the mobile devices currently available on the market that can perform a variety of tasks. We also discuss the operating systems (OSs) available on the market based on the requirements of mobile devices and the advantages and disadvantages of each OS. We further highlight some important differences between mobile device security and personal computer (PC) security to improve our understanding of mobile device security. The chapter also presents a threat model, which identifies the threats against MPSs, the resources to be protected, the features of the attackers, and the potential attack vectors. Finally, it highlights two main mechanisms that are used to avoid various kinds of threats for smartphones: intrusion detection systems and trusted mobile-based solutions.

In Chap. 3, “Architectures and Models for Mobile Payment Systems”, we review the mobile payment models that have been proposed in the literature in the last decade. We classify these models based on the features and technology mostly used by end users. The main goal of this classification is to help readers stay up to date with the state-of-the-art mobile payment models proposed in the literature based on their core features such as micro-payments, cryptographic technique (asymmetric cryptographic and symmetric cryptographic), technology used (short message service, biometric technology, radio-frequency identification (RFID) technology, near-field communication (NFC), 2-D barcode technology, and peer-to-peer technology), Session Initiation Protocol (SIP), communication restriction, mobile agent technology, and wireless application protocol.

Chapter 4, “Security in Mobile Payment Systems”, focuses on transaction security properties that must be satisfied by MPSs to ensure that all the information exchanged between the mobile payment user and the entity with which he/she is communicating is secure at all times during the payment transaction made using mobile devices. We present a brief review of the most commonly used cryptography schemes for secure communications among the parties involved. This chapter also presents a summary of the types of vulnerabilities and threats and their corresponding risks in an MPS environment together with relevant protection solutions. Furthermore, we discuss some obstacles that make the design of secure MPSs still a major challenge.

In Chap. 5, “Future Challenges and Opportunities”, we outline some of the challenges posed by MPSs which rely on new emerging technologies that offer attractive business opportunities. This chapter also discusses security challenges that must be addressed in order to establish a secure environment for ubiquitous mobile commerce (m-commerce). We also identify some of the challenges faced by users in MPSs due to their lack of payment options around their mental model development, usability issues, prepurchase anxiety, trust issues, ease-of-use, and support for routine purchases with mobile payments. We also discuss alternate cryptographic schemes such as elliptic curve cryptography and self-certified public keys and their applications to MPSs. This chapter also highlights opportunities offered by mobile cloud computing (MCC) and vehicular ad hoc networks (VANETs) in the design and development of MPSs.

We thank Simon Rees and Wayne Wheeler at the Springer office in London, United Kingdom, for their constant encouragement, support, and advice throughout the preparation of this book.

Valencia, Venezuela — Jesús Téllez
Lexington, USA — Sherali Zeadally

Contents