Chapter 23
Mobile Commerce Security and Its Prevention

Mona Adlakha
University of Delhi, India

ABSTRACT

Mobile commerce is the next generation of e-commerce, where payments and financial transactions can be carried out with utmost ease using handheld mobile devices. Mobile devices are at a higher security risk due to the large amount of critical financial and personal data available on it. The cause or consequence of these threats could be - malware and spyware attacks; multiple or incorrect m-Commerce payments; breaches due to unauthorized access or disclosure, unauthenticated transactions and risk due to the use of third party networks. This chapter discusses how to manage security risks in m-commerce by first identifying them and then discussing preventive measures for their mitigation. A continuous approach for risk prevention needs to be followed, reviewing the strategy according to the latest challenges. Various risk prevention and mitigation strategies can be adopted. Service providers must follow physical and digital security measures to protect consumer's business information. Independent auditing should ensure compliance with best practice security standards.

INTRODUCTION

Mobile commerce (m-commerce) refers to the buying and selling of goods and services through wireless handheld devices such as smartphones, tablets and PDAs. It is the next generation of e-commerce, where payments and financial transactions can be carried out with utmost ease, all under a user's fingertips. M-commerce is available anywhere you go, and at anytime, even if there is no internet, because the internet is available in your mobile phone. This makes it more convenient and accessible than e-commerce. Smartphone turns into a mobile payment device, where a consumer can keep his electronic record of transactions, avoiding the need to carry multiple credit cards and debit cards. Consumers can make payments and purchases when and where it suits them. The services and transactions available through m-commerce are vast. It is not just restricted to mobile banking (m-banking) and on-line purchasing. Services like retrieval of real-time weather reports, sport scores, flight and reservation information,

DOI: 10.4018/978-1-5225-2599-8.ch023

navigational maps, and stock quotes, also come under m-commerce. The resent technological advancements in handheld devices, wireless communication and the enveloping infrastructure, give users a comfortable environment for mobile commerce. The ease of use of these mobile devices comes with its own disadvantages. There are numerous security risks in m-commerce, which have varying impact. These risks can be due to risks inherent in – the mobile handheld devices (its hardware or OS), the mobile applications installed on the device, the e-commerce transactions, the wireless communication network being used and the cloud being used for data storage. The transactions can be performed over adhoc wireless networks (i.e. wireless trading outside an established computer network).

Thus, mobile adhoc networks are increasingly being used as a cost-effective mode of communication. On the other hand, there are a lot of implementation challenges in its applications. These networks are easily prone to serious network attacks, which make the customer's private resources vulnerable. There is a need for adequate guidelines for designing secure mobile commerce applications. Security issue surfaced in the design of these applications should be dealt with; else it would lead to inappropriate design of routing protocols used in mobile adhoc networks. The dynamic topology of the adhoc networks and the faster consumption of power in the mobile nodes can cause malicious activity to the customer's device. There are certain limitations in the mobile adhoc wireless networks as well.

The objective of this chapter is to discuss the management of security risks in mobile commerce. This includes identifying the possible risks and discussing some possible solutions and preventive measures for their mitigation. The next section discusses different aspects of m-commerce security research done in this area.

BACKGROUND

Throughout this chapter¸ the words customer, consumer, user refer to the user of the handheld mobile device like smart phones tablets and PDA (Personal Digital Assistant). Also, the word organization refers to the company or individual who plays a role in imparting an m-commerce service or is part of a transaction (discussed below).

Prior to understanding the security issues in m-commerce, we need to be aware of all the parties involved in providing m-commerce Services. The Position statement on mobile commerce, (Australian Communications Consumer Action Network (ACCAN), 2014) states that a single m-commerce transaction could involve: a) the consumer, b) the retail merchant whose service/ product is being used/purchase through the transaction, c) each party's bank, d) a credit card provider, e) a communications network provider, f) a mobile hardware manufacturer of the handheld device, g) a mobile operating system developer and h) a mobile application developer of the of the m-commerce app being used. A failure of an m-Commerce transaction might be attributed to any one of these parties involved in providing m-Commerce Services. This complicates matters as one can not single out the root cause.

Researchers have suggested many ways of categorizing security risks in m-commerce. A list of the top five mobile security threats are - loss of mobile devices, mobile application security, data loss on the device, malware and spyware attacks, theft of mobile devices (Actus Mobile Solutions Ltd.). Threat related to data being stored remotely in the cloud is also a cause of concern. A classification of risks related to mobile device are – device risks (like data storage, weak passwords, Wi-Fi hijacking, open hotspots, bandwidth hacking, Bluetooth spoofing and fuzzing) and application risks (trojaned apps, hidden malicious URLs, phishing, smishing, war texting) (Rhodes-Ousley, 2013). The powerful new