Chapter 14

Security Risks of Mobile Commerce

Ashish Kumar
Bharati Vidyapeeth College of Engineering, India

Rachna Jain
Bharati Vidyapeeth College of Engineering, India

Sushila Madan
Delhi University, India

ABSTRACT

Mobile commerce (m-commerce) is evolving as an alternative to E-commerce services. M-commerce is a type of e-commerce which emphasizes on the use of services on handheld devices. It is becoming very popular among users because of ease of connectivity and its usage. With increase in the demand, it becomes essential to provide security to the services used on mobile. The user is using the mobile devices to make their secure payments and transactions. It becomes essential to increase security layers in the m-commerce to provide privacy to the user. The security risks in m-commerce are increasing exponentially. This chapter investigates the security breaches and the solutions associated with the m-commerce. It also focuses on the network services and problem related with device and user authentication. Many algorithms are proposed to make the device and the transaction safe. It is compulsory to make m-payment method very safe and secure, so that user can trust m-commerce to use their sensitive personal information.

INTRODUCTION

M-commerce is a wide term used to refer the growing practice of conducting financial and promotional activities with the help of a wireless handheld device. It is basically e-commerce where users do their business through their mobile devices on Internet in B2B (business to business) or B2C (business to consumer) markets. It recognizes the transactions which may be directed using cell phones, personal digital assistants and other hand held devices and requires Internet access for its operations. M-commerce
allows user to directly do their business and shop directly anytime, anywhere with their smartphones. In today’s scenario, the numbers of mobile users are extending to billions as compared to desktops or laptops users. According to survey conducted by manufactures in 2014, it is observed that more than 1 billion Android devices were shipped. Based on survey and mobile device sales, one might think of emergent mobile industry and its customers. As the numbers of mobile users are cumulatively increasing m-commerce security is a major concern. It includes threat to personal and corporate security. Now a day’s most of the organisations provide mobile applications software to the customers for using their services. As of a survey conducted by Pew Research Centre in May 2013, 63% of the adult use their mobile phones to go online instead of laptops and desktops. It is primarily the responsibility of M-commerce promoters to provide a secure platform for its user, so that customer can trust m-commerce for making their secure and private online money transactions. M-commerce offers instant connectivity and services to the customers irrespective of their geographical location with proactive functionality. It must take the responsibility to secure user data, maintain security and privacy rules, so that more customers will be added to online business through m-commerce. Maintaining data security and privacy in M-commerce is an ongoing process with ever increasing overheads. Business through mobile is widely increasing because it is convenient to use, quick and easy, no need to carry cash and time saving. The concerns which averting it to be very popular are security and privacy, connectivity and Screen size. Security is directly proportional to inaccessibility. The NFS (Near Field Communication), Side loading are the technologies used for transferring data between devices, opening new challenges and threat for the m-commerce. Some of the risks and frauds that come with mobile commerce are access and payments based with fraudulent communications such as text message scams, security and accessibility issues.

The vulnerabilities which cause security hazards to the Desktop PC, all are now affecting the mobile device too. The operating system should be made closed rather open to make it more secure. As mobile OS gains popularity, there is tremendous growth in the malware and attacks on that platform. There are various popular mobile OS available in market like Android, Tizen, iOS, Symbian etc. Android was the first mobile operating system which was affected by a worm. The most popular and secure Mobile OS are also targeted by attackers like iOS which is considered to be virus free, is also under attack. Blackberry OS which considered being totally immune to malware attacks, has been detected with infections. The virus spread through Apps downloaded from third party and this virus leaks private information of the user. The high profile security attacks are found on mobile device like Reverse Heart bleed, ShellShock, Poodle and many more.

Features of Mobile Commerce Security

The mobile commerce security involves protecting device, network and transaction etc. It basically deals with all the intermediate which are involved between the customer and the services on mobile. The following are the features of mobile security which are to be considered when developing solutions (Rashad Yazdanifard & Mohamed Sayed, 2011):

- The m-commerce security solutions must be simple and usable. The customer must be able to customise or personalise the application as per requirement.
- The solution must be universal. It means that whatever environment is being used like one customer to another customer (C2C), or from a business to a customer (B2C) or between businesses (B2B), the security policy should not be changed or altered.