Security Issues of Smartphones Regarding M-Commerce

M

Salva Daneshgadeh
METU, Turkey

Nazife Baykal
METU, Turkey

Bugra Karabey
METU, Turkey

INTRODUCTION

The world of computing and networking are transforming from the traditional static model of the wired internet toward the anywhere-anytime available model of the wireless internet (Yang, Chen & Trappe, 2009). This rapid improvement of wireless and mobile technologies has opened new rooms for business opportunities which is called mobile commerce (m-commerce). Mobile commerce is defined as any transaction with monetary value that is conducted via wireless handheld devices such as mobile phone, smart phone and PDA.

Nowadays, m-commerce accounts for a considerable part of e-commerce. The potential growth of m-commerce is unarguably related to the growth in the number of mobile phone holders and in particular smartphone owners. Today's customers demand new devices, applications and services to perform their m-commerce activities in more effective and efficient manners. Smartphones can be seen as the crucial drivers of m-commerce adoption, because they have introduced new opportunities to search and buy goods and services. For example, smartphones enable in-app-purchase, in-app-advertisement and location-based-marketing in addition to traditional online purchasing through the Internet. Smartphones also enable new forms of business. However, these forms of business opportunities might be compromised by new security risks related to smartphones and wireless access networks. These security risks can be defined as customers' main concern when it comes to trust mobile transactions.

The aim of this study is to explain and analyze some major security risks regarding m-commerce and smartphone-based mobile commerce. The next section presents a background of mobile commerce followed by information on the importance of security in m-commerce, wireless application protocol and possible security attacks against smartphones. Subsequently, potential security risks in m-commerce and some tips to protect mobile phone users against these risks are presented.

BACKGROUND

Mobile commerce was introduced in Finland with the installation of Coca-Cola SMS-enabled vending machine in 1997. Customers could make mobile payment by sending a text message to the vending machine in order to perform mobile transactions. In the same year, the SMS-based mobile banking service was also introduced by Merita Bank in Finland. Then I-mode (a Japanese company) launched the first

DOI: 10.4018/978-1-4666-9787-4.ch103

mobile commerce platform in 1999. While most European and Asian markets had already started to use 3G in 2001, 3G was introduced in the U.S in 2003 (Niranjanamurthy, Kavyashree, Jagannath & Bhargava, 2012). As a result of which the adoption of m-commerce in North America took longer.

In general, m-commerce can be done in different ways: SMS, USSD, WAP, STK and NFC. SMS and USSD are the traditional forms of doing m-commerce. Currently, all of these technologies are available, but today's smartphones utilize STK and NFC technologies the most (Mikesell, 2012).

- **SMS:** The one-way push notification message for adverting, the wireless delivery mechanisms for downloads such as ringtones, and the two-way interaction messages such as asking the mobile operator about the remaining minutes by texting "MINUTE" to a specific number are the types of SMS-based m-commerce.
- **Unstructured Supplementary Service Data (USSD):** It creates a real-time connection that allows for true session-based communications by enabling the texting between a mobile phone and an application program in the network. It also provides push notification and two-way query demands.
- **Wireless Access Protocol (WAP):** Whereas WAP enables the access to the Internet by using XHTML (a variation of HTML for mobile web access), it does not enable the access to the mobile phone features.
- **SIM Application Toolkit (STK):** STK is a standard for GSM which defines how the SIM card should interact with the outside world. Applications can be built on the SIM card, and they request and receive information from the SIM card. They also enable user inputs and communications with external applications. Almost all mobile operators deploy STK for many applications. Currently, the USIM Application Toolkit (USAT) is used for 3G networks.
- **Near Field Communication (NFC):** NFC is a set of standards for smartphones and other wireless handheld devices which uses contactless radio communication to make money transactions and money transfers. It is usually used for micropayments; i.e. any transaction cost lower than $ 10.

THE IMPORTANCE OF SECURITY IN M-COMMERCE

Security is about preventing adverse consequences from the intentional and unwanted actions of others." (Bruce Schneier). For example, in m-commerce, a security risk can be considered the installation of an unauthorized application which can manipulate other applications in the client's smartphone.

According to a report by Goldman Sachs Group Inc., 535 million consumers around the world spent a total amount of $204 billion on m-commerce in 2014. The firm also predicted that this amount will have jumped to $626 billion by 2018. The ability to conduct mobile transactions can be seen as a double-edged sword. It can attract the attention of new customers. On the other hand, it can result in various security risks when participating in any kind of m-commerce. Additionally, this huge amount of transactions targets smartphones with more potential attacks. We believe that m-commerce practices cannot reach their ultimate goals without providing a reasonable level of security. Therefore, security should be regarded as an inseparable part of any m-commerce solution. As a result, it is absolutely essential to plan, organize, lead and control security models to ensure the security of all kinds of m-commerce practices.

In general smart phones are more vulnerable than traditional personal computers or laptops, which in turn makes m-commerce more vulnerable than e-commerce. Smart phones are usually on and with