LD Based Framework to Mitigate Threats in Mobile Based Payment System

Jitendra Singh, Dyal Singh Evening College, University of Delhi, New Delhi, India

ABSTRACT

Smartphones have deeply penetrated in modern lifestyle. Accordingly, usage has grown manifold in the area of social media, collaboration, and mobile-based payment. The security of smartphones is increasingly critical at the user end as well as at service provider’s end due to the involvement of monetary payments and personal information. Despite using a smartphone for mobile payments, strong security measures have not been put into place by a majority of users, particularly those involved with electronic payments. This article is an attempt to identify threats applicable to smartphones and classify them based on a broader category of threats. Existing vulnerabilities have been explored. In the light of the digital India campaign, security preparedness among Indian users has been assessed by carrying out a survey that reveals a poor level of preparedness among mobile users. Finally, the authors have proposed a lotus diagram (LD)-based framework to mitigate threats that can negatively impact mobile-based payment. The proposed method will greatly help in strengthening security and mitigating the threats for the user.

KEYWORDS

Mitigating Security Threats, Mobile Payment, Near-Field-Based Payment, Smartphone Security, Smartphones Threats, Smartphones Vulnerabilities, User’s Awareness

INTRODUCTION

Mobile phones are highly preferred due to their ease of portability and rich features (Singh & Chaubey, 2016). Now the smartphones are also equipped with powerful computational capabilities that are equivalent to that of personal computer (Goasduff & Forni, 2017). Random access memory (RAM) has reached to the tune of 2GB even in ordinary smartphones. Modern Smartphones are exceeding even 6 GB RAM, for instance, Samsung Galaxy C9 Pro, Oppo F3 Plus, Oneplus T5, etc. are the smartphones with 6GB of RAM or exceeding(www.amazon.in). All these smartphones are equipped with high computation processor such as quad core or octa core. Consequently, word processing, games, Internet etc. can be easily accessed by using the Smartphones.

In addition, existence of camera, microphone and earphone has further enhanced its utility in entertainment as well as in educational domain (Wu, Du, & Fu, 2014). Trend of using mobile phones during travelling or commuting has grown manifold (Dickinson et al., 2017). During tour Smart phones can assist the users in locating their destination including hotels, Airport, monuments, etc. Besides,
it is equally helpful in entertaining him and searching information related to the tour (Dickinson, et al., 2017). One can connect to his family and friend during tour at remote places and can share the information related to his well-being. Even more, health related information can be well shared and accessed from remote location (Farnham, et al., 2018).

Around forty four percent of world population is equipped with Smartphones and trend continues to grow. (https://www.statista.com/topics/840/smartphones/). According to Statista, around seventy five percent population of America is already equipped with smartphone by the year 2017 (https://www.statista.com). Despite of smartphone expansion in reach, density of mobile is not evenly distributed within the territory and across the world (Chen & Wellman, 2004). According to an estimate, payment using smartphone was around 450 USD and projected to reach around 1 trillion USD by the end of year 2019 (https://www.statista.com). Therefore, smartphones are also viewed as tool that will supplement the currency based present system to digital payment.

According to statistics, around 299 million Indians are equipped with smartphones which ranks India to third position among global ranking (https://www.statista.com). Trend continues to rise owing to continuous fall in the prices of mobile phones, affordable data usage plan and improvement in technical skill of users. According to an estimate, smartphones have gained the market since 2011, however, during 2014-16 they have witnessed sharp surge in smartphone ownership.

Now, mobile phones are equipped with the operating system such as Android, IOS, Windows, etc. (Kubi, Saleem, & Popov, 2011). Correspondingly, smartphones are now behaving similar to that of computer. Therefore, cyber-attacks that were applicable to computers are now also targeting smartphone (Tam, Feizollah, Anuar, Salleh, & Cavallaro, 2017). According to a report published by Cisco titling “Cisco 2017 annual security report,” it is outlined that growing usage of mobile in data access is hiking the risk factor of a network (Cisco, 2017). Growing usage of mobile has also increased the risk on users’ security. Importantly, user is scarcely aware related to the security of device (Khan & Hengartner, 2014). Ransomware and malware are continued to rise for the android based operating system (SecureWorks, 2016). According to the Dell report, malware and ransomware are targeting the mobile based user and encrypting the data or stealing the personal information stored in it. Afterwards, demanding huge ransom in order to normalize data encrypted or stolen by them (SecureWorks, 2016). Accordingly, question arises whether to pay or not to pay ransom (Everett, 2016).

Rest of the manuscript has been organized as: Section 2 describes about the motivation behind the present manuscript. Section 3 describes the various types of payment methods exist that needs the usage of smartphones. Section 4 describes the vulnerabilities in the Smartphones that may cause losses to the user. Section 5 introduces the various threats that can exploit the vulnerabilities of smartphone and can adversely impact users. Finally, we have proposed our framework that will greatly help in mitigating attacks occurring at various levels.

**MOTIVATION**

Motivation for this work has been derived from the variety of sources namely a) Usage of packet for transferring of data and voice. b) Rise in smartphone attack c) Increasing usage of Mobile services.

**Transmission of Data and Voice as Packets**

Prior to the implementation of long-term evolution (LTE), mobile service providers were using global system for mobile (GSM), cellular digital packet data (CDPD), and general packet radio service (GPRS) etc. Such networks have used proprietary protocol (Narang & Kasera, 2007). Consequently, users were offered restricted access of within their own network, as a result network remained secured and major attacks were not reported. However, with the adoption of LTE, mobile network providers have migrated to IP based network. Consequently, data as well as voice both are transmitted in the form of packets similar to that of legacy network-based packets. Threats and attacks that were applicable in legacy computer-based networks are now applicable to all stakeholders involved in mobile usage
Quest for Economic Empowerment of Rural Women Entrepreneurs in Tanzania: ICTs Leapfrog the Digital Divide
Ladislaus M. Semali (2012). Teaching Cases Collection (pp. 91-102).
www.igi-global.com/chapter/quest-economic-empowerment-rural-women/57989?camid=4v1a

The Digital Divide and the Emerging Virtual Therapeutic System
www.igi-global.com/chapter/digital-divide-emerging-virtual-therapeutic/38317?camid=4v1a