Providing Security for NFC-Based Payment Systems Using a Management Authentication Server

Ali Al-Haj and Mayyadah Adnan Al-Tameemi
Department of Computer Engineering, King Abdullah II Faculty of Engineering
Princess Sumaya University for Technology
Amman 11941, Jordan

***Abstract*—Recent models of mobile phones have been designed to offer many services such as mobile e-commerce, e-ticketing, e-payment, among many other services. Of a particular importance nowadays is the NFC-enabled mobiles in which the NFC technology allowed the integration of services from various applications into one single mobile. However, the EMV protocol, which is currently used to provide the required security for NFC-based payment systems, has two serious vulnerabilities between user payment devices and the merchants' point of sales which could lead to obvious risks for users. These two security vulnerabilities must be treated to secure NFC-based mobile payment transactions. In this paper a protocol is proposed to improve the security of EMV by adding a new security layer. The security provided by the protocol to EMV has been verified against major security attacks.**

Keywords-NFC-based payment systems; EMV protocol; mutual authentication; MAS.

1. INTRODUCTION

The Near Field Communication (NFC) is a wireless technology that facilitates conducting daily tasks through communication between NFC-enabled devices [1]. Nowadays, the NFC technology is playing a major role in different fields of our daily life. It has been successfully applied in various fields such as healthcare, education, location-based services, access control, financial transactions, social applications and entertainment [2]. In the financial sector, the NFC technology is expected to gain popularity especially in mobile-based payments [3]. As successful as they may appear, NFC-based mobile payment systems suffer from serious security flaws. To be specific, the Europay Mastercard and Visa (EMV) protocol, which is currently used to provide the required security for mobile-based payment systems, has two vulnerabilities which could lead to obvious risks for users of such systems [4]. The first vulnerability is that no mutual authentication exists between the point of sale and the user's payment device. The second vulnerability is that no encryption is made for the banking payment data while being transferred from the mobile device to the point of sale, and vise versa.

To provide the needed secured wireless environment for NFC-based payment systems, few protocols have been proposed in literature. These protocols employ different mechanisms to provide the required security properties which include mutual authentication, non-repudiation, confidentiality of banking information, integrity, and validity of banking data. In [5], an authentication center provides authentication to prevent the man-in-the-middle and replay attacks. Hash functions and asymmetric cryptography are used in this technique. The proposed protocol in [6] provides mutual authentication between point of sales and NFC Mobiles. In [7], two protocols have been proposed to ensure mutual authentication for NFC communications: NFCAuthv1 and NFCAuthv2 protocols. In [8], cloud computing is used to manage NFC transactions which leads to secured and flexible management. The study reported in [9] annuls the issues encountered in the EMV protocol and using a Cloud infrastructure and asymmetric cryptography. The proposed protocol in [10] is dedicated to secure payment transactions between the terminals and user payment devices (NFC bank cards). The protocol proposed in [11] overcomes the EMV vulnerabilities by providing remote communication between the NFC-based devices and an authentication server.

In this paper an effective protocol is proposed to improve the security of the messages exchanged in the EMV protocol. The proposed protocol is based on adding a new security layer called the 'Management Authentication Server (MAS)' while taking into consideration the constrained resources of the NFC-enabled devices. The MAS is responsible for providing management and authentication functions for the payment transactions, and for achieving mutual authentication between the NFC-enabled mobile device (M) and the Point of Sale machine (POS). Furthermore, the protocol offloads the verification of the POS authenticity and cryptogram generation from the mobile device (M) to the server (MAS). The protocol leverages the 4G or Wi-Fi interface of the NFC mobile device (M) to communicate remotely with the MAS via a secure channel (TLS). Additional features of the proposed protocol are: ensuring the validity of banking data that are not revoked and minimizing the use of public keys by using lightweight cryptographic operations. The remainder of this paper is organized as follows. Section 2 presents details of the proposed algorithm, while section 3 analyzes its performance with respect to the standard security requirements. Section 4 concludes the paper and suggests directions for future work.

978-1-5386-6147-5/18/$31.00 ©2018 IEEE