Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 705 – 711

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

A lightweight security protocol for NFC-based mobile payments

Mohamad Badra[a], Rouba Borghol Badra[b,]*

[a]*Zayed University, Dubai, UAE*
[a]*RIT, Dubai, UAE*

Abstract

In this work, we describe a security solution that can be used to securely establish mobile payment transactions over the Near-Field Communication (NFC) radio interface. The proposed solution is very lightweight one; it uses symmetric cryptographic primitives on devices having memory and CPU resources limitations. We show that our approach maintains the security of NFC communications and we further demonstrate that our solution is simple, scalable, cost-effective, and incurs minimal computational processing overheads.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Near-Field Communication (NFC); Key Exchange; Authentication; Eavesdropping; Relay Attack; Transport Layer Security (TLS).

1. Introduction

Over the last decade, we have witnessed a rapid emergence of mobile/wireless access and applications/services that have fueled the explosive growth in the number of mobile's users. Wireless communication technologies are paving the way for the development of innovative, interactive and smarter applications and architectures. Nevertheless, many of the emerging wireless services are prone to unauthorized access and eavesdropping are easier as compared to wired communication technologies because a) wireless data is transmitted over the air and usually there is no physical controls over the boundaries of transmissions[1], b) security features designed for wireless communications are sometimes poor, and c) attackers don't have to tap into the network (i.e., due the broadcast nature of radio propagation) to insert rogue wireless access points, increasing the potential for unauthorized access to the transmission[2].

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: mbadra@gmail.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.156

In this paper, we study the security of mobile payment systems that are based on short-range wireless communication technologies. In particular, we focus on Near-Field Communication (NFC)[3] that enables contactless transactions and messages' exchange between two devices at the range of few centimeters. In the NFC communication architecture, a range of devices such as smartphones can implement the NFC standard. The devices can be in active or passive modes. When in active mode, both devices can generate a Radio Frequency (RF) field and start data exchange (role of Initiator), and when in passive mode (e.g., tag or contactless card), only the active device can initiate communication sessions and the role of the passive device is called a target (e.g., ticket counter, code bar, etc.). NFC devices can operate in three modes: reader/writer (an active device communicates with a passive device), peer-to-peer (active devices communicate with passive or active devices) and optional card emulation modes (device emulates a passive element, such as a contactless card[4]).

NFC-enabled mobile devices allow a wide range of applications including, but not limited to, mobile contactless payment, mobile ticketing, information exchange, and access control. NFC-enabled devices and contactless Point-of-Sales (PoS) terminals execute payment transactions using communication protocols that are based on Radio-Frequency IDentification (RFID) standards such as ISO/IEC 14443[3].

Figure 1 shows the case of a mobile device that integrates with the NFC technology. This device is typically composed of various integrated circuits, an NFC interface and Secure Elements (SE). The communications between NFC devices are enabled over the NFC interface. This interface is composed of an NFC Contactless Front-end, an NFC antenna and an NFC controller. NFC-enabled devices incorporate SE to a) securely store confidential information such as user account information, and b) to connect to the NFC controller to perform secure proximity transactions with external NFC devices. The Single Wire Protocol (SWP) [5] is used as an interface between the SE and the NFC controller enabling the communications between the payment application installed on the SE and the contactless readers (e.g., POS) through the NFC interface. The host controller is the part of the NFC system that processes exchanged data and establishes connections between the NFC controller and the SE. The NFC controller is connected to the host controller through the Host Controller Interface (HCI), which is also used for the communication between the NFC controller and SEs over the SWP interface. The UICC uses the ISO 7816 Interface to exchange data to a remote server in the Network. This interface includes a set of Data Packet called Application Protocol Data Unit (APDU) [6] for reading, writing and exchanging data between the host and the UICC card.

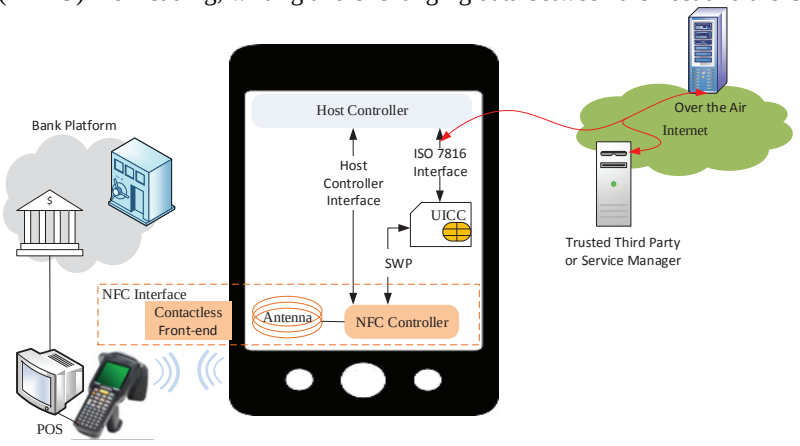

Fig. 1. Architecture of NFC-enabled mobile phone with UICC as a Secure Element.

The lower layers of NFC does not support link-level security primitives[7] which allows unscrupulous attackers to exploit vulnerabilities of eavesdropping and intercepting the data as discussed later or even having the device taken over completely by the attackers. Moreover, there are also concerns related to the privacy of the users because third parties are able to determine the current activities of the consumer and learn about user's behavior.

The rest of this paper is organized as follows. In Section 2 we discuss some approaches that have been recently proposed to protect the NFC-based mobile payments. In Section 3, we review the security issues of the NFC technology and we show its vulnerability to multiple attacks. Section 4 describe the design of our proposed solution