IDA-Pay: a secure and efficient micro-payment system based on Peer-to-Peer NFC technology for Android mobile devices

Luca Mainetti, Luigi Patrono, and Roberto Vergallo

Abstract:**The evolution of modern mobile devices towards novel Radio Frequency (RF) capabilities, such as Near Field Communication, leads to a potential for delivering innovative mobile services, which is still partially unexplored. Mobile proximity payment systems are going to enhance the daily shopping experience, but the access to payment security resources of a mobile device (e.g. the "Secure Element") by third party applications is still blocked by smartphone and Operating System manufacturers. In this paper, the IDA-Pay system is presented, an innovative and secure NFC micro-payment system based on Peer-to-Peer NFC operating mode for Android mobile phones. It allows to deliver mobile-to-POS micro-payment services, bypassing the need for special hardware. A validation scenario and a system evaluation are also reported to demonstrate the system effectiveness and performance.**

Index Terms:**NFC, Android, Micro-payments, Performance Evaluation.**

I. INTRODUCTION

Recently, mobile devices are playing a very important role in linking humans and networks. Currently, a mobile phone can be used to update Facebook status, check-in to physical places, share digital music, and more yet to come. In particular, mobile payments are receiving special attention from a number of business actors: bank institutions, telecom operators, shopkeepers, technology providers, and so on [1].

Mobile payments involve two different areas:

- the Mobile Remote Commerce, i.e. the buying and selling of goods and services through the use of the smartphone (or similar devices);
- the Mobile Proximity Payment, i.e. the using of the smartphone to enable proximity payments.

The adoption of Near Field Communication (NFC) technology in today's smartphones is essential for the delivery of mobile proximity payments. NFC follows exactly the Internet of Things (IoT) paradigm, as it is considered the double-click of the IoT[2]. Cisco has designed an infographic[3] that offers a simple example of how IoT will affect our everyday life. It states that by 2020, there will be 50 billion "things" connected to the Internet - everything from our body, car, alarm clock and even cows.

The special interest of Google's Android towards NFC is favoring the spread of smartphones with embedded NFC readers; such devices are becoming popular and they are going to play a fundamental role in people's life, as they allow to supply a wide range of ubiquitous applications such as: access control, consumer electronics, healthcare, information collection and exchange, loyalty and coupons, payments and ticketing.

Mobile phones create a lot of secure and convenient conditions for payment operations, e.g., battery, keyboard, screen, storage, and 3G network. In future, these smartphones will represent the personal electronic wallet (e-wallet) for most people replacing the current plastic credit cards.

However NFC payments are yet to attain to their market potential [4]. This is mainly because only Google's Android [5] has reached a significant share of the NFC mobile market. Moreover, only the Google Wallet mobile application supports NFC micro-payments in the US for Android mobile phones. Third party applications cannot take advantage of the security resources embedded in Android devices because Google Wallet is the unique application having privileged access to such resource, namely the "Secure Element" (SE). The SE is a special memory area where trusted applications can store and retrieve sensitive user information, such as the credit card number and the Card Verification Value (CVV) code. Furthermore, Google Wallet is limited to work with affiliated credit card issuers (e.g. MasterCard, Visa), so no chance is given to alternative payment ecosystems.

The research work summarized in this paper aims to develop an innovative mobile micro-payment system which can be easily used in alternative ecosystems to implement custom payment scenarios. Such system must ensure the same security level of traditional credit card payments, without the need of any hardware intervention (SIM or SD cards replacement) by smartphone's owners. That is, the user has only to download the application from the market and install it onto the device. Moreover, multiple payment networks (e.g. credit cards, money transfer, couponing) should be easily configurable. Finally, the interaction between the user and the system must be bi-directional, so the system can return rich collectible feedbacks to the user.

Manuscript received November 21, 2012; revised January 7, 2013.

The material in this paper was presented in part at the 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012), Split, Croatia, Sept, 2012.

Authors are with the Department of Innovation Engineering at University of Salento, Lecce, Italy (email: {luca.mainetti, luigi.patrono, roberto.vergallo}@unisalento.it).