

A SECURE MCOUPON SCHEME USING NEAR FIELD COMMUNICATION

HAN-CHENG HSIANG¹, HSIANG-CHOU KUO¹ AND WEI-KUAN SHIH²

¹Department of Information Management
Vanung University
Chungli 32061, Taiwan
{shc; noahk}@vnu.edu.tw

²Department of Computer Science
National Tsing Hua University
HsingChu 30013, Taiwan
wshih@cs.nthu.edu.tw

Received June 2008; revised November 2008

ABSTRACT. *Recently, the communication needs of mobile devices and their mobile users have rapidly grown because of the propagation of such communication and consumer electronics devices. In order to make the establishment of these communications simpler, the Near Field Communication (NFC) technology was created; it is very comfortable for the user as communication starts without any further configuration. This property makes the standard well suitable for the use with mobile coupons (mCoupons). Compared to paper-based coupons, mCoupons differ significantly by the fact that the unprotected data can be easily copied or modified by anyone without significant costs. A large number of uncontrolled copies of coupons may result in a significant loss for the business. In this paper, a secure mCoupon scheme is proposed which is not only secure but also efficient. The proposed scheme may satisfy all the security requirements needed in the mCoupons system using NFC technology.*

Keywords: Near field communication, NFC, mCoupon, mCommerce, Quadratic residue assumption

1. **Introduction.** Near Field Communication (NFC) is a short range high frequency wireless communication technology which enables the exchange of data between devices at about a decimeter distance [9]. The communication always happens between an NFC initiator and an NFC target. The active device can play both roles, whereas a passive device is always the NFC target. The initiator sends requests to the target, the target answers these requests. Two NFC devices start their communication by bringing them closely together (touching). The touching of the components is seen as a declaration of intention from the user.

Coupons are a common and well-established way of marketing. Companies use this means to establish consumer relationships, or to reward the consumer for looking at their advertisement, or out of other reasons to improve their business. We can classify the coupons into two types. The first is called free coupons, which is provided freely by the companies merely for the purpose of sales promotion. For example, the coupons on the conventional newspapers, advertising sheets, or magazines. The second type is called pay-coupon. The consumers can get the pay-coupon only after they have already bought some goods and have paid. They then can use these coupons to trade more discounted goods, services, or to get valuable gifts. There should be some protection measures when