A Simple and Secure Mobile Coupons Scheme

Han-Cheng Hsiang
Department of Information Management
Vanung University
she@vnu.edu.tw

ABSTRACT

This paper describes a simple and secure mobile coupons scheme. Coupons are available as paper-based coupons or electronic coupons. It is a very common way for companies to promote their products or services. Recently, the propagation of mobile devices communication and consumer electronics devices, hence, the communication needs of mobile devices and their mobile users have rapidly grown. To make the establishment of these connections simpler, the Near Field Communication and Bluetooth technology was very comfortable for the user as communication starts without further configuration. This property makes the standard well suitable for the use with mobile coupons. Compared to paper based coupons, mobile coupons differ significantly by the fact that unprotected data is easily copied or modified without significant costs by anyone. In some real events, we found that uncontrolled copies of coupons may result in a significant loss. Hence, we propose a secure mobile coupons scheme which not only simple, secure but also effective for only use few hash functions. The proposed scheme may satisfy the essential security requirements needed in a mobile coupons system using NFC or Bluetooth technology.

Keywords: Near Field Communication, Bluetooth, mobile coupons, mCommence

1. Introduction

Near Field Communication (NFC) is a short range high frequency wireless communication technology which enables the exchange of data between devices over about a decimeter distance [8]. The technology is supported by most leading manufacturers of mobile consumer electronics. NFC can be used for communication between two active devices or between an active and a passive device. It is expected that in the future most of the mobile devices will be equipped with an NFC interface. Many applications are possible, such as: mobile ticketing in public transport, smart poster, mobile payment, electronic tickets, Bluetooth pairing, travel cards, mobile commerce and so on.

The communication always happens between an NFC initiator and an NFC target. The active device can take over both roles, whereas a passive device is always the NFC target. 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. Recently the Internet is getting easier and faster to use, electronic coupon (e-coupon) distribution is becoming a more popular advertising technique. The significant difference of a system of electronic coupons from paper-based coupons is the fact that issue and pay in are performed without human interaction. Attacks can therefore easily be mounted in an automated way. In 2005, Blundo et al. discussed some real examples about how multiple cash-in of e-coupons generated respectable loss [2]. In the published papers [2-3, 9-11], e-coupons are distributed by email or can be collected from web pages and are paid-in directly at the online store of a merchant. The core objective of the e-coupon security system will cause the attacker yield more than it gains when his successful attack.

The mobile coupons are coupons that can be collected and stored on a mobile device which can be carried to a cashier by the client. Existing NFC-based coupon or ticketing solutions mostly require active NFC-terminals or rarely provide any protection of the delivered information. In [4] proposed a mobile coupons system, where the client uses an NFC-enabled device. The user receives a mobile coupon from a passive NFC target and cashes it in at a cashier (the merchant also using the NFC interface). Their system included two schemes—simple mobile coupon protocol and advanced mobile coupons protocol. But, the simple protocol cannot prevent copying of the coupons and cannot verify the client’s identification for client’s authentication. In 2007, [1] proposed a system of secure virtual coupons using NFC technology. Their scheme was already implemented in a side-channel protected AES module and protected against unwanted copies or deliver to others. However, this study found the common weakness still exist in the previous schemes, the backend server and database searching privacy keys and secret keys in a brute way. This significantly impacts are less efficiency for cashing and
authentication. In this paper, we propose a secure mobile coupons scheme which not only simple, secure but also effective for only use few hash functions. The proposed scheme can satisfy all the security requirements needed in a mobile coupons system using NFC and Bluetooth technology.

This paper is organized as follows. In section 2, we will show some security issues about NFC and mobile coupons, which must be considered for the integrity of the proposed protocol. In section 3, describes the proposed secure mobile coupons scheme that not only simple, secure but also effective for only use few hash functions. Section 4 makes the security analysis of the proposed method. Section 5 compares the performance of the proposed scheme with the existing systems. Finally, several concluding comments are included in the last section.

2. Security Considerations of NFC and mobile coupons

There is some security issues about NFC, Bluetooth and mobile coupons, that must be considered for the integrity of the protocol flow described in next section. The main characteristic of NFC is that it is a wireless communication interface, although the communication range of NFC is limited to about 10 centimeters, NFC alone does not ensure secure communications. In 2006, Haselsteiner and Breitfuß described different possible types of attacks [7]. NFC offers no protection against eavesdropping and is also vulnerable to data modifications. Due to unprotected data on mobile coupons can be easily copied or modified without significant costs. In 2007, [4] also described different possible types of security attacks on mobile coupons. There are a couple of security issues that have to be addressed: multiple cash-in, unauthorized generation, manipulation and unauthorized copying. The detail attacks are described as below:

Eavesdropping: When two devices communicate via NFC they use RF waves to talk to each other. An attacker could use an antenna to receive the transmitted signals. The distance from which an attacker is able to eavesdrop the RF signal depends on numerous parameters, but is typically a small number of meters. Besides, eavesdropping is extremely affected by the communication mode. A passive device, which does not generate its own RF field, is much harder to eavesdrop on than an active device.

Data modification: The attacker wants the receiving device to actually receive some valid, but manipulated data. The feasibility of this attack highly depends on the applied strength of the amplitude modulation. Data destruction is relatively easy to realize. One possibility to perturb the signal is the usage of an RFID jammer. The NFC devices could check the RF field while they are sending; it is possible to detect it.

Unauthorized generation: An attacker shall be able to issue his own new valid mobile coupons.

Unauthorized copying: An attacker shall can produce a valid copy of mobile coupons and cash it in.

Manipulation: An attacker can manipulate mobile coupons, and they are valid after a manipulation.

Multiple cash-in: An attacker shall be able to use the same mobile coupons multiple times.

Some of these features are optional; the features depend on the system requirements. The next section we present a secure mobile coupons system which implements countermeasures against the mentioned security threats where some of the features can be omitted.

3. Proposed Scheme

We propose a secure mobile coupons scheme that is resistant to above attacks. The secret key is known by the issuer and the cashier. Only authorized issuers can produce valid mobile coupons (knowing the correct key). The cashier can verify the mobile coupons with the secret key.

In the subsection, we first define the notations in the protocol. Then, we present the secure mobile coupons scheme.

3.1 Notations and definitions

In the scheme, the cashier and the issuer are controlled by the same organization, i.e. that the same party provides the issuer and the cashier with the necessary information to issue and to verify the mobile coupons. The notations used throughout this paper can be summarized as follows:

• Client $C_i$: a user who wants to get a coupon for a particular product or service and he has a mobile device such as PDA, and mobile phone with an NFC initiator where the mobile coupons can be stored.

• Issuer: is a passive NFC target attached to an advertising poster or an advertisement in a newspaper generates and allows issuing a mobile coupons on a request from an NFC initiator device.

• Cashier: is a terminal with an NFC interface to proof the validity of the mobile coupons and provides the goods or service for $C_i$.

• $ID_c$: the identity of $C_i$.

• $ID_i$: the identity of the issuer.

• $e$: the permanent secret key of the issuers and the cashiers.

• Offer: is an additional informative data of a mobile coupons, e.g. about the type, issuing time and

2009 Conference on Information Technology and Applications in Outlying Islands
validity range of the coupon.

\( h() \): a cryptographic hash function.

### 3.2 Secure mobile coupons scheme

Initially, the client has to install a coupon software, managing the mobile coupons on his mobile device. The cashier and all the issuers (NFC targets) share a secret key \( x \) and an Offer. This means, that a secret key \( x \) and an Offer has to be stored in its memory. The secret key \( x \) and Offer has also to be stored by the cashier, which needs it to verify the validity of the mobile coupons. Then, the cashier and all issuers each stores a sorted table consisting of \( h(ID) \) and the corresponding secret key \( x \) and Offer of all the issuers.

The cashier using \( h(ID) \) as the primary sorting key in the cashier database. The mobile device of the client sends his ID that is also used as a part of the issued mobile coupons. The authentication is delayed and verified at cash-in.

There are two phases in our scheme – the issuing phase, the cashing and authentication phase. We show it as follows.

**Issuing phase:**

The initialization of the mobile device can be done automatically without necessary user interaction during the installation procedure of the coupon software on the mobile device. The client has to bring his mobile device, provided with the coupon software, close to the issuer to enable the NFC functionality. The phase works as follows:

1. The client “touches” the issuer and sends a request and \( ID_c \) for the issuer to get a valid mobile coupon.
2. The issuer computes performs the following computations:
   
   \[
   V = ID_i \oplus h(ID_i).
   \]
   
   \[
   C = h(h(ID_i) \oplus x \oplus \text{Offer}).
   \]
3. The issuer sends mobile coupon \( M = \{ V, C \} \) to the client, then client save \( M \) in its memory. The valid mobile coupon consists of the issuer’s ID, the exclusive result of the client’s ID and the hash value of the issuer ID and \( C \) (the hash value). Figure 1 shows the issuing phase for the secure mobile coupons scheme.

**Cashing and authentication phase:**

When the client wants to use the coupon service, he takes the mobile coupons to the cashier, the following operations will perform:

Step 1: The client’s mobile device sends \( ID_c \) and the mobile coupon \( M = \{ V, C \} \) to the cashier.

Step 2: After \( ID_c \) and the mobile coupon \( M \) is received, the cashier performs the computation:
   
   \[
   \text{computes } ID_c \oplus V \text{ to obtain the value } h(ID_i).
   \]

Step 3: After obtaining the values of \( h(ID_i) \), the cashier using binary search and using \( h(ID_i) \) as the searching key to seek for the secret key \( x \) and Offer in the sorted table. The cashier then compares the each \( h(ID_i) \) to \( h(ID) \). Then can get the secret key \( x \) and Offer.

Step 4a: After obtaining the secret key \( x \) and Offer, the cashier according to \( ID_c \) and Offer to check the cashed mobile coupons record of the cashier database whether exists. If it exists, the cashier would reject the request. Otherwise, run the step 4b.

Step 4b: The cashier check Offer to judge whether the cashing date is valid. If it is invalid reject the request. Otherwise, the cashier computes \( h(h(ID_i) \oplus x \oplus \text{Offer}) \) to get \( C_f \). If the computed result \( C_f \) equals the received \( C \), the cashier accepts the client’s cashing request. Otherwise, rejects the cashing request.

Step 5: The cashier stores the \( ID_c \) and the corresponding cashed in mobile coupons record to the cashier’s database, and then sends the Bonus message to the client.

**Figure 1:** The issuing phase for the secure mobile coupons scheme
The step 4a is only necessary, if copying protection is required. In Figure 2, the phase needed for the secure mobile coupons system is shown.

**Figure 2:** The cashing and authentication phase for the scheme

---

### 4. Security Analysis

As described in above, NFC by itself cannot protect against eavesdropping and any kind of data modification attack. It is important to note that data transmitted in passive mode is significantly harder to be eavesdropped on. Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack. In our scheme, the cashier and all the issuers (passive NFC target) share a secret key. The shared secret key \( x \) can be used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data [5]. Hence, our scheme could protect against eavesdropping and any kind of data modification attack.

Copy protection is guaranteed because the client has to authenticate itself at issuing as well as at cashing-in. The cashier can use step 4a in cashing and authentication phase to verify the client’s ID whether multiple cash-in to resist the unauthorized copying and the multiple cash-in attack. If any client uses the same mobile coupon or a valid copy of a mobile coupon will be found and reject his request in step 4a and step 4b of cashing and authentication phase. As the client’s ID is bound to the client’s mobile device, a successful verification of both authentications implies that the same mobile device was used for issuing and cashing-in.

Furthermore, when an attacker shall be able to issue his own new valid mobile coupons or he wants to manipulate mobile coupons to get a valid mobile coupon. But the secret key is only shared by the cashier and all the issuers, the mobile coupons database only used by the cashier. The attacker cannot know the secret key from the mobile coupon and cannot access the mobile coupons database. Therefore, the proposed scheme can resist the unauthorized generation and manipulation attack.

---

### 5. Performance Analysis

In this section, we summarize some performance issue of our scheme. We compare the performance of our system with others, Aigner et al.’s scheme [1] and Dominikus, Aigner’s scheme [4]. The comparisons of the number of rounds among the three schemes are shown in Table 1. Here, for clarity, we assume that there are \( m \) issuers and \( n \) clients in each scheme.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuing phase</strong></td>
<td>4 rounds</td>
<td>4 rounds</td>
<td>2 rounds</td>
</tr>
<tr>
<td><strong>Cashing and authentication phase</strong></td>
<td>5 rounds</td>
<td>4 rounds</td>
<td>2 rounds</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>9 rounds</td>
<td>8 rounds</td>
<td>4 rounds</td>
</tr>
</tbody>
</table>

From Table 1, it appears that our scheme is more efficient than Aigner et al.’s [1] and Dominikus et al.’s [4] schemes in round efficiency. In our scheme, issuers and cashiers share a same secret key. The total rounds in the proposed scheme are four times, whereas the Aigner et al.’s scheme is nine times rounds and Dominikus et al.’s advanced scheme is eight times rounds. In the two schemes, cashier’s database stores \( m \) secret keys for mobile coupons verification and \( n \) public keys for client’s authentication. Each client takes to the mobile coupon to the cashier. The cashier needs to search the records in database and PKI server when each client and mobile coupon authentication. This will increase more computational load in their system. Also from Table 1, it appears that our scheme is same efficient with Dominikus et al.’s simple scheme [4]. However, Dominikus et al.’s simple scheme not only need store \( m \) secret keys in cashier’s database for mobile coupons verification but also cannot verify the client’s identification for client’s authentication. It concludes that our scheme is more efficient than the other three schemes.

---

### 6. Conclusions

2009 Conference on Information Technology and Applications in Outlying Islands
Near Field Communication (NFC) technology allows for communication between active and passive devices, with one and the same interface. NFC is very comfortable for the user as communication starts without any further configuration. In combination with the expected market penetration and the possibility of high volume production of secure passive tags, NFC is the optimal choice for the communication standard for the proposed system of secure mobile coupons. In this paper, we have addressed these security threats about NFC, Bluetooth and mobile coupons. Therefore, we presented a simple and secure mobile coupons scheme that is protected against eavesdropping, data modification, unauthorized copying, multiple cash-in, and unauthorized generation and manipulation. In the secure mobile coupons scheme, we can use NFC in combination with inexpensive passive tags is used or Bluetooth communication to prevent attacks on a commerce application. Whereas the above mentioned mobile coupons systems, our scheme is simpler and more effective.

References