International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.131-138
http://dx.doi.org/10.14257/ijsia.2013.7.5.11

Efficient mCoupon Authentication Scheme for Smart Poster Environments based on Low-cost NFC

Sung-Wook Park* and Im-Yeong Lee*

**Department of Computer Software Engineering Soonchunhyang University, Asan-si, 336-745, Republic of Korea*
{swpark, imylee}@sch.ac.kr

Abstract

Recently, smart devices for various services have been developed using converged telecommunications, and the market for near field communication (NFC) mobile services is expected to grow rapidly. This property makes the standard suitable for mobile coupon applications. However, mCoupons differ significantly from paper-based coupons because unprotected data can be easily copied or modified without significant cost by anyone. A high number of uncontrolled copies of coupons can result in a significant loss. In this paper, we proposed a secure mCoupon authentication scheme that is protected against illegal use in smart poster environment based on low-cost NFC to using limited resources.

Keywords: *mCoupon, NFC, HORS, Light-weight Authentication, Smart poster*

1. Introduction

Near Field Communication (NFC) is a short-range wireless communication standard defined in the ISO/IEC 18092 standard[9]. It is expected that in the future, most of the mobile devices will be equipped with an NFC interface. NFC works at 13.56 MHz and can be used for communication between two active devices or between an active and a passive device. NFC services can be used as a payment method, ID card, coupon, and so on. mCoupons differ significantly from paper coupons because unprotected data can be easily copied or modified without significant cost by anyone. However, a large number of uncontrolled copies of coupons could result in a significant loss. The remainder of this paper is organized as follows. Section 2 analyzes the NFC-based mCoupon scheme. Section 3 analyzes the security requirements of NFC mobile environments and mCoupon. Section 4 proposes a secure mCoupon authentication scheme for NFC mobile environments. Section 5 presents our analysis of the proposed scheme and its security requirements, and Section 6 concludes the paper.

2. Related Work

In this chapter, we describe the NFC mCoupon related scheme and OTS(One-Time Signature) scheme.

2.1. NFC mCoupon

In 2007, Dominikus and Aigner described possible types of security attacks on mCoupons [1, 5]. They also proposed a related scheme; however, their scheme was inefficient because of high computation cost and high traffic. In 2009, Hsiang proposed a new hash-based scheme for solving the Dominikus scheme [6]. This scheme was

ISSN: 1738-9976 IJSIA

efficient because it used hash to perform most of the computation, but an attacker could collect the ID of a legal user for malicious purposes and generate illegal coupons using groups of collected IDs.

2.2. OTS

One-time signature schemes, proposed by Lamport and Rabin, were among the earliest signatures, based on the idea of committing secret keys via one-way functions. For more than 25 years, variants of Lamport and Rabin's schemes have been proposed and investigated by many researchers. Motivated by the applications of signatures to stream authentication and broadcast authentication, Perrig [7] proposed a one-time signature called "BiBa," which had the advantages of fast verification and short signature (BiBa perhaps has the fastest verification of all previously known one-time signature schemes). The disadvantage of BiBa is, however, that the signing time is longer than in other previous schemes. Reyzin and Reyzin [8] proposed a new one-time signature, HORS (Hash to Obtain Random Subset). HORS improves on the BiBa scheme with respect to the overhead necessary for verifying and signing, and reduces the key and signature sizes. This makes HORS the fastest one-time signature scheme currently available.

3. Security Threat

In addition to protecting the data on mCoupons, an NFC mobile coupon service should provide an efficient, secure service, even in an environment with limited devices, to comply with basic security requirements. Therefore, an NFC-based mCoupon scheme should protect against the following security threats [9].

- **Man-in-the-Middle Attack**: Sun *et al.*, stated, "The role of NFC is to support the physical properties of proximity communication. Therefore, DoS Attack and MITM (Man-in-the-Middle) Attack in NFC communication are close to impossible" [2]. However, entity authentication is not performed during the first communication between NFC devices. Therefore, DoS and MITM attacks are possible during NFC communications.

- **Eavesdropping**: NFC communication usually occurs between two devices in close proximity, usually no more than 10 cm apart. The main question is how close an attacker needs to be located to retrieve a usable RF signal. Unfortunately, there is no easy answer because the distance may depend on the following parameters, among others [3]:
  . quality of the attacker's receiver
  . quality of the attacker's RF signal decoder
  . setup of the location where the attack is performed (including barriers such as walls or metal, and the noise characteristics of the floor)
  . power emitted by the NFC device.

- **Data corruption/modification**: Stored data could be deleted or corrupted and could no longer usable. In other cases, it could be modified to produce fake transaction information.

- **Unauthorized generation**: An attacker could issue his own new valid mCoupons.

- **Unauthorized copying**: An attacker could produce a valid copy of an mCoupon and cash it in.

- **Manipulatio**n: An attacker could manipulate mCoupons, and they could remain valid after manipulation.

- **Multiple cash-in**: An attacker could try to use the same mCoupon multiple times.

4. Security Requirements

The proposed scheme needs to address the security threats that affect NFC mCoupon environments (reviewed in Section 3). In addition, the proposed scheme needs to perform efficiently in a limited device environment and fulfill all the basic security requirements [1, 4].

- Multiple Cash-In: An attacker should not use the same mCoupon multiple times.
- Manipulation: mCoupons should not remain valid after a manipulation.
- Unforgeability: Only issuer can offer valid e-coupons, any other entities cannot forge them.
- Preventing Unauthorized Generation: An attacker cannot issue his own mCoupons.
- Confidentiality: An attacker should not be know the shared key generated by the legal object.
- Efficiency: mCoupon should be computationally efficient in a limited device environment.

5. Proposed Scheme

This paper suggests a secure mCoupon authentication scheme that is protected against illegal use in smart poster environment based on low-cost NFC to using limited resources. The proposed scheme consists of a coupon issuing phase and commodities exchange phase as follows.

5.1. System Parameters

The system parameters in the proposed method are as follows.

- $*$: object (*C*: Client, *I*: Issuer, *A*: Cashier)
- ID_* : ID that verifies the identity of *
- IDS_*^m: random *ID* value of *
- *m* : count value of hash chain
- *Offer* : additional mCoupon data, e.g., type, issuing time, and validity range of the coupon
- *h()* : cryptographic hash function
- *f()* : cryptographic hash function
- *x* : the permanent secret key of the issuers and cashiers
- *Rot()* : Rot function

Rot(x, y) is defined to left rotate the value of x with w(y). w(y) is hamming weight of y.

5.2. Lightweight mCoupon Authentication Scheme

5.2.1. Issuing Phase

For a user wanting to use the NFC mCoupon service, the coupon is issued in the following manner.

Step 1: The user installs the coupon service software on their mobile. Using this software, the user downloads the mobile *ID* from the CA (Certification Authority).

Step 2: The client transmits the $IDS_C{}^m$ (m times hashed *ID* value) to the issuer.
$C : IDS_C{}^1 = h(ID_C), IDS_C{}^2{=}h(IDS_C{}^1), \dots , IDS_C{}^m = h(IDS_C{}^{m-1})$
$C \rightarrow I : IDS_C{}^m$

Step 3: The issuer computes the following:
$I : V = IDS_C{}^m \oplus ID_T$
$I : C = IDS_C{}^m \oplus x \oplus Offer \oplus \ n_z$

Step 4: The issuer sends the mCoupon $M = \{V, C\}$ to the client, then the client saves *M* in memory. Issuer is update to seed value n_1 using rot() function. By update of seed value, The coupon is safe from unauthorized generation by attacker.
$I \rightarrow C{:}M{=}V{,}C$
$n_1(seeed)\ update$
$n_1{=}seed$
$n_2{=}rot(n_1{\oplus}x,\ n_1)$
$n_3{=}rot(n_2{\oplus}x,\ n_2)$
$n_z{=}rot(n_z{\oplus}x,\ n_{z-1})$

5.2.2. Cashing and Authentication Phase

When the client wants to use the coupon service, he takes the mCoupon to the cashier and performs the following operations:

Step 1: The client's mobile device sends mCoupon $M = \{V, C\}$, value of hash chain *m,* and the identity of the client ID_C to the cashier.

Step 2: After the message ID_C, *M*, and *m* are received, the cashier computes $IDS_C{}^m = h(IDS_C{}^{m-1})$ and $ID_T = IDS_C{}^m \oplus V$ to obtain $IDS_C{}^{m}$' and ID_T'.
$A : IDS_C{}^1 = h(ID_C), IDS_C{}^2{=}h(IDS_C{}^1), \dots , IDS_C{}^m = h(IDS_C{}^{m-1})$
$A : ID_T = IDS_C{}^m \oplus V$

Step 3: The cashier verifies the integrity of the mCoupon value *C* using the secret value(x and seed table) of identity of the issuer. The next phase proceeds as for the general mCoupon scheme.
$A : C{=}\ C\ ?$

5.3. mCoupon Scheme based on HORS

5.3.1. Issuing Phase

For a user wanting to use the NFC mCoupon service, the coupon is issued in the following manner.

Step 1: The user installs the coupon service software on their mobile. Using this software, the user downloads the mobile *ID* from the CA (Certification Authority).

Step 2: The client transmits the ID_C to the issuer.
$C \rightarrow I : ID_C$

Step 3: The issuer computes the following:
$I : V = ID_C \oplus h(ID_i)$
$I : h = h(V)$
$I : h(V) = h_1 \| h_2 \| \ldots \| h_k$
$I : Sign(V) = (s_{i1}, s_{i2}, \ldots, s_{ik})$
$I : C = h(h(IDi) \oplus x \oplus Offer)$

Step 4: The issuer sends the mCoupon M = {IDC, V, Sign(V), C} to the client, then the client saves M in memory. The valid mCoupon consists of the issuer's ID, the exclusive result of the client's ID, the issuer ID, and C (the hash value).

5.3.2. Verifying Signature Phase

When the client wants to use the coupon service, he takes the mCoupon to the cashier and performs the following operations:

Step 1: The client's mobile device sends the mCoupon $M = \{ID_C, V, Sign(V), C\}$ to the cashier.

Step 2: After the message *M* is received, the cashier computes the following to obtain the value v_k.
$A : h(V) = h_1 \| h_2 \| \ldots \| h_k$
$A : h_i = i_j,\ 1 \leq j \leq k$
$A : f(s_1) = v_1, f(s_2) = v_2, \ldots, f(s_k) = v_k$
$A : h(ID_i)' = V \oplus ID_C$

Step 3: The cashier verifies the integrity of mCoupon value *C* using the identity of the issuer. The next stage proceeds in a manner similar to that in the general mCoupon scheme.
$A : h(h(ID_i)' \oplus x' \oplus Offer) = C\ ?$

6. Analysis of Proposed Scheme

The proposed scheme satisfies the following requirements.

- Multiple Cash-In: An attacker is unable to use the same mCoupon multiple times because of the authentication phase of database.

Table 1. Analysis of the Proposed Schemes

		Aigner	Dominikus	Hsiang	Proposed Scheme 1	Proposed Scheme 2
Authentication		△	△	△	○	△
		ID based	ID based	ID based	Hash ID based	ID based
Multiple Cash-In		○	○	○	○	○
		DB based	DB based	DB based	DB based	DB based
Integrity (Digital Signature)		x	○	x	x	○
		PKI based (be able to attack)	PKI based	no have function	no have function	HORS based
Efficiency		x	x	△	○	△
		Exponential based	Exponential based	Hash based	Bit based	Hash based
Computation Quantities	Registration	1M+1E	2M+1E	2H	5⊕	tH
	Authentication	1M+1E	2M+1E	2H	4⊕	tH
Traffic	Registration	4rounds	4rounds	2rounds	2rounds	2rounds
	Authentication	5rounds	4rounds	2rounds	2rounds	2rounds

○ : offer, secure, △ : usually-offer, × : non-offer, insecure
H: hash algorithm; E: symmetric key cryptography; U: public key cryptography; t: security level

- Manipulation: mCoupons do not remain valid after a manipulation of attacker by update phase of NFC tag.
- Preventing Unauthorized Generation: An attacker cannot issue his own mCoupons. The proposed scheme protects the legal user using the hash chained to the identity RC of the client.
- Efficiency: The proposed method is very efficient because it uses only simple hash operations and bit operations.
- Non-repudiation: Non-repudiation is ensured by the signature generated by the HORS method
- Confidentiality: An attacker does not know the shared key x generated by the legal object.

7. Conclusions

Developments in IT technology are leading to the availability of a wide range of services based on personal information. Accordingly, a variety of authentication technologies have emerged to protect personal information. However, the efficiency and payment information protection of these technologies must be guaranteed if NFC-based mCoupon services are to be widely used. In this paper, we proposed an enhanced secure mCoupon for the protection of a user and service provider in NFC-based mCoupon services environments. Our scheme satisfies the necessary requirements; therefore, our scheme could be effectively applied in an NFC mCoupon environment. However, since we do not have the source code of the proposed scheme, it is difficult to directly compare computational times or other numerical measures. In future work, we will compare our proposed method with previous models through an implementation of proposed scheme.

References

[1] M. Aigner, S. Dominikus and M. Feldhofer, "A System of Secure Virtual Coupons Using NFC Technology", Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), **(2007)**, pp. 362-366.

[2] S. H. Lim, J.W. Jeon, J. I. Jin and O. Y. Lee, "Study on NFC Security Analysis and UICC Alternative Effect", Korea Information and Communications Society, **(2011)**.

[3] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)", Workshop on RFID Security RFIDSec, **(2006)**.

[4] C. C. Chang, C. C. Wu and I. C. Lin, "A Secure E-coupon System for Mobile Users", IJCSNS International Journal of Computer Science and Network Security, vol. 6, no. 1, **(2006)**.

[5] S. Dominikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), **(2007)**, pp. 421-428.

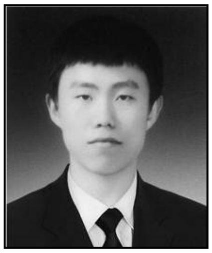
[6] H. C. Hsiang and W. K. Shih, "Secure mCoupons Scheme Using NFC", International Journal of Innovative Computing, Information and Control, **(2009)**, pp. 3901-3909.

[7] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol", Proceedings of the 8th ACM conference on Computer and Communications Security, **(2011)**.

[8] L. Reyzin and N. Reyzin, "Better than BiBa: Short One-time Signatures with Fast Signing and Verifying", ACISP'02, **(2002)**.

[9] Mobile NFC Technical Guidelines, GSMA, **(2007)**.

Authors



Sung-Wook Park received the B.S. and M.S. degrees in Depart of Computer Software Engineering from Soonchunhyang University, Korea, in 2011 and 2013, respectively. He is now a Ph.D. candidate in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include NFC Security, NTRU Cryptography, Ultra Lightweight Cryptography, etc.

Im-Yeong Lee is corresponding author. He received the B.S. degrees in Department of Electronic Engineering from Hongik University, Korea, in 1981 and the M.S. and Ph.D. degrees in Department of Communication Engineering from Osaka University, Japan, in 1986 and 1989, respectively. From 1989 to 1994, he had been a senior researcher at ETRI (Electronics and Telecommunications Research Institute), Korea. Now he is a professor in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include Cryptography, Information theory, Computer & Network security.