Journal of Korea Multimedia Society Vol. 20, No. 5, May 2017(pp. 782-790)
https://doi.org/10.9717/kmms.2017.20.5.782

해시 기반 NFC 모바일 쿠폰 프로토콜

이 재 동†

NFC Mobile Coupon Protocol Based on Hash

Jae-Dong Lee†

ABSTRACT

As most of the recent smart devices have NFC function the NFC mobile coupon will become one of the pervasive NFC applications. We need the secure NFC coupon protocols to issue and use NFC mobile coupon. In this paper, we analyze the security of the previous protocols and point out the problems of security. As the result of analysis, Premium M-coupon Protocol proposed by A. Alshehri and S. Schneider is the most secure but has unnecessary operations. We propose the Modified Premium M-coupon Protocol-1 with the unnecessary operations removed and show this protocol is secure by security analysis. Most of NFC mobile coupon protocols use the cryptography with the shared secret keys. We propose the Modified Premium M-coupon Protocol-2 without the shared secret keys and show this protocol is secure by security analysis.

Key words: NFC, NFC Mobile Coupon, NFC Mobile Coupon Protocol, Premium M-coupon Protocol, Modified Premium M-coupon Protocol

1. 서 론

NFC(Near Field Communication)는 13.56MHz 대역에서 동작하는 NFC 기능을 장착한 장치들(스마트폰, PDA, TV, PC, 프린터 등) 간의 단거리(보통, 10cm 이하) 무선 통신의 표준이다[1]. 이 통신 표준은 수동모드(passive mode)와 능동모드(active mode)로 동작한다. 요즘 출시되는 대부분의 스마트폰에는 NFC 기능을 장착하고 있으며, 3가지 모드(peer-to-peer mode, reader/writer mode, card emulation mode)를 지원한다[2]. 이런 스마트폰을 사용하여 전자 지불 시스템, 출입증 및 신분인증, 모바일 쿠폰 시스템과 같은 응용 비즈니스 모델에 활용하고 있다[3, 4]. NFC는 무선 통신이므로 강력한 보안이 요구된다[5]. 이를 위해, NFC-SEC 표준[6, 7]에서는 peer- to-peer 모드에서 두 NFC 장치 간에 안전한 채널이 수립되도록 요구한다. 하지만, 이것은 장치 간 인증을 제공하지 않으므로 특별한 보안 요구가 필요한 응용에는 적합하지 않다. 어떤 NFC 응용에서는 기밀성, 무결성, 유효성 등의 보안요구를 위해 암호화를 사용하기도 한다.

NFC 모바일 쿠폰(M-coupon: Mobile Coupon) 응용은 널리 사용될 유망한 응용의 하나이다[8]. 모바일 쿠폰 시스템은 모바일 쿠폰의 안전한 발급과 사용을 요구한다. 그렇지 않으면, 기업에 막대한 손실을 가져올 뿐만 아니라 기업의 명성에도 좋지 않은 영향을 미친다. Aigner 등이 NFC를 활용한 모바일 쿠폰 프로토콜의 기본개념, 구조 및 보안 요구사항 등을 처음 소개하였다[9]. 그 후, Dominikus 등은 공개키 기반 모바일 쿠폰 프로토콜을 제안하였다[10]. 이후,

※ Corresponding Author : Jae-Dong Lee, Address: (51767) Kyungnamdaehak-ro 7, Masanhappo-gu, Changwon-si, Gyeongsangnam-do, Korea, TEL : +82-55-249-2214, FAX : +82-55-248-2554, E-mail : jdlee@kyungnam.ac.kr

Receipt date : Feb. 3, 2017, Revision date : Apr. 14, 2017
Approval date : Apr. 19, 2017

† Dept. of Computer Science and Engineering, Kyungnam University

모바일 쿠폰에 대한 많은 연구가 진행되었다[11-17]. 하지만, 대부분의 프로토콜들은 2장에서 언급하는 바와 같이 보안 상 문제점을 가지고 있다. Dominikus 등의 프로토콜[10]은 복제 방지가 불가능하며 비효율적이다. Hsiang 등의 해시기반 프로토콜[12]은 쿠폰의 불법 생성이 가능하고 쿠폰을 중복으로 사용할 수 있을 뿐더러 무결성을 유지할 수 없다. Hsiang 등의 QR 기반 프로토콜[13]은 기밀성을 지킬 수 없음이 알려져 있다[17]. Park 등의 Schnorr 기반 및 Lattice 기반 서명 기법[14]은 쿠폰을 복사하여 사용해도 유효한 쿠폰으로 취급되는 문제점을 가지고 있다. Park 등의 간단한 모바일 쿠폰 인증 스킴(Lightweight mCoupon Authentication Scheme)과 HORS(Hash to Obtain Random Subset)[18]를 기반으로 한 스킴[15]은 위조 쿠폰을 생성할 수 있는 보안 문제가 있다. Ha는 보너스의 암호화 문제를 해결하기 위해 D- H(Diffie-Hellman)의 키 일치 방식에 기초한 프로토콜[16]을 제안하였다. 하지만, 일반적으로 쿠폰에 대한 보너스는 제품(또는 서비스 등)의 할인, 포인트 적립 또는 선물 제공 등이다. 따라서, 보너스의 암호화가 필요한 환경은 아주 제한적이다. 또한, 이 프로토콜은 사용자가 가진 유효한 쿠폰을 무효화 시킬 수 있는 보안 상의 문제점이 있다. Alshehri 등이 제안한 해시 기반 프로토콜인 Premium M-coupon Protocol[11]은 보안 측면에서 안전하다. 하지만, 불필요한 연산들이 포함되어 있다.

본 논문에서는 기존 프로토콜의 문제점들을 자세히 분석하고, 보안 상 안전한 Premium M-coupon Protocol의 문제점인 불필요한 연산들을 제거한 수정 프로토콜-1(Modified Premium M-coupon Protocol-1)을 제안하고 보안 분석을 통해 안전함을 보인다. 또한, Premium M-coupon Protocol을 포함한 대부분의 프로토콜들은 보안을 위해 공유 비밀키를 사용하여 암호화 또는 해시 등에 이용한다. 우리는 공유 비밀키가 없도록 Premium M-coupon Protocol를 수정한 수정 프로토콜-2(Modified Premium M-coupon Protocol-2)를 제안하고 보안 분석을 통해 안전함을 보인다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 M-coupon 시스템의 구성, 보안 요구 조건 및 기존 프로토콜의 분석을 기술하고, 3장에서는 수정 프로토콜-1과 수정 프로토콜-2를 제시하고, 4장에서는 제시한 프로토콜의 보안 요구 조건 분석을 통해 보안에 안전함을 보인다. 5장에서는 결론과 향후연구에 대한 방향을 제시한다.

2. NFC 기반 M-coupon 시스템

2.1 M-coupon 시스템

M-coupon(모바일 쿠폰, mobile coupon)이란 모바일 디바이스(스마트폰, 모바일 PDA 등)를 사용하여 발급받아 저장한 후 사용되는 전자 쿠폰이다. 이 쿠폰은 NFC 태그를 가진 발급자(issuer)가 발급한다. 예를 들어, 발급자는 신문 광고 또는 스마트 포스터에 부착되어 있다. NFC를 사용할 수 있는 모바일 디바이스를 가진 사용자(user)는 발급자를 터치함으로써 M-coupon을 발급받아 디바이스에 저장한다. 사용자가 쿠폰이 저장된 모바일 장치를 출납원(cashier)의 NFC 사용가능 디바이스에 터치함으로써 쿠폰의 보너스(bonus)를 받을 수 있다. 출납원은 쿠폰의 진위 여부를 파악하여 사용자에게 보너스를 제공한다. 기본적인 M-coupon 시스템은 Fig. 1과 같다.

M-coupon 시스템에서 M-coupon의 안전한 발급과 출납을 위해 M-coupon 프로토콜이 필요하다. M-coupon 프로토콜은 Fig. 2와 같이 발급단계(issuing phase)와 출납단계(cashing phase)로 구성된다. 발급단계에서는 사용자가 발급자에게 모바일 디바이

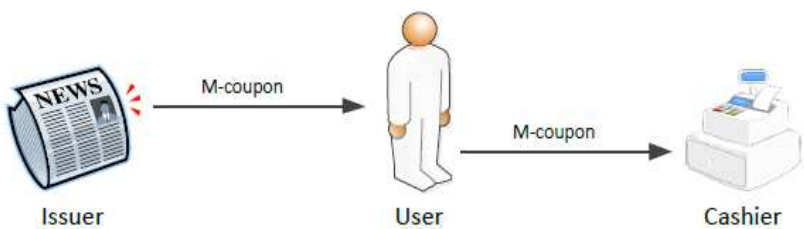

Fig. 1. General NFC mobile coupon system.

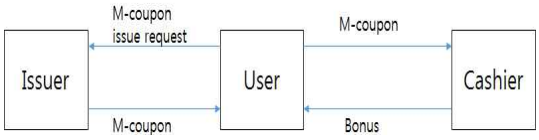

Fig. 2. M-coupon protocol.

스를 터치함으로서 발급요청이 이루어진다. 발급자는 요청 시에 제공되는 사용자의 정보와 자신의 정보를 조합하여 암호화 또는 해시함수 등을 사용하여 M-coupon을 발급하여 사용자에게 전송한다. 사용자는 발급 받은 쿠폰을 모바일 디바이스에 저장해 둔다. 출납단계는 쿠폰을 사용하는 단계이다. 사용자는 쿠폰이 저장된 모바일 디바이스를 출납원의 NFC 사용가능 디바이스에 터치함으로써 쿠폰 사용을 요구한다. 출납원의 장치는 데이터베이스 등을 활용하여 정당한 쿠폰인지를 확인한 후 보너스를 지급한다.

2.2 보안 요구 조건

M-coupon 시스템에서는 다음과 같은 위협요소에 대응할 수 있는 보안사항이 요구된다[11].

- 기밀성(Confidentiality): 공격자는 도청을 통해 정상적인 쿠폰을 획득할 수 없어야 한다.
- 무결성(Data Integrity): 공격자는 통신하는 데이터를 변조할 수 없어야 한다. 즉, 변조되었을 때 이를 처리할 수 있어야 한다.
- 불법생성불가(No Unauthorized Generation): 공격자는 자신이 쿠폰을 불법적으로 발급할 수 없어야 한다.
- 조작불가(No Manipulation): 쿠폰이 조작되면 유효한 쿠폰으로 사용될 수 없어야 한다.
- 불법복제불가(No Unauthorized Copying): 공격자는 쿠폰을 복제하여 사용할 수 없어야 한다.
- 중복사용불가(No Multiple Cash-in): 동일한 쿠폰을 여러 번 사용할 수 없어야 한다.

2.3 기존 프로토콜

2.3.1 기호 및 가정

본 논문에서 설명하는 프로토콜을 위한 표기법은 Table 1과 같다.

2.3.2 Dominikus 등의 프로토콜

Dominikus 등은 단순 프로토콜(Simple Protocol)과 개선된 프로토콜(Advanced Protocol)을 제시하였다[10]. 단순 프로토콜은 대칭 암호화를 기반으로 하며, 개선된 프로토콜은 공개키 기반 구조(PKI, Public Key Infrastructure)를 사용한다. 단순 프로토콜은 발급단계에서 2번의 라운드, 즉, 사용자가 발급자에게 발급요청하는 라운드와 발급자가 M-coupon을 발급하는 라운드로 구성되며, 출납단계 역시 2 라운드로 구성된다. 하지만, 이 프로토콜은 복제방지가 불가능하다[9]. 개선된 프로토콜은 이러한 문제점을 해결하기 위해 PKI 구조에서 발급단계에서 4라운드, 출납단계에서 4라운드를 사용하므로 효율성 측면에서 비효율적이며, PKI 구조로 인한 비용이 증대된다.

Table 1. The meaning of the notation

Notation	Meaning
M or M-$coupone$	mobile coupone
ID_I	ID of the issuer
ID_U	ID of the user
ID_C	ID of the cashier
x	shared secret key between the issuer and the cashier
x_2	shared secret key between the user and the cashier
$offer$	additional M-coupon data, e.g., type, issuing time, and validity range of the coupon
N_C	random nonce
h	hash function
$\oplus$	exclusive OR
$\|\|$	concatenation
ENC_k	encrption with the key k

2.3.4 Hsiang 등의 해시기반 프로토콜

Hsiang 등은 해시함수에 기초한 프로토콜을 제안하였다[12]. 이 프로토콜에서는 발급자와 사용자의 연산량을 줄이기 위해 일방향 해시함수를 사용하였고, 쿠폰 관련 정보들도 출납원의 데이터베이스에서 확인하는 방법을 사용하여 암호화 연산 없이도 기밀성을 유지하도록 하였다. 하지만, 이 프로토콜에서 공격자가 전송되는 데이터를 도청한 후, 자신의 ID로 바꾸어 가짜 쿠폰을 생성할 수 있다. 이 가짜 쿠폰을 출납인에게 제시하여 보너스를 제공받을 수 있다. 따라서, 이 프로토콜은 불법생성불가, 무결성 및 중복사용불가의 보안요구 조건을 지킬 수 없다[11].

2.3.5 Hsiang 등의 QR-기반 프로토콜

Hsiang 등은 QR(Quadratic Residue)에 기반한 프로토콜을 제시하였다[13]. 이 프로토콜은 어떤 값들을 숨기기 위해 이차잉여(quadratic residue)를 사용한다. Alshehri 등은 이 프로토콜의 보안위협과 문제점을 다음과 같이 지적하였다[17]. 사용자가 발급자에게 요청한 쿠폰(M)을 공격자가 가운데서 획득한 후, 공격자는 가짜 쿠폰(M')을 사용자에게 보낸다. 사용자가 출납원에게 제출한 M'은 가짜로 판별되고, 반면 공격자가 제출하는 M은 유효한 쿠폰으로 취급하여 공격자에게 보너스를 지급한다. 이것은 프로토콜에 사용자 인증 부분이 없어서 발생하는 보안위협이다. 또한, 프로토콜에서 처리되는 몇 개의 부분은 없어도 보안에 변화가 없음을 보였다.

2.3.5 Park 등의 Schnorr 기반 및 Lattice 기반 서명 기법

박성욱 등은 Schnorr 기반 서명 기법과 Lattice 기반 서명 기법을 제안하였다[14]. 이 프로토콜에서는 발급자가 암호화된 쿠폰을 원하는 모든 사용자에게 발급하고 발급받은 사용자는 쿠폰을 출납원에게 제시하여 보너스를 받도록 되어 있다. 따라서, 이 프로토콜에서는 쿠폰을 복사하여 사용해도 유효한 쿠폰으로 취급하므로 우리의 보안요구 조건을 만족시킬 수 없는 프로토콜이다.

2.3.6 Park 등의 프로토콜

Park 등은 간단한 모바일 쿠폰 인증 스킴(Lightweight mCoupon Authentication Scheme)과 HORS (Hash to Obtain Random Subset)[18]를 기반으로 한 스킴을 제안하였다[15]. 하지만, 두 스킴 모두 위조 쿠폰을 생성할 수 있는 보안 문제가 있다. 먼저, 간단한 모바일 쿠폰 인증 스킴의 문제점을 알아보자. 사용자가 발급자에게 IDS_U^m(사용자 ID(ID_U)를 m번 해싱한 값)을 전송하면 발급자는 쿠폰 $M = \{V, C\}$를 발급한다. 이때, $V = IDS_U^m \oplus ID_I$, $C = IDS_U^m \oplus x \oplus offer \oplus n_z$이다. 만약 공격자가 IDS_U^m 대신 0을 전송하면 발급자는 쿠폰 $M = \{V, C\}$, $V = ID_I$, $C = x \oplus offer \oplus n_z$ 을 발급한다. 이 때, 공격자는 발급자의 ID인 ID_I를 획득할 수 있고, $x \oplus offer \oplus n_z$의 값을 알 수 있다. 공격자가 자신의 쿠폰을 만들기 위해 자신의 ID인 ID_A를 만들어 m번 해싱한 IDS_A^m을 생성한 후, $V = IDS_A^m \oplus ID_I$, $C = IDS_A^m \oplus x \oplus offer \oplus n_z$ 로 공격자 자신의 쿠폰 $M = \{V, C\}$ 를 생성할 수 있다.

두 번째 프로토콜인 HORS를 기반으로 한 스킴의 보안 문제점을 알아보자. HORS[18]에 따르면 발급자는 비밀키 $SK = (k, s_1, s_2, \cdots, s_t)$를, 출납원은 공개키 $PK = (k, v_1, v_2, \cdots, v_t)$를 가지고 있어야 한다. 제시한 프로토콜에 따라, 사용자가 발급자에게 쿠폰을 발급 받는 과정은 다음과 같다. 먼저, 사용자는 발급자에게 ID_U를 보낸다. 발급자는 $V = ID_U \oplus h(ID_I)$를 구한 후, $h = h(V)$를 계산한다. h를 k개의 부분스트링, 즉, $h = h_1 \| h_2 \| \cdots \| h_k$로 나눈 후, V를 서명한 $Sign(V) = (s_{i_1}, s_{i_2}, \cdots, s_{i_k})$를 HORS를 이용하여 구한다. 즉, h_j를 정수 i_j로 바꾼 후, 비밀키의 s_{i_j}를 h_j의 서명값으로 사용한다. 발급자는 쿠폰 $M = \{ID_U, V, Sign(V), C\}$ 을 생성하여 사용자에게 발급한다. 여기서, $C = h(h(ID_I) \oplus x \oplus offer)$이다. 발급한 쿠폰을 출납원에게 제출하면 출납원은 공개키를 사용하여 $Sign(V)$를 검증하여 쿠폰의 유효성을 파악한다. 이 프로토콜 역시 다음과 같은 보안상의 문제점을 가지고 있다. 공격자가 발급자에게 자신의 ID인 ID_A를 전송하면 $h(ID_I)$를 획득할 수 있다. 공격자는 ID_A와 $h(ID_I)$를 이용해 h를 생성한다. h와 쿠폰에 있는 $Sign(V) = (s_{i_1}, s_{i_2}, \cdots, s_{i_k})$를 알 수 있으므로 여러 번의 시도로 비밀키 SK를 구할 수 있다. 비밀키 SK를 알면 공격자는 유효한 쿠폰을 스스로 생성할 수 있다. 이와 같은 문제는 HORS가 한 번(one-time)의

서명을 위해 제안된 방식이므로 여러 번의 시도에 의해 비밀키가 노출될 수 있기 때문이다. M-coupon 시스템의 발급자는 보통, 신문 광고 또는 스마트 포스터이므로 쿠폰을 발급할 때마다 비밀키/공개키를 변경할 수 없는 환경이므로 이 프로토콜을 사용할 수 없다.

2.3.7 Ha의 프로토콜

보너스의 암호화 문제를 해결하기 위해 D-H (Diffie-Hellman)의 키 일치 방식에 기초한 프로토콜을 제안하였다[16]. 하지만, 일반적으로 쿠폰에 대한 보너스는 제품(또는 서비스 등)의 할인, 포인트 적립 또는 선물 제공 등이다. 따라서, 보너스의 암호화가 필요한 환경은 아주 제한적이다. 또한, 이 프로토콜은 보안상의 문제점이 있다. 이 프로토콜에서는 사용자가 쿠폰 발급을 위해 발급자에게 ID_U와 P_U(사용자의 공개키)를 전송하면, 발급자는 $E_I = Enc_x((ID_I \oplus ID_U), offer, P_U)$를 생성하여 쿠폰 $M=(ID_I, E_I)$을 발급한다. 사용자는 쿠폰을 사용하기 위해 $V_U = h(ID_I, ID_U, P_U)$를 생성하여 (ID_I, E_I, V_U)를 출납원에게 제출하면 출납원은 쿠폰의 진위를 파악하여 보너스를 지급한다. 하지만, 이 프로토콜에는 다음과 같은 보안상의 결함이 있다. 쿠폰의 발급단계에서 ID_U, ID_I, P_U, E_I가 노출되므로 공격자는 $V_U = h(ID_I, ID_U, P_U)$를 생성할 수 있다. 따라서, 공격자는 이미 확보한 ID_I와 E_I를 이용하여 출납원에게 (ID_I, E_I, V_U)를 제출하면 유효한 쿠폰으로 판단하여 보너스를 지불하게 된다. 이 프로토콜에서처럼 보너스를 암호화하여 전달할 경우, 공격자는 보너스를 받을 수는 없지만 다른 사용자가 가진 유효한 쿠폰을 무효화 시킬 수 있다.

2.3.8 Alshehri 등의 프로토콜

Alshehri 등은 해시 기반 프로토콜인 Premium M-coupon Protocol을 제안하였다[11]. 이 프로토콜은 Fig. 3과 같이 동작한다. 발급자, 사용자 및 출납원은 모두 자신의 ID를 가진다. 발급자와 출납원은 비밀키(x)를 공유하고, 사용자와 발급자는 비밀키($x2$)를 공유한다. 사용자가 쿠폰을 발급받기 위해 자신의 ID의 해시값을 발급자에게 보내면 발급자는 발급자 ID, 비밀키 x, 쿠폰정보 *offer* 및 사용자 ID의 해시값을 해시한 값과 발급자 ID의 해시값으로 구성된 쿠폰을 발급한다. 즉, $M-coupon = h(ID_I, x, offer, h(ID_U)), h(ID_I)$. 사용자가 쿠폰을 사용하기 위한 출납단계에서는 출납원이 먼저 난수(N_c)와 자신의 ID를 사용자에게 보낸다. 사용자는 쿠폰, 자신의 ID, 그리고 출납원이 보낸 난수(N_c), 비밀키($x2$), 출납원의 ID, 사용자의 ID를 해시한 값, 즉, $h(N_c, x2, ID_C, ID_U)$을 출납원에게 보낸다. 출납원은 쿠폰의 정당성을 체크하기 위해 $h(ID_I)$를 이용하여 $(h(ID_I), x, ID_P offer)$가 저장되어 있는 테이블을 검색하여 x, ID_I, *offer*를 추출하여 쿠폰의 값과 비교하여 쿠폰의 정당성을 검사한다. 또한, 사용자 ID(ID_U)를 사용하여 $(ID_U, x2)$가 저장된 테이블에서 $x2$를 추출하여 사용자가 보낸 해시값 $h(N_c, x2, ID_C, ID_U)$의 값이 올바른가를 검사한다. 이는 정당한 사용자인가를 검정하는 사용자 인증을 위한 부분이다. 마지막으로 쿠폰 테이블을 검색하여 사용여부를 조사한다. 이는 쿠폰의 이중 사용을 막기 위한 대책이다. Alshehri 등은 이 프로토콜을 Casper FDR[19]로 분석하여 보안상 안전함을 보였다.

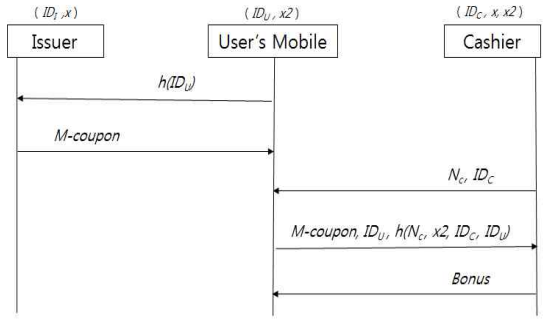

Fig. 3. Premium M-coupon Protocol.

3. 수정 Premium M-coupon Protocol

2.3.8절에서 설명한 Premium M-coupon Protocol (이하 PMP라 함)은 우리의 보안요구 조건을 충족시킨다. 하지만, 이 프로토콜에 불필요한 연산들이 있음을 발견하고 이를 개선하기 위한 2가지 방안을 제시한다. 먼저, 이 프로토콜에서는 불필요한 해시연산을 수행하고 있다. 이를 개선한 수정 프로토콜-1 (Modified Premium M-coupon Protocol-1)을 제시한다. 두 번째, 대부분의 프로토콜과 마찬가지로 이 프로토콜에서도 공유 비밀키를 사용하고 있다. 발급자와 출납원은 공유 비밀키 x를 공유하고 있으며, 사

용자와 출납원은 공유 비밀키 x2를 공유하고 있다. 이들 공유 비밀키를 제거한 수정 프로토콜-2(Modified Premium M-coupon Protocol-2)를 제시한다.

3.1 수정 프로토콜-1

수정 프로토콜-1은 Fig. 4와 같다. 수정 프로토콜-1과 PMP의 차이점은 사용자가 쿠폰을 발급하기 위해 발급자에게 보내는 메시지는 $h(ID_U)$ 대신 ID_U로 변경하고, 쿠폰 M-$coupon$은 필요 없는 부분을 없애고 $h(ID_I)$ 대신 ID_I로 변경하여

$M-coupon = h(x, offer, ID_U), ID_I$ 로 한다. 구체적인 수행 과정은 아래와 같이 PMP와 유사하다. 발급자, 사용자 및 출납원은 모두 자신의 ID를 가진다. 발급자와 출납원은 비밀키(x)를 공유하고, 사용자와 발급자는 비밀키($x2$)를 공유한다. 발급자와 출납원이 공유하는 비밀키(x)는 쿠폰을 발급할 발급자(신문광고 또는 스마트 포스터 등)를 생성할 시 발급자의 NFC에 저장하고 또한 출납원이 사용할 데이터베이스에 저장한다. 사용자와 발급자가 공유하는 비밀키($x2$)는 사용자가 모바일 쿠폰을 사용하기 위해 앱을 다운받을 때 또는 이 서비스를 사용하기 위해 등록할 때 모바일 디바이스에 저장되고 이것은 출납원의 데이터베이스에 저장한다.

사용자가 쿠폰을 발급받기 위해 자신의 ID인 ID_U를 발급자에게 보내면 발급자는 비밀키 x, 쿠폰정보 $offer$ 및 ID_U를 해시한 값과 발급자 ID(ID_I)로 구성된 쿠폰을 발급한다. 즉,

$M-coupon = h(x, offer, ID_U), ID_I$ 이다. 사용자가 쿠폰을 사용하기 위한 출납단계에서는 출납원이 먼저 난수(N_c)와 자신의 ID(ID_C)를 사용자에게 보낸다. 사용자는 쿠폰, 자신의 ID, 그리고 출납원이 보낸 난수(N_c), 비밀키($x2$), 출납원의 ID, 사용자의 ID를 해시한 값, 즉, $h(N_c, x2, ID_C, ID_U)$을 출납원에게 보낸다. 출납원은 쿠폰의 정당성을 체크하기 위해 ID_I를 이용하여 $(ID_I, x, offer)$가 저장되어 있는 테이블을 검색하여 x, $offer$를 추출하여 $h(x, offer, ID_U), ID_I$를 계산하여 쿠폰의 값과 비교하여 쿠폰의 정당성을 검사한다. 또한, 사용자 ID(ID_U)를 사용하여 (ID_U, $x2$)가 저장된 테이블에서 $x2$를 추출하여 사용자가 보낸 해시값 $h(N_c, x2, ID_C, ID_U)$의 값이 올바른가를 검사한다. 이는 정당한 사용자인가를 검정하는 사용자 인증을 위한 부분이다. 마지막으로 쿠폰 테이블을 검색하여 사용여부를 조사한다. 모든 검사 결과, 쿠폰이 유효하고 정당한 사용자이며 사용되지 않은 쿠폰이면 보너스를 지불한다.

3.2 수정 프로토콜-2

수정 프로토콜-2는 Fig. 5와 같이 동작한다. 기존 PMP에서 발급자와 출납원의 공유키 x와 사용자와 출납원의 공유키 $x2$를 제거한다. 발급자, 사용자 및 출납원은 각각의 ID인 ID_I, ID_U, ID_C를 가진다. 사용자가 쿠폰을 발급 받기 위해 $h(ID_U)$를 발급자에게 보내면 발급자는 쿠폰

$M-coupon = h(ID_I, offer, h(ID_U)), h(ID_I)$를 사용자에게 발급한다. 사용자가 쿠폰을 사용하기 위한 출납단계에서는 출납원이 먼저 사용자 인증을 위해 난수(N_c)와 자신의 ID(ID_C)를 사용자에게 보낸다. 사용자는 쿠폰(M-$coupon$), 자신의 ID(ID_U)의 해시값(즉, $h(ID_U)$) 그리고 출납원이 보낸 난수(N_c), 출납원의 ID(ID_C,)와 사용자의 ID(ID_U)를 해시한 값, 즉, $h(N_c, ID_C, ID_U)$을 출납원에게 보낸다. 출납원은 사용자가 전송한 $h(ID_U)$와 $h(N_c, ID_C, ID_U)$를 전송 받아,

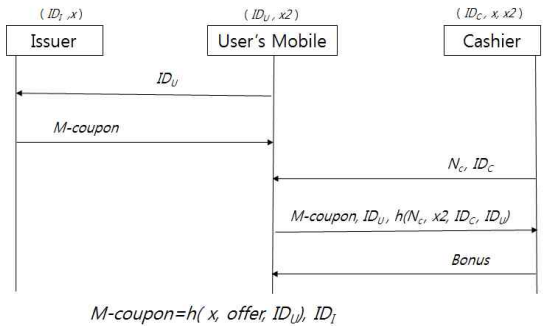

Fig. 4. Modified Premium M-coupon Protocol-1.

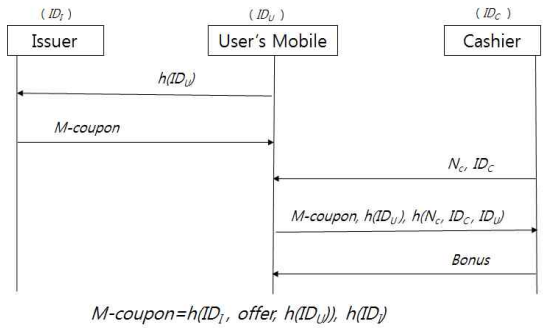

Fig. 5. Modified Premium M-coupon Protocol-2.

($h(ID_U)$, ID_U)쌍들의 테이블을 참조하여 ID_U를 찾아 $h(N_c, ID_C, ID_U)$가 올바른 값인가를 확인하여 사용자를 인증한다. 인증이 끝나면, *M-coupon*의 정당성을 확인하기 위해 ($h(ID_I)$, ID_I, *offer*)쌍들의 테이블을 참조하여 *M-coupon*의 $h(ID_I)$에 대한 ID_I와 *offer*를 추출하여 *M-coupon*의 $h(ID_P, offer, h(ID_U))$가 올바른 값인지를 확인하여 쿠폰의 정당성을 확인한다. 마지막으로 쿠폰 테이블을 검색하여 사용 여부를 조사한다. 모든 검사 결과, 쿠폰이 유효하고 정당한 사용자이며 사용되지 않은 쿠폰이면 보너스를 지불한다.

4. 보안 요구 조건 분석

본 장에서는 3장에서 제안한 수정 프로토콜-1과 수정 프로토콜-2가 2.2절에서 기술한 보안 요구 조건을 만족하는지를 분석한다.

4.1 수정 프로토콜-1의 보안 요구 조건 분석

기존 PMP와 수정 프로토콜-1과의 차이점은 발급 단계에서 사용자가 쿠폰 발급 요청 시 $h(ID_U)$대신 ID_U로 변경한 것과 *M-coupon*을 $M-coupon = h(ID_P, x, offer, h(ID_U)), h(ID_I)$대신 $M-coupon = h(x, offer, ID_U), ID_I$로 변경한 것이다. 기존 PMP는 2.3.8절에서 언급했듯이 보안 요구 조건을 만족한다. 따라서, 변경된 사항들이 보안에 미치는 영향을 분석하면 수정 프로토콜-1의 보안을 분석할 수 있다.

PMP에서 ID_U는 출납단계에서 노출될 수 있다. 따라서, $h(ID_U)$대신 ID_U를 사용해도 보안에는 변화가 없다. 즉, 공격자가 발급단계에서 사용자들의 ID의 해시값들을 획득한 후, 출납단계에서 ID_U를 획득하면 각 사용자들의 ($h(ID_U)$, ID_U) 쌍을 알 수 있다. PMP에서의 *M-coupon*의 첫 번째 해시값 $h(ID_P, x, offer, h(ID_U))$에서 ID_I와 x는 발급자가 안전하게 관리하는 정보이므로 ID_I 없이 x만 사용해도 공격자가 해시값을 구할 수 없다. 또한, 앞에서 언급한 바와 같이 $h(ID_U)$는 ID_U로 바꾸어도 보안 상 문제가 없다. *M-coupon*의 두 번째 값은 굳이 ID_I의 해시값을 사용할 필요가 없다. 왜냐하면, 공격자가 ID_I를 획득해도 x를 모르면 *M-coupon*을 생성할 수 없으므로 보안에 영향을 미치지 않기 때문이다. 이상에서 언급한 바와 같이 수정 프로토콜-1은 우리의 보안 요구 조건을 모두 만족한다.

4.2 수정 프로토콜-2의 보안 요구 조건 분석

수정 프로토콜-2가 우리의 보안 요구 조건을 만족하는지를 분석한다.

- 기밀성: 공격자가 도청을 통해 사용자(ID_U)의 *M-coupon*을 획득할 수 있다. 하지만, 공격자가 쿠폰을 사용할 때, 쿠폰의 진짜 소유주인 사용자의 ID(ID_U)를 모르기 때문에 사용자 인증 단계에서 실패하여 쿠폰을 사용할 수 없다. ID_U는 출납원의 데이터베이스 테이블에 저장되어 있으므로 출납원만이 알 수 있다.
- 무결성: 쿠폰이 변조되었을 때, 출납원이 쿠폰의 유효성 검사 과정에서 유효한 쿠폰이 아님을 알 수 있다.
- 불법생성불가: 공격자가 자신의 쿠폰을 불법적으로 생성하기 위해서는 발급자의 ID인 ID_I를 알아야 한다. 하지만, 이 프로토콜에서는 ID_I가 노출되지 않는다. 따라서, 공격자가 자신의 쿠폰을 불법적으로 생성할 수 없다.
- 조작불가: 쿠폰 $M-coupon = h(ID_P, offer, h(ID_U)), h(ID_I)$로 구성된다. 이 쿠폰이 변경되었다고 가정하자. 먼저, *M-coupon*의 첫 번째 해시값이 변경된 경우를 생각해 보자. 이 쿠폰을 출납원에게 제출했을 때 출납원은 $h(ID_I)$를 이용하여 테이블에서 추출한 ID_I, *offer* 및 사용자가 제출한 $h(ID_U)$를 이용하여 해시값 $h(ID_P, offer, h(ID_U))$를 계산한다. 제출된 쿠폰의 해시값과 출납원이 계산한 해시값이 같지 않으므로 유효한 쿠폰으로 인정되지 않는다. 쿠폰의 두 번째 해시값이 변경되었을 경우, 변경된 $h'(ID_I)$를 테이블에서 찾을 수 없으므로 이 쿠폰 역시 유효한 쿠폰으로 인정되지 않는다.
- 불법복제불가: 공격자가 정당한 사용자의 유효한 쿠폰을 복제하여 출납원에게 제출한 경우, 출납원은 사용자 인증 절차를 거친다. 공격자는 사용자의 ID인 ID_U를 알지 못함으로 올바른 $h(N_c, ID_C, ID_U)$ 값을 제시할 수 없다. 따라서, 사용자 인증을 받을 수 없어 이 쿠폰을 사용할 수 없다.
- 중복사용불가: 쿠폰의 중복 사용을 막기 위해, 출납원은 쿠폰 테이블을 검색하여 사용 여부를 조사

한다. 이미 사용된 쿠폰은 허용되지 않는다.

위에서 분석한 바와 같이 수정 프로토콜-2는 우리의 보안 요구 사항들을 모두 만족시킨다.

5. 결 론

요즘 출시되는 대부분의 스마트폰에는 NFC 기능이 장착되어 있어서 NFC 모바일 쿠폰은 널리 사용될 유망한 응용의 하나이다. NFC 모바일 쿠폰을 발급하고 사용하기 위해서는 보안에 안전한 프로토콜이 필요하다. NFC 모바일 쿠폰을 위한 많은 프로토콜들이 제시되었다.

본 논문에서는 기존 프로토콜의 보안 분석을 통해 문제점들을 지적하였고, 보안에 안전한 Premium M-coupon Protocol의 문제점인 불필요한 연산들을 제거한 수정 프로토콜-1을 제안하고 보안 분석을 통해 안전함을 보였다. 또한, Premium M-coupon Protocol을 포함한 대부분의 프로토콜들은 보안을 위해 공유 비밀키를 사용하여 암호화 또는 해시 등에 이용한다. 우리는 공유 비밀키가 필요 없는 Premium M-coupon Protocol를 수정한 수정 프로토콜-2를 제안하고 보안 분석을 통해 안전함을 보였다.

향후, 제안한 프로토콜을 구현하여 실제 환경에 적용할 프로토타입의 설계가 필요하다. 이를 위해, NFC 태그의 설계, 스마트 폰 앱의 작성 및 출납원(예를 들어, POS)시스템의 설계 등이 요구된다.

REFERENCE

[1] International Organization for Standardization, *ISO/IEC 18092: Information Technology-Telecommunication and Information Exchange between Systems-Near Field Communication-Interface and Protocol*, 2004.

[2] V. Coskun, K. Ok, and B. Ozdenizci, *Near Field Communication: from Theory to Practice*, John Wiley and Sons, United Kingdom, 2012.

[3] V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication Technology," *Wireless Personal Communications*, Vol. 71, No. 3, pp. 2259-2294, 2013.

[4] H.M. Kang, H.S. Choi, and K.A. Cha, "Development of Vehicle Status Alerts System for Personal Information Leakage Protection using the NFC-based GCM Service," *Journal of Korea Multimedia Society,* Vol. 19, No. 2, pp. 317-324, 2016.

[5] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication," *Proceeding of Workshop on RFID and Lightweight Crypto*, pp. 3-13, 2006.

[6] ECMA International, *NFC-SEC: NFCIP-1 Security Services and Protocol,* 2010.

[7] ECMA International, *NFC-SEC-01: NFC-SEC Cryptography Standard Using ECDHand AES,* 2010.

[8] Juniper Research, *Mobile Coupons-Ecosystem Analysis and Marketing Channel Strategy 2011-2016,* Juniper Research, Technical Report, 2011.

[9] M. Aigner, S. Dominikus, and M. Feldhofer, "A System of Secure Virtual Coupons Using NFC Technology," *Proceeding of Pervasive Computing and Communications Workshops*, pp. 362-366, 2007.

[10] S. Domonikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)," *Proceeding of Advanced Information Networking and Applications Workshops,* pp. 421-428, 2007.

[11] A. Alshehri and S. Schneider, "Formal Security Analysis and Improvement of a Hash-Based NFC M-Coupon Protocol," *Proceeding of Smart Card Researchg and Advanced Application Conference*, *Lecture Notes in Computer Science*, pp. 152-167, 2014.

[12] H. Hsiang and W. Shih, "Secure m-Coupon Scheme Using NFC," *Proceeding of International Conference on Business and Information,* pp. 3901-3909, 2008.

[13] H. Hsiang, H. Kuo, and W. Shih, "Secure m-Coupon Scheme Using Near Field Communication," *International Journal of Innovative Computing, Information and Control*, Vol. 5,

No. 11, pp. 3901-3909, 2009.

[14] S.W. Park and I.Y. Lee, "A Study on Light-Weight Signature Scheme for NFC mCoupon Service," *Journal of The Korea Institute of Information Security and Cryptology,* Vol. 24, No. 2, pp. 275-284, 2014.

[15] S.W. Park and I.Y. Lee, "Efficient mCoupon Authentication Scheme for Smart Poster Environments Based on Low-Cost NFC," *International Journal of Security and Its Applications,* Vol. 7, No. 5, pp. 131-138, 2013.

[16] J.C. Ha, "Security Analysis on NFC- Based M-Coupon Protocols and Its Countermeasure," *Journal of Korea Academia-Industrial Cooperation Society,* Vol. 16, No. 2, pp. 1388-1397, 2015.

[17] A. Alshehri and S. Schneider, "A Formal Framework for Security Analysis of NFC Mobile Coupon Protocols," *Journal of Computer Security,* Vol. 23, No. 6, pp. 608-707, 2015.

[18] L. Reyzin and N. Reyzin, "Better than Biba: Short One Time Signatures with Fast Signing and Verifying," *Information Security and Privacy, Lecture Notes in Computer Science,* Vol. 2384, pp. 144-154, 2002.

[19] G. Lowe, "Casper: A Compier for the Analysis of Security Protocols," *Journal of Computer Security,* Vol. 6, No. 1, pp. 53-84, 1998.

이 재 동

1983년 2월 서울대학교 계산통계학과 이학사
1985년 2월 서울대학교 전산과학전공 이학석사
1995년 2월 서울대학교 전산과학전공 이학박사

1986년~현재 경남대학교 컴퓨터공학과 교수
관심분야 : 실시간 시스템, 임베디드 시스템, 컴퓨터 보안