Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 2 pp. 1388-1397, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.2.1388
ISSN 1975-4701 / eISSN 2288-4688

NFC에 기반한 모바일 쿠폰 프로토콜에 대한 안전성 분석 및 대응 방안

하재철[1*]
[1]호서대학교 정보보호학과

Security Analysis on NFC-based M-coupon Protocols and its Countermeasure

Jae-cheol Ha[1*]
[1]**Dept. of Information Security, Hoseo University**

요 약 최근 NFC 기반의 모바일 디바이스를 이용하여 모바일 쿠폰 시스템을 구현하는 응용 비즈니스 모델이 제안되었다. 본 논문에서는 안전한 모바일 쿠폰 시스템을 위한 보안 요구 사항을 살펴보고 기존에 제시된 프로토콜에 대해 보안성 침해 요소를 분석하였다. 그리고 구현의 효율성과 안전성을 고려하여 D-H(Diffie-Hellman) 키 일치 기법에 기반한 새로운 모바일 쿠폰 프로토콜을 제안하였다. 제안한 프로토콜은 공개 키 기반 구조나 비밀 키 분배 문제를 해결하면서 사용자 인증 기능을 제공하며 중계 공격에도 대응할 수 있도록 설계되었다.

Abstract Recently, an application business model was proposed to implement an M-coupon system using the NFC-based mobile devices. In this paper, the security requirements were surveyed for a secure M-coupon system and to analyze the threats on the existing NFC-based M-coupon protocols. After considering the implementation efficiency and security, this paper presents a novel M-coupon protocol based on the Diffie-Hellman key agreement scheme. This protocol can be an alternative to solve the security problems related to the PKI (Public Key Infrastructure) and secret key distribution. Furthermore, this M-coupon protocol is designed to provide user authentication and counteract the relay attack.

Key Words : D-H Key Agreement, NFC-based M-coupon, protocol, Relay Attack, User Authentication

1. 서 론

NFC(Near Field Communication)는 스마트 폰이나 PDA와 같은 모바일 단말기간의 데이터 통신을 지원하는 단거리 무선 통신의 표준이다[1, 2]. 이 통신 표준은 13.56MHz의 주파수에서 동작하며 수동 모드(passive mode)와 능동 모드(active mode) 형태로 동작하게 된다. 최근 출시되는 휴대폰 등에는 대부분 NFC 기능을 장착하고 있으며, 이를 이용한 전자 지불 시스템, 출입증 및 신분 인증 그리고 쿠폰 시스템과 같은 응용 비즈니스 모델이 개발되고 있다[3]. 그러나 NFC 기반의 응용 서비스가 이동성과 편리성을 제공하지만 무선 통신이라는 약점으로 인해 보안을 위협하는 여러 공격들이 등장하게 되었다[4].

이러한 가운데 최근에는 NFC 표준에 기반한 모바일 쿠폰(M-coupon) 시스템에 대한 연구가 활발히 진행되고 있다[5-10]. 모바일 쿠폰은 종이 쿠폰에 비해 사용이 편리한 장점은 있지만 복제나 변조 등의 공격을 받을 수 있다. 예를 들어, 쿠폰 그 자체는 매우 저가이지만 불법 복사 등에 의해 쿠폰이 대량으로 제작된다면 쿠폰을 발행한 회사는 금전적 피해는 물론 광고 이미지에 큰 손실을 입게 된다.

*Corresponding Author : Jae-cheol Ha(Hoseo Univ.)
Tel: +82-41-540-5991 email: jcha@hoseo.edu
Received September 11, 2014 Revised (1st October 6, 2014, 2nd October 14, 2014) Accepted February 12, 2015

NFC를 활용한 모바일 쿠폰 시스템에 대한 개념은 Aigner 등에 의해 처음 도입되었으며 쿠폰을 활용하기 위한 기본 구조와 보안 요구 사항 등이 제시되였다[5]. 그 후 Dominikus 등은 공개 키 서명 시스템에 기반한 모바일 쿠폰 프로토콜을 제안하였다[6]. 그러나 이 프로토콜은 사용자 인증을 위해 공개 키 인증서가 필요하고 이를 관리하는 제 3의 신뢰 기관이 필요하다는 점에서 시스템을 구축하거나 운영하는데 부담스런 점이 있다. 따라서 경량화된 시스템 개발을 목표로 Hsiang 등은 해시 함수에 기초한 모바일 쿠폰 프로토콜을 제시하기도 하였다[7]. 그러나 이 프로토콜은 데이터 무결성 등 여러 보안 요구 사항을 만족하지 못하고 있다. 최근에는 Alshehri 등이 쿠폰 사용자에게도 비밀 키를 발행하는 조건하에서 사용자 인증을 제공하는 보다 개선된 프로토콜을 제안한 바 있다[10].

본 논문에서는 모바일 쿠폰 시스템의 구성 요소 및 보안 요구 사항을 분석한다. 그리고 지금까지 제시된 쿠폰 프로토콜의 안전성 침해 요소를 살펴보고 공격의 성공 요인을 분석한다. 이와 같은 분석을 바탕으로 모바일 쿠폰 시스템을 구현하는데 필요한 보안 요구 사항을 만족하면서 구현 효율성을 높인 D-H (Diffie-Hellman)의 키 일치 기법[11]에 기반한 모바일 쿠폰 프로토콜을 제안한다.

2. NFC 기반 모바일 쿠폰 프로토콜

2.1 모바일 쿠폰 시스템의 구성

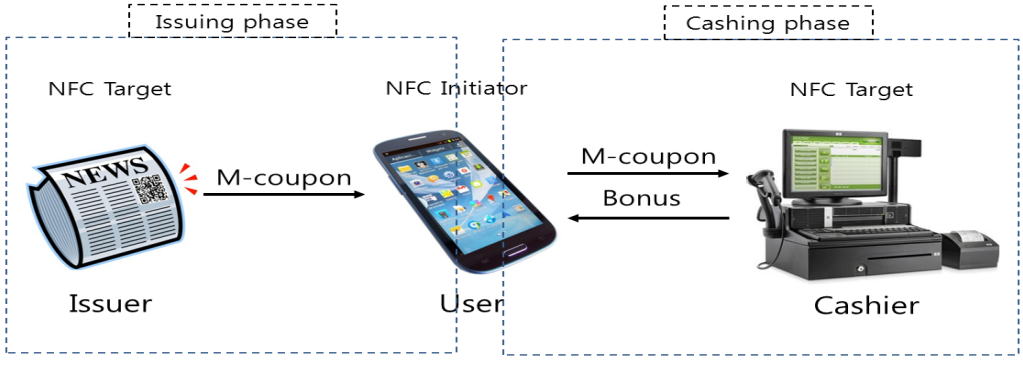
모바일 쿠폰 시스템은 발행자(issuer), 사용자(user) 그리고 출납원(cashier)으로 불리는 3가지 객체로 구성된다. 다음 Fig. 1은 일반적인 모바일 쿠폰 시스템을 도시화한 것이다. 여기서 발행자는 수동적인 NFC 태그를 의미하는데 보통 광고용 포스터나 신문 광고, 잡지 등에 붙여 사용자에게 전달된다. 발행자는 능동적인 모바일 사용자에게 NFC 인터페이스를 통해 쿠폰을 발행하게 된다. 발행자의 태그는 자체적인 전원 공급 장치가 없으므로 수동 모드로 동작하며 모바일 디바이스로부터 전원을 받아 AES나 해시 함수 같은 비교적 간단한 암호 알고리듬을 수행할 수 있다고 가정한다[12, 13].

사용자는 클라이언트(client)라고도 하는데, 쿠폰을 받는 고객을 의미하며 NFC 모바일 디바이스를 가진 사람이다. 사용자는 발행인으로부터 모바일 쿠폰을 받아 이를 출납인에게 제출하고 원하는 제품이나 보너스를 받는다. 사용자는 쿠폰을 발행받기 전에 자바 애플릿과 같은 모바일 쿠폰 응용 프로그램들을 웹 사이트를 통해 자신의 기기에 다운받아 설치해 두어야 한다. 그 후 사용자는 설치된 응용 프로그램을 이용하여 암호나 디지털 서명과 같은 정보보호 기능을 수행할 수 있게 된다.

출납인은 NFC 인터페이스 장치를 가진 터미널을 의미한다. 출납인은 사용자의 모바일 디바이스에 있는 쿠폰을 받아 쿠폰이 정확히 발행된 것임을 확인한 후 해당하는 서비스를 제공한다. 이를 위해서 발행자의 ID나 쿠폰의 종류 등을 데이터베이스화하여 저장하기도 한다. 이와 같은 모바일 쿠폰 시스템에서는 발행자와 출납원은 동일한 회사나 기관이 되고, 하나의 모바일 디바이스에는 동일 종류의 쿠폰을 하나만 저장할 수 있다고 가정한다.

2.2 보안 요구 사항 및 대응 방법

모바일 쿠폰 시스템에서는 다음과 같은 위협 요소에 대응할 수 있는 보안 사항이 요구된다[6, 7, 10].



[Fig. 1] General NFC mobile coupon system

① 불법 생성(unauthorized generation)

공격자는 자신이 원하는 새로운 쿠폰을 불법적으로 발행할 수 없어야 한다.

② 조작(manipulation)

모바일 쿠폰을 조작한 후에는 유효한 상태를 유지할 수 없어야 한다.

③ 불법 복제(unauthorized copying)

공격자는 상환이 되는 유효한 모바일 쿠폰을 복사할 수 없어야 한다.

④ 쿠폰 중복 사용(multiple cash-in)

공격자는 동일한 모바일 쿠폰을 여러 번 사용할 수 없어야 한다.

⑤ 기밀성(Confidentiality)

공격자는 도청에 의해 정상적인 쿠폰을 얻을 수 없어야 한다.

⑥ 무결성(Data Integrity)

공격자는 통신하는 도중 전송되는 데이터를 변조할 수 없어야 한다.

위의 보안 요구 사항 중 처음 ①~④는 모바일 쿠폰 개념을 정립한 논문 [6]에서 제시한 것이며 ⑤와 ⑥은 Hsiang 등에 의해 추가된 것이다[6, 7]. 이러한 보안 위협 가운데 불법 생성과 조작 공격은 발행자와 출납원이 공유한 비밀 키를 사용하여 관련 정보를 암호화하는 방법으로 막을 수 있다. 또한 쿠폰의 중복 사용 문제는 출납원의 단말기와 쿠폰의 데이터베이스를 연결하여 한 번 사용한 쿠폰은 두 번 이상 사용되지 않도록 검사하는 방법을 이용하여 방어할 수 있다.

보안 위협 가운데 가장 문제가 되는 것이 불법 복제에 관한 것이다. 이것의 정확한 정의는 공격자나 사용자가 정당한 모바일 쿠폰을 다른 디바이스로 복사할 수 없다는 것이다. 이를 위해서는 사용자는 쿠폰을 발행받을 때 인증을 받고 출납원에게도 인증을 받아야 한다. 그러나 발행자는 이러한 인증 기능을 수행할 능력이 부족하므로 대부분 출납원에게 위임하게 된다. 즉, 출납원은 발행자로부터 받은 인증 데이터를 검사하여 쿠폰 발행 과정에서 사용한 키와 자신이 가진 비밀 키가 동일함을 확인함으로써 정당한 사용자의 쿠폰임을 확신하게 된다. 즉, 공격자는 발행자가 인증할 때 사용된 비밀 키를 알지 못하면 출납원에게 자신을 인증할 수 없게 된다.

특히, Alshehri 등은 불법 복제 문제를 크게 양도 불가(not transferable)와 사용자 인증(user authentication) 문제로 나누어서 고려하였다[10]. 양도 불가는 쿠폰의 발행 단계에서 사용된 ID가 프로토콜이 진행되는 동안에 변경되지 않도록 해야 한다는 성질이다. 반면, 사용자 인증이란 쿠폰을 발행받은 사람만이 출납원으로부터 해당 보너스나 서비스를 받아야 한다는 성질이다.

3. 모바일 쿠폰 프로토콜의 안전성 분석

본 장에서는 지금까지 제시된 주요 모바일 쿠폰 프로토콜을 안전성과 효율성 측면에서 분석하고 공격이 성공할 수 있는 보안 위협 요소를 살펴본다.

3.1 모바일 쿠폰 시스템의 구성

모바일 쿠폰 프로토콜은 전체적으로 두 단계로 이루어진다. 하나는 사용자가 발행자로부터 모바일 쿠폰을 발행받아 자신의 디바이스에 쿠폰을 저장하는 발행 단계(issuing phase)이며 다른 하나는 이 쿠폰을 출납원에게 제출하고 필요한 보너스나 서비스를 받는 출납 단계(cashing phase)이다. 여기서 서비스는 상품을 직접 받을 수도 있지만 일정한 가치를 가진 금전 데이터를 다시 모바일 디바이스로 전송받을 수도 있다고 가정한다.

본 논문의 모바일 쿠폰 시스템에서 사용하는 프로토콜을 설명하기 위해 사용된 기호와 약어는 다음과 같다.

- ID_i, ID_u : 발행자 및 사용자의 ID
- R_i, R_u : 발행자 및 사용자의 랜덤 수
- K : 발행자와 출납원간의 비밀 키
- $K2$: 사용자와 출납원간의 비밀 키
- EK : 사용자와 출납원간의 세션 공유 키
- $r_u(P_u)$, $r_c(P_c)$: 160비트 정도의 사용자 및 출납원의 개인 키(공개 키)
- $Sign_u(\ )$, $Verify(\ )$: 사용자의 서명 및 검증자의 검증 연산
- $Enc_K(\ )$, $Dec_K(\ )$: 비밀 키 K에 의한 암호 및 복호
- $h(\ )$: 메시지 해시 함수

- $L(x)$: x값의 하위 비트를 특정 길이(블록 암호의 키 길이)만큼 절단하는 함수
- $Check()$: 메시지의 내용과 유효성을 검사 하는 함수
- $Offer$: 쿠폰의 형태, 발행 시간 그리고 유효 기간 등을 나타내는 정보
- p : 1024비트 정도의 소수
- g : $GF(p)$에서의 생성자(generator)

3.2 Dominikus 등의 방식

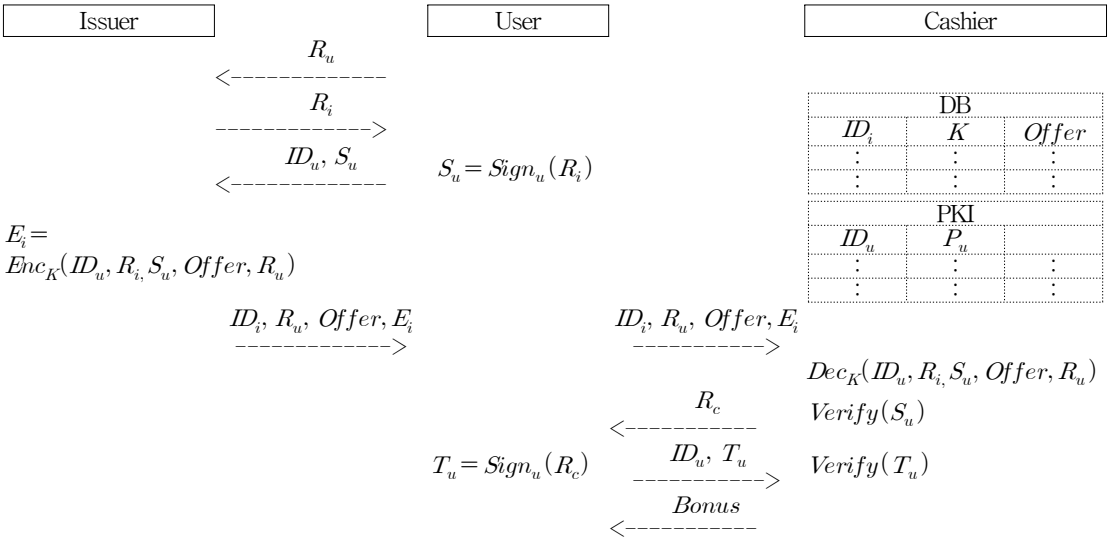
Dominikus 등은 모바일 쿠폰 시스템의 개념을 처음으로 정립하는 단계에서 보안 요구 사항을 정리하였으며 이를 만족하는 보안 프로토콜을 제시하였다[6]. 저자들은 논문에서 단순 프로토콜(simple protocol)과 개선된 프로토콜(advanced protocol)을 제시하였는데 단순 프로토콜은 사용자를 인증하는 기능이 없어 복사 방지가 불가능한 프로토콜이다.

이에 반해 개선 프로토콜에서는 사용자가 쿠폰을 발행받을 때 자신의 개인 키로 발행자의 랜덤 수에 서명을 하고, 출납원에게도 자신의 서명을 한 번 더 제출함으로써 자신이 쿠폰을 받은 정당한 사용자임을 증명하게 된다. 즉, 이 프로토콜에서는 사용자가 수행하는 두 번의 디지털 서명을 통해 불법 복사를 방지할 수 있는 기능을 추가하였다. 이 과정을 자세히 나타낸 것이 Fig. 2이다.

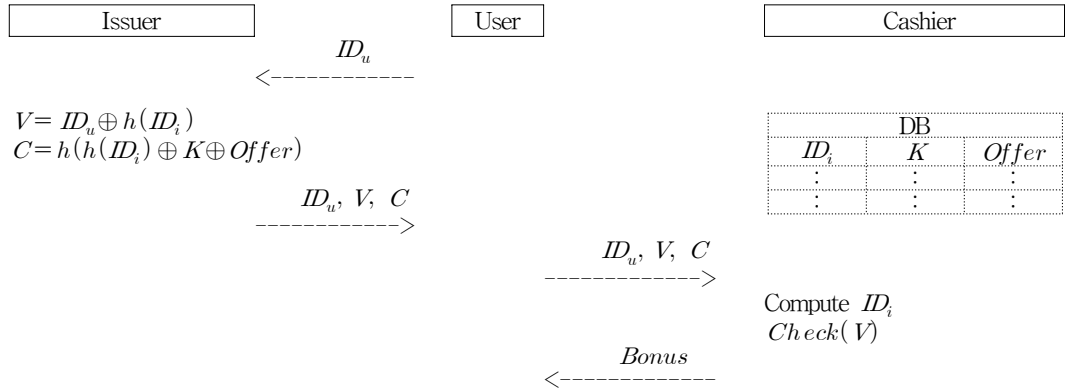
이 프로토콜의 단점은 사용자가 자신을 인증하기 위해 개인 키를 사용하게 되고 이를 검증하는 출납원은 사용자의 공개 키를 먼저 검증해야만 한다는 것이다. 따라서 공개 키 기반 구조(PKI, Public Key Infrastructure)가 필요하며 이를 통해 공개 키 인증서를 발급받고 확인하는 절차가 필요하다. 따라서 출납원은 매 쿠폰을 확인할 때마다 제 3의 신뢰 기관으로부터 공개 키 인증서를 받아야 하므로 쿠폰 시스템 자체가 전체적으로 커질 뿐만 아니라 프로토콜의 연결 수가 많아지게 되고 모바일 디바이스의 계산량도 늘어나게 된다.

안전성 측면에서 볼 때 이 프로토콜은 몇 가지 취약점이 있음이 지적되었다. Alshehri 등은 이 프로토콜에서 공격자가 사용자와 출납원 사이의 통신에 끼어들어 데이터의 중계 기능을 수행하면서 마지막 단계의 보너스 전송 단계에서 출납원이 전송하는 보너스만 가로채는 공격이 가능함을 지적하였다[8, 9]. 즉, 공격자는 Fig. 2의 프로토콜에서 도청(eavesdropping)과 중계 공격(relay attack)을 통해 사용자의 서명을 발행자와 출납인에게 중계한다. 그리고 마지막 단계에서 출납원이 보내는 보너스를 사용자에게 중계하지를 않고 자신이 가져가는 일종의 가로채기 공격을 시도할 수 있다[14, 15].

이러한 중계 공격은 출납원이 마지막 보너스를 전송할 때 데이터를 암호화 하거나 다른 인증과정 없이 보내기 때문에 발생하게 된다. 따라서 프로토콜의 마지막 단계에서 출납원이 보너스를 도청할 수 없도록 암호화하여 전송하는 보안 기법이 필요하다.



[Fig. 2] The advanced M-coupon protocol



[Fig. 3] The hash-based M-coupon protocol

3.3 Hsiang 등의 방식

Hsiang 등의 프로토콜은 비교적 계산량이 많은 Dominikus 등의 프로토콜을 개선한 것으로서 해시 함수에 기초하고 있다[7]. 이 프로토콜을 단계적으로 설명한 것이 Fig. 3이다. 그림에서 보는 바와 같이 발행자는 쿠폰 발행 단계에서 사용자의 ID_u와 발행자의 ID_i를 배타적 논리합으로 결합한 V 및 쿠폰 정보를 담은 C를 전송한다.

이 프로토콜에서는 발행자와 사용자의 연산량을 줄이기 위해 일방향 해시 함수를 사용하였고 쿠폰 관련 정보들도 출납원의 데이터베이스에서 확인하는 방법을 사용하여 암호화 연산 없이도 기밀성이 유지되도록 하였다.

그러나 이 프로토콜은 공격자가 전송되는 데이터를 도청한 후 자신의 ID_a로 바꾸어 쿠폰을 재활용할 수 있다[10]. 즉, 공격자는 V와 ID_u로부터 간단히 $h(ID_i)$ 값을 구할 수 있다.

$h(ID_i) = ID_u \oplus V$

그리고 자신의 불법 V'를 다음과 같이 만들어 ID_a, C와 함께 전송하게 된다.

$V' = h(ID_i) \oplus ID_a$

이와 같은 경우 출납인은 모든 검사 과정을 정상적으로 마치게 되며, 결국 공격자에게 보너스를 제공하게 된다. 따라서 이 프로토콜은 보안 요구 사항 중 양도 불가, 데이터 무결성 그리고 쿠폰 중복 사용 공격에 취약함을 알 수 있다. 이러한 공격을 방어하기 위해서는 아래와 같이 전송 정보 C에 ID_u를 해시 연산의 입력으로 사용하면 이 문제점은 해결되지만 불법 복제 중 사용자 인증 문제는 여전히 해결할 수 없다[10].

$C = h(h(ID_i), K, Offer, ID_u)$

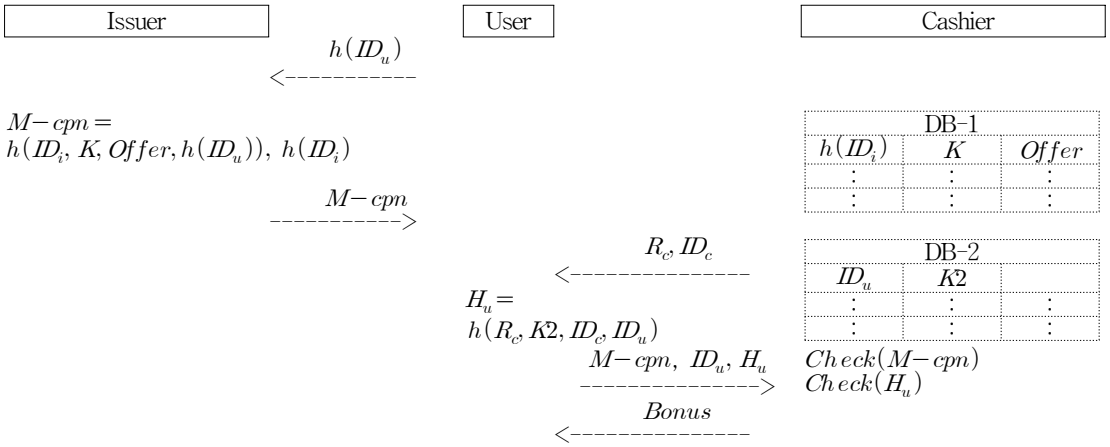
이러한 문제가 발생하게 되는 근본적인 이유는 발행자가 검사 값 C를 만드는 과정에서 발행자의 정보만 활용하기 때문에 공격자는 C값에 관계없이 V를 조작하여 정당한 쿠폰을 발행받은 것처럼 위장할 수 있기 때문이다. 따라서 발행자는 출납원이 사용자의 신분을 확인할 수 있는 의미있는 정보를 만들어 전송할 수 있어야 한다.

3.4 Alshehri 등의 방식

최근, Alshehri 등은 사용자에게 비밀 키를 부여하는 방식으로 해시 함수에 기반한 모바일 쿠폰 프로토콜을 제안하였다. 저자들은 논문에서 football 프로토콜과 premium 프로토콜을 제안 하였는데 football 프로토콜은 불법 복제 문제를 해결할 수 없는 프로토콜이다. 반면 premium 프로토콜은 양도 불가 및 사용자 인증 기능을 추가하여 불법 복제 문제를 해결하였다.

Fig. 4는 Alshehri 등이 제안한 premium 모바일 쿠폰 프로토콜을 나타낸 것이다. 그림에서 보는 바와 같이 발행자는 쿠폰 정보를 전달하기 위해 해시 함수를 이용하고 있으며 출납원과 공통의 비밀 키 K를 공유하고 있다. 발행자는 이 비밀 키를 이용하여 출납원에게 쿠폰을 발행한 태그임을 간접적으로 증명하게 된다.

이 프로토콜의 가장 큰 특징은 사용자가 출납원에게 자신을 인증하기 위해 비밀 키 $K2$를 사용한다는 점이다. 즉, $h(R_c, K2, ID_c, ID_u)$와 같이 사용자는 자신이 가진 비밀 정보와 다른 ID_u정보를 같이 해시하여 쿠폰을 받을 수 있는 유일한 사람임을 인증하게 된다.



[Fig. 4] The premium M-coupon protocol

하지만 이 프로토콜의 문제점은 각 사용자에게 출납원과 공유할 수 있는 비밀 키 $K2$를 어떻게 분배하는가 하는 것이다. 즉, 쿠폰을 받을 수 있는 각 사용자들은 비밀 키 $K2$를 공격자가 알지 못하게 얻을 수 있는 다른 방법이 필요하지만 이에 대한 언급은 없다. 즉, 이 프로토콜은 사용자 인증 문제를 해결하기 위해 사용자와 출납원이 공유한 비밀 키를 이용하지만 이를 분배하는 시스템을 별도로 갖추어야 한다는 점에서 키 분배에 관한 원론적인 문제를 가지고 있다.

4. 제안하는 모바일 쿠폰 프로토콜

상기한 바와 같이 지금까지 제시된 모바일 쿠폰 프로토콜들은 보안상 몇 가지 취약점을 가지고 있다. 논문에서는 이러한 분석을 바탕으로 모바일 쿠폰 시스템의 보안 요구 사항을 만족하는 프로토콜을 제시하고자 한다.

4.1 D-H의 키 일치에 기초한 쿠폰 프로토콜

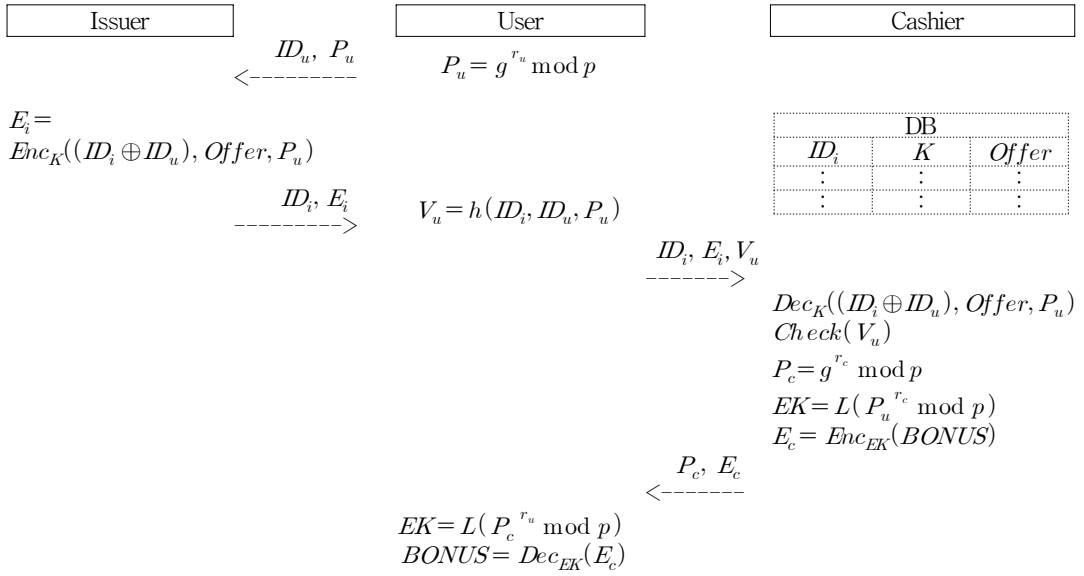
기존의 모바일 쿠폰 프로토콜을 분석한 결과, 보안 요구 사항을 만족하지 못하는 경우도 있었으며 여러 공격에 대응하기 위한 대응책들이 규모가 커져 실제로 운영하기에는 비효율적인 면이 있었다. 특히, 사용자가 출납원에게 인증을 받기 위해서는 PKI 기반 공개 키 시스템을 이용하거나 별도의 비밀 키를 분배해야 하지만 쿠폰 시스템의 규모에 비해 효율성이 떨어지게 된다. 즉, PKI와 같은 시스템에 의한 사용자 인증은 효과적이지만 공개 키 인증서가 필요하게 되고 이를 위해서는 신뢰할 수 있는 제 3자의 역할이 필수적이므로 쿠폰 시스템의 규모가 너무 커져 운영하기가 쉽지 않다.

또한, 모바일 쿠폰 시스템에서 문제가 되는 점은 Alshehri 등의 공격에서와 같이 사용자와 출납원 사이의 통신에 공격자가 끼어들어 출납원이 전송하는 보너스만 가로채는 중계 공격이다[8, 9]. 이 문제를 해결하기 위해서는 사용자와 출납원만이 아는 비밀 키를 공유하여 보너스를 암호화하여 전송할 수 있도록 해야 한다.

따라서 본 논문에서는 모바일 쿠폰 시스템에서 문제점으로 지적된 사용자 인증 문제와 보너스 암호화 문제를 해결할 수 있도록 D-H의 키 일치 방식에 기초한 보안 프로토콜을 제안하고자 한다. 제안하는 프로토콜을 전체적으로 도시한 것이 Fig. 5이다.

그림에서 보는 바와 같이 사용자는 발행 단계에서 자신의 개인 키 r_u를 생성하고 이에 대응하는 공개 키 $P_u = g^{r_u} \bmod p$ 를 만들어 발행자에게 전송한다. 발행자는 사용자의 공개 키 및 ID_u, ID_i를 자신의 비밀 키로 암호화하여 사용자에게 전송한다.

사용자는 출납 단계에서 자신과 발행자의 ID, 그리고 공개 키를 검사할 수 있도록 해시한 결과를 전송한다. 출납원은 사용자로부터 받은 쿠폰 관련 정보를 복호화하고 사용자의 공개 키의 무결성을 검사한다. 그리고 출납원도 자신의 개인 키 r_c를 생성하고 공개 키 $P_c = g^{r_c} \bmod p$ 를 계산한다. 그리고 사용자와 같이 공



[Fig. 5] Proposed M-coupon Protocol

유할 세션 키 $EK = L(P_u^{r_c} \bmod p)$를 만들게 된다. 출납원은 이 세션 키를 이용하여 보너스를 암호화한 뒤 사용자에게 전송한다. 마지막으로 사용자는 출납원과 공유할 세션 키를 $EK = L(P_c^{r_u} \bmod p)$와 같이 생성하여 보너스를 복호화한 후 사용하게 된다.

결국, 이 프로토콜에서 사용자와 출납원은 아래와 같은 D-H의 키 일치 방식에 따라 공통의 세션 키를 공유하여 서로를 인증함과 동시에 보너스를 암호화하여 전송하는데 활용하게 된다.

사용자 : $EK = L(P_c^{r_u} = g^{r_c \cdot r_u} \bmod p)$

출납원 : $EK = L(P_u^{r_c} = g^{r_u \cdot r_c} \bmod p)$

4.2 안전성 분석

본 절에서는 제안하는 모바일 쿠폰 프로토콜이 2장에서 기술한 보안 요구 사항을 만족하는지 살펴본다. 보안 요구 사항에 따른 각 프로토콜의 안전성 분석 결과를 정리한 것이 Table 1이다. 분석 테이블에서는 각 보안 요구 사항을 만족하기 위해 제공되는 암호학적 메커니즘을 구체적으로 표시하였다. 먼저 제안 프로토콜에서는 발행자가 가진 비밀 키를 이용하여 쿠폰을 암호화하여 처리함으로써 공격자가 쿠폰에 접근하는 것을 근본적으로 차단

[Table 1] Robustness of protocols against security threats

Threats & protocols	Dominikus[6]		Hsiang[7]		Alshehri[10]		Proposed	
	Function	Security	Function	Security	Function	Security	Function	Security
Unauthorized generation[6]	E_k	O	E_k	O	E_k	O	E_k	O
Manipulation[6]	E_k	O	E_k	O	E_k	O	E_k	O
Unauthorized copying[6]	S	O	-	X	h_{K2}	O	E_k+E_{EK}	O
Multiple cash-in[6]	DB	O	-	X	DB	O	DB	O
Confidentiality[7]	E_k	O	h+DB	O	h+DB	O	E_k+E_{EK}	O
Data integrity[7]	S	O	-	X	h	O	h+E_k	O
Relay attack[8]	-	X	-	X	-	X	E_{EK}	O

Cryptographic function : E_k(Encryption between issuer and cashier), DB(Checking Offer Database in cashier), S(Signature of user), h_{K2}(Hashing on $K2$), h(Hashing on Offer), E_{EK}(Encryption between user and cashier)
Security : O(Secure), X(Not secure)

하게 된다. 따라서 불법 생성, 조작 공격 그리고 기밀성에 대해서는 안전하다고 할 수 있다. 또, 무결성 공격에 대해서는 발행자가 쿠폰 및 관련 정보를 복호하는 과정과 V_u 값을 검사하는 과정을 통해 변조 여부를 확인할 수 있어 방어가 가능하다. 이외에도 쿠폰의 중복 사용 문제도 출납원의 DB에서 한 번 사용한 쿠폰을 확인하는 과정이 있으므로 방어가 된다.

마지막으로 불법 복제 공격을 방어하기 위해서는 양보 불가 기능과 사용자 인증 기능이 필요하다. 제안 프로토콜을 양도 불가 측면에서 볼 때 발행자는 $(ID_i \oplus ID_u)$ 값을 암호화하여 전송하므로 비밀 키를 모르는 공격자는 임의로 ID_u를 변경할 수 없다. 따라서 공격자가 ID_u를 변경하여 타인에게 쿠폰의 사용권을 양도하는 공격은 불가능하다. 또한 사용자 인증에 있어서 출납원은 P_u는 쿠폰을 발행받은 정당한 사용자만이 유일하게 생성할 수 있고 그 공개 키를 이용해야만 암호화된 보너스를 복호화할 수 있다는 사실을 간접적으로 알 수 있다. 따라서 제안 프로토콜에서는 불법 복사 방지를 위해 묵시적인 사용자 인증(implicit user authentication) 기능을 제공하고 있다.

한편, 기존의 프로토콜들은 마지막 단계의 도청 및 중계를 통해 공격자가 보너스를 가져가는 가로채기 공격을 막을 수 없었다. 그러나 제안 방식에서는 보너스를 사용자와 출납원 사이의 공유 비밀 키 EK로 암호화하여 전송하므로 사용자의 개인 키 r_u를 알지 못하는 공격자는 쿠폰을 받을 수는 있겠지만 제대로 복호화하여 사용할 수는 없다. 따라서 제안 프로토콜은 공격자의 중계 기능을 이용한 보너스 가로채기 공격을 방어할 수 있다.

본 논문에서는 사용자와 출납원간의 보너스 암호화와 인증 문제를 동시에 해결하기 위해 D-H의 키 일치 시스템을 활용하였다. 사실 보너스의 암호를 위해 비밀 키 암호 시스템을 사용한다는 것은 키 분배 문제로 인해 매우 비현실적이라고 볼 수 있다. 그러므로 공개 키 암호 시스템에서 사용하는 키 전송 기법이나 키 일치 기법을 사용해야 한다. 하지만 키 전송 기법은 상대방의 공개 키를 이용하여 공유 비밀 키를 암호화하여 전송하는 형태이므로 공개 키에 대한 인증이 필수적이다.

따라서 공개 키 인증을 위한 PKI 기반 구조가 설계되어야 한다. 결론적으로 키 분배 문제와 PKI 개발 문제를 동시에 해결할 수 있는 것이 D-H의 키 일치 시스템이므로 본 논문에서는 이를 채택하였다. 또한, D-H의 키 일치 기법은 인증된 두 사용자만이 상대방의 공개 키에 자신의 비밀 키를 조합해야 공유 키가 생성된다는 것을 알고 있기 때문에 묵시적 인증이 가능하다는 장점이 있다.

여기서 고려할 점은 D-H의 키 일치 시스템은 근본적으로 중간자 공격(man-in-the-middle attack)에 취약하다는 것이다[16]. 즉, 공격자는 두 사용자의 통신 중간에 끼어들어 자신의 비밀 키와 공개키를 사용하여 신분을 속이고 메시지를 도청하거나 조작할 수 있다. 하지만 제안하는 모바일 쿠폰 프로토콜에서는 이러한 중간자 공격이 현실적으로 불가능하다. 왜냐하면 모바일 쿠폰 프로토콜은 발행 단계와 출납 단계로 구별되는데 이 두 과정은 운영 시간과 공간이 구별된 상태에서 수행되기 때문이다. 즉, 모바일 쿠폰 시스템에서 중간자 공격을 성공하기 위해서는 공격자는 쿠폰 발행 단계와 출납 단계에서 중계 공격을 두 번 수행하여야 한다. 그러나 사용자의 쿠폰을 발행받는 위치와 시간은 출납 단계의 위치나 시간과는 전혀 다르므로 공격자가 동일한 사용자를 대상으로 시간과 장소를 알지 못하는 곳에서 두 번을 연속해서 중계 공격을 하는 것 자체가 불가능하다

결국, D-H 키 일치 시스템에서 원래 중간자 공격은 한 번의 중계 공격을 통해서 성공하기는 쉽지만 모바일 쿠폰 시스템과 같이 장소가 다른 곳에서 시차를 두고 프로토콜이 2번 이상 수행되는 환경에서는 임의적으로 중계 공격을 수행할 수가 없다. 결국, 프로토콜을 수행하는 시간과 공간의 연결성이 없는 경우에는 중간자 공격을 적용하기가 어렵기 때문에 D-H의 키 일치 시스템을 안전하게 사용할 수 있다.

4.3 효율성 분석

모바일 쿠폰 시스템에서는 안전성 못지않게 구현에 필요한 계산 효율이 매우 중요하다. Table 2는 지금까지 설명한 모바일 쿠폰 프로토콜의 구현 효율성을 비교한 것이다. 각 프로토콜구현하는데 사용된 주요 연산은 암호화와 복호화, 멱승(exponentiation) 그리고 해쉬 연산으로 구분할 수 있는데 발행 단계 및 출납 단계에서의 각 객체별 연산을 구별하여 상술하였다. 본 논문에서는 프로토콜에서 필요한 연산량 비교를 용이하게 하기 위해 서명 생성 및 검증은 DSS[17]와 같은 이산 대수 문제에 기반한 표준 알고리듬을 사용한다고 가정하였다. 따라서 서명 생성 및 검증 그리고 D-H의 키 일치 시스템에서 필요한 한 번의 멱승 연산량은 모두 동일하다고 가정하였

[Table 2] Efficiency comparison for protocol implementation

Protocols			Dominikus[6]	Hsiang[7]	Alshehri[10]	Proposed
User Authentication			PKI-based	-	Secret key distribution	D-H key agreement
Main Operation			Signature & Verification	Hashing	Hashing	Exponentiation for D-H scheme
Computational load	Issuing phase	Issuer	$1E$	$2H$	$2H$	$1E$
		User	$1P_S$	-	$1H$	P_K
	Cashing phase	User	$1P_S$	-	$1H$	$1P_K+1D+1H$
		Cashier	$4P_V+1D$	$2H$	$2H$	$2P_K+1E+1D+1H$

Computation : E(Encryption), D(Decryption), $E=D$
P_S, P_V, P_K(Exponentiation for signature, verification, and D-H key agreement), $P_S=P_V=P_K$
H : Hashing

다. 예를 들어 공개키 암호 시스템의 안전도를 고려하여 약 1024비트의 소수 p와 160비트의 개인 키(r_u 혹은 r_c)를 사용한다고 가정하였다.

일반적으로 사용자의 모바일 디바이스나 출납 시스템에서 필요한 암호 연산들은 수 msec안에 처리가 가능하므로 현재 컴퓨팅 능력을 고려하면 사용자나 출납원의 암호화나 멱승 등은 실시간 처리가 충분히 가능한 것으로 여겨진다.

한편, 발행자는 수동 모드로 통신을 하고 저용량, 저성능을 가지고 있음을 고려해야 한다. 그럼에도 제안하는 모바일 쿠폰 프로토콜에서 발행자는 쿠폰 발행을 위해 암호화 연산을 필수적으로 수행할 수 있어야 한다. 실제로 모바일 쿠폰 시스템을 처음 제안했던 Feldhofer 등은 NFC와 비슷한 환경하에서 수동형 RFID 태그에 AES를 충분히 구현할 수 있음을 보이기도 하였다[13]. 또한 최근에는 제한된 구현 환경을 고려하여 PRESENT나 LEA 등과 같은 초경량화 암호 알고리듬[18, 19]들이 제안되고 있으므로 이를 활용하면 발행자의 쿠폰 발행 비용을 최소화할 수 있다.

앞 장의 프로토콜별 분석 과정에서 언급한 바와 같이 Dominikus 등의 프로토콜은 PKI에 기반하여 동작하게 되므로 공개 키 기반 구조를 별도로 구축해야 하는 문제가 있다. Hsiang 등의 프로토콜은 해시 함수를 기반으로 하고 있어 고속 수행이 가능하다, 그러나 계산량이 적은 반면 언급한 바와 같이 안전성 면에서는 여러 가지 취약한 특성을 가지고 있다. Alshehri 등의 프로토콜에서는 사용자와 출납원간의 비밀 키를 어떻게 공유하는 할 것인가 하는 키 분배 문제가 그대로 남아 있어 인증 문제를 해결하지 못한 프로토콜이라고 할 수 있다.

반면 제안 프로토콜은 대부분의 보안 요구사항을 만족하면서 시스템을 구성하는데 부담이 적은 장점이 있다. PKI 기반 구조를 구축하거나 비밀 키 분배와 같은 기능이 없어도 구동이 가능하며 보너스를 암호화하여 중계 공격도 막을 수 있다.

계산의 효율성 측면에서 볼 때 제안 프로토콜은 Dominikus 등의 프로토콜에 비해 사용자의 계산량 다소 늘어나지만 쿠폰 발행자는 한 번의 암호 연산만 수행하게 되므로 연산량의 증가는 없다고 할 수 있다. 반면 출납원이 수행해야 할 계산량은 줄어들게 된다. 즉, Dominikus 등의 프로토콜에서 출납원은 4번 이상의 멱승을 수행해야 하지만 제안 프로토콜에서는 2번만 수행하면 된다. 그럼에도 위에서 언급한 바와 같이 사용자의 모바일 디바이스나 출납용 장치는 현재의 제안하는 암호 알고리듬을 충분히 실시간 내에 처리할 수 있을 것으로 여겨진다.

5. 결 론

최근 출시되는 스마트 폰을 비롯한 모바일 디바이스에는 NFC 통신을 위한 인터페이스를 제공하고 있으며 이를 이용한 새로운 비즈니스 모델들이 제시되고 있다. 출입 및 신분 인증과 같은 단순 기능을 넘어 모바일 전자지불, 금융 거래, 모바일 쿠폰 시스템과 같은 응용 서비스를 시행하는 단계에 진입하고 있다.

본 논문에서는 모바일 쿠폰 시스템을 안전하게 구현하기 위한 기존의 보안 프로토콜에 대한 안전성을 분석하였다. 이러한 분석을 바탕으로 D-H 키 일치 기법을 기

반으로 하는 새로운 보안 프로토콜을 제시하였다. 제안한 프로토콜은 키 분배 문제뿐만 아니라 사용자 인증과 중계 공격 문제를 동시에 해결할 수 있도록 설계되었다. 따라서 이 프로토콜은 상기한 보안 요구 사항들을 만족하는 NFC 기반의 모바일 쿠폰 시스템을 효과적으로 구현할 수 있다.

References

[1] International Organization for Standardization (ISO), "ISO/IEC 18092: Information Technology - telecommunication and information exchange between systems - Near Field Communication- interface and protocol(NFCIP-1)," 2004.

[2] ECMA, "Near Field Communication Interface and Protocol (NFCIP-1)- 2nd Edition ECMA-340," 2004.

[3] A. Kusuma, "Real World Applications of Near Field Communication," *Interactive Multimedia Conference (IMC'12)*, 2012. Available From: http://mms.ecs.soton.ac.uk/2012/

[4] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)," *Workshop on RFID and Lightweight Crypto (RFIDSec'06),* pp. 3-13, 2006.

[5] M. Aigner, S. Dominikus, and M. Feldhofer, "A system of secure virtual coupons using NFC technology," *Pervasive Computing and Communications Workshops (PerComW'07)*, pp. 362 - 366, 2007.

[6] S. Domonikus and M. Aigner, "mCoupons: An application for near field communication (NFC)," *Advanced Information Networking and Applications Workshops (AINAW'07),* pp. 421-428, 2007.

[7] H. Hsiang H. Kuo, and W. Shih, "Secure mcoupons scheme using NFC," *International Journal of Innovative Computing, Information and Control,* vol. 5, no. 11, pp. 3901-3909, 2009.

[8] A. Alshehri, and S. Schneider, "Formal security analysis of NFC M-coupon protocols using Casper/ FDR," *International Workshop on Near Field Communication (NFC'13),* pp. 1-6, 2013.

[9] A. Alshehri, and S. Schneider, "Formally defining NFC M-coupon requirements, with a case study," *International Conference for Internet Technology and Secured Transactions (ICITST'13),* pp. 52-58, 2013. DOI: http://dx.doi.org/10.1109/ICITST.2013.6750161

[10] A. Alshehri, and S. Schneider, "Formal security analysis and improvement of a hash-based NFC M-coupon protocol," *CARDIS'13, LNCS 8419,* pp. 152-167, 2014.

[12] National Institute of Standards and Technology, "Advanced Encryption Standards," NIST FIPS PUB 197, 2001.

[11] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory,* vol. IT-22, no. 6, pp. 644-654, Nov. 1976. DOI: http://dx.doi.org/10.1109/TIT.1976.1055638

[13] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID system using the AES algorithm," *CHES'04, LNCS 3156,* pp. 357-370, 2004.

[14] G. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," Journal of Computer Security, vol. 19, no. 2, pp. 259-288, 2011.

[15] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," *Workshop on RFID and Lightweight Crypto (RFIDSec'10),* pp. 35-49, 2010.

[16] R. Rivest and A. Shamir, "How to expose an eavesdropper," *Communications of the ACM,* vol. 27, no. 4, pp. 393 - 395, 1984. DOI: http://dx.doi.org/10.1145/358027.358053

[17] National Institute of Standard and Technology, "Digital Signature Standard : FIPS-PUB 186-3," 2009.

[18] D. Hong, J. Lee. D. Kim. D. Kwon, K. Ryu, and D. Lee, "LEA : A 128-bit block cipher for fast encryption on common processors," *WISA'13, LNCS 8367,* pp. 3-27, 2013.

[19] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," *CHES 2007, LNCS 4727,* pp. 450 - 66, 2007.

하 재 철(Jaecheol Ha) **[종신회원]**

- 1989년 2월 : 경북대학교 전자공학과 (공학사)
- 1993년 8월 : 경북대학교 전자공학과 (공학석사)
- 1998년 2월 : 경북대학교 전자공학과 (공학박사)
- 1998년 3월 ~ 2007년 2월 : 나사렛대학교 정보통신학과 부교수
- 2007년 3월 ~ 현재 : 호서대학교 정보보호학과 교수

<관심분야>
정보보호, 네트워크 보안, 부채널 공격