情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

안전한 모바일 쿠폰 프로세스 스킴에 관한 연구

박 현 아*, 박 재 현**

요 약

전자 쿠폰(e-쿠폰)의 패턴이 모바일 쿠폰(m-쿠폰)으로 그 주류를 형성해 나가면서 모바일 쿠폰 보안 시스템에 관한 연구와 운영이 필요하게 되었다. 하지만 지금까지 e-쿠폰의 보안 시스템에 관한 연구도 드물 뿐만 아니라 m-쿠폰의 보안에 관한 연구는 극히 드물며, 설령 있다 하더라도 청산(clearing) 단계에 대한 보안 프로토콜은 설계하지 않았었다. 그렇지만 쿠폰의 위조(forgery)나 이중사용(double spending) 뿐만 아니라 도/소매업자 및 청산소(clearing house)에 의한 청산 단계 조작(clearing manipulation)에 의해서도 기업측에 엄청난 손실을 가할 수 있다. 본 논문에서는 청산 단계를 포함한 공식화된 모바일 쿠폰 프로세싱에 대한 보안 프로토콜을 우리나라 현실 상황을 고려하여 설계하고, 보안요구사항을 모바일 쿠폰 서비스/무선 환경/소형 단말기 측면으로 나누어 분석하고, 효율적이며 상태 관리 용이함을 분석하였다.

Ⅰ. 서 론

판매촉진의 한 수단인 쿠폰(coupon)은 불어에서 어원이 유래하였으며, '상품가격의 할인'을 의미한다 [1]. 이 논문에서 다루고자 하는 모바일 쿠폰은 전자상거래의 패턴이 electronic-commerce에서 mobile-commerce로 바뀌면서 결제 시스템에도 변화가 일어나게 되어 모바일 결제 시스템이 등장하게 되면서 쿠폰 역시 e-쿠폰에서 m-쿠폰으로 그 주류를 형성해 나가고 있다. 우리 나라에서도 현재 기프티콘, 기프트쇼, e-쿠폰 등의 명칭으로 SKT, KT, 옥션 등에서 여러 업체들의 할인 쿠폰을 소비자들에게 제공하는 모바일 쿠폰이 있으며, 피자나 다른 패스트푸드 및 외식 업체에서 이벤트 행사의 일환으로 할인 쿠폰을 그들의 웹사이트에서 소비자들에게 직접 제공하는 등 그 사용이 젊은 층을 중심으로 범용화 되어가고 있다.[1)]

이런 사용 증가와 더불어 문제시 되는 것이 부정행위(fraud)로 인한 금융사고이다. 다른 금융사고와는 달리 쿠폰의 피해자는 일반 사용자가 아닌 기업이다. 소비자들의 쿠폰 위조(forgery)나 이중사용(double spending)과 같은 부정행위(fraud)로 인한 기업 측의 손실뿐만 아니라 청산소(clearing house, 은행 혹은 특정 금융기관)나 도/소매업자(retailer) 같은 참여자에 의한 조작행위로 인한 기업의 손실 역시 엄청나다. 현재 제조업자들은 청산 과정에서 도/소매업자들을 신임하지 못하여 '구매 증거(proof of purchase)'를 도/소매업자들로부터 바로 보고받지 않고 제 3기관인 청산소를 별도로 두어 도/소매업자들이 청산소에게 보고하게 하고 청산소가 도/소매업자들에게 해당 금액을 치르고 제조업자에게 보고하는 형식을 취하고 있다. 하지만, 결산 시 쿠폰을 더 끼워 넣는다거나 송장을 조작하는 등 도/소매업자들의 부정행위로 발생하는 많은 손실뿐만 아니라 제 3기관인 청산소의 부정행위도 역시 보고되고 있다 [24].

이 논문에서는 이러한 fraud로 인한 손실을 줄이기 위한 안전한 모바일 쿠폰 시스템을 제안한다. 현대의 모든 서비스 및 시스템이 모바일폰으로 집약되고 모바일폰이 모든 생활의 중심이 되어 수많은 네트워크와

1) 현재 우리 나라의 쿠폰 패턴은 e-쿠폰과 m-쿠폰 중 한 가지를 선택해서 사용하게 되어있다. m-쿠폰은 핸드폰 같은 모바일 디바이스를 이용하여 서비스를 이용하는 것이고, e-쿠폰은 모바일 디바이스가 아닌 PC 같은 단말기로 쿠폰을 다운 받아 그것을 출력하여 매장에 제시하는 것을 의미한다.

본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성·지원사업"의 연구결과로 수행되었음 (NIPA-2010-C1090-1001-0004).

* University of Arizona, Eller College of Management, Artificial Intelligence Lab. (kokokzi@naver.com)
** Case Western Reserve University, Weatherhead School of Management, Department of Information System, (jxp354@case.edu)

연결되어 있는 상황에서 e-쿠폰을 위한 범용적인 보안 시스템으로 m-쿠폰의 안전성을 논할 수는 없다. 또한, 기존의 관련 연구로 안전한 전자 결제 시스템에 관한 연구가 다소 있기는 하지만, e-쿠폰에 관한 연구는 드문 편이며, 특히 m-쿠폰에 관한 연구는 찾아보기 힘들고 Chang et al.의 연구가 유일하다 [8]. 하지만, Chang et al.의 연구 또한 다른 e-쿠폰 연구들과 마찬가지로 쿠폰 프로세스에서 중요한 손실을 유발하는 청산(clearing)과정에 대한 언급 및 보안 대책이 없다. 오로지 쿠폰의 발급 및 배포 과정과 상품교환(redemption) 단계에서 사용자들의 쿠폰 위조(forgery)와 이중사용(double spending)을 막기 위한 연구만이 있을 뿐이다. 따라서 본 논문에서는 공식화되어 있는 쿠폰 프로세스 3단계에 입각하여 청산(clearing) 단계까지 모두 포함한 우리나라 현실 상황을 고려한 안전한 모바일 쿠폰 프로세스 스킴을 제안한다. 이 스킴은 모바일 쿠폰서비스의 '선물하기' 기능도 지원한다. 자세한 공헌도는 다음과 같다.

1.1. 공헌도

1) Delivery(발급), Redemption(상품교환), Clearing (청산)의 단계로 공식화되어 있는 쿠폰 프로세스에 맞춰서 실시간 모바일 쿠폰 보안 프로토콜을 설계하였다 (이 과정에 맞춰서 스킴을 설계한 기존 연구는 현재까지 없다).

2) 기존 논문에서는 찾아 볼 수 없었던 청산(Clearing) 단계에 대한 보안 프로토콜도 설계함으로써 사용자에 의한 쿠폰 위조(forgery)나 이중사용(double spending) 같은 fraud 뿐만 아니라 기업, 소매업자, 청산소(clearing house)에 의한 청산과정 조작(clearing manipulation) 역시 막을 수 있다.

3) 우리 나라 현실 상황을 고려한 스킴을 설계한다. 결제 과정이 선행하는 특성을 고려하여 기존 쿠폰 프로세스 단계에 등록 및 결제 단계를 추가한 4단계 보안 프로토콜을 설계하였다.

4) 모바일 쿠폰 시스템이 요구하는 보안 요구 사항을 서비스 이용시/무선 환경/소형 단말기와 관련한 3가지 측면으로 나누어 제시하고 제시한 스킴이 이를 만족하는지를 분석한다.

5) 효율적이다. 공개키 연산을 최소화하고 비밀공유키를 이용한 대칭키 암호화 기법을 사용한다. 이는 개인 소형 단말기라는 모바일폰의 하드웨어적인 제약 사항을 극복하는 방법의 일환이기도 하다.

6) 상태 관리가 용이하다(States Manageability) [13, 14]. 쿠폰 발급자는 쿠폰 프로세스 테이블을 유지/관리 함으로써 쿠폰의 프로세스 상태를 실시간으로 체크할 수 있으며 이 체크를 통해서 쿠폰의 유효성을 확인한 후 다음 과정으로 진행할 수 있게 하여 모든 참여자들에 의한 부정행위(fraud)를 막을 수 있게 하였다.

7) 사용자의 프라이버시를 보호한다. 사용자는 등록시 가명(pseudonyms)을 발급받아 서비스 이용시 아이디 대신 사용함으로써 가익명성(pseudonymity)을 보장 받을 수 있다. 서비스 사용시 권한(authorization) 및 인증(authentication)이 필요하지만 프라이버시 보호를 위해 개인 인증(identification)이 되어져서는 곤란하기 때문에 가명(pseudonyms)의 사용이 바람직하다 [17].

8) 쿠폰 전달 프로토콜을 설계하여 모바일 쿠폰 서비스의 '선물하기' 기능을 가능하게 하였고 이 역시 위조(forgery)나 이중사용(double spending)과 같은 모든 부정행위(fraud)의 위협으로부터 안전하게 설계되었다.

Ⅱ. 모바일 쿠폰

2.1. Couponing Process

Couponing Process는 Delivery, Redemption, Clearing의 3가지 과정으로 이루어진다 [4, 23].

2.1.1 Delivery(발급)

사용자가 쿠폰을 발급받는 과정으로 다시 Pull과 Push의 두 가지 과정으로 구성된다.

- 요청(Pull) - 사용자는 모바일 쿠폰(mobile-coupon, m-쿠폰)을 발급 받거나 이메일 혹은 우편으로 쿠폰을 전송받기 위해 요청 메시지를 보낸다. 그리고 발급자의 어플리케이션을 다운로드하고 'Push'를 활성화 시킨다.
- 전송(Push) - 발급자가 사용자의 'Pull' 요청에 대해 쿠폰을 사용자에게 전송한다. SMS(short message service)나 MMS(multimedia message service)로 모바일 쿠폰을 전송받거나 이

메일이나 우편으로 쿠폰을 발급받는다. 이때 사용자에게 발급되어진 쿠폰은 다른 사용자에게 전달(transfer) 가능하다.

2.1.2 Redemption(상품교환)

사용자가 발급받은 쿠폰으로 상점(POS, point of sale)에서 물품과 교환하는 과정이다.

- 실시간 리뎀션(Real-time Redemption) - 상품 구매를 위해 WAP(wireless application protocol)에 링크하는 경우를 말한다. 사용자가 m-쿠폰을 상점(POS)에 제시하면, 상점은 비치된 스캐너로 m-쿠폰의 바코드를 스캔하고 그것을 인증하기 위해 중앙 데이터베이스에 접속한다. 이러한 인증 절차를 거쳐 유효한 쿠폰임이 입증되면 사용자는 상품을 수령하게 된다. 이때 상점은 상품 구매에 대한 물리적인 증거로 청산쿠폰(clearing coupon)이라 불리는 티켓을 출력할 수도 있다.
- 오프라인 리뎀션(Offline Redemption) - 리스트에 명시되어 있거나 어떤 독특한 형태로 포맷되어 있는 코드를 가진 쿠폰을 사용한다. 상점은 쿠폰의 유효성 입증을 위해 중앙 데이터베이스에 접속할 필요가 없는 경우이다. 따라서 상점은 상품 구매의 입증과 clearing(청산)을 위해 '청산쿠폰(clearing coupon)'을 반드시 출력해야 한다.

2.1.3 Clearing(청산)

구매 완료 후, 상점은 완벽한 구매증거(proof of purchase)를 은행이나 특정 금융기관 같은 청산소(clearing house)에 보낸다. 청산소(clearing house)는 쿠폰에 대한 구매증거를 확인하고 상점에게 해당 금액을 지불한다.

- 자동화(automatic) - '청산쿠폰(clearing coupon)' 없이 청산 과정이 이루어진다. 특히, 디지털 상품의 구매와 같은 경우로 실시간 리뎀션에서의 청산 과정이다. 따라서 각 구매마다 실시간으로 구매증거를 청산소에 보낸다.
- 수동화(manual) - 상점은 일과가 끝날 때 그날 리뎀션한 청산쿠폰을 모아, 그 꾸러미를 상점 연합 공동 사무실로 보낸다. 그곳에서 연합된 수많은 상점들로부터 온 쿠폰이 계산되어진 후, 그 상점의 청산소로 청산쿠폰 꾸러미를 보낸다.

2.2 관련 연구

모바일 쿠폰이 최근들어 크게 호응을 얻고 있기는 하지만 모바일 쿠폰의 보안과 관련한 연구는 매우 드물며, 모바일 쿠폰보다 좀 더 넓은 개념인 전자 쿠폰(electronic coupon)의 보안에 관한 연구가 다소 있기는 하지만, 이 역시 많지는 않다. 이 장에서는 e-쿠폰의 보안과 관련한 선행 연구들을 먼저 살펴보고, 모바일 쿠폰의 보안과 관련한 Chang et al.의 연구를 간략히 소개한 후, e-쿠폰과 m-쿠폰과의 차이점을 비교한다.

2.2.1 관련연구

Anand et al.은 인터넷에서 e-쿠폰을 발급하는 시스템을 제안하였다. 이 시스템은 사용자들이 인터넷 상에서 온라인 스토어(online store)에 방문할 때 적절한 시기에 e-쿠폰을 사용자에게 제공한다. 그들은 특히 e-쿠폰의 컨텐츠, 라이프 사이클(life cycle), 사용자들의 구매 욕구 충동을 불러일으키기 위해 e-쿠폰을 배부하는 방법에 대해 집중적으로 연구하였다 [2].

Chang et al.은 [9,10]에서 디지털 기프트 증서와 모바일 결제 매카니즘에 대해 연구하였다. 전자 백화점(electronic department store)의 계산 복잡도를 줄이기 위한 2가지 스킴을 제안하였으며, 이는 보안적인 측면 뿐만 아니라 효율성 역시 고려한 것으로 실제 환경에 적용 가능하다.

Bao는 [5]에서 PTD(personal trusted device)를 위한 디지털 티켓을 고안하였다. 이 티켓은 이벤트 티켓, 디지털 화폐(cash 또는 check), 디지털 쿠폰 등 이 모든 것을 포괄하는 광범위한 개념으로, 이런 디지털 티켓들의 다양한 특성을 포괄하는 일원화된 PTD를 위한 티켓 포맷을 개발하고, PTD의 작은 스크린에 적합한 티켓 컨텐츠를 디스플레이하는 스킴을 제안하였다.

[21]에서 Shojima et al.은 동기(incentive)가 첨부된 P2P(peer to peer) e-쿠폰 시스템을 제안하였다. 이 시스템에서 사용자는 중개자들에게 동기를 제공함으로써 향후 소비자가 될 사용자들에게 e-

쿠폰은 전송하고, 서비스 제공업자들은 e-쿠폰 안에 배포(distribution) 기록을 저장한다. 이 때 그 기록이 악의적으로 변경되는 문제를 해결하기 위하여 queue 구조가 사용되고, 공개키 (public key queue)를 이용하여 모바일 기기 상에서 전자 서명을 함으로써 배포 기록이 변경되지 않고 유지되게 하는 메소드이다.

Blundo et al.은 [6,7]에서 웹 상에서 배포와 생성이 효율적인 e-쿠폰 프로토콜을 설계하였다. 그들은 효율성과 더불어 등록 과정을 제거함으로써 사용자의 익명성을 유지하여 프라이버시를 보호하고 그들이 제시한 보안 요구 사항을 만족하는 2개의 프로토콜을 제안하였다.

Garg et al.은 이중 사용(double spending)을 막기 위한 제 3기관 기반의 쿠폰 민트(coupon mint)를 제안한다. 쿠폰 민트는 할인 금액이나 상품 설명 등과 같은 프로모션의 세부 사항을 전혀 알 수 없으며, 단지 온라인 쿠폰 인증을 위한 인프라만을 제공하는 안전한 e-쿠폰 시스템이다 [15].

지금까지 e-쿠폰 보안과 관련한 연구들을 살펴보았다. Chang et al.은 [8]에서 모바일 사용자들을 위한 안전한 e-coupon 시스템을 제안한다. 이 시스템은 모바일 단에서의 지수승 연산과 같은 복잡한 계산 과정을 제거하여 모바일 사용에 적합하게 하였으며, 발급된 쿠폰에 시리얼 넘버를 부여하여 이중 사용을 막고, 발급자로 하여금 쿠폰에 서명을 하게 함으로써 상점이 쿠폰을 인증할 수 있으며, 쿠폰 위조를 막을 수 있다. 하지만, 이 시스템 역시 다른 e-coupon 연구와 마찬가지로 clearing 과정에 대해서는 고려하지 않았다. clearing 과정은 m-쿠폰이 다른 일반 e-쿠폰 시스템과 두드러진 차이를 보이는 부분이다.

2.2.2 e-쿠폰과 m-쿠폰과의 차이점

일반 e-쿠폰 시스템의 청산(clearing) 과정은 구매 종료 후 상점이 '청산쿠폰(clearing coupon)'을 모아 뒀다가 하루 일과가 끝나면 그 모아진 쿠폰을 '청산소(clearing house)'에 전송하지만, 모바일 쿠폰에서는 구매 종료와 동시에 구매에 대한 증거를 청산소에 보내게 된다. 이런 과정상 차이 뿐만 아니라 보안상에 있어도 청산은 상당히 중요한 부분이다. 리뎀션 과정에서는 사용자에 의한 이중 사용이나 위조 공격으로 인한 기업측의 손실이 크지만, 청산 과정에서는 악의적인 상점의 직원이나 고용주, 혹은 청산소의 부정 행위에 의한 손실이 크다. 현재까지 다음과 같은 사고를 막을 수 있는 적절한 시스템은 없는 것으로 알려져 있다 [24].

- 부도덕한 상점이 일과를 마친 후 청산쿠폰 꾸러미에 몇 장의 쿠폰을 더 끼워 넣거나 송장 차감액을 조작하는 경우
- 상점이 보고한 높은 리뎀션 비율을 불만스러워 하는 제조업자는 상점에게 전액을 지급하려 하지 않거나 정산서(adustments)와 청구액 환급(charge back)을 조작하는 경우
- 부패한 청산소가 쿠폰 제출(submission), 차감(deduction), 청구액 환급(charge back)이나 정산서(adustments)를 조작하는 경우

이 논문에서는 모바일 쿠폰 시스템에서 실시간으로 모든 과정이 안전하게 이루어지도록 하여 이러한 문제점들을 해결하고, 특히 기존 연구들에선 볼 수 없었던 청산 과정까지 안전하게 설계한다.

모바일 쿠폰이 e-쿠폰의 한 종류이긴 하지만, 휴대형 개인 정보 기기라는 다른 e-쿠폰과 구분되는 엄격한 차이점을 가지고 있다. 따라서 소형 단말기가 갖는 하드웨어 및 소프트웨어적 한계점과 더불어 유선 상 보안 뿐만 아니라 무선 상에서의 보안 취약점 또한 고려되어져야 한다. 또한, 모바일 뱅킹이나 모바일 주식 거래가 보편화되는 등 모바일 폰이 디지털 만능기기(All in One)로 변신하면서 e-쿠폰 역시 모바일 쿠폰의 형태로 집중되어져가는 현상을 보이고 있다. 이러한 이유로 기존의 e-쿠폰을 위한 보안 시스템으로 모바일 쿠폰의 안전한 시스템을 장담할 수 없기 때문에 모바일 만을 위한 안전한 couponing process의 설계가 필요한 것이다.

Ⅲ. Preliminaries

이 장에서는 본 논문에서 구축할 스킴의 제반 사항에 대해서 알아본다.

3.1 응용 환경

3.1.1 쿠폰의 유형과 프로세스

쿠폰은 판매촉진의 한 수단이며, 판매촉진은 제조업체가 유통업체, 도매상, 또는 소매상 등과 같은 중간상에게 제공하는 업계촉진과 소매상이 주체가 되어 소비자에게 제공하는 소매상촉진, 그리고 제조업체가 직접 소비자에게 제공하는 소비자촉진 등 3가지로 구분된다 [1]. 본 논문에서는 현재 우리 나라 모바일 쿠폰의 주 형태 중의 하나인 기프티쇼, 기프티콘, 또는 옥션의 e-쿠폰처럼 인터넷을 매체로 하여 제공하는 업계촉진 수단 쿠폰을 모델로 하여 안전한 쿠폰 프로세스 (SMCP, secure mobile couponing process)를 설계한다.

이와 같은 현재 우리 나라 모바일 쿠폰들은 2장에서 설명한 쿠폰 프로세스 3단계를 거치기 전에 결제 과정이 선행하는 특성이 있다. 우리 나라 현실에 맞는 스킴 설계를 위하여 등록 및 결제(Registration and Payment) 과정을 추가한 4단계 모바일 쿠폰 프로세스를 제안한다.

3.1.2 참여자 및 응용 시나리오

- 발급자(issuer(I) 혹은 manufactuer) - 쿠폰 기반의 광고를 함으로써 상품을 선전하려는 상품의 제조업자로 본 논문에서는 쿠폰 프로세스 테이블을 유지 관리함으로써 쿠폰의 상태 관리를 용이하게 하고 각 참여자들의 부정행위를 막는다.
- 소매업자(retailer(R) 혹은 POS(point of sale)) - 상품을 판매하는 상점의 소유주.
- 광고업자(advertiser(A)) - 온라인 광고를 통해 소비자들에게 쿠폰을 배포한다.
- 소비자(user(U) 혹은 customer) - 광고업자의 웹페이지에서 광고를 보고 쿠폰 발급을 요청하고 소매업자의 상점(오프라인(현장)/온라인)에서 상품을 구매한다.
- 청산소(clearing house(CH)) - 은행 혹은 다른 특정 금융 기관으로, 소비자가 쿠폰을 제출하여 제품을 구입하면 발급자는 소매업자로부터 구매완료에 대한 증거를 직접 회수하거나 청산소(clearing house)를 거쳐 회수하고, 청산소는 소매업자에게 회수한 내용에 상응하는 금액을 지불한다.

응용 시나리오. 소비자 U_i는 광고업자 A의 웹페이지에서 발급자 I의 제품 광고를 보고 모바일 쿠폰을 발급받기 위하여 발급자 회사에 등록하고 그 상품에 대해 결제를 한다. 결제 완료 후 소비자는 발급자에게 쿠폰 발급을 요청하고 소매업자 R_n의 상점에서 제품을 구매하면 소매업자는 그 구매 완료에 대한 증거를 바로 청산소 CH_m에 보내고 청산소는 소매업자에게 해당 금액을 지불하고 그 결과를 발급자에게 최종 보고한다.

3.2 보안 요구사항

모바일 쿠폰 시스템에서의 보안 취약점은 크게 다음과 같은 이유로 인해서 발생한다: 1. 모바일 쿠폰 서비스와 관련, 2. 유/무선 환경, 3. 소형 개인 단말기. 이 논문에서는 다른 일반 전자 시스템과 공통적인 문제인 유선 환경에서의 보안 문제는 따로이 고려하지 않으며 다음 세 가지 항목에 대한 보안 요구 사항을 살펴본다.

3.2.1 모바일 쿠폰 서비스와 관련한 보안 요구 사항

1) 인증(authentication) 및 권한(authorization) - 사용자는 자신이 단말기의 소유주이며 그 서비스와 쿠폰을 사용할 정당한 권한을 가졌음을 입증하여야 한다.

2) 가익명성(pseudonomity) - 사용자의 프라이버시를 보호하고 인증 가능하기 위해 가명(pseudonym)을 사용한다. 가익명성(pseudonomity)은 하나 이상의 가명(pseudonyms) 하에서 사용자가 그의 identity를 드러내지 않고 서비스나 리소스를 이용할 수 있도록 하는 것으로, 사용자가 그의 행위에 책임을 져야 하고 익명성을 제공받지 못할 때 사용자의 identity를 보호할 수 있다 [17].

3) 위조 방지(unforgeability) - 발급자만이 유효한 쿠폰을 제공할 수 있으며, 다른 어떤 참가자나 공격자가 그것을 위조할 수 없다 [8].

4) 부인 방지(non-repudiation) - 각 참여자는 자신이 관여한 트랜잭션을 부인할 수 없다.

5) 이중사용 방지(preventing from double-

spending) - 사용자가 같은 쿠폰을 한번 이상 사용하는 것으로부터 제조업자를 보호하여야 한다 [8].

6) 무결성(integrity) - 쿠폰의 유효기간, 수량, 제공하는 서비스와 같은 쿠폰의 컨텐츠를 사용자나 다른 공격자에 의해 변경되지 않고 전송 에러 없이 안전하게 원래와 같은 상태로 전송되는 것을 말한다.

7) 청산 조작 방지(preventing from clearing manipulation) - 청산 과정에서 앞서 설명한 소매업자, 제조업자, 청산소에 의한 악의적인 쿠폰 조작을 막는다 [24].

3.2.2 무선 인터페이스 보안 요구 사항

1) 인증 및 권한 [18] - 무선 인터페이스와 관련하여 사용자 및 서버의 서비스 인증이 제대로 이루어지지 않았을 경우 시스템 상에서 발생할 수 있는 문제는 다음과 같다.

- 데이터로의 인가되지 않은 접근
- 도청
- 무결성 위협
- 서비스 거부(DoS)
- 시스템으로의 인가되지 않은 접근
- 또 다른 시스템으로 가장 : 침입자는 네트워크 상에서 또 다른 사용자로 가장할 수도 있다. 침입자는 사용자를 향해 기지국인척 가장할 수도 있으며 그때 인증을 수행한 후에 연결을 하이젝킹할 수도 있다.

2) 전파 간섭(Frequency Jamming)으로부터의 보호 [18] - 무선 환경에서 강한 주파수 간섭을 발생시켜 서비스거부공격을 유도하는 주파수 간섭 공격으로부터 보호되어져야 한다.

3) 해킹/ 악성코드에 대한 방어 [18,19] - 현재 모바일 폰에서는 폰 바이러스가 창궐하고 있는 추세로 이는 점차 고도화 되어 다른 정보기기(PC, PDA 등)로 전이된 사례도 있다. 폰 바이러스나 폰 웜(Worm)은 모바일 폰의 개인정보를 파괴하거나 다른 폰으로 무차별 전송할 수 있기 때문에 이에 대한 철저한 보안적 관리가 요구된다.

3.2.3 소형 개인 정보기기 보안 요구 사항

1) 분실 시 단말기 오/남용 방지와 개인정보 보호 [18,19] - 모바일폰을 도난 당하거나 잃어버렸을 경우, 그 안에 저장되어 있는 개인정보가 노출되고 습득자 및 도난자에 의해 'false biometric'처럼 모바일폰 내에 저장되어 있는 정보가 변경되는 등 모바일폰이 잘못 사용되는 것을 막아야 한다.

2) 불법복제 단말의 위협으로부터 보호 [18] - 기존 이동통신의 경우, 핸드폰 고유 식별자인 ESN (Electronic Serial Number) : 무선 전화기의 마이크로칩 속에 생산자가 삽입해 넣은 32비트의 전세계 고유 번호로, 가입자가 통화를 시도하면 자동으로 ESN과 전화기 사업자의 MIN(Mobile Identification Number)이 송출되며 기지국을 통해 이 번호가 인증이 되면 통화를 연결하고 번호를 복사하여 복제폰을 만드는 것이 가능하다. 이 불법복제에 의한 피해가 계속 발생하고 있는데 이로부터 보호되어져야 한다.

3) 서비스 거부(DoS) 공격에 대한 방어 [18,19] - 소형 단말기의 제한적인 계산 능력과 저장 공간은 서비스 거부(DoS) 공격에 취약하므로 이에 대한 보안 대책이 요구된다.

Ⅳ. SMCP (Secure Mobile Couponing Process)의 설계

4.1 등록 및 결제 (Registration and Payment)

4.1.1 등록 및 결제 프로토콜

[소비자 U_i --〉모바일폰 MP_i]:
1. 입력: pw_i', v_i', i_i'[MP_i]:
2. 계산: $h(pw_i')$
3. 검증: $h(pw_i')=h(pw_i)$, $v_i'=v_i$, $i_i'=i_i$
   [U_i/ MP_i ---〉〉 발급자 I]:
4. 전송: $a=E_{P_j}(U_i, k_i)$, $b=UC_i$, $c=h(a|b)$

[발급자 I]: 5. 검증/복호화: $h(a|b)=c$,
$D_{S_I}(E_{P_i}(U_i, k_i))=U_i, k_i$

[U_i/ MP_i 〈〈--- I]: 6.전송: $E_{k_i}(p_i)$

[U_i/ MP_i]: 7.복호화: $D_{k_i}(E_{k_i}(p_i))=p_i$

[U_i/ MP_i ---〉〉 I]: 8.전송: $E_{k_i}(p_i, M_{ij}|G_j)$

[U_i/ MP_i 〈〈--- I]: 9.전송: $E_{k_i}(R_{i\_}M_{ij}|G_j)$

4.1.2 등록 및 결제 프로토콜의 상세과정

1. 소비자 U_i는 그의 모바일폰 MP_i에 사용자 인증을 하기 위해 패스워드 pwi′와 음성정보 v_i', 이미지 정보 i_i'를 입력한다.

2. 모바일폰 MP_i는 입력받은 pw_i'값으로 $h(pw_i')$를 계산한다.

3. 모바일폰 메모리에 미리 저장되어 있던 $h(pw_i)$, v_i, i_i값으로 $h(pw_i')=h(pw_i)$, $v_i'=v_i$, $i_i'=i_i$를 검증한다.

4. 검증에 모두 성공하면, 소비자 U_i와 모바일폰 MP_i는 하나의 주체로 간주된다. U_i/MP_i는 자신이 원하는 쿠폰을 발급 받기위해 우선 쿠폰의 발급자 I에게 등록한다. U_i는 소비자를 나타내는 정보이고, UC_i는 소비자 U_i의 인증서이며 k_i는 Ui/MP_i가 생성한 랜덤값이다. U_i와 k_i는 발급자의 공개키 P_I로 암호화하여 전송한다.

5. I는 전송받은 데이터의 무결성을 체크; $h(a|b)=c$한 후, 자신의 비밀키 S_I를 이용하여 $D_{S_I}(E_{P_I}(U_i,k_i))=U_i,k_i$를 복호화하고 UC_i로 U_i를 인증한다.

6. I는 복호화한 k_i로 p_i를 암호화하여 전송한다. p_i는 서비스 사용시 쓸 U_i/MP_i의 가명(pseudonyms)이고, k_i는 4번 과정에서 생성한 랜덤값으로 U_i/MP_i와 발급자 I가 공유한 비밀키 값이 된다.

7. U_i/MP_i는 k_i로 전송받은 데이터를 복호화 하여 p_i를 구한다.

8. U_i/MP_i는 k_i로 p_i와 $M_i|G_j$를 암호화하여 I에게 전송한다. Gj는 U_i가 원하는 상품에 관한 설명이고, M_{ij}는 상품 Gj에 대해 U_i가 지불한 금액이다.

9. I는 전송받은 데이터를 k_i로 복호화하여 $M_i|G_j$를 확인하고, 영수증 $R_{i_}M_{ij}\|G_j$를 암호화하여 U_i/MP_i에게 전송한다.

4.2 발급 (Delivery)

발급 단계는 요청(Pull)과 전송(Push)의 두 단계로 이뤄진다.

4.2.1 요청(Pull) 프로토콜

〔소비자 U_i/ 모바일폰 MP_i〕: 1.랜덤값 생성: α

2.계산: $a=h(k_i)$, $b=a\alpha$, $c=E_{k_i}(R_{i\_}M_{ij}|G_j)$,

$d=E_{k_i}(ct)+\alpha, e=h(p_i|b|c|d)$

〔U_i/MP_i ---〉〉 발급자 I〕: 3.전송: p_i, b, c, d, e

〔발급자 I〕: 4. 검증: $e=h(p_i|b|c|d)$

4.2.2 전송(Push) 프로토콜

〔발급자 I〕: 5.계산:

$\frac{b}{h(k_i)}=\alpha,\ d-\alpha=E_{k_i}(ct), D_{k_i}(E_{k_i}(ct))=ct$

〔Ui/MPi 〈〈--- I〕: 6.전송: C_{ij}, $S_{S_I}(h(C_{ij}))$.

$C_{ij}=Display|E_{k_i}(Non-Display)$,

$Display=$ {B_Code_{ij} 혹은 CCK_{ij}, TTL_{ij}(time to live), Pdt, Amt, Mnf, Offer},

$Non\text{-}Display=$ {Prc, Ui, $Ri\_M_{ij}|G_j$}

4.2.3 발급(Delivery) 프로토콜의 상세과정

1. 등록 과정에서처럼 사용자 인증을 마친 Ui/MPi는 랜덤값 α를 생성한다.

2. U_i/MP_i는 α를 가지고 다음을 계산한다;

$a=h(k_i), b=a\alpha, c=E_{k_i}(R_{i\_}M_{ij}|G_j), d=E_{k_i}(ct)+\alpha,$

$e=h(p_i|b|c|d)$. 여기서 ct는 현재 시간(current time)을 의미한다.

3. U_i/MP_i는 자신의 가명 p_i와 계산한 값들 b, c, d, e를 전송한다.

4. I는 $h(p_i|b|c|d)$를 계산하고 $e=h(p_i|b|c|d)$를 검증한다.

5. 검증이 성공적이면, I는 p_i를 보고 자신의 테이블에 저장되어 있는 U_i/MP_i에 관한 데이터에 접근해 k_i를 찾아내고 다음을 계산한다;

$\frac{b}{h(k_i)}=\alpha,\ d-\alpha=E_{k_i}(ct), D_{k_i}(E_{k_i}(ct))=ct$.구해낸 ct가 허용된 오차 범위 내에서 현재 시각과 일치하는지 검증한다.

6. 검증이 성공적이면, I는 상품 Gj에 대한 U_i/MP_i의 쿠폰 C_{ij}와 발급자의 개인키 S_I를 이용해 쿠폰 C_{ij}의 서명을 생성해서 U_i/MP_i에게 전송한다. 쿠폰 C_{ij}는 다음과 같이 구성되어 있다;

$C_{ij}=Display|E_{k_i}(Non-Display)$, 여기서 $Display=$ {B_Code_{ij} 혹은 CCK_{ij}, TTL_{ij} (time to live), Pdt, Amt, Mnf, Offer}로 구성되고, $Non\text{-}Display=$ {Prc, U_i, $R_i\_M_{ij}|G_j$}로 구성된다. B_Code_{ij}는 쿠폰 C_{ij}의 바코드이고 CCK_{ij}는 쿠폰 C_{ij}를 인증할 수 있는 식별 가능한

고유번호이며 TTL_{ij} (time to live)은 쿠폰 C_{ij}의 유효기간이다. Pdt는 제품명, Amt는 수량, Mnf는 제조업자, $Offer$는 제공되는 서비스를 말하며, Prc는 가격, U_i,는 소비자 개인에 대한 정보, $R_i_M_{ij}/G_j$는 상품 G_j의 영수증이다. 5번에서 계산한 α는 쿠폰 C_{ij}의 관련 정보로 쿠폰 프로세스 테이블에 같이 저장해 둔다.

4.3 상품 교환 (Redemption)

4.3.1 상품교환 (Redemption) 프로토콜

〔소비자 U_i/ 모바일폰 MP_i〕; 1.계산:
$\gamma = E_\alpha(TTL|rt), a = h(k_i)\gamma, b = C_{ij} + \gamma, c = E_{k_i}(rt),$
$d = h(B\_Code_{ij}|a|b|c|e) e = E_{k_i}(rt + \alpha + 11)$
〔U_i/MP_i ---〉〉 소매업자 R_n〕; 2.전송: B_Code_{ij} (혹은 CCK_{ij}), a, b, c, d, e, $S_{S_I}(h(C_{ij}))$
〔소매업자 R_n〕; 3.스캔(혹은 확인): B_Code_{ij}(혹은 CCK_{ij})
4.검증: $d = h(B\_Code_{ij}|a|b|c|e)$
〔소매업자 R_n --〉〉 발급자 I〕; 5.전송:
$B\_Code_{ij}|E_{P_I}(n), E_{k_n}(a,b,c,d,e)$
〔발급자 I〕; 6.복호화: $D_{S_I}(E_{P_I}(n)) = n,$
$D_{k_n}(E_{k_n}(a,b,c,d,e)) = a,b,c,d,e$
7.검증: $d = h(B\_Code_{ij}|a|b|c|e)$
8.계산: $\frac{a}{h(k_i)} = \gamma,\ b - \gamma = C_{ij},$
$D_{k_i}(e) = D_{k_i}(E_{k_i}(rt + \alpha + 11)) = rt + \alpha + 11$
9.검증: Cij = Cij′ 확인 후, 쿠폰 프로세스 테이블에서 리뎀션 여부를 확인한다.
10.계산:
$D_\alpha(\gamma) = D_\alpha(E_\alpha(TTL|rt)) = TTL|rt$
11.검증: $rt \in TTL, D_{k_i}(e) - rt - \alpha = 11$
〔소매업자 R_n 〈〈-- 발급자 I〕; 12.전송:
$E_{k_n}(C_{ij}, D_{k_i}(e))$
〔소매업자 R_n〕; 13.복호화/서명 검증:
$D_{k_n}(E_{k_n}(C_{ij},\ D_{k_i}(e))) = C_{ij}, D_{k_i}(e)\ /\ S_{S_I}(h(C_{ij}))$
〔U_i/MP_i 〈〈—소매업자 R_n〕;14.상품전달/영수증 전송: $RGj/E_{D_{k_i}(e)}(rB\_Code_{ij})$. 〔$U_i/MP_i$〕; 15.상품수령
$rB\_Code_{ij} = (n,\ B\_Code_{ij},\ RN_{ij},\ rt,\ Pdt,\ Amt,\ Mnf)$
및 영수증 복호화:
$D_{(rt+\alpha+11)}(E_{D_{k_i}(e)}(rB\_Code_{ij})) = rB\_Code_{ij}$

4.3.2 상품교환 (Redemption) 프로토콜의 상세과정

1. 등록 과정에서처럼 사용자 인증을 마친 U_i/MP_i는 다음을 계산한다. $\gamma = E_\alpha(TTL|rt),\ a = h(k_i)\gamma, b = C_{ij} + \gamma,$ $c = E_{k_i}(rt), d = h(B\_Code_{ij}|a|b|c|e), e = E_{k_i}(rt + \alpha + 11)$

2. U_i/MP_i는 소매업자 R_n에게 B_Code_{ij}(혹은 CCK_{ij}), a, b, c, d, e, $S_{S_I}(h(C_{ij}))$을 전송한다.

3. 데이터를 전송 받은 소매업자 R_n은 B_Code_{ij} (혹은 CCK_{ij})를 스캔(혹은 육안으로 확인)한다.

4. R_n은 $h(B_Code_{ij}|a|b|c|e)$를 계산하고 이 값이 d와 일치하는지 검증한다. 이것은 데이터가 전송 에러 없이 그대로 잘 전달되었음을 의미한다.

5. 검증에 성공하면 R_n은 발급자 I에게 $B\_Code_{ij}|E_{P_I}(n)$, $E_{k_n}(a,b,c,d,e)$을 전송한다. P_I는 I의 공개키이고, k_n은 I와 R_n의 비밀 공유키이다.

6. I는 전송받은 데이터를 다음과 같이 복호화한다. $D_{S_I}(E_{P_I}(n)) = n, D_{k_n}(E_{k_n}(a,b,c,d,e)) = a,b,c,d,e$. 여기서 n은 R_n의 고유한 식별 번호이고, n을 구해낸 I는 저장되어 있는 k_n(I와 R_n의 비밀 공유키)을 찾아내어 a,b,c,d,e를 복호화낸다. S_I는 I의 개인키이다.

7. I는 $h(B_Code_{ij}|a|b|c|e)$를 계산하고 이 값이 d와 일치하는지 검증한다. 이 역시 데이터가 전송 에러 없이 그대로 잘 전달되었음을 의미한다.

8. 검증에 성공하면 I는 바코드 B_Code_{ij}로 쿠폰 프로세스 테이블에서 k_I를 찾아내어 $\frac{a}{h(k_i)} = \gamma,$ $b - \gamma = C_{ij}$ $D_{k_i}(e) = D_{k_i}(E_{k_i}(rt + \alpha + 11)) = rt + \alpha + 11$을 계산한다.

9. I는 8번에서 구한 쿠폰 C_{ij}와 쿠폰 프로세스 테이블에 저장되어 있는 바코드 B_Code_{ij}의 쿠폰 C_{ij}'가 일치하는지 확인한 후, 리뎀션 여부를 테이블에서 확인한다. 이미 리뎀션이 시행된 쿠폰이면 프로토콜은 여기서 종료하고 소매업자에게 유효하지 않음(N/A)을 알린다. 아직 리뎀션이 시행되지 않은 쿠폰이면 프로토콜을 계속 수행한다.

10. 테이블에 저장되어 있는 α값으로 $D_\alpha(\gamma) = D_\alpha(E_\alpha(TTL|rt)) = TTL|rt$을 계산한다.

11. I는 $rt \in TTL$을 검증하고, k_i로 $D_{k_i}(e)$를 계산한

〔표 1〕 쿠폰 프로세스 테이블

B_Code_{ij}	가명 p	비밀키 k	α	Cij	등록일	결제일	요청일(Pull)	전송일(Push)
983678938	길동->꽃님 (8.15)	4234439->98 54234(8.15)	12345->9876 5(8.15)	1983678938ji 13048...:	20100807->20 100815(8.15)	20100807	20100807->20 100815(8.15)	20100807->20 100815(8.15)
.....	.....	.....	.....	.....	.....	.....	.....	.....

리뎀션(rt)	소매업자(n)	rB_Code_{ij}	청산일	청산소(m)	$\_rB\_Code_{ij}$	전달일(T_date)
20100815	11110098	48570583	20100815	8474747	346892398	20100815
.....	.....	.....	.....	.....	.....	.....

후, $D_{k_i}(e)-rt-\alpha=11$을 검증한다.

12. 이 모든 검증이 성공하면 I는 테이블에 현재 리뎀션이 시행되었음을 표시하고 R_n에게 다음을 전송한다: $E_{k_n}(C_{ij}, D_{k_i}(e))$.

13. R_n은 $D_{k_n}(E_{k_n}(C_{ij}, D_{k_i}(e)))$을 복호화하여 $C_{ij}, D_{k_i}(e)$을 구하고, 쿠폰 C_{ij}로 서명 $S_{S_I}(h(C_{ij}))$를 검증한다. 여기까지의 검증에 성공했다는 것은 소매업자 R_n이 서명 $S_{S_I}(h(C_{ij}))$를 검증했을 뿐만 아니라 발급자 I가 소비자가 제시한 쿠폰이 유효하다는 것을 동시에 입증하는 것이기도 하다.

14. 검증에 성공하면 R_n은 실제 상품 RG_I를 소비자에게 전달하고 13번에서 구한 $D_{k_i}(e)$로 영수증 rB_Code_{ij}를 암호화하여 소비자에게 전송한다. 영수증 rB_Code_{ij}는 다음과 같이 구성되며: $rB\_Code_{ij}=(n,\ B\_Code_{ij},\ RN_{ij},\ rt,\ Pdt,\ Amt,\ Mnf)$, 여기서 n은 상품을 구매한 상점의 고유번호, RN_{ij}는 영수증 일련번호, rt는 리뎀션 시간, Pdt는 상품명, Amt는 수량, Mnf는 제조업자를 뜻한다.

15. 소바자 U_I는 상품을 수령하고 U_I/MP_I는 $D_{k_i}(e)=rt+\alpha+11$을 비밀키로 하여 영수증을 다음과 같이 복호화한다:

$$D_{(rt+\alpha+11)}(E_{D_{k_i}(e)}(rB\_Code_{ij}))=rB\_Code_{ij}.$$

4.4 청산 (Clearing)

4.4.1 청산(clearing) 프로토콜

〔소매업자 R_n --〉〉 청산소 CH_m〕: 1.전송:
$E_{p_m}(n), E_{k_{nm}}(rB\_Code_{ij})$
〔청산소 CH_m〕: 2.복호화/저장:
$D_{s_m}(E_{p_m}(n))=n$
$D_{k_{nm}}(E_{k_{nm}}(rB\_Code_{ij}))=rB\_Code_{ij}$
〔CH_m --〉〉 발급자 I〕: 3.전송:
$E_{P_I}(m),\ E_{k_m}(rB\_Code_{ij})$
〔발급자 I〕: 4.복호화: $D_{S_I}(E_{P_I}(m))=m$,
$D_{k_m}(E_{k_m}(rB\_Code_{ij}))=rB\_Code_{ij}$
5.쿠폰 프로세스 테이블 체크/저장:
rB_Code_{ij}
〔CH_m 〈〈-- I〕: 6.전송: $E_{k_m}(1|rB\_Code_{ij})$
〔R_n 〈〈-- CH_m〕: 7.복호화/전송:
$D_{k_m}(E_{k_m}(1|rB\_Code_{ij}))=1|rB\_Code_{ij}/$
$M\_rB\_Code_{ij}, E_{k_{nm}}(\_rB\_Code_{ij})$
〔R_n --〉〉 I〕: 8.전송: $E_{P_I}(n), E_{k_n}(\_rB\_Code_{ij})$
〔발급자 I〕: 9.복호화: $D_{S_I}(E_{P_I}(n))=n$,
$D_{k_n}(E_{k_n}(\_rB\_Code_{ij}))=\_rB\_Code_{ij}$/저장

4.4.2 청산(clearing) 프로토콜의 상세 과정

1. 구매가 완료되어 상품 및 영수증 수령이 끝나고 나면, 소매업자 R_n은 $E_{p_m}(n), E_{k_{nm}}(rB_Code_{ij})$을 청산소 CH_m에 전송한다. p_m은 CH_m의 공개키이고 k_{nm}은 R_n과 CH_m이 공유한 비밀키이다.

2. CH_m은 $D_{s_m}(E_{p_m}(n))=n$을 복호화해내고 이것으로 k_{nm}을 찾아내어 영수증 rB_Code_{ij}을 복호화 및 저장한다. s_m은 CH_m의 개인키이다.

3. CH_m은 $E_{P_I}(m),\ E_{k_m}(rB_Code_{ij})$을 계산하여 발급자 I에게 전송한다. P_I는 I의 공개키, k_m은 I와 CH_m이 사전에 공유한 비밀키이다.

4. I는 $D_{S_I}(E_{P_I}(m))=m$를 복호한다. m은 CH_m의 고유한 식별번호이고, 이것으로 k_m을 찾아내어 $D_{k_m}(E_{k_m}(rB_Code_{ij}))=rB_Code_{ij}$을 복호화한다.

5. 영수증 $rB_Code_{ij}=(n,\ B_Code_{ij},\ RN_{ij},\ rt,\ Pdt,\ Amt, Mnf)$의 정보로 쿠폰 프로세스 테이블을 체크할 수 있다. 만약 이미 저장된 영수증이 있다면, fraud가 일어난 것이기 때문에 즉각 사고 조처 단계로 들어간다. 저장된 영수증이 없으면 I는 다른 내용들을 확인한 후 영수증 일련번호를 저장한다.

6. I는 CH_m에게 $E_{k_{im}}(1|rB_Code_{ij})$를 전송한다.

7. CH_m은 $D_{k_{im}}(E_{k_{im}}(1|rB_Code_{ij}))=1|rB_Code_{ij}$를 복호화한다. $1|rB_Code_{ij}$은 영수증 rB_Code_{ij}은 정당한 것으로 그 안에 적혀있는 소매업자 R_n에게 금액을 지불하라는 의미이다.[2] CH_m은 R_n에게 대금 $M_rB_Code_{ij}$을 지불하고 영수증을 암호화 $E_{k_{mn}}(RM_rB_Code_{ij})$하여 전송한다. 대금에 대한 영수증 $RM_rB_Code_{ij}$의 구성은 다음과 같다; $RM\_rB\_Code_{ij}=(B\_Code_{ij}, RN_{ij}, rt, M\_rB\_Code_{ij}, MRN_{ij})$. 여기서 MRN_{ij}는 대금 영수증의 일련번호이다.

8. 대금에 대한 영수증을 받은 R_n은 발급자 I에게 $E_{P_I}(n), E_{k_n}(RM_rB_Code_{ij})$을 전송한다.

9. I는 $D_{S_I}(E_{P_I}(n))=n$을 복호화하여 k_n을 찾아내고 $D_{k_n}(E_{k_n}(_rB_Code_{ij}))=_rB_Code_{ij}$을 복호화한다. 대금 영수증 $RM_rB_Code_{ij}=\ (B_Code_{ij}, RN_{ij}, rt,\ M_rB_Code_{ij}, MRN_{ij})$의 정보로 쿠폰 프로세스 테이블에서 그 내용을 확인하고 대금 영수증 일련번호 MRN_{ij}를 테이블의 대금 영수증 $RM_rB_Code_{ij}$에 저장한다.

V. 스킴 분석 및 논의

5.1 안전성 분석

제안한 프로토콜 SMCP를 3장에서 언급한 보안 요구 사항을 가지고 분석한다.

5.1.1 모바일 쿠폰 서비스와 관련한 보안 요구 사항

1) 인증(authentication) 및 권한(authorization) - 본 논문에서는 $h(pw_i')=h(pw_i)$, $v_i'=v_i$, $i_i'=i_i$ 과정의 사용자와 모바일폰 기기 사이의 인증을 거쳐야만 모바일폰의 메모리나 서비스 사용을 가능하게 하였다. 이러한 사용자-기기의 인증을 통과한 U_i/MP_i는 하나의 주체로서 모바일 쿠폰 서비스 시스템의 소비자로서 역할을 하게된다. U_i/MP_i와 발급자 I사이의 인증은 I가 부여한 U_i/MP_i의 가명 pi와 비밀키 ki를 공유하여 암호 통신을 함으로써 메시지 암호뿐만 아니라 상호 인증 역시 가능하게 하였다. U_i/MP_i와 소매업자 R_n사이의 인증은 두 주체간의 직접적인 통신으로 이루어지지 않고, U_i/MP_i가 R_n에게 전송한 데이터를 R_n이 I에게 전송하여 I가 쿠폰 검증 뿐만 아니라 소비자 U_i/MP_i의 개체 인증까지 대신 수행하게 하였다. R_n과 I, R_n과 청산소 CH_m, CH_m과 I사이의 인증도 각 주체간의 비밀 공유키 k_n, k_{mn}, k_m을 사전에 공유하여 암호 통신을 하게 함으로써 메시지 암호와 상호 인증을 동시에 가능하게 하였다.

2) 가익명성(pseudonomity) - 소비자 U_i/MP_i는 서비스 사용시 본인의 아이디를 사용하지 않고 등록 과정시 발급받은 가명 p_i를 사용한다. 등록 과정시 발급자에게 제공하는 사용자 정보 U_i도서비스 사용에 필요한 최소한의 정보로 제한한다. 서비스 사용 시, 소비자의 프라이버시 보호를 위해서 개인 식별(identification)이 되어서는 안되지만, 서비스를 사용할 수 있는 정당한 사용자이며 권한을 가졌는지를 증명하기 위해 개체 인증(authentification)이 필요하기 때문에 가명 사용이 합당하다고 보여진다.

3) 위조 방지(unforgeability) - 발급자 I의 개인키로 쿠폰에 서명을 하였기 때문에 그 키가 노출되지 않는 한, 다른 어떤 참가자나 공격자가 그것을 위조할 수 없다.

4) 부인 방지(non-repudiation) - 발급자 I의 서명은 공개 검증 가능하며, 모든 세션에서 모든 데이터가 각 주체간 사전에 공유한 비밀키로 암호화되어 전송된다. 그 키를 아는 사람만이 그 암호문을 생성할 수 있으므로 그 데이터 전송에 대한 사실을 부인할 수가 없다.

5) 이중사용 방지(preventing from double-spending) - 발급자 I는 모든 쿠폰에 시리얼 넘버 같은 고유한 바코드 B_Code_{ij}나 CCK_{ij}를 부여하고, [표 1]과 같은 쿠폰 프로세스 테이블을 유지하여 모바일폰을 통해 실시간으로 현장에서 일어난 일들을 전송받아 쿠폰 프로세스 과정을 실시간 체크함으로써 이중사용을 막을 수 있다.

2) 반면, 0이면 영수증이 타당하지 않으므로 대금하지 말라는 의미다.

6) 무결성(integrity) - 무결성 체크를 위해 이 논문에서는 각 단계별로 해쉬 함수를 이용한 전송 메시지 검증 과정을 두어 메시지의 위/변조를 막았다. 추가로, 전 시스템의 원활한 작동을 위해 TPM(Trusted Platform Module) 칩을 사용할 수 있다. TPM은 하드웨어 기기나 소프트웨어가 정상적으로 작동하는가를 인증하기 위한 칩으로 모바일폰 뿐만 아니라 전 시스템에 탑재하여 시스템 작동을 모니터링 할 수 있다 [19].

7) 청산 조작 방지(preventing from clearing manipulation) - 이 역시 발급자 I가 바코드 B_Code_{ij}나 CCK_{ij}를 쿠폰에 부여하고, 쿠폰 프로세스 테이블을 유지하여 모바일폰으로 실시간 으로 모바일 프로세싱 과정을 체킹하고 검증한 후 다음 과정이 이루어지게 함으로써, 청산 과정에서 일어나는 악의적인 쿠폰 조작을 막을 수 있다.

5.1.2 무선 인터페이스 보안 요구 사항

1) 인증 및 권한 - 이 논문에서는 무선 환경에서 일어날 수 있는 도청, 시스템 및 데이터로의 인가되지 않은 접근, 가장 공격, 서비스 거부(DoS), 무결성 위협과 같은 문제를 암호학적인 방법을 사용하여 해결하였다. 전송되는 모든 메시지를 암호화하여 도청, 시스템 및 데이터로의 인가되지 않은 접근, 가장 공격을 막을 수 있으며 동시에 상호 인증 역시 가능하다. 해쉬 함수를 이용한 검증 과정을 둠으로써 무결성 위협을 막았으며, 이런 검증 과정과 개체인증을 통과하지 않으면 다음 과정으로 진행하지 못하게 함으로써 서비스 거부(DoS) 공격도 어렵게 한다.

2) 전파 간섭(Frequency Jamming) - 주파수 간섭 공격은 강한 시그널을 사용하여 주파수 간섭 공격에 의한 간섭을 최소화하거나, 주파수 모니터링 장비를 통해 사전에 공격을 탐지하고 대응할 수 있다. 우선 전파간섭 사실을 중앙전파 관리 연구소에 신고 하는 것과 공격자를 추적하거나 비정상적인 동작을 하는 단말을 모니터링 하는 것이 대책이 될 수 있다 [18].

3) 해킹/ 악성코드 - 비정상트래픽 모니터링하고, 침입차단시스템, 침입탐지시스템, 가상사설망, 바이러스월등 각종 네트워크 보안제품을 사용할 수 있다. 특히 폰 바이러스나 폰 웜(Worm)을 막기 위해서는 Ahnlab V3 Mobile, Virobot Mobile, Norton Smartphone Security for Android Beta/Symbian, Kaspersky Mobile Security 8.0과 같은 모바일폰용 백신 프로그램을 사용할 수 있다.

5.1.3 소형 개인 정보기기 보안 요구 사항

1) 분실 시 단말기 오/남용 방지와 개인정보 보호 - 이 논문에서는 기기와 사용자 간의 인증 과정 $h(pw_i')=h(pw_i)$, $v_i'=v_i$, $i_i'=i_i$을 두어, 이 과정을 거치지 않고는 서비스 사용 및 메모리 접근이 불가능하게 만들어 분실시 단말기가 잘못 사용되고 개인정보가 노출되는 것을 막을 수 있다. 또한 [19]에 의하면, Kaspersky Mobile Security 8.0은 백신 프로그램 기능 뿐만 아니라, SMS Block, SMS Clean, SIM Watch와 같은 도난 솔루션을 제공한다. 이와 같은 상용 프로그램의 사용도 이러한 문제를 해결하는 방법 중의 하나이며, 분실 시에는 사용자가 서비스에게 신고하도록 하여 서버측에서 사용자의 메모리에 저장된 내용을 사용자의 패스워드로 암호화되게끔 하는 메카니즘도 생각해 볼 수 있다.

2) 불법복제 단말의 위협으로부터 보호 - 불법 단말기의 사용을 방지하기 위해서는 단말기 자체에 대한 인증 과정이 필요하다. 디바이스가 서비스의 주체가 되어 서비스 도매인간의 인증기능 로밍이 가능한 멀티도메인 인증기술이 요구되어지는데, 본 논문에서는 1)번에서 말한 기기와 사용자 간의 인증 과정을 두었기 때문에 단말기가 불법 복제되더라도 서비스 사용 및 데이터 접근이 불가능한 무용지물이 되게 하였고, 이 사용자-기기간의 인증 과정이 성공적으로 이루어지면 모바일 쿠폰 시스템의 소비자 U_i/MP_i로서 하나의 주체로 역할하게 하여 모든 서비스를 사용할 수 있게 하였다.

3) 서비스 거부(DoS) 공격에 대한 방어 - 무선 인터페이스 보안 요구 사항에서도 언급하였듯이개체인증과 무결성 검증 과정을 통과하지 않으면 다음 과정으로 진행하지 못하게 함으로써 서비스 거부(DoS) 공격을 어렵게 할 수 있다.

5.2. 효율성 분석

5.2.1 계산 및 통신량의 최소화

제안 스킴 SMCP의 통신은 소비자 U_i/MP_i가 개입

하는 무선환경과 다른 참여자간의 유선환경으로 나눠질 수 있다. 소비자 U_i/MP_i의 모바일폰은 개인 소형 단말기로서 계산과 저장 능력이 다소 제약적이기 때문에 모바일 단에서의 계산량과 전송량을 최소화하는 것에 스킴 설계의 초점을 두었다. 모바일 단에서의 연산은 대부분이 비밀 공유키를 이용한 대칭키 기반 암호화 메소드를 이용하였고, 등록 초기 과정에서 비밀키 공유를 위해 단 한 번의 공개키 연산을 필요로 한다; $a=E_{P_i}(U_i, k_i)$. 이 정도의 공개키 연산은 [19]의 실험에서 보듯이 현재 상용 모바일폰에서도 충분히 가능함을 알 수 있다. 128 bytes 메시지의 공개키 연산 2회, 해쉬 함수 1회, 대칭키 연산(AES) 4회를 모바일폰(Qualcomm QSD8250 1 GHz on Scorpion, 512 MB NAND flash memory, 512 MB DDR SDRAM)에서 수행 하는데 0.098ms가 소요되고 512/1024 bytes(1KB) 메시지에 대해서는 28.68/89.59ms가 소요된다. 본 논문에서 비밀키 k_i를 160 bits 정도로 잡고 사용자 정보 U_i를 최대 500 bytes로 설정한다 해도(실제 200bytes면 충분하다) 총 메시지 길이가 512 bytes를 넘지 않고 단 1회의 연산만을 수행 하므로, 해쉬함수 및 대칭키 연산 소요시간을 무시한다 해도 최대 소요시간이 14ms를 넘지 않는다. 또, 마이크로소프트의 "Pharos Traveler 137"은 '진보된 무선 서비스(Advanced Wireless Services (AWSs))'의 좋은 예로서 다음과 같은 프로세싱 능력을 가지고 있다; Qualcomm 7201A 528 MHz, ROM: 512 MB, RAM: 256 MB, 제공하는 서비스들 - 3.5 G 고속 인터넷, triband UMTS/HSDPA/HSUPA, 기업형 7.2 Mb/s 다운로드와 2 Mb/s 업로드를 제공하는 quad-band GSM/GPRS/EDGE 셀룰러 모뎀 [25]. 현재 또는 향후 모바일폰과 네트워크 상태를 고려해 볼 때, 본 논문에서 모바일폰의 공개키 연산은 전혀 문제가 되지 않을 것으로 보여진다.

유선 환경에서의 통신 역시 각 참여자 간의 비밀키를 사전에 공유케하여 대칭키 기반의 암호화 기법을 주로 사용하였고, 공개키 암호는 리뎀션 단계에서 소매업자 R_n이 발급자 I에게 자신의 고유 식별번호를 암호화하여 전송($E_{P_I}(n)$)하는 것과 청산 단계에서 소매업자 R_n이 발급자 I에게, R_n이 청산소 CH_m에게, CH_m이 I에게 자신의 식별번호를 암호화하여 전송하는 것이 전부이다.

공개키 기반의 암호화와 대칭키 기반의 암호화 성능의 차이는 [12]에서 알수 있듯이, 대칭키 기반의 암호화 기법이 공개키에 비해 약 1000배 가량 빠르다. 특히, 개인 소형 단말기의 계산 및 저장 능력의 제한적인 결함 요소를 가진 모바일폰을 사용하는 본 시스템에서 대칭키 기반의 암호화 기법의 사용은 피할 수 없는 선택인 것이다.

5.2.2 상태 관리 용이성(States Manageability)

상태 관리 용이성(States Manageability)이라 함은 쿠폰이 소비되었는지 아닌지는 그 시스템 내에서 고려되어져야 한다는 것이다 [13,14]. 본 논문에서는 발급자 I가 쿠폰 프로세스 테이블을 유지, 관리 함으로써 실시간으로 쿠폰의 상태를 체크할 수 있게 하였고, 이 체크를 통해서 쿠폰의 유효성을 확인한 후 다음 과정으로 진행할 수 있게 하여 쿠폰의 이중 사용(double spending) 방지와 청산과정의 조작(clearing manipulation)을 막을 수 있게 하였다.

Ⅵ. 쿠폰 전달 (Coupon Transfer)

쿠폰 기능 중에는 '선물하기'라는 것이 있다. 발급 초기에 바로 본인이 아닌 타인에게 발급을 요청하거나 발급받은 후 타인에게 전송하는 두 가지 경우가 있는데, 전자의 경우는 주체만 바뀔 뿐 앞서 설계한 스킴과 별반 차이가 없고 후자의 경우 추가적인 프로토콜이 요구되어진다. 이 장에서는 쿠폰 전달 프로토콜을 설계한다. 응용 시나리오는 다음과 같다.

응용 시나리오. 소비자 U_i는 2010. 8. 7에 발급받은 쿠폰을 자신의 친구 U_t에게 선물하려 한다. U_i는 8.15에 발급자 I에게 쿠폰 선물하기 기능을 요청하여 U_t에게 쿠폰 전달을 요청한다.

6.1. 쿠폰 전달 프로토콜

[소비자 U_i/MP_i ---〉〉 발급자 I]: 1.전송: p_i, $a=E_{k_i}(B\_Code_{ij}, U_t, r_t)$, $b=h(p_i|a)$

[소비자 U_i/MP_i ---〉〉 소비자 U_t/MP_t]: 2.전송: $E_k(r_t)$

[발급자 I]: 3.검증/복호화: $h(p_i|a)=b/$

$D_{k_i}(E_{k_i}(B\_Code_{ij},\ U_t, r_t)) = B\_Code_{ij},\ U_t, r_t$

〔U_t/MP_t 〈〈--- I〕: 4.전송: $E_{r_t}(p_t,\ k_t)$

〔U_t/MP_t〕: 5.복호화: $D_k(E_k(r_t)) = r_t$,

$D_{r_t}(E_{r_t}(p_t, k_t)) = p_t,\ k_t$

6. 발급(Delivery) 단계를 진행한다.

6.2. 쿠폰 전송 프로토콜 상세과정

1. 사용자-기기 인증을 마친 소비자 U_i/MP_i는 소비자 U_t/MP_t에게 쿠폰 C_{ij}를 선물하기 위하여 발급자 I에게 $p_i,\ a = E_{k_i}(B_Code_{ij},\ U_t, r_t),\ b = h(p_i/a)$를 전송한다. 여기서 U_t는 사용자 U_t의 모바일폰 번호와 같은 개인정보이고 는 rt는 발급자 I와 U_t가 임시로 사용하게 될 비밀 공유키이다.

2. U_i/MP_i 는 소비자 U_t/MP_t에게 $E_{k_{it}}(r_t)$를 전송한다. kit는 U_i와 U_t가 사전에 미리 공유한 비밀 공유키이다.

3. 발급자 I는 전송받은 데이터를 $h(p_i/a) = b$와 같이 검증하고, p_i로 k_I를 쿠폰 프로세스 테이블에서 찾아내어 다음을 복호화한다;

$D_{k_i}(E_{k_i}(B\_Code_{ij},\ U_t, r_t)) = B\_Code_{ij},\ U_t, r_t$.

4. 발급자 I는 rt로 $E_{r_t}(p_t,\ k_t)$을 암호화하여 U_i의 모바일폰 번호로 전송한다. p_t는 사용자 U_i의 가명이고 k_t는 앞으로 발급자 I와 소비자 U_t/MP_t가 사용하게 될 비밀공유키이다.

5. U_t/MP_t는 $D_k(E_k(r_t)) = r_t$을 복호호하여 rt를 구해내어 $D_{r_t}(E_{r_t}(p_t, k_t)) = p_t,\ k_t$을 복호화하여 가명 p_t와 비밀공유키 k_t를 구해낸다.

6. 주어진 p_t와 k_t를 가지로 앞서 제시한 쿠폰 요청 프로토콜부터 그대로 수행하여 쿠폰을 발급받고, 발급자 I는 전이일(T_date)과 변경된 정보들(가명(p), 비밀키(k), α, 등록일, 요청일(Pull), 전송일(Push))을 쿠폰 프로세스 테이블에 업데이트한다.

이러한 전송 프로토콜 과정을 거치면, 만약 쿠폰 C_{ij}에 관한 정보를 아는 소비자 U_i/MP_i가 악의적인 마음을 먹고 이중사용을 시도할지라도, U_i/MP_i는 업데이트된 p_t, k_t, α 값들을 모르기 때문에 발급자의 확인과 검증을 통과할 수가 없다.

Ⅶ. 결 론

모바일쿠폰은 제조업자에게 판매촉진의 한 수단일 뿐만 아니라 소비자들에게는 경제적인 소비 패턴을 위한 지급 결제 수단으로 사용되는 것으로서 그 사용이 m-커머스의 성장과 더불어 나날이 증가하고 있는 반면, 각 참여자들의 부정행위(fraud)로 인한 손실 역시 적지 않은 문제를 낳고 있다. 이 논문에서는 이러한 모든 참여자들의 부정행위를 막을 수 있는 안전한 모바일 쿠폰 프로세스 스킴을 제안하였다. 이는 대칭키 암호화 시스템 기반으로 효율적이며 쿠폰 상태 관리가 용이하다.

향후 과제로는 현행 실시하고 있는 청산소(clearing house), 즉 제 3기관이 개입하는 청산 과정이 아닌 도/소매업자가 발급자에게 직접 청산하는 안전한 청산 단계 프로토콜을 설계하는 것이 다음 목표이다.

참고 문헌

[1] 송재일, "패밀리 레스토랑의 판매촉진 수단으로서 쿠폰 분석: 인터넷을통해 제공되는 쿠폰을 중심으로", 관광연구논총, 12(0), pp.145-162, 2000

[2] R. Anand, M. Kumar and A. Jhingran, "Distributing E-Coupon on the Internet", Proceedings of the 9th Annual Conference of the Internet Society (INET'99), 1999.

[3] J. Andrews and A. Bhappu, "A Propositional Research Framework for the Conceptual and Technological Adoption of Digital Coupons in the US", Proceedings of the 43rd Hawaii International Conference on System Sciences, pp.1-9, 2010

[4] S. Banerjee and S. Yancey, "Enhancing mobile coupon redemption in fast food campaigns", Journal of Research in Interactive Marketing Vol. 4 No. 2, pp. 97-110, 2010

[5] F. Bao, "A Scheme of Digital Ticket for Personal Trusted Device", Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004), Vol. 4, pp. 3065-3069, 2004.

[6] C. Blundo, S. Cimato, and A. D. Bonis, "A Lightweight Protocol for the Generation and

Distribution of Secure Ecoupons", Proceedings of the 11th international conference on World Wide Web, pp. 542 - 552, 2002

[7] C. Blundo, S. Cimato, and A. D. Bonis, " Secure E-Coupons", Electronic Commerce Research, 5, pp. 117 - -139, 2005

[8] C. C. Chang, C. C. Wu, I. C. Lin, "A Secure E-coupon System for Mobile Users", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.1, January 2006

[9] C. C. Chang and Y. F. Chang, "Schemes for Digital Gift Certificates with Low Computation Complexity," 2005.

[10] C. C. Chang, Y. F. Chang and J. S. Lee, "Mobile Payment for Off-line Vender Machines," International Journal of Computer Science and Network Security, pp. 119-126, Sept. 2005

[11] S. Chari, P. Kermani, S. Smith, and L. Tassiulas, "Security Issues in M-Commerce: A Usage-Based Taxonomy", E-Commerce Agents, LNAI 2033, pp. 264-282, 2001

[12] C. I. Fan, W. K. Chen and Y. S. Yeh, "Date Attachable Electronic Cash," Computer Communications, Vol. 23, Issue: 4, pp. 425-428, Feb. 2000.

[13] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine, "Digital-Ticket-Controlled DigitalTicket Circulation," Proceedings of the 8th USENIX Security Symposium, Washington D.C., USA, pp. 229-238, Aug. 1999.

[14] K. Fujimura and Y. Nakajima, "General-Purpose Digital Ticket Framework," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, Boston, Massachusetts, USA, pp. 177-186, Aug 1998

[15] R. Garg, P. Mittal, V. Agarwal, "An Architecture for Secure Generation and Verification of Electronic Coupons", Proceedings of the General Track: 2002 USENIX Annual Technical Conference, pp. 51 - 63, 2002

[16] N. C. Juul and N. Jørgensen, "Security Issues in Mobile Commerce Using WAP", 15th Bled Electronic Commerce Conference, pp. 444-462, 2002

[17] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems", SAC'99, LNCS 1758 pp. 184-199, 2000

[18] H. A. Park, J. T. Choi, J.I. Lim, and D. H. Lee, "The study on personal information protection from the mobile environments", KIISC, 2007. 8

[19] H. A. Park, J. W. Hong, J. H. Park, J. Zhan, and D. H. Lee, "Combined Authentication based Multi-Level Access Control in Mobile Application for DailyLifeService", IEEE Transactions on Mobile Computing, 9(6), pp. 824-837, 2010.6.

[20] V. Patil and R.K. Shyamasundar, "e-coupons: An Efficient, Secure and Delegable Micro-Payment System", Information Systems Frontiers 7: 4/5, pp. 371-389, 2005

[21] T. Shojima, Y. Ikkai and N. Komoda, "A Method for Mediator Identification Using Queued History of Encrypted User Information in an Incentive Attached Peer to Peer Electronic Coupon System", Proceedings of the 2004 IEEE International Conference on System, Man and Cybernetics, pp. 1086-1091, 2004.

[22] GS1 Mobile Com., "Mobile Commerce:opportunities and challenges", White Paper, February 2008

[23] MMA(mobile marketing association), "Introduction to Mobile Coupons", 2007

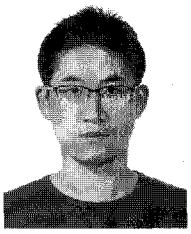
[24] ScanAps, "New direction is needed for electronic coupon clearing", a white paper from ScanAps, 2007

[25] http://www.pharosgps.com/products/proddetail.asp?prod=001_PTL137_8.00&cat=147, 2010

〈著者紹介〉

박 현 아 (Park, Hyun-A)

2003년 2월 : 고려대학교 수학과 졸업
2005년 2월 : 고려대학교 정보경영공학전문대학원 정보보호학과 석사
2010년 2월 : 고려대학교 정보경영공학전문대학원 정보보호학과 공학박사
2010년 3월~현재 : 아리조나 대학 엘러 칼리지에서 공동연구 수행중
<관심분야> 데이터베이스 보안, 클라우드 컴퓨팅, 모바일 보안, 소셜 네트워킹, 프라이버시 기술



박 재 현 (Park, Jae Hyun)

2004년 2월 : 서울대학교 미술대학 동양화 / 시각디자인과 졸업
2007년 5월 : Illinois Institute of Technology / MDes in Human Centered Design Communication and Planning
2007년 5월~현재 : Case Western Reserve University / Weatherhead School of Management / PhD Candidate in Information System
<관심분야> Knowledge Management, Design Information System, Boundary Objects and Social Interactions in Social Computing Technologies