情報保護學會論文誌
第20卷 第3號, 2010. 6

# 통합인증센터를 활용한 일회용 가상카드번호 생성 및 결제 서비스 프로토콜

서 승 현[†‡]
한국인터넷진흥원

# One-Time Virtual Card Number Generation & Transaction Protocol using Integrated Authentication Center

Seung-Hyun Seo[†]
Korea Internet & Security Agency

요 약

최근 유명 온라인 쇼핑몰 사이트가 해킹을 당해 많은 사용자들의 ID, 패스워드, 계좌번호, 주민등록번호, 신용카드 번호와 같은 개인 정보들이 누출되었다. 해커들은 계속해서 온라인 쇼핑몰 사이트 에 대한 공격을 하고 있으며 해킹 피해자들의 수도 증가하고 있다. 신용카드 번호가 누출되면, 해커들이 금전적인 이득을 취하기 위해 누출된 카드번호를 악용할 수 있어 특히 위험하다. 2007년 Financial Cryptography 학회에서 Ian Molly 등이 최초로 일회용 가상카드번호 생성 스킴을 제안한 바 있으나, 재사용불가의 특성을 제공하지 못한다. 본 논문에서는 Ian Molly 스킴의 취약성을 분석하고, 휴대단말기를 활용하여 일회용 가상카드번호의 보안요구사항을 만족하는 새로운 일회용 가상카드번호 생성 스킴을 제안하였다. 또한, 이를 기반으로 사용자 편의성과 보안성강화를 위해 통합인증센터를 활용한 일회용 가상카드 결제 프로토콜을 설계한다.

ABSTRACT

Recently, famous online shopping websites were hit by hacking attack, and many users' personal information such as ID, password, account number, personal number, credit card number etc. were compromised. Hackers are continuing to attack online shopping websites, and the number of victims of these hacking is increasing. Especially, the exposure of credit card numbers is dangerous, because hackers maliciously use disclosed card numbers to gain money. In 2007 Financial Cryptography Conference, Ian Molly et al. firstly proposed dynamic card number generator, but it doesn't meet reuse resistant. In this paper, we analyzed security weaknesses of Ian Molly's scheme, and we proposed a new one-time virtual card number generator using a mobile device which meets security requirements of one-time virtual card numbers. Then, we propose one-time credit card number generation and transaction protocol using Integrated Authentication Center for user convenience and security enhancement.

**Keywords:** One Time Password, Virtual card generation, One-way hash function

## I. 서 론

현금을 대신해서 결제할 수 있는 신용카드는 그 편리함으로 인해 온·오프라인 상점에서 지불결제 수단으로 각광을 받고 있다. 특히 비대면으로 상거래가 이루어지는 인터넷 쇼핑과 홈쇼핑에서 신용카드는 거래수단의 대부분을 차지하고 있다. 인터넷 쇼핑몰의 신용카드 거래를 살펴보면, 신용카드 번호, 만기일 등을 고객이 쇼핑몰 사이트의 결제 페이지 또는 신용카

접수일(2009년 8월 20일), 수정일(1차: 2009년 10월 22일, 2차: 2010년 1월 21일), 게재확정일(2010년 2월 23일)
† ‡ 주저자, seosh@kisa.or.kr

드회사에서 띄운 결제 팝업창에 입력하고 난 후, 신용카드사로 신용카드정보가 전송되어 유효성체크를 하고 결제승인을 받는 형태이다. 홈쇼핑의 경우 구매의사가 있는 고객이 홈쇼핑 회사에 전화통화를 하여 판매 직원에게 카드번호와 유효기간 등을 알려주고 홈쇼핑 회사는 그 정보를 신용카드회사로 전송하여 유효성체크를 하고 거래승인을 받는 형태이다. 이 과정에서 일부 홈쇼핑 회사나 인터넷 쇼핑몰 사이트들은 고객의 편의를 제공한다는 이유로 고객의 개인정보와 함께 신용카드 번호 등을 내부 데이터베이스에 저장하고 있어 고객 정보유출 위협이 높으며, 보안이 취약한 인터넷 쇼핑몰 사이트의 경우 고객이 입력하는 신용카드번호 정보가 그대로 외부에 누출될 위험이 있다.

실제로 인터넷 해킹사고나 내부직원의 고의적인 고객정보 유출 과실로 인해 고객ID, 비밀번호, 신용카드 정보 등이 유출되어 악용되는 금융 사고들이 급증하고 있다. 2008년 9월에 발생하여 1,100만명의 고객정보 유출 피해를 낸 GS 칼텍스 사건은 내부직원에 의한 고의적인 정보유출 사고의 대표적 사례이며, 2008년 2월 발생하여 1,000만 명 이상 고객정보 유출 피해를 입힌 (주)옥션해킹 사고는 대표적인 온라인 해킹사고 사례라 할 수 있다. 2007년 2월에 발생한 씨티 카드 해킹사고는 온라인 카드결제 시스템 취약점을 이용한 해킹사고로 유출시킨 고객의 신용카드 정보를 이용해 5,000여 만원을 무단 결제한 피해를 입혔다[2,3,4,6]. 이처럼 신용카드정보가 유출되면, 온라인 지불 결제, 홈쇼핑 전화 결제 등에 손쉽게 활용할 수 있기 때문에 신용카드회사, 은행, 온라인 전자상거래 업체 등은 이에 대한 대응책을 마련하는데 고심하고 있다. 해외의 경우, 고정된 신용카드번호의 문제점을 개선하고자 실제 카드번호 대신 가상카드번호를 사용하는 시도를 하고 있으며 대표적으로 BoA(Bank of America)의 'ShopSafe®', Citibank의 'Virtual Account Numbers', Discover®사의 'Secure Account Number', PayPal사의 'Virtual Debit Card' 등이 있다[9,10,11,12]. 그러나 이들 모두 해당 은행이나 카드사 고객전용으로 제공되는 서비스로 한계점을 가지며 실제 카드번호 대신 가상카드번호를 사용한다는 것에 초점을 두고 있기 때문에 한번 생성된 가상번호가 이후에 재사용이 가능하다는 단점이 있다. 그밖에 Ian Molly 등이 2007년 FC(Financial Cryptography) 학회에서 제안한 동적인 가상 신용카드번호 생성 스킴은 재사용공격에 취약한 문제점이 있다[8].

따라서 본 논문에서는 해외에서 사용중인 일회용 가상카드번호 서비스들과 Ian Molly 등이 제안한 스킴의 취약성을 분석하고, 이를 개선한 일회용 가상카드번호 생성 스킴과 국내 금융권 통합인증센터를[1] 활용한 일회용 가상카드번호 생성 및 결제 프로토콜을 제안한다. 제안한 프로토콜에서 사용하고 있는 일회용 가상 카드번호 생성 스킴은 위조불가능성 및 재사용불가, 완전성, 건전성, 일회용 가상카드번호의 일방향성 등의 보안요구사항을 만족하며, 휴대폰 단말기를 이용하여 별도 기기를 소지하는 불편을 없애고, 카드 발급 시 휴대 단말기에 생성모듈을 다운로드받아 편리하게 카드번호를 생성하는 기능을 가진다. 또한, 제안한 일회용 가상카드번호 생성 및 결제 프로토콜은 전 세계적으로 유일하게 국내 금융권에서 운영되고 있는 통합인증센터를 활용한 것으로 사용자가 한 기관에서 일회용 가상카드번호 생성모듈을 한번만 다운로드 받고나면 해당 카드사 전용이 아니라 소지하고 있는 여러 신용카드들의 일회용 가상카드번호를 생성하여 편리하게 이용할 수 있다는 장점을 가진다.

본 논문의 구성은 다음과 같다. 2장에서는 해외에서 시범서비스중인 가상카드번호 서비스와 Ian Molly 등이 제안한 가상카드번호 생성 스킴의 취약성을 분석한다. 3장에서는 일회용 가상카드번호 생성기들이 기본적으로 만족해야하는 보안요구사항을 제시하고 본 논문에서 사용할 기호 및 용어들을 정의한 후, 휴대단말기를 이용한 일회용 가상카드번호 생성 스킴을 제안한다. 4장에서는 통합인증센터를 활용한 일회용 가상카드번호 생성 및 결제 프로토콜을 제안한다. 5장에서는 제안하는 프로토콜의 기본 모듈인 일회용 가상카드번호 생성모듈의 안전성을 분석하고 제안한 프로토콜과 현재 사용중인 서비스들의 비교분석을 기술한다. 끝으로 결론 및 향후 연구 방향을 제시한다.

## II. 관련 연구

본 장에서는 현재 해외에서 서비스 중인 가상카드번호 서비스들의 특징을 간략히 기술하고 문제점을 분석한다. 또한 Ian Molly 등이 제안한 스킴의 취약점을 분석하도록 한다.

### 2.1 해외에서 사용중인 가상카드번호 서비스

해외 금융기관에서 시범 서비스 중인 일회용 가상카드번호 서비스로는 BoA(Bank of America)의

'ShopSafe®', Citibank의 'Virtual Account Numbers', Discover®사의 'Secure Account Number', PayPal사의 'Virtual Debit Card' 등이 있다[9,10,11,12]. 현재 제공되고 있는 일회용 가상신용카드 서비스는 모두 해당 은행이나 카드사 고객전용으로 제공되는 서비스로서, 다른 카드사나 은행을 사용하는 고객의 경우 해당 서비스를 지원받지 못하는 한계점이 있다. 또한 이를 활용하기 위해서 사용자가 추가적인 소프트웨어 프로그램을 PC에 다운로드 받아서 설치하거나 인터넷뱅킹 사이트 혹은 카드회사 사이트에 로그인하여 프로그램을 구동시켜야 하는 번거로움이 있다. 각 서비스의 특징을 요약하면 아래와 같다.

(1) BoA의 ShopSafe®

BoA(Bank of America)에서 제공하는 ShopSafe®는 사용자가 온라인 결제를 수행할 때마다 일회용 가상카드번호를 생성해서 사용하는 서비스로, 온라인 구매전에 온라인 뱅킹 계좌에 로긴하고 ShopSafe® 솔루션에 접속하여 사용자의 카드번호, 구매금액, 카드 유효기간을 입력하면, 가상의 카드번호가 자동으로 생성된다. ShopSafe® 서비스는 BoA의 온라인 뱅킹서비스와 신용카드를 이용하는 사용자에게만 제공된다. ShopSafe® 서비스는 한 상점 당 하나의 가상카드번호를 사용할 수 있어서, A라는 상점에서 123456이라는 카드번호를 사용했다면, B라는 상점에서는 123456 번호를 사용할 수 없는 특징을 가진다. 그러나 해당 상점에서는 사용했던 가상카드번호를 계속 재사용할 수 있기 때문에, 재사용 불가의 특성을 만족하지 못하여 한 상점에서 사용하고 있는 가상카드번호가 누출된다면 그 상점에서는 악용 가능한 소지가 있다.

(2) Citibank의 'Virtual Account Numbers'

Citibank의 일회용 가상신용카드 서비스는 사용자가 온라인계좌에 로긴을 하고, 'Virtual Account Numbers'를 선택하여 일회용 가상신용카드 생성기를 웹에서 구동시키거나 PC로 다운로드받을 수 있다. Citibank 카드를 이용하는 고객에게만 서비스가 제공되며, 일회용 가상신용카드 생성기에 실제 카드번호를 입력하면 새로운 가상카드번호가 생성되고 생성된 가상카드번호를 해당 인터넷쇼핑몰에서 사용하면 된다. 가상카드번호에서 원래 카드번호를 추출할 수 없고 가상카드번호가 생성될 때마다 생성된 날짜를 기준으로 다음 달에 만기되도록 만들어지며, 경우에 따라서는 가상카드번호 만기일을 설정할 수도 있다. 따라서 가상카드번호는 설정한 만기일까지 사용될 수 있기 때문에, 재사용불가의 특성을 만족시키지 못한다.

(3) Discover®의 'Create Secure Account Number'

Discover®카드사에서 제공하는 일회용 가상신용카드 생성기 'Create Secure Account Number'는 PC 혹은 인터넷 브라우저에서 구동하여 사용할 수 있다. PC에서 활용할 경우, 해당프로그램을 다운로드 받아야 하는데 다운로드 받은 이후에는 구매시마다 자동으로 실행되어 가상카드번호를 생성한다. 인터넷 브라우저에서 사용할 경우, Discover®사의 온라인 계좌번호에 접속하여 'Create Secure Account Number'를 선택하면 가상카드번호가 생성된다. 가상번호는 실제 카드의 만기일 까지 사용될 수 있기 때문에, 카드 만기일 전까지의 가상번호는 재사용이 가능하므로 재사용불가의 특성을 만족시키지 못한다.

(4) PayPal의 'Virtual Debit Card'

PayPal에서 제공하는 가상카드번호 서비스인 'Virtual Debit Card' 역시 PayPal 고객에 한정된 서비스이며, 온라인쇼핑몰에서 사용할 수 있는 일회용 가상신용카드번호 생성기 프로그램을 다운로드 받아서 사용한다.

### 2.2 Molly-Li-Li의 가상카드번호 생성스킴의 취약성

Ian Molly 등이[8] 제안한 스킴은 카드발급기관과 사용자 사이에 비밀 패스워드 P가 사전에 공유되어 있고, 카드 발급기관은 사용자의 계좌번호 C, 지불결제정보(사용자 이름과 주소를 포함하는 정보) B를 알고 있다고 가정한다. 또한 $F_K(.)$는 비밀키 K를 사용하는 해쉬함수, H(.)는 일방향 해쉬함수, E는 만기일, M은 상점코드, T는 거래금액, C는 사용자 계좌번호, P는 패스워드를 의미하고 거래정보는 $\sigma = E||B||M||T$이며, 비밀키 $K=H(C||P)$으로 구성된다. 가상카드번호를 생성하기 위한 기본 모듈은 $V=F_K(\sigma) \bmod 10^n$ (n: 출력하고자 하는 가상 카드번호의 길이)으로 사용자가 신용카드 결제를 하기 위해서 가상카드번호 생성 모듈을 구동하여 카드번호를 생성해낸다. 따라서 매번 카드번호를 생성할 때마다 신규성을 제공하는 값이 입력으로 포함되어있지 않다.

즉, Molly-Li-Li 스킴의 기본모듈 입력값으로 카드 만기일을 표시하는 정보 E를 포함하고 있다 하더라도, 카드 만기일은 매번 바뀌는 값이 아닌 카드 사용 가능한 기한을 의미하므로 신규성을 제공하는 정보가 아니다.

사용자가 A 온라인상점(상점코드:101)에서 가격이 T′인 물품 m을 결제하기 위해 생성한 일회용 가상카드번호 $V'=F_K(E||B||101||T') \bmod 10^n$와 거래내역(여기서 거래내역은 상품 가격, 상품코드, 상점코드 등을 포함하는 정보로 온라인 상점의 사용자 상품구매 및 결제 창에 입력됨)이 키보드 해킹 등을 통해 공격자에게 유출되었다고 가정하자. 그러면 공격자는 거래내역을 이용해서 거래금액을 알아내고, 유출된 가상카드번호 V′를 그대로 재전송하여, A 상점에서 같은 금액대의 물품들을 얼마든지 구매요청을 할 수 있게 된다. 즉, 유출된 가상카드번호 V′은 m과 같은 가격대의 물건 m′를 구매하는데 그대로 이용될 수 있다. 공격자가 재전송한 가상카드번호가 상점 A를 통해서 카드 발급기관에 전송되었다 할지라도, 카드발급기관은 공격자에 의해서 재전송된 값인지 실제 사용자가 만기일내에 같은 상점에서 같은 금액의 물품 m′를 구매한 것인지 구분할 수 없다. 따라서 거래승인 통보를 온라인 상점에 전달하게 된다.

따라서 Molly-Li-Li 스킴은 신규성을 제공하지 않기 때문에 재전송공격에 취약하며 이로 인해 가상카드번호를 재사용하는 취약성이 존재한다.

## III. 제안하는 일회용 가상카드번호 생성 스킴

본 장에서는 일회용 가상카드번호 생성 스킴이 만족해야하는 보안 요구사항을 분석하고, 본 논문에서 사용할 용어 및 기호를 정의하며 휴대 단말기를 이용한 일회용 가상카드번호 생성 스킴을 제안한다.

### 3.1 보안 요구사항

본 논문에서 제안하는 일회용 가상카드번호 생성 스킴이 만족해야하는 보안 요구사항은 다음과 같다.

(1) 완전성(Completeness):
- 신용 카드소지자라면, 누구라도 신용카드 번호, 거래내역 등의 정보를 가지고 일회용 가상카드번호를 생성해낼 수 있다.

(2) 건전성(Soundness):
- 사용자 식별코드를 포함한 공개 거래 내역정보와 이에 해당하는 일회용 가상카드번호가 주어지면, 카드 발급기관은 사용자 식별코드를 통해 일회용 가상카드번호와 연관된 사용자를 식별하고 일회용 가상카드번호의 유효성을 검증 할 수 있다.

(3) 일회용 가상카드번호의 일방향성(Onewayness of One-time Virtual Card Number):
- 공개 거래 내역정보와 일회용 가상카드번호가 공격자에게 노출되더라도, 주어진 일회용 가상카드번호로부터 원래의 카드번호를 알아내는 것은 암호학적으로 불가능하다.

(4) 위조 불가능성(Forgery Resistant):
- 카드 분실 및 도난 등으로 실제 카드번호가 누출되었다 하더라도 공격자는 누출된 카드번호를 이용해서 유효한 일회용 가상카드번호를 위조할 수 없다.

(5) 재사용 불가(Reuse Resistant):
- 한번 생성된 가상카드번호는 일회용이며, 이후에 재사용 할 수 없다.

### 3.2 용어 및 기호

- K: 사용자와 센터간에 공유되는 비밀키, K = H(MasterKey||[PIN])
- MasterKey: 휴대폰 USIM 칩 혹은 휴대폰 내부 저장장치에 저장
- PIN: 사용자가 가상카드번호 발급단계에서 설정하는 비밀번호(4자리), 일회용 가상카드번호 생성모듈 시작시 입력함(휴대폰 도난 및 분실시 안전장치)
- [ ]: 선택사항
- H(): 암호학적 일방향 해쉬함수
- σ: 실제 카드번호에 대한 정보, σ=H(RealN||Exp)
- n: 생성된 일회용 가상카드번호 자리수 (ex: 16자리)
- RealN: 실제 신용 카드번호
- Exp: 유효기간(Expiration date)
- Amount: 사용금액
- Mcode: 상점(쇼핑몰) 코드
- Time: 일회용 가상카드번호 생성시간

### 3.3 일회용 가상카드번호 생성 스킴

본 절에서는 휴대 단말기를 이용한 일회용 가상카드번호 생성 스킴을 제안한다. 제안한 스킴은 카드 발급시 휴대 단말기에 일회용 가상카드번호 생성모듈을 다운로드받아 편리하게 카드번호를 생성하는 기능을 가지며, 위조불가능성 및 재사용불가, 완전성, 건전성, 일회용 가상카드번호의 일방향성 등의 보안요구사항을 만족한다.

#### 3.3.1 일회용 가상카드번호 생성기 발급 단계

(1) 사용자는 신용카드 발급기관에서 신원확인을 한 후에, PIN번호를 설정한다.
(2) 카드발급기관은 사용자의 신원을 확인하여 사용자 식별코드를 설정하고, PIN번호와 함께 신용카드와 연계된 계좌번호 및 사용자 정보를 저장한 후, 사용자의 휴대 단말기에 MasterKey가 탑재된 가상카드번호생성 모듈을 제공한다. 이때 신규성을 제공하기 위한 Count값과 발급기관의 인증서버와 동기화된 Time이 설정된다.

#### 3.3.2 일회용 가상카드번호 생성 단계

(1) 사용자는 신용카드 유효기간 및 신용카드 번호를 휴대폰 단말기에 탑재된 일회용 가상카드번호 생성기에 입력하여, 실제 소지하고 있는 신용카드 번호에 대한 정보 $\sigma=H(RealN||Exp)$를 계산한다.
(2) 사용자가 거래내역 정보 Amount와 Mcode를 생성기에 입력하면, 일회용 가상카드번호 생성기는 자동으로 $T=Amount||Mcode||Time$와 Count를 1증가시킨 Count'를 생성한다. 여기서 Time은 일회용 가상카드번호를 생성한 시각정보로 휴대폰에서 자동으로 입력된다.
(3) 사용자는 카드 발급기관과 사전에 공유된 비밀키 $K=H(MasterKey||PIN)$를 생성한다.
(4) 사용자는 비밀키 K와 σ, T, HMAC-SHA $256_K()$함수를[7] 이용하여 다음과 같이 일회용 가상카드번호 $OVCN=HMAC\text{-}SHA256_K(\sigma||T||Count') \bmod 10^n$ (n=16)를 생성한다. 여기서 n값은 카드번호의 길이로, n값을 몇 자리로 설정하느냐에 따라 OVCN값의 길이가 결정된다.

#### 3.3.3 일회용 가상카드번호 검증 단계

카드 발급기관은 상점으로부터 사용자의 식별코드, Amount, Mcode, 사용자의 일회용 가상카드번호 OVCN를 받고 다음과 같은 과정을 통해서 사용자의 일회용 가상카드번호를 검증할 수 있다.

(1) 카드 발급기관은 DB에 저장되어 있는 사용자 식별코드에 연결된 MasterKey와 PIN번호를 찾고, 비밀키 $K'=H(MasterKey||PIN)$를 계산한다. 또한 사용자의 신용카드번호와 유효기간을 찾아 $\sigma'=H(RealN||Exp)$를 계산한다.
(2) 카드 발급기관은 상점으로부터 받은 정보를 이용해서 $T=Amount||Mcode||Time$를 계산하고, 저장되어있는 Count'(이전 Count값에서 1증가된 값)를 이용해 $VCN'=HMAC\text{-}SHA256_K'(\sigma'||T||Count') \bmod 10^n$ (n=16)을 생성한다. 여기서 Time은 현재시간을 기준으로 사용자의 가상카드번호 생성기의 Time 정보와 동기화 되어 있다.
(3) 카드 발급기관은 VCN값과 VCN'값을 비교하여 값이 서로 틀리면 프로토콜을 종료하고, 같을 경우 사용자의 결제내역을 승인한다.

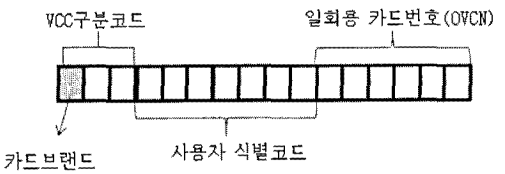
## IV. 통합인증센터를 활용한 일회용 가상카드 번호 결제 프로토콜

본 장에서는 국내 금융기관에서 사용 중인 OTP 통합인증센터(이후 통합인증센터)를 활용한 일회용 가상카드번호 생성 및 결제 프로토콜을 제안한다. OTP 통합인증센터는 현재 은행, 증권사, 상호저축은행, 새마을금고연합회, 우정사업본부 등 59개 국내 금융기관들이 참여하고 있으며, 인터넷뱅킹 및 텔레뱅킹 서비스 등 안전한 전자금융거래를 위한 OTP(One-Time-Password 일회용 패스워드) 통합인증 서비스를 제공하고 있다[1]. 본 논문에서는 효율적인 일회용 가상카드번호 거래 승인을 위해 통합인증센터와 국내 카드사간 네트워크 전용선이 연결되어 있다고 가정하고 결제 프로토콜을 설계하도록 한다.

### 4.1 일회용 가상카드번호 체계

현재 시중에서 사용되고 있는 신용카드 번호는 13자리부터 최대 19자리까지 다양하지만, 16자리를 기준으로 카드번호 체계를 설명하자면, 카드번호는 BIN(Bank Identifier Number) 번호, 발행기관의 일련번호, 검증번호(check digit)로 구성되어있다. BIN 번호는 전 세계적으로 발행기관(은행, 카드사 등)을 인식할 수 있는 번호로 첫 번째 자리 숫자는 카드 브랜드를 의미하는데, 3이면 JCB, 아멕스, 다이너스, 4이면 VISA 카드, 5이면 Master 카드, 9이면 국내전용 카드를 의미한다. 일반적으로 BIN 번호를 카드대분류(일반/특별/법인/체크카드 등)로 사용하여 카드번호만으로 카드종류를 인식할 수 있도록 많이 사용하며, 발급기관은 각 카드브랜드(VISA, Master, JCB, 아멕스 등)로부터 BIN 번호를 부여받고, 카드발급을 해준다. 발급기관별로 수십개의 BIN번호를 가지고 있다[5].

본 논문에서 제안하는 일회용 가상카드번호 체계는 그림 1과 같이, VCC(Virtual Credit Card) 구분코드, 사용자 식별코드(카드사에서 개별로 부여한 사용자 고유번호), 일회용으로 생성된 카드 번호로 구성되며, 기존의 신용카드번호 체계와 같이 16자리 숫자를 사용한다.



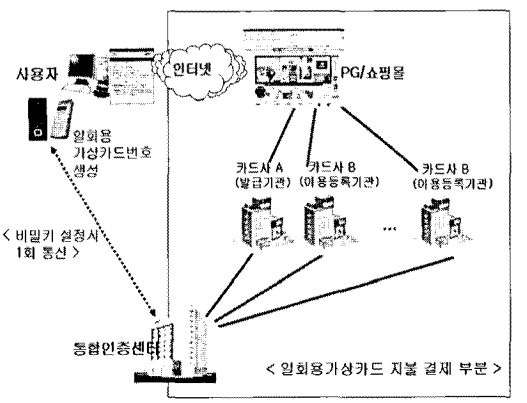

[그림 1] 일회용 가상카드번호 체계

VCC 코드는 세자리로 구성되는데, 첫 번째 자리는 VCC 발급 카드사 브랜드를 알려주는 값이고, 나머지 두자리 VCC 구분코드는 일회용 가상카드번호 인지 일반 신용카드 번호인지를 구분해주는 역할을 한다. 또한 7자리 사용자 식별코드는 카드사에서 개별 사용자에게 부여하는 개인 고유코드로서 사용자를 식별하는데 사용한다. 물론 10진수 7자리로 구성되었기 때문에, 한 카드사당 천만명 정도의 사용자에게만 적용할 수 있다는 한계점은 존재한다. 사용자 식별코드와 VCC 구분코드 등은 일회용 가상카드번호 생성기 발급단계에서 카드사가 설정하여 사용자의 휴대 단말기에 저장하며, 사용자가 일회용 가상카드번호를 생성할 때 자동적으로 사용자에게 보여지도록 한다. 6자리 일회용 가상카드번호(OVCN: One-time Virtual Card Number)는 본 논문 3.3절에서 제안하는 일회용 가상카드번호 생성기를 이용해 생성해낸 일회용 가상카드번호를 말한다. 즉, 3.3.2절 일회용 가상카드번호 생성단계 (4)에서 n값을 6으로 설정하면 6자리 일회용 가상카드번호가 출력된다. 사용시마다 변경되는 일회용 가상카드번호 OVCN값은 현재 금융권에서 사용하고 있는 OTP(One-Time Password, 일회용 패스워드)와 유사한 특성을 가진다. OVCN 값이나 OTP 값의 길이가 길면 길수록 추측공격 및 전수조사 공격 등에 대한 안전성이 더 증가하겠지만, 사용자 편의성을 고려해서 현재 금융권 OTP는 6자리로 사용되고 있다. 실제로 OTP는 매분마다 변경되는 특성 때문에 1분 이내에 추측공격이나 전수조사 공격을 통해 OTP 값을 알아낸다는 것은 불가능하며, 현재까지 이에 대한 보안 취약성이 발견되지 않고 있어, 본 논문에서도 OVCN 값을 6자리로 설정한다.

### 4.2 시스템 구성도

본 절에서는 제안하는 일회용 가상카드번호 결제 프로토콜이 수행되기 위한 시스템 구성도를 설명한다.

그림 2에서 보는 바와 같이, 통합인증센터와 카드사간에는 안전한 네트워크 전용선이 연결되어 있으며, 카드사와 PG/쇼핑몰간에는 VPN 또는 네트워크 전용선이 연결되어 있다고 가정한다. 일반 사용자와 PG/쇼핑몰의 웹사이트는 인터넷으로 연결되며, 사용자는 휴대폰에 장착된 일회용 가상카드번호 생성기의 비밀키를 생성하기 위해서 통합인증센터와 무선통신을 수행한다.




[그림 2] 일회용 가상카드번호 결제 시스템 구성도

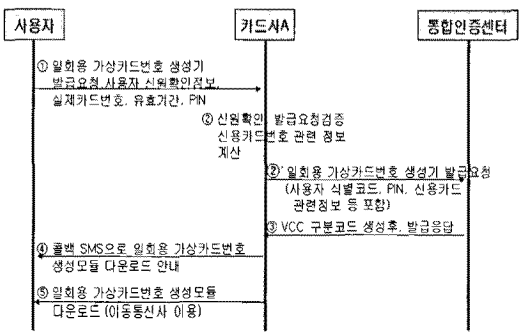
### 4.3 일회용 가상카드번호 결제 프로토콜

본 절에서는 일회용 가상카드번호 결제 프로토콜을 제안한다. 제안하는 프로토콜의 특징은 여러 카드사의 카드를 소지하고 있는 사용자가 한 카드사에서 일회용 가상카드번호 생성기를 발급받아 통합인증센터에 등록하면, 여러 개의 일회용 가상카드번호 생성기를 발급 받을 필요 없이, 사용하고 있는 여러 카드사에 이용등록 하여 쓸 수 있다는 장점을 가진다. 이때, 일회용 가상카드번호 생성기는 카드 발급시 휴대 단말기에 생성모듈을 다운로드받아 사용하며, 위조불가 및 재사용불가, 완전성, 건전성, 계좌숨김 등의 보안요구사항을 만족한다.

본 프로토콜을 기술하기에 앞서, A사와 B사의 신용 카드를 소지하고 있는 사용자가 A사로부터 일회용 가상카드번호 생성기를 발급받은 후, B사에 이용등록을 신청한다고 가정한다. 제안하는 프로토콜은 일회용 가상카드번호 생성기 발급 단계, 센터와 사용자간 비밀키 공유 단계, 타기관 이용등록 단계, 일회용 가상카드번호 결제 및 승인 단계로 구성된다.

#### 4.3.1 일회용 가상카드번호 생성기 발급 단계

일회용 가상카드번호 생성기 발급 단계는 오프라인 형태로 진행되어야 하며, 사용자가 카드사에 직접 방문하여 신원확인을 한 후, 실제 카드 번호 정보를 제공하고 생성기를 발급받도록 한다. 만약 사용자 편의성을 위해 온라인 발급을 허용한다면, 일반적으로 사용자의 개인 컴퓨터는 보안에 취약하므로 발급과정에서 전송되어야 하는 주요 카드 번호 정보, 신원 정보들이 외부로 노출되어 보안 사고에 악용될 수 있기 때문에 주의해야 한다. 발급 단계는 그림 3에 요약되어 있다.




〔그림 3〕 일회용 가상카드번호 생성기 발급 단계

(1) 사용자는 A카드사에 일회용 가상카드번호 생성기 발급 요청을 한다. 이때, 사용자는 신원확인 정보를 제공하고, 실제 카드번호 $RealN_{Ⓐ}$, 유효기간 $Exp_{Ⓐ}$, 일회용 가상카드번호 생성기를 이용하기 위해 사용할 PIN 번호 등을 제공한다.

(2) A카드사는 사용자의 신원확인 및 발급 요청 내용 등을 검증하고, 사용자의 신용 카드 번호와 유효기간 정보를 입력 값으로 일방향 해쉬함수를 계산하여, 사용자의 신용카드 번호에 대한 정보 $\sigma_{Ⓐ}=H(RealN_{Ⓐ}||Exp_{Ⓐ})$를 계산한다. 통합인증센터에 사용자의 고유 식별코드(ex: H(주민번호)), $\sigma_{Ⓐ}$, PIN 등을 포함한 일회용 가상카드번호 생성기 발급 요청 메시지를 통합인증센터에 전송한다. 통합인증센터와 카드사 간에는 네트워크 전용선으로 연결되어 안전한 채널을 형성하고 있다.

(3) 통합인증센터는 해당 사용자의 정보를 저장하고 사용자의 VCC 구분코드를 생성한 후, VCC 구분 코드를 포함하여 A카드사에 발급 요청에 대한 응답 메시지를 전송한다.

(4) A카드사는 통합인증센터로부터 받은 응답메시지를 확인하고, 콜백SMS를 통해서 사용자에게 일회용 가상카드번호 생성모듈 다운로드 페이지를 안내하면서 사용자의 VCC 구분 코드 및 식별코드를 제공한다.

(5) 사용자는 일회용 가상카드번호 생성 모듈 다운로드 페이지에서 모듈을 다운로드한 후, VCC 구분 코드와 식별코드를 입력한다. 그러면 VCC 구분코드와 사용자 식별코드는 휴대폰에 안전하게 저장된다.

#### 4.3.2 비밀키 생성 및 등록 단계

비밀키 생성 및 등록 단계에서 사용자는 통합인증센터와 통신하여 일회용 가상카드번호 생성기를 동작시킬 수 있는 비밀키를 공유한다. 이 과정은 사용자의 휴대단말기와 통합인증센터간의 무선통신을 통해 이뤄지며, 보안상 취약할 수 있는 무선 네트워크 구간에서 이뤄지기 때문에, 키 공유를 위해서 별도의 온라인 비밀키 배포 프로토콜((ex)IETF Symmetric Key Provisioning Protocol)을 이용한다. 최종적으로 사용자와 통합인증센터간에 공유하는 비밀키의 형태는 $K = H(MasterKey||PIN)$이다. 여기서 PIN은

사용자가 발급단계에서 설정한 비밀번호 4자리이며, 발급단계에서 통합인증센터가 PIN 값을 저장한다. MasterKey는 통합인증센터가 생성하여 사용자에게 전송하는 키로, 사용자는 휴대단말기 내부 저장장치(혹은 USIM 칩)에 저장한다.

#### 4.3.3 일회용 가상카드번호 생성기 타기관 이용등록 단계

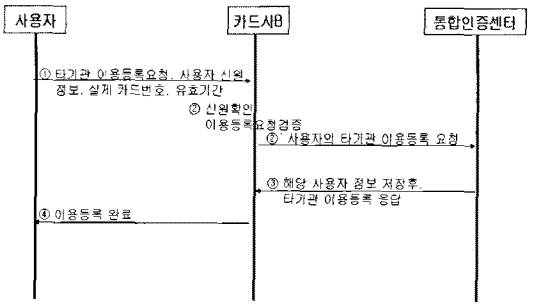
일회용 가상카드번호 생성기 타기관 이용등록 단계는 사용자가 발급받은 일회용 가상카드번호 생성기를 타 기관에서도 이용할 수 있도록 이용등록을 하는 단계이다. 본 단계는 온라인 또는 오프라인 형태로 진행될 수 있으며, 온라인으로 진행될 때는 공인인증서를 통해 신원확인을 하는 것으로 한다.

(1) 사용자는 A카드사에서 발급받은 일회용 가상카드번호 생성기를 B카드사에서도 이용하기위해서 B카드사에 이용등록을 요청한다. 사용자 신원확인과 함께 실제 카드번호 $RealN_{Ⓑ}$, 유효기간 $Exp_{Ⓑ}$ 등의 정보가 B카드사에 제출되어야 한다. 사용자가 직접 B카드사에 방문할 경우 주민등록증과 같은 신분증을 이용해 신원확인을 하고 관련정보를 제출하며, B카드사 홈페이지에서 이용등록을 요청할 경우 공인인증서를 이용해 신원확인을 하고 기타 관련 정보들을 입력한다. 온라인에서 이용등록이 수행될 경우, B카드사 홈페이지는 E2E 암호화모듈 (E2E: End to End 암호화는 사용자 PC로부터 금융기관의 서버까지 사용자의 비밀정보를 암호문의 형태로 유지하여 비밀정보에 대한 기밀성을 보장함), 키보드보안모듈, 개인 방화벽 등 보안 프로그램들을 사용자 PC에 설치될 수 있도록 하는 등의 안전한 환경을 제공해야 한다.

(2) B카드사는 사용자의 신원확인 및 발급 요청 내용 등을 검증하고, 통합인증센터에 일회용 가상 카드번호 생성기 타기관 이용등록 요청 메세지를(사용자의 Unique-ID (ex: H(주민번호), $\sigma_{Ⓑ}=H(RealN_{Ⓑ}||Exp_{Ⓑ})$ 등) 전송한다.

(3) 통합인증센터는 해당 사용자의 정보를 저장하고, B카드사에 타기관 이용등록 완료 응답 메세지를 전송한다.

(4) B카드사는 사용자에게 타기관 이용등록 완료를 알린다.




〔그림 4〕 일회용 가상카드번호 생성기 타기관 이용등록 단계

#### 4.3.4 일회용 가상카드번호 결제 및 승인 단계

일회용 가상카드번호 결제 및 승인 단계에서는 사용자가 인터넷 쇼핑몰에서 물품을 구입한 후 일회용 가상카드번호로 결제 요청을 하고 최종 승인되는 전 과정을 포함하고 있다.

(1) 사용자는 인터넷쇼핑몰에서 구매요청(상점/상품코드, 사용금액 등 입력)을 한 후, 신용카드 결제 요청을 한다.

(2) 사용자가 A카드사 카드를 이용하겠다고 선택하면, 사용자의 웹 화면에는 A카드사 결제용 윈도우 팝업창이 뜬다.

(3) 사용자는 윈도우 팝업창에 다음과 같이 일회용 가상카드번호 생성모듈에서 생성한 가상카드번호를 입력한다.

- 일회용 가상카드번호 생성
  - i) 사용자는 휴대폰에 PIN 번호를 입력하여, 일회용 가상카드번호 생성모듈을 구동시킨다.
  - ii) 사용자는 실제 카드번호 $RealN_{Ⓐ}$, 유효기간 $Exp_{Ⓐ}$을 입력한다. ($\sigma_{Ⓐ}=H(RealN_{Ⓐ}||Exp_{Ⓐ})$값 자동 계산)
  - iii) 사용자는 사용금액 Amount과 상점/상품코드 Mcode를 입력한다.
  - iv) 사용자의 휴대폰에 탑재된 일회용 가상카드번호 생성모듈은 사용자가 입력한 값들을 가지고 일회용 가상카드번호 $OVCN=HMAC\text{-}SHA256_K(\sigma_{Ⓐ}||T||Count') \bmod 10^n$ (n=6)을 계산한다. (K는 휴대 폰 저장장치에 저장되어 있는 사용자와 센터간의 비밀키 K=H(MasterKey||PIN), T=Amo-

unt||Mcode||Time. Time은 현재 시각, Count'은 카운터 값으로 이전에 휴대폰에 저장되어 있었던 Count값을 1 증가시킨 결과이다.)

v) 일회용 가상카드번호 생성모듈은 사용자의 VCC 구분코드, 식별코드 10자리와 지금 생성한 6자리 OVCN값을 합한 16자리 카드번호를 휴대폰 화면에 출력한다. (카드번호 체계는 그림 1 참고)

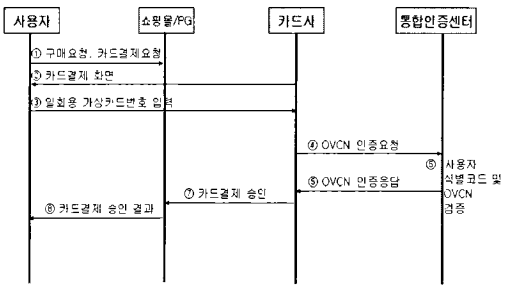
(4) A카드사는 VCC 구분 코드를 통해 사용자가 입력한 카드번호가 일회용 가상카드번호인지 실제카드번호인지 구분하여, 일회용 가상카드번호의 경우 통합인증센터에 해당카드번호에 대한 인증요청을 전송한다. 인증요청 메시지에는 카드사 코드, VCC 구분코드, 사용자 식별코드, OVCN 값 8자리, 금액(Amount), 상점/상품코드(Mcode) 등이 포함된다.

(5) 통합인증 센터는 일회용 가상카드번호 인증요청 메시지를 수신하고, VCC 구분코드와 사용자 식별코드를 확인한 후, 해당 OVCN을 다음과 같이 검증한다.

■ 일회용 가상카드번호 검증

i) VCC 구분코드와 사용자 식별코드에 연결된 해당카드사의 $\sigma_{Ⓐ}$값과, 사용자의 비밀키 K값을 찾는다.

ii) $OVCN' = HMAC\text{-}SHA256_K(\sigma_{Ⓐ}||T||Count') \bmod 10^n$ (n=6)을 계산한다. 여기서, T=Amount ||Mcode||Time이며, Count'는 저장되어있는 Count 값을 1증가시켜 계산한 값이다. Count 값과 Time 값은 사용자의 일회용 가상카드번호 생성 모듈과 통합인증센터의 인증 서버간에 동기화되어 있는 값으로서, Count는 사용자가 일회용 가상카드번호 검증을 요청할 때마다 1씩 증가하고 Time은 현재 시각을 나타낸다. 다만 시간 유효범위 t를(사용자가 일회용 가상카드번호를 생성한 후 전송하기까지 걸리는 시간과 네트워크 지연시간을 고려하여 설정하며, t의 범위가 짧을수록(예를 들어 1분이내) 안전성은 높아지지만 사용자 편의성은 감소될 수 있다.) 설정해놓고, 서버는 유효시간범위의(Time-t≤Time≤Time+t)




〔그림 5〕 일회용 가상카드번호 결제 및 승인 단계

OVCN' 값을 모두 계산한다.

iii) 전송받은 OVCN 값과 ii)에서 계산한 OVCN' 값이 유효한 시간범위 Time-t≤Time≤Time+t내에서 같은지 검증한다.

예를 들어 t=1일 때, 유효시간범위는 Time-1≤Time≤Time+1이 되고 서버가 계산하는 OVCN'은 $HMAC\text{-}SHA256_K(\sigma_{Ⓐ}||Amount||Mcode||Time-1||Count+1) \bmod 10^6$, $HMAC\text{-}SHA256_K(\sigma_{Ⓐ}||Amount||Mcode||Time||Count+1) \bmod 10^6$, $HMAC\text{-}SHA256_K(\sigma_{Ⓐ}||Amount||Mcode||Time+1||Count+1) \bmod 10^6$이다. 만약 사용자가 생성해서 전송한 OVCN 값이 위의 세가지 중 하나일 경우라면 서버는 사용자의 OVCN 값이 유효하다고 판단한다.

(6) 통합인증 센터는 해당 카드사에 OVCN 인증요청에 대한 응답을 보낸다.

(7) 카드사는 인증결과를 바탕으로, 쇼핑몰/VAN/PG사에 승인응답을 한다.

(8) 쇼핑몰/VAN/PG사는 사용자에게 카드승인 결과를 통보한다.

## V. 제안하는 프로토콜의 분석

본 장에서는 본 논문에서 제안하고 있는 일회용 가상카드번호 생성 및 결제 프로토콜의 안전성을 분석하기 위해, 결제 프로토콜의 기반이 되고 있는 일회용 가상카드번호 생성모듈을 3.1절의 보안요구사항에 따라 분석하고, 관련연구들과 안전성 및 편의성 부분을 비교 분석한다.

### 5.1 일회용 가상카드번호 생성 스킴의 안전성 분석

3.1절의 보안요구사항에 따라 제안한 일회용 가상카드번호 생성 스킴의 안전성을 분석한다. 본 논문에서 제안한 일회용 가상카드번호 생성 스킴은 3.3절에 기술되어 있다.

(1) 완전성(Completeness):

정당한 사용자라면 휴대단말기에 PIN 번호를 입력하여 휴대폰 모듈에 저장되어있는 Master Key를 이용해 비밀키 K=H(MasterKey ||PIN)를 생성할 수 있으며, 실제 신용카드번호 및 만기일을 입력하여 σ=H(RealN ||Exp)를 생성할 수 있다. 또한 σ와 함께 거래 금액 및 상점 코드, 거래시간, count, time 등을 일회용 가상카드번호 생성기에 입력하면 쉽게 일회용 가상카드번호를 생성할 수 있다. count 값은 휴대폰에 저장되어 있는 값으로 일회용 가상카드번호 모듈을 구동하여 일회용 가상카드번호를 생성할 때마다 자동으로 count값이 하나 증가되어 같이 계산된다. time값 역시 현재 생성시간을 의미하며 휴대폰 시간을 이용한다.

(2) 건전성(Soundness):

발급기관은 상점으로부터 사용자 식별코드, Amount, Mcode, 일회용 가상카드번호를 받으면, 발급기관 인증서버 DB에 저장된 해당 사용자의 비밀키 K=H(MasterKey||PIN),σ=H(RealN ||Exp)를 확인할 수 있으며, $HMAC\text{-}SHA256_K(\sigma||T||Count) \bmod 10^n$ (n=8)을 계산하여 상점으로부터 받은 일회용 가상카드번호와 같은지를 비교함으로써 유효성을 검증할 수 있다.

여기서, T=Amount||Mcode||Time이며, Time은 인증서버의 현재 시간, Count는 저장되어있는 Count 값을 1증가시켜 계산한 값이다.

(3) 일회용 가상카드번호의 일방향성(Onewayness of One-time Virtual Card Number):

제안한 스킴에서 각 구간별 전송되는 정보는 사용자에 의해 생성된 일회용 가상카드번호 $OVCN=HMAC\text{-}SHA256_K(\sigma||T||Count)$, 사용자 식별코드, Amount, Mcode이다. 일회용 가상카드번호 생성 스킴은 기본적으로 비밀키를 사용한 일방향 해시함수 HMAC-SHA256에 기반하고 있기 때문에, 출력값인 OVCN과 부분 입력값들을 알았다 하더라도 일방향 해시함수의 특성에 의해 입력 값인 신용카드번호를 알아내는 것은 암호학적으로 불가능하다.

(4) 위조 불가능성(Forgery Resistant):

도난 또는 분실로 인하여 사용자의 카드번호가 공격자에게 누출되었고, 공격자가 기존에 사용되었던 일회용 가상카드번호를 알아내었다 할지라도, 공격자는 일회용 가상카드번호를 생성하는데 필요한 비밀키 K를 알지못하기 때문에 공격자는 새로운 일회용 가상카드번호를 생성하지 못한다. 즉 비밀키 K는 사용자와 발급기관간에 사전공유된 MasterKey와 PIN번호로 구성되어있는데, MasterKey는 사용자의 휴대폰 메모리에 암호화된 상태로 저장되어 있으며 PIN은 사용자가 기억하는 비밀패스워드이기 때문에 실제 카드번호 누출만으로 유효한 일회용 가상카드번호를 위조할 수 없다. 그밖에도 일회용 가상카드번호 생성시마다 PIN 번호를 사용하기 때문에 휴대 단말기와 신용카드가 함께 분실되었을 경우라 하더라도, 공격자가 PIN을 알아내지 못하면 일회용 가상카드번호가 타인에 의해 생성되어서 악용되는 피해를 예방할 수 있다.

(5) 재사용 불가(Reuse Resistant):

제안한 일회용 가상카드번호 생성 스킴의 경우, 카드생성시각 정보 및 카운터 값을 입력 값으로 포함하고 있기 때문에, 발급기관의 인증서버에서 카드번호의 유효성을 검증할 때, 이에 대한 검증도 함께하며 검증 후에는 카운터 값을 증가시킨다. 따라서, 사용자가 전송한 일회용 가상카드번호를 공격자가 알아내어 재전송한다 하더라도 인증서버에서 이미 사용자가 사용했던 일회용 가상카드번호로 인식을 하기 때문에 인증실패 결과를 전송하고 카드결제가 이뤄지지 않는다. 즉, 전송되는 일회용 가상카드번호와 거래내역 등을 도감청하여 알아내었다 할지라도 이미 카드번호 생성 시각과 공격자가 사용하려는 시각이 다르며 서버의 count값도 이미 증가된 상태이기 때문에 공격자가 그것을 다른 상품을 구매하는데 재사용할 수 없다.

### 5.2 관련연구와의 비교 분석

본 절에서는 관련연구들과 제안한 프로토콜(4.3절에 기술함)간의 안전성 및 사용자 편의성 등을 비교분석하였으며 그 결과는 표 1과 같다. 3.3절에 기술한 일회용 가상카드번호 생성 스킴과 Ian Molly 스킴의 효율성을 비교해보면 표 2와 같으며, Ian Molly 스킴에 비해서 일방향 해시함수 계산횟수와 연접(concatenation)계산횟수가 다소 많음을 알 수 있다. 이는 본 논문의 제안 스킴이 일회용 가상카드번호의 일회성을 보장하고 재사용 불가의 요구사항을 만족하기

위해 Time값과 Count값을 같이 연접하여 입력 값으로 사용하고, 안전성을 위해 실제 카드번호와 유효기간의 정보를 한번 더 해시하여 계산에 활용하였기 때문이다. 그러나 일방향 해시함수를 수행하는 연산과 연접연산은 속도가 매우 빠르기 때문에 전체적인 계산 오버헤드에 크게 영향을 미치는 요인이 아니며, 스킴의 전체적인 수행 속도에 영향을 줄 수 있는 모듈러스 계산은 Ian Molly 스킴과 같다. 따라서 본 논문의 제안 스킴은 기존 연구와 비교했을 때 연산의 효율성을 크게 떨어뜨리지 않으면서 기존 연구들에서 대부분 제공하지 못했던 재사용불가의 기본 요구사항을 만족하고 있다고 할 수 있다.

또한 본 논문에서 제안하고 있는 일회용 가상카드번호 결제 프로토콜은 기존의 신용카드 결제 시스템의 문제였던 카드번호 노출로 인한 무단카드 결제, 도용 등의 문제점들을 획기적으로 개선하였다. 현재 해외 카드사를 중심으로 이런 온라인 신용카드 결제 시스템의 위협들을 극복해보고자 인터넷 쇼핑몰에서 실제 카드번호 대신 가상의 카드번호를 생성해서 사용하는 방식들이 시범서비스로 제공 중이다.

그러나 각 서비스마다 자사의 신용카드에 한해서만 가상카드번호를 생성할 수 있도록 생성모듈을 제공하기 때문에 서비스 제공범위가 한정적이다. 보통 3~4개 이상의 신용카드/직불/체크카드 등을 소지하고 있는 사용자들의 경우는 각 카드마다 해당 모듈들을 각각 다운로드받아 설치해야하는 불편함이 존재한다. 이들 방식들의 근본적인 문제점은 대부분의 서비스들이 소프트웨어로 개인 PC에 다운로드 받거나 인터넷뱅킹 사이트를 통해 웹에서 생성하거나 웹브라우저 형태로 제공되고 있어서 사용자 PC가 악성코드에 감염되었을 경우, 감염된 PC에서 사용자가 가상카드번호 생성 모듈을 구동시킨다면 이때 입력하는 실제 카드번호 노출이 불가피하다는 점이다. 또한 일부 방식의 경우, 재사용불가의 특성을 만족시키지 못하는 취약점이 있어 가상카드번호가 재사용되는 문제점이 있다.

본 논문에서 제안하는 신용카드 결제 프로토콜은 국내 금융권 통합인증센터를 활용하여 하나의 가상카드번호 생성모듈을 여러 신용카드사가 공통으로 이용할 수 있도록 설계되었다. 제안하는 일회용 가상카드번호는 기존의 신용카드번호의 자리수와 같은 16자리를 이용하기 때문에 온라인 쇼핑몰이나 PG사의 결제창이나 결제 시스템이 변경되지 않고서도 쉽게 적용이 가능하다. 다만 신용카드 발급기관인 카드사와 통합인증센터간의 전용네트워크가 연결되어야 하고, 카드사가 상점으로부터 받은 카드번호가 일회용 가상카드번호인지 실제 카드번호인지를 구분하여 가상 카드번호일 경우 통합인증센터로 전송하고 승인 결과를 전달받아야 하는 등의 부가적인 통신이 필요하고 가상카드번호의 결제가 통합인증센터에 집중된다는 단점은 있다.

그러나 통합인증센터를 활용하였기 때문에 해외 카드사의 시범서비스들의 문제인 서비스 제공 범위의 한계점을 개선하고 사용자 편의성을 향상시킬 수 있었으며 카드사 자체적으로 일회용 가상카드번호를 승인하기 위한 별도의 인증 서버 및 기타 인프라를 구축하지 않아도 된다는 장점을 가진다. 또한 기본적으로 본 결제 프로토콜에서 사용하고 있는 일회용 가상카드번호 스킴은 위조불가능성 및 재사용불가, 완전성, 건전성, 일회용 가상카드번호의 일방향성의 기본 보안 요구사항을 만족하여 안전성이 기존 방식들에 비해 높기 때문에 온라인 상점에서 카드번호가 누출되어 무단 결제되는 문제를 예방할 수 있다.

그밖에도, 본 프로토콜은 휴대 단말기에 생성모듈을 다운로드받아 카드결제시마다 휴대폰에서 일회용 가상카드번호를 생성하여 사용하는 방식이기 때문에 보안이 취약한 PC에서 카드결제를 수행한다 할지라도 원래의 신용카드번호가 노출될 염려가 없다. 또한 이점은 온라인 상거래를 수행할 때 두 번에 걸쳐 인증을 제공하는 방식이 될 수 있어 더욱 안전하다. 즉, 온라인 상거래를 위해 1차적으로 기본적인 사용자 인증(ID/패스워드, 공인인증서)을 수행하고 소지 기반 휴대폰의 생성모듈을 활용하여 일회용 가상카드번호를 생성하고 입력함으로써, 2차적으로 소지기반 사용자 인증이 한번 더 수행되게 된다. 즉, 생성모듈이 탑재된 휴대폰을 소지하지 않는다면, 일회용 가상카드번호를 생성해낼 수 없으며, 한번 사용된 일회용 가상카드번호는 재사용이 불가능하기 때문에 재전송 공격들이 불가능하다. 해커가 피싱 사이트 등을 이용해 일회용 가상카드번호를 일부 얻어냈다 하더라도 특정시간이 지나거나 생성카운트 범위가 넘어가는 경우에는 사용할 수 없기 때문에 현실적으로 공격이 성공하기 어렵다.

## VI. 결 론

IT 기술과 인터넷의 발달은 온라인 상거래 서비스를 급격히 발전시켰으며, 온라인 신용카드 결제 방식이 전자상거래를 위한 보편화된 결제 수단으로 자리잡을 수 있게 하였다. 그러나 최근에 일어난 온라인 포털 사이트 해킹 사건과 대량의 개인정보 유출 사건

〔표 1〕 일회용 가상번호 생성프로토콜간의 비교분석

| | ShopSafe® | Citibank | Discover® | PayPal | Ian Molly 스킴 | 제안 스킴 (4.3절) |
|---|---|---|---|---|---|---|
| 재사용불가성 | × | ○ | × | ○ | × | ○ |
| 위조불가 | | ○ | ○ | ○ | ○ | ○ |
| 완전성 | ○ | ○ | ○ | ○ | ○ | ○ |
| 건전성 | ○ | ○ | ○ | ○ | ○ | ○ |
| 계좌숨김 | ○ | ○ | ○ | ○ | ○ | ○ |
| PC에 악성코드가 설치되었을때 보안 | 인터넷뱅킹로그인시 사용/ 카드번호 입력.PC가 악성코드 있을 때 취약 | 소프트웨어 다운로드, 또는 홈페이지에서 구동 | 소프트웨어다운로드(데스크탑) 또는 인터넷브라우저 구동 | 소프트웨어다운로드 | 소프트웨어다운로드 | 휴대단말기 탑재, PC 악성코드와 무관 |
| 서비스제공범위 | 한정적, 자사고객만 가능 | 한정적, 자사고객만 가능 | 한정적, 자사고객만 가능 | 한정적, 자사고객만 가능 | 한정적 | 타기관 이용가능 |
| 사용자편의성 | × | × | × | × | × | ○ |

〔표 2〕 Ian Molly 스킴과 제안 스킴의 효율성 비교

| | 연접계산 | | 일방향 해시함수 계산 | | 모듈러스 계산 | |
|---|---|---|---|---|---|---|
| | 생성 | 검증 | 생성 | 검증 | 생성 | 검증 |
| Ian-Molly 스킴 | 4 | 4 | 2 | 2 | 1 | 1 |
| 제안하는 스킴(3.3절) | 6 | 6 | 3 | 3 | 1 | 1 |

등은 신용카드번호 무단 결제의 피해를 양산시킴으로써 전자상거래를 이용하는 사용자들을 불안에 떨게 하고 있다. 이에 몇몇 카드 회사들은 자구책으로 일회용 가상신용카드번호를 생성시켜 사용하게 하는 방식을 시범서비스로 제공하고 있다. 그러나 서비스의 범위가 한정적이고 악성코드가 감염된 PC에서 사용할 경우 원래의 신용카드번호를 그대로 노출시키는 위협이 존재하며 일부 방식들은 재사용 불가의 기본 보안 요구사항을 만족하지 못하고 있다.

본 논문에서는 해외에서 서비스되고 있는 일회용 가상카드번호 생성 서비스들과 Ian Molly 등이 제안한 일회용 가상카드번호 생성 스킴의 취약성을 분석하고, 일회용패스워드 기술을 적용하여 신규성을 제공하는 새로운 일회용 가상카드번호 생성 스킴을 제안하였다. 또한 이를 기반으로 하여 국내 통합인증센터를 활용한 일회용 가상카드번호 생성 및 결제 프로토콜을 설계하였다. 제안한 스킴은 완전성, 건전성을 만족하며 암호학적인 일방향 해시함수에 기반하여 생성스킴을 설계하였기 때문에 일회용 가상카드번호의 일방향성과 위조불가능성도 만족하고, 카드생성시각정보와 카운터 값 등을 부가적인 정보로 생성스킴에 입력함으로써 신규성을 제공하고 재사용불가 특성을 만족한다. 기존 연구들이 신규성 및 재사용불가 등을 제공하지 못하여 일회용 가상카드번호의 중요한 특성을 만족시키지 못해 문제가 되고 있는 반면, 제안한 스킴은 기존 연구들에 비해 연산의 효율성을 크게 떨어뜨리지 않으면서 기존 연구들의 취약점들을 개선하였다.

따라서 안전한 온라인 지불결제 시스템에 대한 수요가 확대되고 있는 상황에서, 제안하는 결제 프로토콜은 휴대 단말기를 활용하여 편리하게 일회용 가상카드번호를 생성하게 하며, 일회성을 보장하기 때문에 온라인상 신용카드번호 유출로 인한 피해를 예방할 수 있는 장점을 가진다. 또한 국내 금융권 통합인증센터를 활용하여 하나의 일회용 가상카드번호 생성모듈로 사용자가 소지하고 있는 모든 카드의 가상카드 번호를 생성할 수 있게 함으로써 사용자 편의성을 개선시키고 카드사들이 별도의 인프라 구축없이 서비스를 제공받을 수 있게 하였다.

## 참 고 문 헌

〔1〕 서승현, 강우진, "OTP 기술현황 및 국내 금융권

OTP 도입사례," 정보보호학회지, 17(3), pp. 18-25, 2007년 6월.
[2] 세계일보, "신용카드 일련번호 규칙성 뚫렸다," 2007년 4월.
[3] 아시아경제, "옥션 해킹 피해자, 1081만명에 달해," 2008년 4월.
[4] 연합뉴스, "1천만명 정보유출," 2008년 9월.
[5] 위키백과, "신용카드," http://ko.wikipedia.org/wiki/%EC%8B%A0%EC%9A%A9%EC%B9%B4%EB %93%9C
[6] 한국경제신문, "씨티銀 인터넷 뱅킹 해킹 사고··카드 결제대행 보안 시스템 뚫어 '충격'," 2007년 2월.
[7] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," CRYPTO'96, LNCS 1109, pp.1-15, 1996.
[8] I. Molly, Jiangtao, and N. Li, "Dynamic Virtual Credit Card Numbers," Financial Cryptography and Data Security, 11th International Conference, FC 2007, LNCS 4886, pp. 208-223, 2007.
[9] Citigroup, Citi identity theft solutions: Virtual account numbers, http://www.citibank.com/us/cards/cardserv/advice/van.htm
[10] Discover Bank, Discover card: Secure online account numbers, http://www.discovercard.com
[11] ShopSafe, ShopSafe Service: Safe Online Shopping from Bank of America, http://www.bankofa merica.com/privacy/ index.cfm?template=learn_about_shopsafe
[12] PayPal, PayPal Virtual Debit Card, http://www.paypal.com/cgi-bin/webscr?cmd=xpt/cps/account/VDCFrequently Asked, Questions-outsid

## 〈著者紹介〉

서 승 현 (Seung-Hyun Seo) 종신회원
2000년 2월: 이화여자대학교 수학과 졸업
2002년 2월: 이화여자대학교 대학원 컴퓨터학과 석사
2006년 2월: 이화여자대학교 대학원 컴퓨터학과 박사
2006년 5월~2006년 11월: 고려대학교 정보경영공학전문대학원 연구전임강사
2006년 12월~2010년 1월: 금융보안연구원 주임연구원
2010년 2월~현재: 한국인터넷진흥원 선임연구원
〈관심분야〉 암호프로토콜, 암호이론, 네트워크 및 시스템 보안