Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.5

효율적인 인증을 위한 해시 저장방식의 가상카드번호 결제 시스템*

박 찬 호,† 김 건 우, 박 창 섭‡
단국대학교

Virtual Credit Card Number Payment System with Stored Hash Value for Efficient Authentication*

Chan-ho Park,† Gun-woo Kim, Chang-seop Park‡
Dankook University

요 약

초고속 인터넷과 무선통신망의 발달로 전자상거래는 급증하는 추세이다. 그러나 최근 이동통신사, 금융사 등의 해킹 사건으로 인해 많은 수의 개인정보가 유출되었다. 특히 신용카드정보의 경우 온라인 거래에 악용되어 결제를 시도할 수 있고 이에 따른 피해는 카드소지자가 입게 된다. 이를 막기 위해 실제카드번호 대신 가상카드번호를 사용하는 기법들이 제안되었다. 하지만 기존의 제안들은 취약점이 존재하고 추가적인 보안 인프라가 필요하다. 본 논문에서는 기존에 제안된 가상카드번호 기법들을 분석하고 카드 사용자가 공개키/비밀키 키쌍을 생성하고 공개키를 카드사에 사전등록 함으로써 보안 요구사항을 충분히 만족시키면서도 추가적인 보안 인프라 없이 효율적으로 결제할 수 있는 가상카드번호 기법을 제안한다.

ABSTRACT

Electronic transactions have been increasing with the development of the high-speed Internet and wireless communication. However, in recent years financial corporations and mobile carriers were attacked by hackers. And large numbers of privacy information have been leaked. In particular, in the case of credit card information can be misused in the online transaction, and the damage of this given to cardholder. To prevent these problems, it has been proposed to use a virtual card number instead of the actual card number. But it has security vulnerability and requires additional security infrastructure. In this paper, we analyzed the proposed virtual card number schemes. and we propose a new virtual credit card number scheme. In the newly proposed scheme, cardholder generates a key pair (public key/private key) and pre-register public key to the issuer. then, cardholder can pay no additional security infrastructure while still efficiently satisfy the security requirements.

Keywords: Online Transaction, E-Commerce, Virtual Credit Card Number, Authentication

접수일(2014년 8월 22일), 수정일(2015년 1월 6일), 게재확정일(2015년 1월 6일)
* 본 연구는 2014년도 한국연구재단의 기초연구사업 지원(NRF-2014R1A1A2055074)과 미래창조과학부의 방송통신정책연구센터 운영지원 사업의 연구결과로 수행되었음(KCA-2013-003).
* 본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원(NRF-2011-0023118)과 미래창조과학부의 방송통신정책연구센터 운영지원 사업의 연구결과로 수행되었음 (KCA-2013-003).
† 주저자, chpark6737@gmail.com
‡ 교신저자, csp0@dankook.ac.kr(Corresponding author)

I. 서 론

초고속 인터넷 서비스, 무선통신망의 발달 및 스마트폰 등 새로운 정보통신매체가 보급·활성화됨에 따라 전자금융서비스는 보편화 되고 이용률이 해마다 증가하고 있다. 이러한 전자금융서비스를 통해 상품 또는 서비스를 거래하는 전자상거래 (E-Commerce)는 판매자와 구매자가 직접 만나지 않고 거래하는 '비대면 거래'라는 특성으로 인해 상호인증 및 결제수단인증에 유의해야 한다. 특히 신용카드의 경우 신용카드 자체에 대한 인증뿐만 아니라 신용카드 사용자에 대한 인증이 필수다. 신용카드 결제는 카드번호, 유효기간, CVV (Card Verification Value)등 카드정보를 검증하는 방식을 사용한다. 온라인 쇼핑몰에서 해킹 등의 방법을 통해 고객의 신용카드정보들이 유출될 경우 악의적 의도로 전자상거래 결제에 사용될 수 있고, 이에 대한 피해는 고스란히 고객들에게 전가된다. 그래서 이러한 피해를 예방하기 위하여 지금까지 다양한 기법들이 제안되었다.

Ian Molloy 등[1]이 제안한 DVCC (Dynamic Virtual Credit Card scheme) 기법은 이러한 피해를 예방하기 위해 실제카드번호 대신 가상카드번호를 사용하는 기법을 제안하고 있다. 하지만 가상카드번호를 획득할 경우 재사용공격을 통해 결제에 사용할 수 있는 취약점이 있다. OVCN (One-time Virtual Credit card Number scheme) 기법[2]은 DVCC 기법이 재사용 공격에 취약한 점을 보완하여 재사용이 불가능한 일회용 가상카드번호를 사용하도록 제안한 기법이다. 하지만 OTP 통합인증센터[8]와의 연동을 통해 가상카드번호의 검증을 받아야 하기 때문에 제3의 신뢰기관을 필요로 한다. 3-D Secure[3,4]는 SSL/TLS를 이용한 채널을 통해 카드사가 카드 소지자를 직접 인증하도록 하는 기법이다. 그러나 판매자가 악의적 의도를 가질 경우, 카드사와 카드 소지자 사이에 오가는 정보들을 도청할 수 있는 취약점이 존재한다[5].

본 논문에서는 DVCC 기법, OVCN 기법, 3-D Secure 기법 등을 살펴보고 취약점을 분석한 뒤, 이를 보완한 새로운 신용카드결제 기법을 제안한다. 제안하는 기법은 카드 사용자가 공개키/비밀키 키쌍을 생성하고 카드사에 사전등록 하는 과정이 필요하지만 일회적인 키쌍 등록과정만 거치면 거래의 신규성(freshness)을 보장하면서도 CA (Certificate Authority)와 같은 추가적인 보안 기반구조(security infrastructure) 없이 효율적인 인증 및 거래가 가능하다. 본 논문에서는 2장에서 온라인 카드결제에 대한 보안 요구사항을 정의하고 3장에서는 신용카드 번호체계의 국제표준과 일반적인 신용카드결제 흐름에 대해 알아본 뒤, DVCC 기법, OVCN 기법, 3-D Secure 기법을 분석한다. 4장에서는 기존 기법들의 취약점을 보완한 새로운 기법을 제안한다. 그리고 5장에서는 기존의 기법들과 제안하는 기법을 비교·분석하고 6장에서는 향후 연구 과제를 제시하며 결론을 맺는다.

II. 온라인 신용카드결제에 대한 보안 요구사항

본 장에서는 안전한 온라인 신용카드결제를 위해 필요한 보안 요구사항들을 살펴본다.

(1) 신용카드정보의 기밀성

거래과정에서 실제카드정보가 노출될 경우 공격자에 의해 유출되어 다른 거래에 사용되는 등 악용될 수 있으므로 실제 신용카드정보가 직접적으로 노출되어서는 안 된다.

(2) 거래정보의 무결성

카드 소지자에 의해 작성된 거래정보 (구매자정보, 상품정보, 결제정보 등)가 위·변조 되지 않고 카드사에 전달되어 검증되어야 한다.

(3) 부인방지

온라인 거래 후 카드 소지자가 구매를 하였음을 증명하여 거래사실에 대해 부인할 수 없도록 해야 한다.

(4) 거래의 신규성

매 거래마다 달라지는 값을 통해 거래에 사용되는 정보가 재사용 된 것이 아닌 새로운 값이라는 것을 보장해야 한다.

(5) 가상카드번호의 일방향성

가상카드번호와 가상카드번호를 생성하는데 사용된 정보(실제카드번호를 제외하고)가 공격자에게 노출되더라도, 주어진 가상카드번호로부터 원래의 실제카드번호를 알아내는 것은 암호학적으로 불가능해야한다.

(6) 가상카드번호의 재사용 불가

공격자가 가상카드번호를 획득했다고 할지라도 재

사용하여 거래에 성공할 수 없어야 한다.

III. 관련 연구

본 장에서는 신용카드번호 체계와 일반적인 카드결제 과정에 대해서 알아보고 기존의 온라인 카드결제 기법들을 일반적인 카드결제 과정의 형태에 맞추어 정리·분석해 보도록 한다.

3.1 신용카드 번호체계

ISO/IEC 7812는 식별카드-발행자 인증 (Identification card - Identification of issuers) 에 관한 내용을 2개의 부분으로 나누어 정의하고 있다. 신용카드 번호체계는 그 중 ISO 7812-1[6]에서 명시하고 있다. 카드사 (Issuer)에 따라 차이는 있지만 일반적으로는 16자리의 신용카드 번호체계를 사용하고 그 구성은 Fig. 1. 과 같다. 첫째 자리는 주 산업 식별자(Major Industry Identifier, MII)로 카드가 사용되는 주 업종을 나타낸다. 그리고 MII를 포함한 첫 6자리는 발급자 식별번호 (Issuer Identifier Number, IIN)로 카드의 발급기관을 식별하기 위해 사용한다. 그 뒤 9자리는 개인 계좌식별 번호 (Individual Account Identification Number)로 각 카드사가 임의의 규칙에 따라 카드 소지자 (Card holder)에게 부여하는 식별코드이다. 그리고 마지막 1자리는 카드번호 검증 값(Check digit)으로 Luhn algorithm[6]을 통해 카드번호의 유효성을 검증하기 위한 값이다.

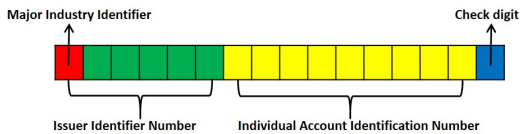

Fig. 1. Credit card Numbering System

3.2 일반적인 카드결제 과정

본 장에서는 기존의 신용카드결제 기법들을 살펴보기 전에 일반적인 카드결제 과정에 대해 정리해보도록 한다. 카드 소지자는 판매자의 고객이라는 관점에서 편의성을 위해 Client라고 지칭하였다.

일반적으로 카드거래는 카드 소지자 (Client)의

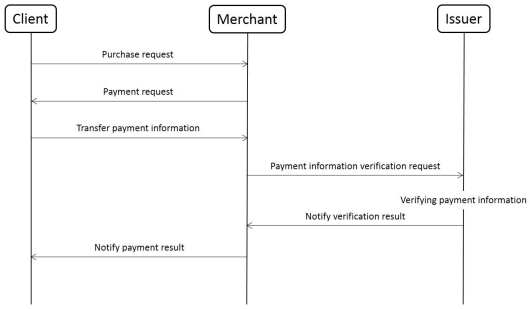

Fig. 2. Traditional Credit card Processing

구매요청으로 시작된다. 판매자 (Merchant)로부터 구매할 상품 혹은 서비스를 선택한 카드 소지자는 결제수단으로 카드를 선택한 뒤 구매요청을 한다. 그러면 판매자는 해당 상품 혹은 서비스에 대한 정보와 가격을 보여주며 결제요청을 한다. 카드 소지자는 이름, 주소, 카드번호, 유효기간 등 결제에 사용할 결제정보를 판매자에게 제공하여 결제를 시도한다. 판매자는 사용자로부터 받은 결제정보를 카드사 (Issuer)에게 보내 결제정보 승인을 요청한다. 카드사는 받은 정보들을 확인하고 카드 소지자 정보와 카드번호를 검증한 뒤 거래 승인결과를 판매자에게 통보한다. 판매자는 거래 승인결과를 확인한 뒤 카드 소지자에게 결제결과를 통보하면 일반적인 카드결제 과정이 끝나게 된다.

3.3 표기법

기존에 제안된 여러 기법들을 비교·분석의 목적으로 정리해 보는 만큼 각 기법마다 제각각 다른 표기법을 사용하지만 공통적인 요소들 또는 동일한 기능을 하는 요소들의 표기법을 통일시켰다. 본 논문에서 사용하는 표기법은 Table 1. 과 같다.

3.4 DVCC 기법

Ian Molloy등[1]이 제안한 DVCC 기법의 전체적인 거래과정은 일반적인 카드결제와 동일하지만 실제카드번호 대신 가상카드번호를 사용하는 것이 특징이다. 카드 소지자가 결제과정에서 가상카드번호를 동적으로 생성하여 실제카드번호 대신에 사용함으로써 실제카드정보의 유출을 방지하고 가상카드번호가 유출되더라도 유효기간 등을 통해 사용을 제한하여 피해를 예방하도록 하는 기법이다. DVCC 기법을 사용한 결제과정은 Fig. 3. 과 같다. 결제요청을 받은 카드

Table 1. Notations

Symbol	Description
Client	Cardholder
Merchant	Online shopping mall
Issuer	Credit card issuer
ClientInfo	Cardholder information
ItemInfo	Item information
R-Card	Real credit card numbers
V-Card	Virtual credit card numbers
R-Exp	Real expiration dates
V-Exp	Virtual expiration dates
IIN	Issuer identifier number
PIN	Personal identification number
Password	Cardholder password
MK	Master key
K	Symmetric key
$H(.)$	One-way hash function
$F_K(.)$	HMAC-SHA1 or HMAC-SHA256
TS_x	The timestamp of x
PK_x	The public key of x
SK_x	The private key of x
$SIG(SK_x,\sigma)$	Signature value, signed with a private key of x for transaction information σ
C	Synchronized count value

소지자 (Client)는 결제에 사용할 가상카드정보를 생성한다. 우선 가상카드 유효기간(V-Exp)을 설정한다. 가상카드 유효기간은 결제일이 속한 달의 말일로 한다. 그리고 실제카드번호 (R-Card)와 사전 공유된 비밀정보 (PIN 또는 Password)에 SHA1 함수를 적용하여 대칭키 K를 획득한다. 카드 소지자 정보 (ClientInfo), 가상카드 유효기간, 상품정보 (ItemInfo)를 통해 결제정보(σ)를 생성하고 결제정보와 대칭키 K를 이용해 HMAC-SHA1[7] 함수 $F_K(\sigma) \bmod 10^n$ (n은 출력하고자 하는 자릿수)를 계산한다. 이렇게 생성된 값 중 끝의 3자리는 가상 CVV코드로 사용하고 남은 숫자는 앞에는 카드사 식별번호(IIN)를 붙이고 뒤에는 Luhn algorithm [6]을 적용한 검증코드를 붙여 가상카드번호 (V-Card)로 사용한다.

카드 소지자는 이렇게 생성한 가상카드정보를 판매자 (Merchant)에게 보내 결제를 시도한다. 판매자는 카드 소지자 정보, 상품정보, 가상카드정보를 카드사(Issuer)에 보내 검증 및 결제승인을 요청한다. 카드사는 카드 소지자의 정보, 실제카드번호, 사전 공유된 비밀정보를 알고 있기 때문에 카드 소지자와 동일한 과정을 거쳐 가상카드정보를 생성하고 판매자로부터 받은 가상카드정보와 비교하여 검증을 한다. 그리고 승인결과를 판매자에게 통보하고 판매자는 다시 카드 소지자에게 결제결과를 통보하면 결제과정이 끝나게 된다.

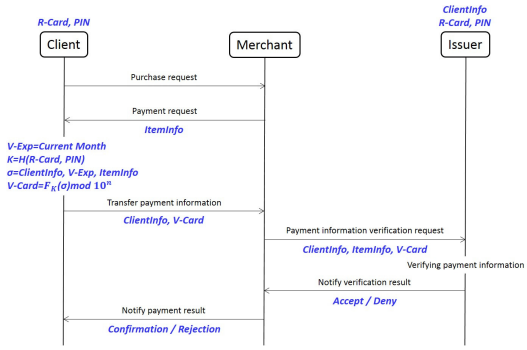

Fig. 3. DVCC scheme Processing

3.5 OVCN 기법

OVCN 기법[2]은 DVCC 기법[1]의 취약점을 보완하고 국내 금융기관에서 사용 중인 OTP 통합인증센터[8]를 연동하여 한 번만 사용 가능한 일회용 가상카드번호를 생성하여 사용하자는 제안이다. DVCC 기법에서 가상카드번호를 생성할 때, 신규성을 제공하는 값이 없어 재사용 공격에 취약한 점을 지적하고 타임스탬프와 카드 사용자·통합인증센터 간 동기화된 카운트 값을 통해 신규성을 제공하여 재사용 공격을 방지할 수 있도록 하였다.

OVCN 기법도 DVCC 기법과 마찬가지로 전체적인 거래과정은 일반적인 카드결제와 동일하다. 다소 다른 부분은 결제요청과정에서 사용자가 선택한 카드사의 결제 팝업창을 통해 사용자가 생성한 일회용 가상카드번호를 입력하여 결제시도를 하게 된다. OVCN 기법은 자체적으로 제안한 16자리의 가상카드번호 체계를 사용하는데 그 구성은 Fig. 4. 와 같다

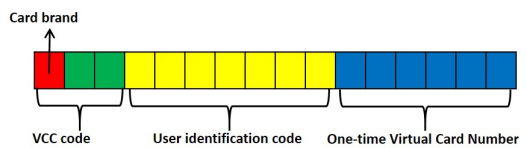

Fig. 4. OVCN scheme Numbering system

[2]. 맨 앞의 3자리는 VCC 구분코드로 3자리 중 첫 번째 숫자는 지정된 카드 브랜드를 의미하고 나머지 두 자리는 가상카드번호인지 실제카드번호인지 구분해주는 역할을 한다. 다음 7자리는 사용자 식별코드로 카드사가 카드 사용자에게 부여하는 식별코드(예; 주민등록번호에 해시함수를 적용한 값)이다. 마지막 6자리는 OVCN 모듈을 통해 생성한 일회용 가상카드번호 (OVCN 값)이다. VCC 구분코드와 사용자 식별코드는 일회용 가상카드번호 생성모듈 발급단계에서 카드사가 설정하여 사용자의 휴대 단말기에 저장하며 사용자가 모듈을 사용할 때 자동적으로 보여 지도록 한다.

OVCN 기법을 사용한 결제과정은 Fig. 5. 와 같다. 카드 소지자 (Client)는 구매할 상품 또는 서비스를 결정한 뒤 카드결제를 선택하고 카드사 (Issuer)를 지정하여 판매자 (Merchant)에게 구매요청을 한다. 판매자는 결제모듈을 통해 카드사와 연동하여 카드 소지자의 화면에 지정한 카드사의 결제용 윈도우 팝업창을 보여주며 결제요청을 한다. 결제요청을 받은 카드 소지자는 통합인증센터로부터 사전 공유된 마스터키 MK와 가상카드 서비스 신청 시 직접 설정한 PIN에 일방향 해시함수를 적용하여 대칭키 K를 획득한다. 통합인증센터와 동기화된 카운트 값 C를 증가시켜 C'을 계산한다. 카운트 값 C는 카드 소지자가 가상카드 서비스를 신청하고 자신의 기기에 일회용 가상카드번호 생성 모듈을 발급받는 과정에서 통합인증센터와 동기화 된 값이다. 그리고 실제카드번호 (R-Card)와 실제카드 유효기간 (R-Exp)에 일방향 해시함수를 적용해 H(R-Card, R-Exp)를 계산하고 카드 소지자 정보 (ClientInfo), 직접 생성한 타임스탬프(TS_C)등과 함께 종합하여 결제정보(σ)를 생성한다. 그리고 결제정보와 대칭키 K를 통해

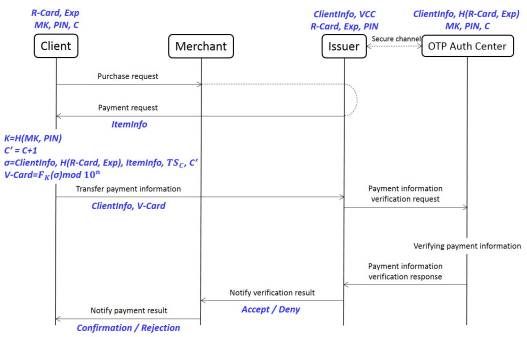

Fig. 5. OVCN scheme Processing

HMAC-SHA256 함수[7] $F_K(\sigma) \bmod 10^n$ (n =6)를 계산하여 6자리의 OVCN 값을 획득한다. 계산이 완료되면 모듈에서 선택한 카드사의 VCC 구분코드와 사용자 식별코드가 OVCN 값과 함께 출력되며 이 3가지를 합쳐 총 16자리의 숫자를 일회용 가상카드번호(V-Card)로 사용하게 된다. 카드 소지자는 위의 과정을 거쳐 생성한 16자리의 일회용 가상카드번호를 입력하여 결제를 시도한다. 입력한 가상카드번호는 카드사로 전송되며 카드사는 VCC 구분코드를 통해 가상카드번호임을 알게 되고 상품정보와 함께 통합인증센터에 인증요청을 한다. 통합인증센터는 VCC 구분코드와 사용자 식별번호를 통해 DB에서 사전 공유된 마스터키(MK), 사용자가 설정한 PIN, 실제카드정보 (H(R-Card, R-Exp)), 동기화된 카운트 값 C 등을 획득하고 카드 소지자와 같은 과정을 통해 OVCN 값을 생성하여 카드사로부터 받은 값과 비교하여 검증을 수행한다. 원활한 인증을 위해 전송속도 등을 고려하여 타임스탬프의 오차범위를 정하고 범위 안에 포함될 경우에만 인증이 성공한다. 통합인증센터는 검증결과를 카드사에게 통보하고 카드사는 판매자에게 판매자는 이를 다시 카드 소지자에게 통보하며 결제과정을 마치게 된다.

3.6 3-D Secure 기법

Visa에서 최초 제안한 것으로 온라인 거래 시 카드사(Issuer)가 직접 카드 소지자 (Client)를 인증하도록 하는 국제 표준 프로토콜이다 [3,4]. 3-D Secure는 온라인 거래를 Issuer domain (발급사 영역), Acquirer domain (매입사 영역), Interoperability domain (상호 운용 영역)으로 나누어 각각의 역할을 제시하는 3-Domain 개념을 기반으로 하고 있다. 발급사 영역은 발급사와 카드 사용자의 관계를 정의한 것으로 카드사, 카드 사용자, 접근 제어 서버 (Access Control Server, ACS)로 구성되어 있다. 매입사 영역은 가맹점(판매자)과 매입사의 관계를 정의한 것으로 매입사 (Acquirer), 판매자 (Merchant), MPI (Merchant Plug-In)으로 구성되어 있다. 상호 운영 영역은 발급사 영역과 매입사 영역 사이의 관계를 정의한 것으로 VDS (Visa Directory Server), AHS (Authentication History Server)로 구성되어 있다. 3-D Secure를 사용한 결제과정은 Fig. 6. 과 같다. 카드 소지자

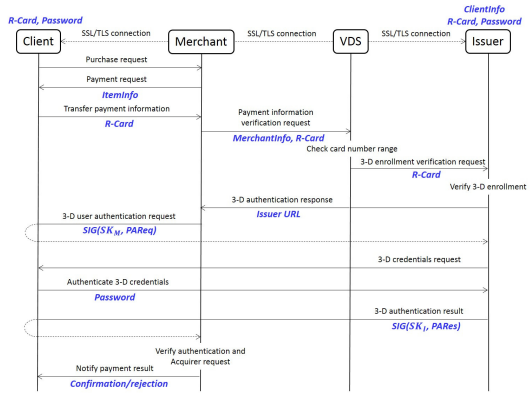

Fig. 6. 3-D Secure Processing

(Client)는 구매할 상품 또는 서비스를 선택한 뒤, 결제방법으로 3-D Secure 결제를 선택하고 실제카드번호 (R-Card)를 선택하여 결제를 시도한다. 판매자 (Merchant) 측에서는 이때 MPI (Merchant Plug-In)가 활성화 되고, MPI는 카드 소지자로부터 받은 실제 카드번호를 VDS (Visa Directory Server)에 보내 검증을 요청한다. VDS는 실제카드번호의 범위를 확인한다. 확인이 되면 VDS는 카드사 (Issuer)에 3-D인증 가능 여부를 확인한다. 3-D인증 등록이 확인되면 카드사는 ACS (Access Control Server)에 직접 접속할 수 있는 URL을 VDS를 통해 판매자에게 보낸다. 판매자의 MPI가 거래정보 등을 이용하여 PAReq (Payer Authentication Request) 양식을 만들어 자신의 개인키로 서명하고 카드 소지자에게 보낸다. PAReq를 받은 카드 소지자의 쇼핑화면(웹브라우저 등)은 URL을 통해 카드사의 ACS로 전달되고 ACS는 사용자의 3-D 자격증명을 요구한다. 자격증명으로는 3-D 비밀번호, 스마트카드 또는 국내에서는 공인인증서를 사용할 수 있다. 사용자가 미리 등록한 자격증명을 통해 인증을 한다. ACS는 인증결과를 PARes (Payer Authentication Response)로 만들어 자신의 개인키로 서명하여 카드 소지자에게 보낸다. 카드 소지자의 쇼핑화면은 다시 판매자 쇼핑몰로 전달되고 PARes는 MPI에게로 보내진다. MPI는 PARes를 확인한 뒤 매입사 (Acquirer)에게 승인 요청을 한다. 그리고 카드 소지자에게 결제결과를 통보하며 거래를 마치게 된다.

IV. 제안하는 기법

관련 연구에서는 DVCC 기법 [1], OVCN 기법 [2], 3-D Secure [3,4] 등 여러 카드결제 기법들을 일반적인 카드결제 흐름에 맞추어 정리해 보았다. 본 장에서는 앞서 살펴본 기법들의 장점은 충족하고 단점은 보완하면서도 더 효율적인 새로운 기법을 제안한다. 제안하는 기법은 신용카드발급 단계에서 카드 소지자가 비대칭키를 생성하여 카드사에게 공개키를 사전 공유하고 카드번호의 해시값과 공개키에 해시함수를 적용하여 계산한 값을 실제카드번호 대신 인증할 수 있는 가상카드번호로 사용한다. 가상카드번호를 사용함으로써 실제카드번호의 유출에 의한 피해를 예방하고, 결제과정에서 타임스탬프를 사용하여 신규성을 보장하며 카드 소지자가 생성한 개인키를 통해 전자서명을 하여 부인방지와 무결성을 충족시킬 수 있다. 또한 카드 소지자의 개인키와 공개키 키 쌍에 대한 신뢰성을 카드사가 보장함으로써 신용카드를 발급받은 카드사 외에 추가적인 보안 기반구조 (security infrastructure)가 필요하지 않아 효율적인 인증이 가능하다.

본 논문에서 제안하는 온라인 카드결제 기법은 Fig. 7. 과 같이 카드 소지자 (Client), 판매자 (Merchant), 카드사 (Issuer) 3개의 엔티티로 구성되어 있다. 카드사는 고객 (카드 소지자)에게 신용카드를 발급하여 결제에 사용할 수 있도록 한다. 그리고 판매자로부터 요청된 결제 정보를 검증한 뒤, 결과를 통보해주는 역할을 한다. 본 제안에서는 카드 소지자가 카드사로부터 신용카드를 발급 받을 때, 비대칭키를 생성하고 안전한 채널을 통해 공개키를 카드사에게 분배한다. 그리고 카드 소지자의 실제카드번호와 공개키를 이용해 가상카드번호를 생성하여 사용한다. 가상카드번호를 생성하는 방식은 수식(1)과 같다.

$$V-Card = H(PK_C, H(R-Card)) \quad (1)$$

카드사는 실제카드번호 (R-Card)에 해시함수를 적용하여 얻은 값 (H(R-Card))과 카드 소지자의 공개키 (PK_C)에 다시 해시함수를 적용하여 획득한 값을 실제카드번호 대신에 사용할 가상카드번호 (V-Card)로 저장하여 관리하며 결제정보 검증 시 사용한다. 판매자는 온라인으로 상품 또는 서비스를 판매하며 고객(카드 소지자)으로 부터 받은 결제정보를

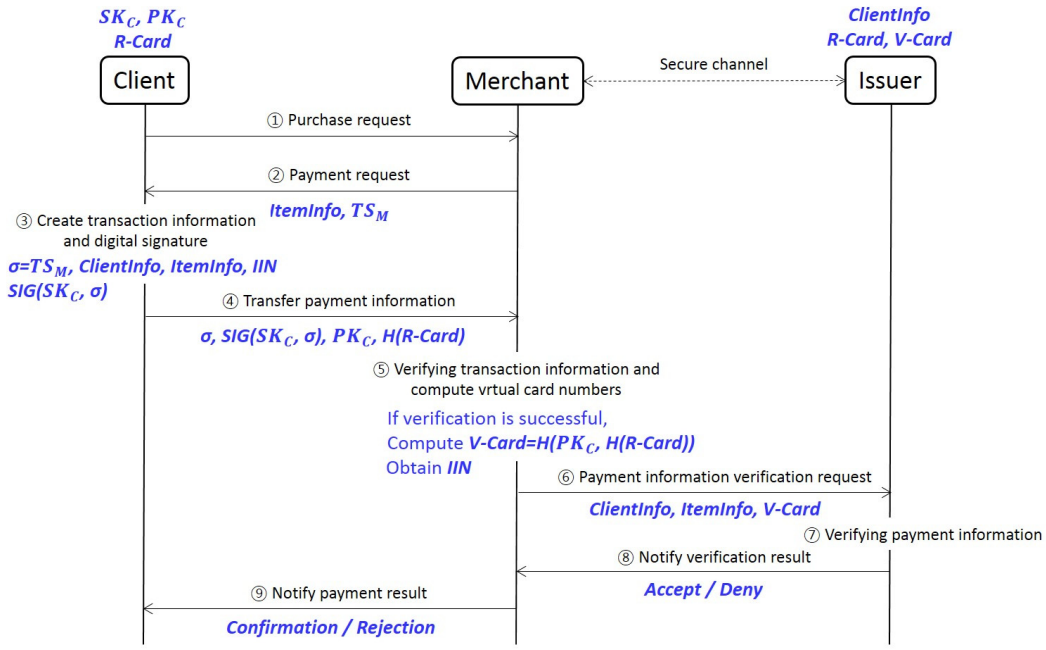

Fig. 7. Our Proposed scheme Processing

카드사에 보내 승인을 요청한다. 고객이 가상카드번호 방식의 결제를 선택했을 경우, 타임스탬프를 통해 거래의 신규성을 보장하고 전자서명을 통해 결제정보 값의 무결성을 검사하여 이상이 없으면, 가상카드번호를 생성해 카드사에 승인요청을 한다. 일반적으로 온라인 쇼핑 시, 결제과정은 판매자가 직접 하지 않고 VAN사 (Value Added Network) 또는 PG사 (Payment Gateway)에 위탁하여 하게 되는데, 본 제안에서는 VAN사 또는 PG사가 온라인 쇼핑몰과 함께 판매자 엔티티에 포함되어 있는 것으로 간주하였다. 그리고 판매자는 PG를 통해 카드사와 가상카드결제를 위한 안전한 채널을 구성하고 있는 신뢰된 판매자로 가정하였다. 제안하는 기법을 이용한 온라인 결제과정은 다음과 같다.

(1) 카드 소지자 (Client)는 구매할 상품 혹은 서비스를 선택한 뒤, 결제방식으로 가상카드결제를 선택하여 판매자 (Merchant)에게 구매요청을 한다.

(2) 판매자는 카드 소지자가 구매요청한 상품의 정보 (ItemInfo)와 직접 생성한 타임스탬프 (TS_M)를 카드 소지자에게 전송하여 결제요청을 한다.

(3) 카드 소지자는 판매자로부터 받은 타임스탬프, 카드 소지자 정보 (ClientInfo), 상품정보, 카드사 식별번호 (IIN) 등을 모아 결제정보(σ)를 생성한다. 그리고 결제정보를 자신의 서명용 개인키(SK_C)로 서명한다.

(4) 카드 소지자는 결제정보, 결제정보의 서명 값 ($SIG(SK_C,\sigma)$), 실제카드번호에 해시함수를 적용하여 계산한 값 (H(R-Card))을 판매자에게 보내 결제를 시도한다.

(5) 판매자는 PG (Payment Gateway)로 결제정보들을 전송한다. 일반적인 전자서명의 검증 절차는 PKI (Public Key Infrastructure)를 통해 키 쌍의 유효성을 검증한 뒤, 서명 값을 확인하는 순서로 진행된다. 하지만 본 제안에서는 PKI와 같은 추가적인 보안 인프라 없이 인증을 하기 위해 우선 PG가 카드 소지자의 서명 확인용 공개키 (PK_C)로 결제정보의 전자서명을 확인한다. 그리고 확인이 성공하면, 카드 소지자의 공개키와 실제 카드번호의 해시 값에 해시함수를 적용하여 가상카드번호 (V-Card)를 생성하고 결제정보에 포함된 카드사 식별번호(IIN) 를 통해 해당 카드사에 결제정보 승인을 요청한다. 판매자는 카드사의 가상카드번호 승인결과에 따라

키 쌍의 유효성 여부를 판단하게 된다. 결제가 승인될 경우 공개키가 카드 소지자가 생성한 것임이 간접적으로 인증되어 부인방지와 결제정보의 무결성을 입증하는 효과를 갖는다. 하지만 전자서명 확인이 실패하거나 가상카드번호의 검증이 실패하면 유효한 키가 아닌 것으로 판단하고 카드 소지자에게 결제 거부를 통보하며 거래가 끝나게 된다.

(6) PG는 카드사 식별번호를 통해 해시함수가 적용된 실제카드번호가 어느 카드사 (Issuer)의 것인지 확인한다. 그리고 해당 카드사에 카드 소지자 정보, 상품정보, 가상카드번호를 전송하여 결제정보 승인을 요청한다.

(7) 카드사는 카드 소지자 정보를 통해 해당 사용자의 가상카드번호를 찾고 판매자로부터 받은 가상카드번호와 비교하여 검증한다.

(8) 카드사는 검증과정을 통해 얻은 결과에 따라 승인/거부 (Accept/Deny) 여부를 판매자에게 통보한다. 이때, 판매자가 승인통보를 받는다면 (5)에서 받은 전자서명에 사용한 카드 소지자의 개인키와 검증에 사용한 공개키의 키 쌍이 카드 소지자가 생성한 정당힌 키 쌍임을 카드사로부터 간접적으로 인증 받는 효과를 갖는다. 따라서 제3의 신뢰기관이 없이도 정당한 거래임을 확인할 수 있게 된다.

(9) 판매자는 카드사로부터 받은 결과에 따라 결제 성공/실패 (Confirmation/Rejection) 여부를 카드 소지자에게 통보하고 거래가 종료된다.

V. 비교·분석

본 장에서는 관련연구에서 살펴본 기법들과 제안하는 기법을 2장에서 제시한 보안 요구사항들을 기준으로 비교·분석 해보도록 한다.

5.1 신용카드정보의 기밀성

본 논문은 신용카드정보가 유출되고 악용되어 카드 소지자가 받게 되는 피해를 예방할 수 있는 기법을 제안하는데 목적이 있으므로 신용카드정보의 기밀성은 필수적인 요구사항이다. 관련연구에서 살펴본 기법들과 제안한 기법은 모두 신용카드정보의 기밀성을 만족한다. DVCC 기법과 OVCN 기법은 거래과정에서 실제카드정보에 HMAC 해시함수를 적용하여 가상카드번호를 생성한 뒤 결제에 사용하므로 실제카드정보가 직접적으로 노출되지 않는다.

3-D Secure는 거래과정에서 SSL/TLS 연결을 사용한 안전한 채널을 통해 암호화된 카드정보를 주고받으므로 안전하다고 볼 수 있다. 그러나 판매자가 악의적 의도를 가질 경우 카드 소지자와 카드사 사이의 정보를 redirect시키는 대신 proxy처럼 동작하여 카드 소지자의 상세정보를 획득하게 될 위험성이 제기되었다[5]. 제안하는 기법에서는 실제카드번호 대신 실제카드번호에 해시함수를 적용한 값과 사전 공유된 카드 소지자의 공개키를 거래에 사용하기 때문에 실제카드정보가 직접적으로 노출되지 않아 신용카드정보의 기밀성이 보장된다.

5.2 거래정보의 무결성

온라인 거래는 비대면 거래라는 특징 때문에 거래과정에서 중간에 공격자가 개입할 가능성이 있으므로 거래정보가 위·변조 되지 않았음을 확신할 수 없다. 따라서 무결성을 보장하여 카드 소지자가 보낸 정보가 그대로 카드사에게 전달되었음을 입증할 수 있어야 한다. DVCC 기법과 OVCN 기법은 가상카드번호를 생성하는 과정에서 카드 소지자 정보, 상품정보 등을 포함하여 결제정보를 생성하고 거기에 HMAC 해시함수를 적용한다. 또한 검증 시에도 동일한 정보들에 HMAC 해시함수를 적용하여 나온 값을 비교하여 검증하므로 결제정보가 승인될 경우 거래정보의 무결성이 보장되었다고 볼 수 있다. 3-D Secure는 SSL/TLS 연결을 통해 거래정보를 교환하고, 인증과정에서도 결제정보들을 종합하여 생성하는 PAReq와 PARes에 각자의 개인키로 서명을 하므로 무결성을 보장한다. 그러나 판매자가 악의적 의도를 갖는다면, 거래정보들을 도청하고 위·변조를 할 수 있는 취약점이 있다[5]. 제안하는 기법에서는 카드 소지자가 거래정보가 포함된 결제정보를 판매자에게 전송할 때 자신의 개인키로 서명하여 전송하고 판매자는 이를 검증한다. 그리고 안전한 채널을 통해 카드사에게 가상카드번호를 검증받음으로써 카드 소지자의 비대칭키에 대한 유효성을 확인할 수 있어 거래정보의 무결성이 보장된다.

5.3 부인방지

온라인 거래는 비대면 거래이고, 오프라인거래보다

Table 2. Comparison of the Credit Card Payment schemes

	DVCC scheme	OVCN scheme	3-D Seucre	Proposed scheme
Confidentiality of credit card information	O	O	O	O
Integrity of transaction information	O	O	O	O
Non-repudiation	×	×	×	O
Reuse resistant	×	O	×	O
Onewayness of Virtual card number	O	O	not use virtual card number	O
No need for additional security infrastructure	O	×	×	O

디지털 자료인 거래내역의 위·변조 가능성이 크기 때문에 부인방지는 필수적인 요구사항이다. DVCC 기법과 OVCN 기법은 대칭키 방식을 사용하여 결제정보에 대한 전자서명을 포함하지 않기 때문에 부인방지 기능을 제공하지 않는다. 또한 3-D Secure 기법도 구매자의 전자서명을 포함하지 않아 부인방지기능을 제공하지 않는다. 본 논문에서 제안하는 기법은 신용카드를 발급받을 때 카드 소지자가 비대칭키를 생성하고 카드사에게 공개키를 사전 공유한다. 카드 소지자는 이 비대칭키 중 서명용 개인키를 이용하여 결제정보에 대한 전자서명을 하고 판매자(PG)가 공개키를 통해 서명을 검증한다. 하지만 판매자는 서명에 사용된 개인키와 검증에 사용한 공개키가 카드 소지자의 것이 맞는지 키의 유효성을 확인해야할 필요성이 있다. 일반적인 경우 PKI를 통해서 비대칭키의 신뢰성을 검증하지만 본 제안에서는 가상카드번호를 통해 검증하게 된다. 전자서명 검증에 사용한 공개키와, 카드 소지자의 실제카드번호에 해시 값에 다시 해시함수를 적용하여 가상카드번호를 생성하고 카드사에 검증을 요청한다. 카드사가 검증성공을 통보하면 판매자는 카드 소지자의 실제카드번호와 비대칭키의 연관성을 간접적으로 확인하게 되어 PKI와 같은 추가적인 보안 기반구조와의 연동 없이도 효율적인 인증 및 부인방지가 가능하다.

5.4 거래 신규성 보장 및 재사용 공격 불가

DVCC 기법의 경우 가상카드 유효기간을 설정하여 사용의 한도를 줄이긴 했지만 가상카드 유효기간이 최대 한 달까지 설정될 수 있기 때문에 여전히 재사용될 위험성은 남아있다. OVCN 기법은 타임스탬프와 카운트 값을 통해 가상카드번호의 신규성을 보장하기 때문에 재사용 공격을 방지할 수 있다. 제안하는 기법은 가상카드번호 생성 시 신규성을 제공하는 값을 포함하지는 않지만 카드 소지자가 타임스탬프가 포함된 결제정보에 자신의 개인키로 서명하고 이를 판매자가 공개키를 사용하여 검증함으로써 신규성이 보장된 정당한 거래임을 증명한다. 또한 이 검증을 통과해야만 판매자가 사용자의 결제정보를 사용하여 가상카드번호를 생성하고 안전한 채널을 통해 카드사에 검증요청을 하는 과정을 진행하므로 재사용 공격을 방지할 수 있다. 그리고 가상카드번호자체가 유출되어도 카드 소지자의 개인키가 안전하다면 유출된 가상카드번호만으로는 결제에 성공할 수 없기 때문에 재사용 공격에 대한 위험성은 없다.

5.5 가상카드번호의 일방향성

가상카드번호를 사용하여 결제를 할 때 실제카드번호와 카드 소지자 정보, 상품정보 등을 통해 가상카드번호를 생성하게 된다. 이때, 실제카드번호를 제외한 다른 값들은 공개 될 수 있지만 실제카드번호는 결제에 사용될 수 있기 때문에 공개되어서는 안 된다. 가상카드번호와 실제카드번호를 제외하고 가상카드번호를 생성하는데 사용된 정보들을 공격자가 알게 되었다 하더라도 가상카드번호는 일방향 해시함수를 통해 생성되었으므로 실제카드번호를 알아내는 것은 암호학적으로 불가능해야한다. DVCC 기법은 HMAC-SHA1 함수를, OVCN 기법은 HMAC-SHA256 함수를 통해 가상카드번호를 생성한다. 제안하는 기법 또한 일방향 해시함수를 통해 가상카드번호를 생성하므로 공격자가 가상카드번호를 획득했다고 하더라도 역으로 실제카드번호를 계산하는 것은 암호학적으로 불가능하다.

5.6 추가적인 보안 인프라 불필요

DVCC 기법의 경우 추가적인 보안 인프라가 필요하지 않다. 그러나 가상카드번호의 재사용에 대한 취약점이 존재한다. OVCN 기법은 이런 DVCC 기법의 취약점을 보완하기 위해 통합인증센터와 연동을 하였다. 카드 소지자와 통합인증센터 간 동기화 된 카운트 값을 통해 거래의 신규성을 보장하여 가상카드번호의 재사용 공격을 방지하도록 했다. 또한 제3의 신뢰기관인 통합인증센터에 등록함으로써 간단한 절차를 통해 여러 카드사의 카드를 등록하여 사용할 수 있도록 한 장점이 있다. 그러나 카드사와 통합인증센터간의 전용네트워크가 연결되어야 하고 카드사가 판매자로부터 받은 카드번호가 가상카드번호인지 실제카드번호인지를 구분하여 가상카드번호일 경우 통합인증센터로 검증을 요청하고 결과를 전달받아야 하는 등의 부가적인 통신이 필요한 단점이 있다. 또한 가상카드번호의 결제가 통합인증센터에 집중된다는 점도 문제가 될 수 있다. 3-D Secure 기법은 판매자와 카드사의 사이에서 인증을 중재하는 VDS (Visa Directory Server)가 필요하다. 본 논문에서는 이러한 제3의 기관에 대한 의존성을 개선하기위해 해시 저장방식의 가상카드번호 결제 시스템을 제안하였다. 카드 발급 시 카드 소지자가 공개키와 개인키를 생성하여 카드사에게 공개키를 분배하고 실제카드번호의 해시 값과 공개키에 다시 일방향 해시함수를 적용한 값을 가상카드번호로 저장하여 인증에 사용한다. 카드 소지자는 결제하는 과정에서 판매자가 생성한 타임스탬프 값을 포함한 결제정보에 자신의 개인키로 전자서명을 하고 판매자는 공개키를 통해 서명을 검증함으로써 거래의 신규성을 검사한다. 또한 이 검증을 통과하는 경우에만 가상카드번호를 카드사에 전송하여 결제를 시도할 수 있으므로 추가적인 보안 인프라에 의존하지 않고도 거래의 신규성을 보장하고 재사용 공격을 예방하며 부인방지의 기능까지 충족시킬 수 있어 효율적인 인증이 가능하다고 할 수 있다. 그러나 카드사가 CA와 같은 제3의 신뢰기관과의 통신 없이 자체적으로 인증을 수행하더라도 기존에 사용되지 않던 카드 소지자의 가상카드번호에 대한 관리가 필요하게 되었으므로 오버헤드를 완전히 제거했다고 할 수는 없다. 효율적인 구현을 통해 이를 최소화 할 수 있도록 해야 할 것이다.

VI. 결 론

인터넷의 발달로 인한 전자상거래의 사용량이 증가한 만큼 그로인한 피해도 함께 증가하고 있다. 따라서 그에 대한 해결책이 시급한 가운데 여러 가지 기법들이 제안되고 있다. 본 논문에서는 여러 기법들 중 실제카드번호 대신에 사용하여 결제할 수 있는 가상카드번호 기법들을 살펴보고 기존의 기법들을 보완한 새로운 기법을 제안하였다. 제안하는 기법에서는 실제신용카드 정보를 직접 사용하지 않아 기밀성을 보장하고 결제정보에 카드 소지자의 개인키로 서명을 함으로써 거래정보의 신규성과 무결성을 보장하고 실제카드번호를 사용하지 않고도 자신이 정당한 카드소지자 임을 증명할 수 있다. 또한 결제정보에 타임스탬프를 포함시켜 거래의 신규성을 보장하고 신규성 검증이 성공했을 때에만 결제정보 검증요청을 하여 재사용 공격을 미연에 방지하였다. 또한 기존의 제안과의 가장 큰 특징은 카드 소지가 신용카드 발급 시 비대칭키 키 쌍을 생성하여 공개키를 카드사에게 사전공유 하고 이를 이용해 서명, 인증 등에 사용함으로써 추가적인 보안 인프라가 필요하지 않게 되어 제3의 기관과의 추가적인 통신을 줄여 효율적인 인증 및 거래가 가능하게 되었다. 향후에는 사용자가 생성한 공개키를 안전하고 효율적으로 카드사에 사전분배 하는 방법에 대한 연구가 필요할 것으로 보인다.

References

[1] I. Molloy, J. Li and N. Li, "Dynamic Virtual Credit Card Numbers," Proc. of the Financial Cryptography, LNCS 4886, pp. 208-223, 2007.

[2] Seung-Hyun Seo, "One-Time Virtual Card Number Generation & Transacti on Protocol using Integrated Authen tica-tion Center," Journal of The Korea Institute of Information Security & Cryptology, 20(3), pp. 9-21, June 2010.

[3] Visa International Service Associa -tion. 3-D Secure Protocol Specifica -tion: Core functions version 1.0.2, July 2002.

[4] Visa International Service Associa -tion. 3-D Secure Protocol Specifica -tion: System over-view version 1.0.2, July

2002.
〔5〕 M. Assora and A. Shirvani, "Enhanc -ing the Security and Efficiency of 3-D Secure," ICS'06 Proc. of the 9th international conference on Informa -tion Security, pp. 489-501. 2006.
〔6〕 ISO/IEC 7812-1:2006, "Identification cards -- Identification of issuers -- Part 1:Numbering system," 2006.
〔7〕 M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," CTYPTO'96, LNCS 1109, pp. 1-15, 1996.
〔8〕 Seung-Hyun Seo, Woo-Jin Kang, "Current situation of OTP technique and Example of OTP introduction in Domestic Financial Institutions," Review of KIISC, 17(3), pp. 18-25, June 2007.

〈저자소개〉

박 찬 호 (Chan-ho Park) 학생회원
2013년 8월: 단국대학교 멀티미디어공학과 졸업
2014년 3월~현재: 단국대학교 소프트웨어보안전공 석사과정
〈관심분야〉 정보보호, 네트워크 보안, 금융보안

김 건 우 (Gun-woo Kim) 학생회원
2013년 2월: 단국대학교 컴퓨터과학과 졸업
2013년 3월~현재: 단국대학교 소프트웨어보안전공 석사과정
〈관심분야〉 정보보호, 네트워크 보안, 금융보안

박 창 섭 (Chang-seop Park) 종신회원
1983년 2월: 연세대학교 경제학과 졸업
1987년 2월: Lehigh University 컴퓨터과학과 석사
1990년 2월: Lehigh University 컴퓨터과학과 박사
1990년 3월~현재: 단국대학교 컴퓨터과학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 무선 인터넷 및 모바일 컴퓨팅 보안, 금융보안