Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1175

대면거래환경에서 효율적인 인증을 위한 공개키 기반의 가상카드번호 결제 기법*

박 찬 호,† 박 창 섭‡
단국대학교

Public Key based Virtual Credit Card Number Payment System for Efficient Authentication in Card Present Transaction*

Chan-ho Park,† Chang-seop Park‡
Dankook University

요 약

신용카드사용이 증가하는 만큼 금융사고 또한 증가하고 있다. 자기 띠 카드 방식은 신용카드 정보가 평문으로 노출되고 사용자 인증 또한 허술한 취약점으로 인해 향상된 보안성을 제공하는 스마트카드 방식으로 전환되는 추세에 있다. 또한 최근에는 IT와 금융상품을 접목한 핀테크 (FinTech) 열풍이 불면서 대면거래환경에서도 카드가 아닌 모바일 기기들을 기반으로 하는 결제 기법들이 많이 제안되고 있다. 본 논문에서는 카드 소지자 모바일기기를 기반으로 카드 소지자의 공개키를 이용해 생성하는 가상카드번호를 카드사에 사전 등록함으로써 대면거래환경에서 PKI와 인증서 없이 효율적으로 사용자를 인증하여 편의성을 증가시키면서도 신용카드 정보에 대한 보안성을 제공하는 가상카드번호 결제 기법을 제안하고 대면거래환경에서 보안성을 제공하는 대표적인 신용카드 결제 방식인 EMV 기법과 비교·분석 해 보도록 한다.

ABSTRACT

Financial fraud has been increasing along with credit card usage. Magnetic stripe cards have vulnerabilities in that credit card information is exposed in plaintext and cardholder verification is untrustworthy. So they have been replaced by a smart card scheme to provide enhanced security. Furthermore, the FinTech that combines the IT with Financial product is being prevalent. For that reason, many mobile device based payment schemes have been proposed for card present transaction. In this paper, we propose a virtual credit card number payment scheme based on public key system for efficient authentication in card present transaction. Our proposed scheme is able to authenticate efficiently in card present transaction by pre-registering virtual credit card number based on cardholder's public key without PKI. And we compare and analyze our proposed scheme with EMV.

Keywords: Card Present Transaction, Virtual Credit Card Number, Authentication, EMV, FinTech

I. 서 론

신용카드사용의 증가와 함께 금융사고 또한 지속적으로 증가하고 있다. 기존 MS 카드 (Magnetic Stripe Card) 방식의 신용카드는 자기 띠의 자성을 이용하여 정보를 저장하므로 자기장에 의해 데이

접수일(2015년 8월 11일), 수정일(1차: 2015년 9월 30일, 2차: 2015년 10월 7일), 게재확정일(2015년 10월 7일)
* 본 연구는 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었음.(NRF-2014R1A1A2055074)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2015년도 정보보호 석사과정 지원사업"의 연구결과로 수행되었음.
† 주저자, chpark6737@gmail.com
‡ 교신저자, csp0@dankook.ac.kr(Corresponding author)

터가 변형 또는 삭제 될 수 있고 단말기에 인식할 경우 신용카드 정보가 평문으로 노출되어 탈취, 위·변조 및 복제 등의 방식으로 제3자에 의해 사용될 수 있어 많은 금융사고의 원인이 되었다. 이를 보완하기 위해 IC칩 (Integrated Circuit chip)을 탑재한 스마트카드 방식의 신용카드가 제안되었다. 스마트카드는 프로세서와 메모리, 운영체제 등을 통해 신용카드 정보를 저장함으로써 여러 계좌를 한 카드에 등록하여 사용할 수 있으며 접촉식 및 비 접촉식 결제방식을 제공하고 암호화 등의 기능을 통해 자기 띠 방식의 카드보다 향상된 보안을 제공한다. 본 논문에서는 대면거래 환경에서 카드 소지자의 공개키를 카드사에 등록함으로써 PKI와 같은 제3의 인증기관 없이 효율적으로 거래할 수 있는 가상카드번호 결제 기법을 제안하고 대면거래환경에서 대표적인 스마트카드 결제 표준인 EMV 기법과 비교·분석 해 본다.

II. 관련 연구

2.1 EMV

EMV는 EuroPay, MasterCard, Visa가 제안한 신용카드 결제 규격[1,2,3,4]으로 사실상 전세계적으로 스마트카드를 사용하는 금융거래의 표준으로 사용되고 있다. 규격은 접촉 방식의 스마트카드 표준인 ISO-7816[5]과 비 접촉방식의 스마트카드 표준인 ISO-14443[6]을 기반으로 하고 있으며 EMV를 제안한 3사가 공동 설립한 EMVCo가 규격의 보급, 갱신 및 인증을 담당하고 있다[7]. 현재는 MasterCard, Visa, Discover, American Express, JCB, UnionPay 등이 EMVCo에 속해 있다. 최신 버전은 2011년 11월 발표된 4.3 이다.

2.2 EMV 거래

일반적으로 EMV 거래를 3단계로 분류하는데 카드 인증, 카드 소지자 확인, 거래 승인을 EMV 거래의 3단계라고 한다[8]. Fig.1. 은 대면거래 환경에서의 EMV 기법의 거래 흐름을 나타내고 있으며 본 장에서는 이를 단계별로 상세하게 설명하고자 한다.

2.2.1 카드 인증 (Card Authentication)

카드 인증은 EMV 단말기가 카드로부터 데이터를 읽고 검증함으로써 카드가 복제 또는 위·변조 되지 않았는지 확인하는 단계이다. 인증 방식은 SDA

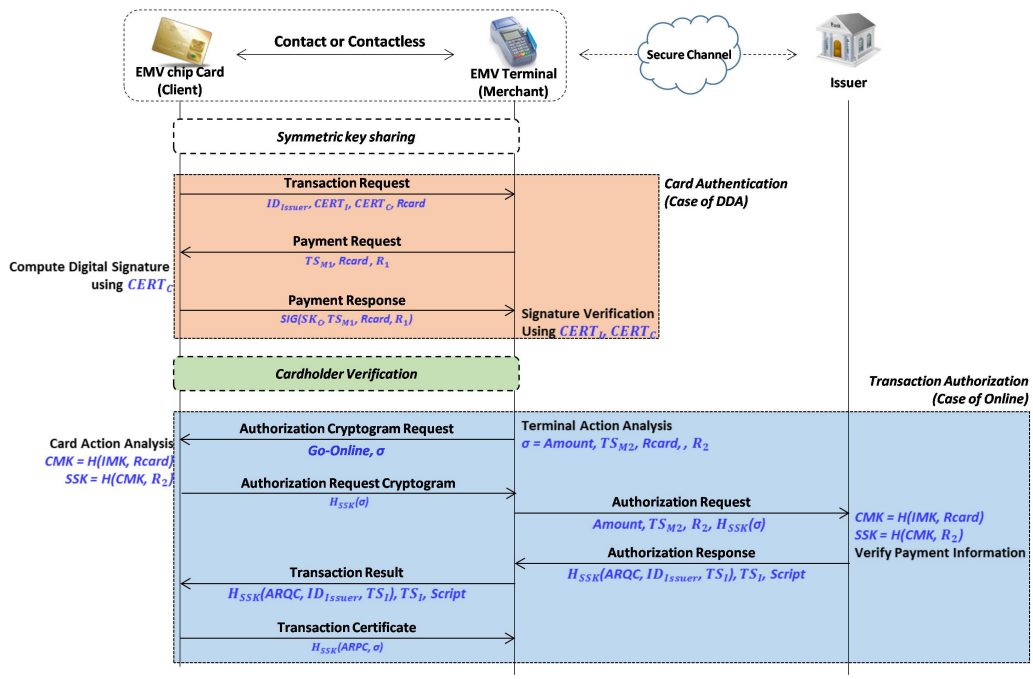

Fig. 1. EMV Transaction flow

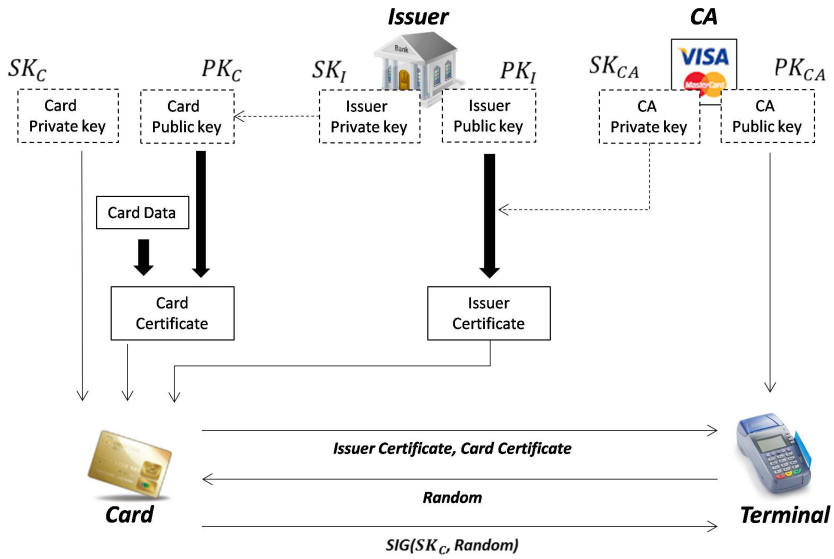

Fig. 2. Dynamic Data Authentication

(Static Data Authentication), DDA (Dynamic Data Authentication), CDA (Combined DDA) 등 세 가지 방식을 제공하는데 Fig.1.과 Fig.2.는 DDA 방식을 나타내고 있다. EMV는 Visa, MasterCard와 같은 카드사들이 최상위 인증기관(CA)이 되는 PKI (Public Key Infrastructure) 구조를 가지고 있다. 또한 Fig.2.와 같이 EMV 표준 인증을 받은 단말기(Terminal)는 최상위 인증기관의 공개키(PK_{CA})를 탑재하고 있고 DDA를 지원하는 카드(Card)는 카드 자체의 서명용 개인키(SK_C)와 카드사(Issuer)로부터 발급된 공개키 인증서 (Card Certificate)를 가지고 있다. 카드는 카드 공개키 인증서, 카드사 공개키 인증서(Issuer Certificate)를 단말기에 보내고 단말기는 난수(Random)를 challenge값으로 보낸다. 카드는 난수에 대한 서명 값($SIG(SK_C, Random)$)을 돌려주고 단말기는 앞서 카드로부터 받은 인증서와 탑재되어 있는 인증기관의 공개키를 통해 서명을 검증함으로써 카드 데이터의 위·변조 여부를 확인할 수 있다.

2.2.2 카드 소지자 확인 (Cardholder Verification)

카드 소지자 확인은 신용카드를 사용해서 거래를 시도하는 사람이 카드를 발급받은 정당한 사용자가 맞는지 확인하는 과정이다. EMV에서는 전통적인 서명(Signature) 방식을 비롯해 오프라인으로 카드와 단말기의 통신만을 통해 확인하는 Offline plaintext PIN, Offline enciphered PIN과 온라인으로 카드사를 통해 확인하는 Online PIN 등 다양한 카드 사용자 확인 방식 (Cardholder Verification Methods, CVMs)을 제공한다. 이러한 CVMs는 거래금액 등 여러 옵션에 따라 적용될 수 있으며 최근에는 일정금액 이하의 소액결제의 경우 카드 사용자 확인을 하지 않는 No CVMs방식도 제공되고 있다.

2.2.3 거래 승인 (Transaction Authorization)

거래 승인은 거래 금액에 대해 결제할 수 있는 카드인지 카드사로부터 승인을 받는 과정으로 EMV에서는 오프라인 승인과 온라인 승인의 두 가지 방식을 제공한다. 오프라인 승인은 통신비용을 절감할 수 있으나 도난·분실여부, 한도액 등 카드 외적인 요인에 대한 위험성이 있을 수 있고 온라인 승인은 통신비용의 증가와 카드사 시스템 부하 등의 문제가 있을 수 있다. 따라서 EMV에서는 Terminal Risk Management, Terminal Action Analysis, Card Action Analysis와 같은 과정을 통해 오프라인 또는 온라인 승인 방식을 사용하도록 결정한다. Terminal Action Analysis에서는 일정 기준 이

상의 금액일 경우 온라인으로 거래하게 하는 Floor Limit Checking과 단말기 내에 설정된 비율에 따라 무작위로 온라인으로 거래하게 하는 Random Selection 그리고 연속 거래 횟수, 누적 금액을 설정하고 설정된 금액을 초과할 경우 온라인으로 거래하게 하는 Velocity Checking 등의 과정을 거친다. 이 결과를 통해 Terminal Action Analysis에서는 단말기가 먼저 오프라인 또는 온라인 승인 방식을 선택하여 카드에게 요청한다. 카드는 단말기의 요청을 다시 검토하고 Card Action Analysis를 통해 최종적으로 승인 방식을 결정하게 되는데 온라인 승인 방식으로 결정했을 경우 사전에 카드사로부터 분배받은 카드 마스터 키(Card Master Key, CMK)와 단말기가 생성한 난수에 해시함수를 적용하여 세션키를 생성하고 이 세션키를 통해 거래정보의 MAC 값 (Message Authentication Code value)인 ARQC(Authorization ReQuest Cryptogram)를 계산한다. 카드는 ARQC를 단말기에 보내고 단말기는 이를 카드사에 전달한다. 카드사는 카드와 동일한 과정을 거쳐 세션키를 생성하고 ARQC를 검증한 뒤 그에 대한 답변으로 다시 MAC 함수를 통해 ARPC (Authorization ResPonse Cryptogram)를 생성하여 단말기를 통해 카드에게 보낸다. 이때, 도난신고 된 카드를 잠금처리 하거나 잠금을 해제하는 등 카드에서 처리해야 할 작업이 있을 경우 그에 대한 스크립트를 포함하여 보냄으로써 카드에 대한 제어를 할 수 있다. 카드는 ARPC 값을 검증한 뒤 성공했을 경우 TC를 실패했을 경우 AAC를 단말기에 전송하며 거래를 마친다.

2.3 EMV 취약점 관련 연구

MS카드 방식의 취약한 보안성으로 인해 EMV방식을 채택하여 사용하는 카드사 및 은행들이 늘어나면서 그에 대한 연구들도 많이 진행되었다. 본 장에서는 EMV를 이용한 거래에서 발견된 취약점 및 그에 대한 기존의 연구들에 대해 설명한다.

2.3.1 No-PIN attack

No-PIN attack은 카드 소지자 확인 과정에서 발생할 수 있는 취약점으로 카드와 단말기 사이에 악의적인 장치를 배치하여 수행하는 중간자 공격(man in the middle attack)방식의 취약점이다[9]. PIN을 모르는 카드를 획득한 공격자는 단말기와 카드 사이에 악의적 중간자 장치를 배치시킨다. 카드를 인식시킨 뒤, Offline-PIN 인증 요청을 받으면 임의의 PIN을 입력한다. 그리고 악의적인 중간자 장치는 단말기에는 PIN 인증이 성공했다는 메시지를, 카드에는 단말기가 PIN 인증 방식의 CVMs를 지원하지 않아 카드 소지자 확인을 생략 또는 Signature 방식으로 대체하여 수행했다고 알린다. 이렇게 되면 결과적으로 공격자는 카드에 대한 PIN을 알지 못하더라도 거래에 성공할 수 있게 된다.

2.3.2 Yes-card attack

Yes-card attack은 EMV거래 중 카드 인증 단계에서 SDA 방식의 취약점[10]을 이용하는 공격이다[11]. SDA 방식의 카드에 저장되어 있는 정적 인증 값(카드정보에 대한 카드사의 서명값)을 획득한 공격자는 임의의 다른 IC카드에 이 정보를 복사하여 복제카드를 만들 수 있다. 이때, 복제카드의 칩에 어떠한 PIN을 입력하더라도 인증에 성공하도록 프로그래밍 할 수 있다. 하지만 온라인 방식의 EMV 거래에서는 Yes-card attack이 성공할 수 없으며 오프라인 방식에서도 이를 방지하기 위해 DDA와 같은 동적 인증 방식이 제안되어 사용되고 있다.

2.3.3 Pre-play attack

Mike Bond 등은 [12]에서 EMV 거래의 취약점 중 하나인 pre-play attack에 대해 소개하였다. EMV의 거래 과정 중 카드 인증 과정에서 단말기가 카드에게 challenge 값을 보내는데 이 값을 생성할 때 암호학적으로 안전한 난수가 아닌 간단한 counter 값 등을 사용하기 때문에 challenge 값을 예측 가능하게 된다. 또한 단말기의 식별정보(identity)가 아닌 국가코드(country code)만을 포함하여 인증코드를 생성한다. 그에 따라 공격자는 이후의 거래에서 사용될 인증코드를 위조하여 거래할 수 있게 된다.

2.3.4 Relay attack

Relay attack은 카드 사용자가 자신의 카드가 어떤 단말기와 통신하고 있는지 알지 못하는 것을 이용한 공격이다[11]. 공격자(악의적인 판매자)는 카

드 사용자에게 가짜 단말기의 거래금액을 보여주고 카드를 넣도록 유도한다. 그리고 가짜 단말기는 다른 제3의 단말기와 통신을 통해 거래한다. 또한 공격자는 제3의 단말기에 원하는 거래금액을 입력할 수 있다. 예를 들어, 카드 소지자가 주차장에 설치된 가짜 단말기에서 거래금액 2만원을 확인하고 카드를 통해 결제를 시도하면 가짜 단말기는 전혀 다른 도시에 있는 제3의 단말기로 카드정보를 전송할 수 있다. 그리고 공격자는 제3의 단말기에 200만원을 입력하면 카드 소지자는 2만원을 결제했다고 생각하지만 실제로는 200만원의 피해를 입게 된다.

2.3.5 Misreporting by terminal

Steven J. Murdoch 등은 [13] 에서 Misreporting by terminal 이라는 취약점에 대해 소개하였다. 카드사 거래 기록에는 PIN 인증을 이용한 거래라고 기록되어 있는 반면에 영수증에는 Signature 인증 방식을 사용했다고 하는 거래기록들이 발견되었다. 이렇게 불일치되는 기록들이 발생하는 이유는 PIN인증 방식의 수수료가 더 저렴하고 결제 취소가 발생할 확률이 낮기 때문이다. 따라서 판매자들은 이러한 이점들을 위해 터미널을 통해 거래 기록을 조작하고 그로 인해 카드에 의한 거래정보(card reported value)와 단말기에 의한 거래정보(terminal reported value)에 차이가 나타나게 되는 취약점이다.

III. 제안 기법

본 장에서는 사용자 기기를 기반으로 대면거래 환경에서 결제할 수 있는 가상카드번호 기법을 제안한다. 제안 기법에서 사용하는 표기법은 Table 1. 과 같다.

3.1 제안 기법 등록

카드 소지자 (Client)는 스마트 폰과 같이 NFC (Near Field Communication)를 사용할 수 있는 스마트 기기에 신용카드결제 앱을 설치하고 SMS 인증 등 다른 인증수단을 통해 본인의 기기임을 인증한다. 그리고 카드 소지자의 공개키/개인키 키 쌍 (PK_C, SK_C)을 생성하고 공개키를 통해 수식(1)과 같은 방식으로 가상카드번호($Vcard$)를 계산하고 안전한 채널을 통해 카드사에 보낸다.

Table 1. Notations

Client	Cardholder (User device)
Merchant	Store (POS Terminal)
Issuer	Credit card issuer
ID_C	Cardholder information (name, billing address)
ID_I	IIN (Issuer Identifier Number)
$Rcard$	Real credit card numbers
$Vcard$	Virtual credit card numbers
$Amount$	Transaction amount
K	Symmetric Key
MK	Master Key
RK	Random Key generated by *Merchant*
$H(.)$	Cryptographic hash function
$H_K(.)$	Keyed MAC function
TS_X	Time stamp generated by X
PK_X, SK_X	Public and Private Keys of X
$SIG(SK_X, \sigma)$	Signature of transaction information σ using SK_X
$E(K, ...)$	Symmetric Key Encryption with K
$[...]_{PK_X}$	Asymmetric Key Encryption with Public Key of X

$$Vcard = ID_I \| H(PK_C \| ID_C \| ID_I) \quad (1)$$

카드사는 중복되는 값이 없는지 검사한 뒤 유일한 가상카드번호임이 확인되면 데이터베이스에 등록한다. 그리고 카드사 마스터 키 (Issuer Master Key, IMK)와 실제카드번호에 해시함수를 적용하여 카드 마스터 키 (Card Master Key, CMK)를 계산하고 사용자 기기에게 전송한다. 사용자 기기는 카드 마스터 키를 저장한다. 그리고 카드 소지자로부터 비밀번호를 입력받아 비밀번호의 해시 값을 키 암호화 키 (Key Encryption Key, KEK)로 사용하여 카드 소지자의 개인키(SK_C)를 암호화 하고 저장한다. 이때, 사용자 기기에 저장되는 정보들은 안전한 저장소인 SE (Secure Element)에 저장한다고 가정한다. 이렇게 등록을 하게 되면 가상카드번호를 사용하여 결제를 시도했을 때, 일치하는 가상카드번호가 존재하는 경우 판매자는 해당 카드사를 통해 사용자 공개키의 유효성을 확인하고 이를 통해 PKI와 인증서를 사용하지 않고 신용카드정보의 유효성과 결제를 시도하는 사람이 정당한 카드 소지자임을 인증할 수 있다.

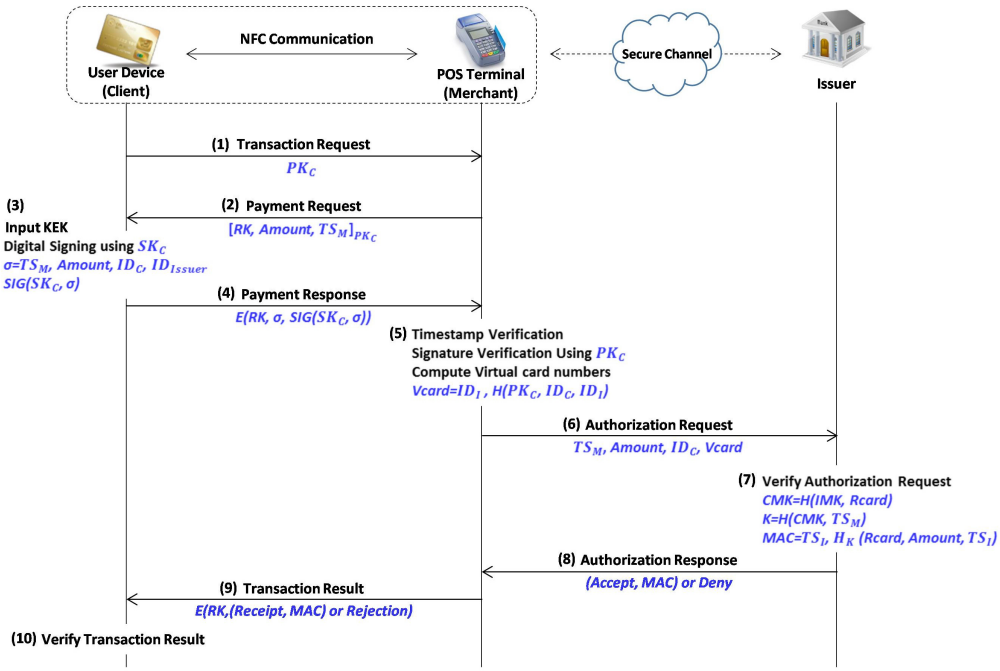

Fig. 3. Proposed scheme Transaction flow

3.2 제안 기법 거래

본 장에서는 대면거래환경에서 제안 기법을 통해 PKI 없이 등록한 가상카드번호를 이용하여 거래하는 방식에 대해 설명한다. 대면거래환경에서는 카드 소지자(Client)가 상점에서 구매할 상품 혹은 서비스를 선택하여 판매자(Merchant)에게 제시한다. 판매자는 POS 단말기(Point Of Sales Terminal)에 가격을 입력하고 결제를 요청하면 거래를 하기 위한 준비가 끝난다. 제안 기법의 거래 흐름은 Fig.3.와 같으며 사용자 기기(User Device)와 단말기(Terminal)는 NFC 통신을 하고 단말기와 카드사(Issuer)는 안전한 채널(Secure Channel)을 통해 통신하며 사용자 기기에 저장된 정보들은 보안 저장소인 SE에 저장되어 안전하다고 가정한다.

(1) 카드 소지자는 단말기 화면을 통해 거래금액(Amount)을 확인하고 결제를 하기 위해 미리 등록한 사용자 기기에서 결제 앱을 실행시킨 뒤 단말기에 인식시킨다. 그러면 NFC 통신을 통해 사용자 기기의 SE에 저장되어있던 카드 소지자 공개키(PK_C)가 단말기에 전송된다.

(2) 단말기는 임의의 대칭키 RK와 거래요청 시점의 판매자 타임스탬프(TS_M)를 생성한다. 그리고 거래금액과 함께 사용자 기기로부터 전달받은 카드 소지자 공개키로 암호화하여 사용자 기기에 보내 결제 요청을 한다.

(3) 사용자 기기는 KEK 인증을 요청하고 카드 소지자는 등록 시 설정한 비밀번호를 입력한다. 올바른 비밀번호를 입력하면 인증에 성공하고 KEK를 통해 암호화된 상태로 저장되어 있던 카드 소지자 개인키(SK_C)를 획득한다. 그리고 단말기로부터 받은 메시지를 복호화하여 임의의 대칭키 RK와 판매자의 타임스탬프(TS_M), 거래금액 등의 정보를 획득한다. 그리고 타임스탬프, 거래금액, 카드 소지자 정보(ID_C), 카드사 식별자(ID_I)를 모아 거래정보(σ)를 생성한다. 그리고 거래정보와 카드 소지자 개인키를 이용해 거래정보의 서명값($SIG(SK_C, \sigma)$)을 계산한다.

(4) 거래정보와 그에 대한 서명값을 RK를 통해 암호화하여 단말기에 전송한다.

(5) 단말기는 받은 메시지를 RK로 복호화 하고 거래정보와 서명값을 획득한다. 그리고 거래정보에 포함되어 있는 타임스탬프와 자신이 생성했던 값을 비교하여 메시지가 재사용된 값이 아님을 검증한다. 거래의 신규성이 확인되면 이전에 받았던 카드 소지

자의 공개키를 이용해 서명값을 검증한다. 이 과정에서 타임스탬프 또는 서명값의 검증에 실패하면 바로 사용자 기기에 거래 실패를 통보하며 거래를 마친다. 또한 타임스탬프와 서명값의 검증에 성공했다 하더라도 PKI를 기반으로한 공개키 인증서가 아닌 단순한 공개키를 통해 검증을 수행했으므로 공개키의 유효성이 입증되지 않은 상태이기 때문에 완전한 인증이 이루어졌다고 할 수 없다. 단말기는 거래정보와 카드 소지자 공개키를 통해 수식(1)과 같은 방식으로 가상카드번호($Vcard$)를 계산한다.

(6) 단말기는 타임스탬프와 거래금액, 카드 소지자 정보 그리고 가상카드번호를 카드사에 보내 거래 승인을 요청한다.

(7) 카드사는 카드 소지자 정보(ID_C)를 통해 등록된 가상카드번호를 검색하고 받은 값과 비교·검증한다. 그리고 그 결과에 따라 판매자 단말기에 승인 응답 메시지를 보낸다. 실패 했을 경우 승인 거부 메시지를 보내고 성공했을 경우에는 거래가 정상적으로 승인되었음을 확인할 수 있는 MAC 값을 생성하는 과정을 진행한다. 카드사는 먼저 카드사 마스터키(IMK)와 실제카드번호($Rcard$)에 해시함수를 적용하여 카드 마스터키(CMK)를 계산하고 카드 마스터키와 판매자의 타임스탬프에 해시함수를 적용하여 MAC 함수에 사용할 세션키(K)를 생성한다. 그리고 거래승인 시점의 카드사 타임스탬프(TS_I)를 생성하고 '무슨카드'로 '얼마'를 '언제' 결제했는지 확인시켜주기 위해 실제카드번호, 거래금액, 카드사 타임스탬프와 세션키를 이용하여 수식(2) 와 같은 방식으로 MAC 값을 계산한다.

$$MAC = TS_I \| H_K(Rcard \| Amount \| TS_I) \qquad (2)$$

(8) 카드사는 판매자 단말기에게 MAC 값, 카드사 타임스탬프를 포함한 거래 승인 메시지 또는 거래 승인 거부 메시지를 보낸다.

(9) 판매자는 카드사로부터 받은 메시지를 확인하고 그에 따라 카드 소지자에게 거래 성공 또는 실패 메시지를 보낸다. 거래 승인 메시지를 받았을 경우 판매자는 가상카드번호가 등록되어 있는 값임을 확인한다. 그리고 자신이 카드 소지자로부터 받아 서명값 검증 및 가상카드번호 생성에 사용한 공개키가 카드 소지자가 가상카드번호를 등록할 때 사용했던 정당한 공개키임을 알게 된다. 따라서 이 시점에서 완벽한 인증이 이루어졌다고 할 수 있으며 결과적으로 PKI 없이 효율적으로 인증을 수행하였다. 그리고 MAC 값을 포함한 거래성공 메시지를 RK를 통해 암호화하여 사용자 기기에 전송한다. 거래 승인 거부 메시지를 받았을 경우 거래 실패 메시지를 RK로 암호화하여 보내 거래 실패를 알린다.

(10) 카드 소지자는 판매자로부터 받은 거래 결과 메시지를 RK로 복호화 하여 확인한다. 거래 실패 메시지를 받았을 경우 그대로 거래를 종료한다. 거래 성공 메시지를 받았을 경우 가상카드번호 등록 시 계산하여 저장했던 카드 마스터키와 판매자의 타임스탬프를 이용해 세션키를 생성하고 거래 성공 메시지에 포함된 카드사 타임스탬프와 자신의 카드정보, 거래정보를 이용하여 카드사와 동일하게 수식(2)와 같은 방식으로 MAC 값을 계산한다. 그리고 거래 성공 메시지에 포함된 MAC 값과 비교하여 거래과정에서 중간에 거래 정보에 대한 위변조 없이 정상적으로 승인되었음을 확인하고 거래를 종료한다.

IV. 비교·분석

4.1 초기 정보

EMV 기법은 카드사와 카드가 실제카드번호, 유효기간, PIN, 카드 마스터 키 등을 사전분배하여 가지고 있다. 또한 카드는 카드의 공개키, 개인키 키 쌍을 가지고 있으며 오프라인 거래 승인(Offline Authorization)을 위해 카드정보를 카드의 개인키로 서명한 값을 가지고 있다. 그리고 사용자의 공개키 인증서와 카드사 공개키 인증서를 가지고 있으며 POS 단말기가 CA 공개키를 탑재하고 있어 거래 시 오프라인 서명검증만으로도 카드정보의 신뢰성을 확인하여 거래를 승인할 수 있다.

제안 기법의 경우 기본적으로 카드사와 카드 소지자가 사용자 정보, 실제카드번호, 유효기간, PIN 등을 분배하고 있으며 카드 소지자가 가상카드번호 서비스를 등록할 때 공개키, 개인키 키 쌍을 생성하여 보관하게 된다. 그리고 카드사로부터 카드 마스터키를 받아 저장한다. 카드사는 사용자 및 카드정보 외에 카드 소지자가 공개키를 기반으로 생성하여 등록 신청한 가상카드번호를 추가적으로 저장·관리 하게 된다. POS 단말기의 경우 사전 분배받는 정보는 없으며 타임스탬프 생성, 대칭키 또는 비대칭키를 이용한 암·복호화 및 해시함수 연산 능력이 필요하다.

Table 2. Comparison of EMV and Proposed scheme

		EMV	Our proposed scheme
Initialized information	Client	Signed card information, Card private key, Card public key certificate, Issuer public key certificate, Card master key	Card information, Cardholder information, Key pair, Card master key
	Merchant	Item Information, CA public key	Item Information
	Issuer	Card information, Cardholder information Issuer master key	Card information, Cardholder information, Issuer master Key, Virtual card numbers
Card Authentication		PKI based Sign verification	Sign & Vcard verification
Cardholder Verification		No CVM, Signature, Offline-PIN, Online-PIN	Key Encryption Key of cardholder's private key
Transaction Authorization		ARQC & ARPC verification	Sign & Vcard verification

4.2 카드 인증

기존의 마그네틱 방식의 카드의 경우 무조건 신용카드 정보를 카드사에 보내 검증받는 방식을 사용하였으며 복제 또는 위조된 카드의 경우에도 똑같이 사용할 수 있는 문제점이 있었다. EMV 기법에서는 이러한 마그네틱 방식의 비효율성을 개선하기 위해 거래금액 등 여러 조건에 따라 오프라인 거래 승인 또는 온라인 거래 승인을 정하게 된다. 오프라인 방식의 경우 최근에는 전자서명 생성 및 검증을 할 수 있는 성능의 카드와 단말기가 보급되면서 DDA 또는 CDA 방식을 사용하고 있다. EMV 카드가 카드 공개키 인증서와 카드사 공개키 인증서를 단말기로 전송하면 단말기는 카드에게 난수를 challenge 값으로 보낸다. 카드는 결제정보 및 난수에 대한 전자서명을 계산하여 단말기에 보내고 단말기는 카드 공개키 인증서를 통해 단말기의 서명 값을 검증한다. 그리고 카드 공개키에 대한 유효성은 카드사 공개키 인증서를 통해 검증하고 카드사 공개키에 대한 유효성은 단말기에 사전 탑재된 CA 공개키를 통해 검증함으로써 온라인 연결 없이도 신용카드 정보에 대한 유효성을 확인함으로써 오프라인 상태로 거래를 승인할 수 있다. 또한 데이터가 변경되지 않았다는 사실도 확인할 수 있어 마그네틱 방식의 취약점이었던 위·변조 및 복제된 카드의 여부도 확인할 수 있다는 장점이 있다.

제안 기법에서는 실제카드번호를 주고받으며 인증받는 대신 사전 등록한 가상카드번호를 통해 사용자-카드정보-키 쌍의 연관성을 카드사로부터 검증 받음으로써 신용카드 정보의 유효성 및 무결성을 검증받게 된다. 카드 소지자는 거래에 대한 서명을 생성하고 판매자는 공개키를 사용하여 서명에 대한 검증을 한다. 그리고 가상카드번호의 등록여부를 카드사로부터 검증 받아 거래의 전자서명 검증에 사용한 공개키의 유효성을 간접적으로 확인하여 사용자 및 카드정보에 대한 유효성을 확인한다. 또한 거래정보에 타임스탬프가 추가되어 있기 때문에 재사용되지 않은 결제정보라는 것 또한 확인할 수 있다. 제안 기법은 이렇게 EMV가 Visa, MasterCard 등을 Root CA로 하는 PKI를 기반으로 전자서명 검증을 제공하여 신용카드 데이터를 인증하는 것과 달리 사전 등록한 가상카드번호를 통해 사용자 공개키의 유효성을 확인시켜 줌으로써 제3의 인증기관 없이 효율적으로 카드 소지자 인증을 제공한다고 할 수 있다.

4.3 카드 소지자 확인

EMV 기법에서는 거래금액, 카드와 단말기의 성능 등에 따라 여러 가지 카드 소지자 확인 방식(CVMs)을 제공한다. 일정금액 이하는 본인확인을 생략하는 No CVM 방식을 비롯해 서명, 오프라인 PIN, 온라인 PIN 등 많은 방식을 선택적으로 제공하고 있다.

제안 방식에서는 카드 소지자가 가상카드번호 서비스 등록을 하는 과정에서 개인키를 사용자 기기에 암호화하여 저장하기 위해 설정하는 키 암호화 키(KEK)를 통해 사용자를 인증한다. EMV 기법과 비교했을 때 오프라인 PIN 방식과 유사하다고 볼 수 있다.

4.4 거래 승인

EMV 기법에서는 오프라인 또는 온라인 방식으로 거래 승인을 하게 된다. 오프라인 거래 승인 방식의 옵션을 만든 이유는 매번 네트워크를 통해 검증받는 비용을 줄이기 위함이다. 일반적으로 거래금액이 기준보다 낮을 경우 오프라인 방식으로 진행하게 되지만 Terminal Risk Management, Terminal Action Analysis, Card Action Analysis 등의 과정을 거쳐 최종적으로 오프라인 또는 온라인 판정을 받게 된다. 오프라인의 경우 4.2절에서 설명했던 DDA 또는 CDA 방식을 통해 거래를 승인하게 된다. 온라인의 경우 1차적으로 오프라인 방식의 검증을 한 뒤, 검증에 성공하면 2차적으로 온라인 방식을 진행하게 된다. EMV카드는 사전 탑재된 카드 마스터 키와 임의의 난수에 해시함수를 적용하여 세션키를 생성한다. 이렇게 생성한 세션키를 이용하여 거래정보값에 MAC 함수를 적용하여 ARQC를 생성하고 단말기를 통해 카드사에 보내 거래 승인을 요청한다. 카드사는 EMV 카드와 같은 과정을 거쳐 세션키를 생성하고 MAC 값을 생성하여 비교 검증한다. 그에 따라 결과를 전송하는데 거래 승인일 경우, 세션키를 사용하여 ARQC, 카드사 식별자, 승인시간정보에 MAC 함수를 적용하여 ARPC 값을 계산하여 보내게 된다. 이를 받은 카드 역시 카드사와 같은 과정을 통해 ARPC를 생성하여 비교 검증하고 단말기에 TC를 전송하면 정상적으로 거래를 마치게 된다.

제안 기법에서는 온라인 거래 승인 방식만을 제공한다. 카드 소지자 기기는 단말기로부터 받은 거래정보와 거래요청시간정보 값에 대한 서명 값을 생성하여 보내고 단말기는 카드 소지자 공개키로 서명을 검증한다. 검증이 성공했다 하더라도 공개키에 대한 유효성이 확인되지 않아 완전한 카드정보 검증 및 거래 승인이 이루어지지 않았다. 따라서 판매자 단말기는 카드 소지자 공개키와 정보, 카드사 식별자에 해시함수를 적용하고 앞에 카드사 식별자를 붙여 가상카드번호를 생성한다. 그리고 해당 카드사에 가상카드번호 검증을 요청한다. 카드사는 가상카드번호의 등록여부를 통해 거래 승인 또는 거부 메시지를 카드사에 보내게 되고 카드사는 승인 메시지를 받은 시점에서 공개키에 대한 유효성을 확인하게 되므로 이 때, 완전한 거래 승인이 이루어 졌다고 할 수 있다. 또한 카드사는 거래를 승인하는 경우 카드사 마스터키와 실제카드번호에 해시함수를 적용하여 카드 마스터키를 계산하고 다시 거래요청시간정보와 함께 해시함수를 적용하여 세션키를 획득한다. 그리고 세션키를 이용하여 실제카드번호, 거래금액, 거래승인시간정보에 MAC 함수를 적용하여 거래승인 확인 값을 생성하여 판매자 단말기를 통해 카드 소지자 기기에 전송한다. 카드 소지자는 카드사와 같은 과정을 통해 MAC 값을 생성하고 거래승인 확인 값과 비교함으로써 거래 중간에 오류 또는 악의적 공격에 대한 피해 없이 정상적으로 거래를 마쳤음을 알 수 있다.

4.5 제안하는 가상카드번호 안전성 분석

본 논문에서 제안하는 가상카드번호를 이용한 카드 소지자 인증의 안전성은 카드사 데이터베이스에 등록되어 있는 가상카드번호들에 대한 위조 불가능성에 기반을 두고 있다. 등록된 가상카드번호를 위조한다는 것은 공격자가 $H(PK_C \| ID_C \| ID_I)$가 포함된 가상카드번호를 공격의 대상으로 할 때, $PK_C' \neq PK_C$ 이면서 $H(PK_C' \| ID_C \| ID_I) = H(PK_C \| ID_C \| ID_I)$를 만족하는 키 쌍 (PK_C', SK_C')을 찾는다는 것을 의미한다. 만약 위조에 성공하면, 공격자는 해당 카드 소지자로 위장할 수 있다. 위 공격의 성공 가능성은 가상카드번호의 길이와 관련이 있다. 만약 다항식 l과 보안 매개변수 n 대해 $|H(.)| = l(n)$ 이면, 공격자는 공격대상의 가상카드번호를 생성할 수 있는 공개키를 찾기 위해서 거의 $2^{l(n)}$ 번의 계산을 수행해야 한다. 누구든지 임의의 키 쌍으로부터 임의의 가상카드번호를 생성할 수 있다. 그러나 카드사에 사전 등록되어있지 않으면 사용할 수 없다. *Formal proof*을 위해 해시함수를 다시 정의한다. 즉, Gen_H이 보안매개변수 1^n을 입력 값으로 하고 키 s를 출력하는 probabilistic algorithm이라고 할 때, 해시 함수는 PPT (probabilistic polynomial-time) 알고리즘$\Pi = (Gen_H, H^S)$로 정의된다. 그리고 $H^S: \{0,1\}^* \rightarrow \{0,1\}^{l(n)}$는 알려진 키 s를 사용하는 해시함수이다. 다음 Experiment는 Π, 공격자A 그리고 보안매개변수 n에 대해서 정의된다.

제2 역상 찾기 Experiment $2PR_{\Pi,A}(n)$

- $s \leftarrow Gen_H(1^n)$.
- 공격자 A는 (s,x)을 입력받고, x'를 출력한다. 이때, $x, x' \in \{0,1\}^*$
- $2PR_{\Pi,A}(n)=1$ if and only if $x \neq x'$ and $H^S(x)=H^S(x')$.

정의1

만약 모든 PPT 공격자들 A에 대해서 $\Pr[2PR_{\Pi,A}(n)=1] \leq negl(n)$의 조건을 만족하는 negligible function, $negl(.)$이 존재한다면, 해시함수 $\Pi=(Gen_H, H^S)$는 제2 역상 저항성을 만족한다.

정리1

만약 $\Pi=(Gen_H, H^S)$가 제2 역상 저항성을 만족하는 해시 함수라면, 수식 (1) 은 위조 공격에 대해 안전하다.

증명

Π'가 수식 (1)을 나타내고 B는 특정 카드 소지자 ID_C의 가상카드번호를 위조하기 위해 Π'를 공격하는 PPT 공격자라고 하자. 그러면 다음의 Experiment를 정의할 수 있다.

가상카드번호 위조 Experiment $Vforge_{\Pi',B}(n)$

- 공격자 B는 (s, PK_C, ID_C, ID_I)을 입력받고, PK_C를 출력한다.
- $Vforge_{\Pi',B}(n)=1$ if and only if $PK_C' \neq PK_C$ and $H^S(PK_C' \| ID_C \| ID_I) = H^S(PK_C \| ID_C \| ID_I)$

공격자 B를 서브루틴으로 사용하여 $2PR_{\Pi,A}(n)$의 Π를 공격하는 다음의 공격자 A를 고려해보자.

공격자 A:

- (s,x)을 입력받는다. $(x = PK_C \| ID_C \| ID_I.)$
- $z := x$.
- $B(s,z)$를 실행. B는 $z' = PK_C' \| ID_C \| ID_I$를 리턴. $(PK_C' \neq PK_C)$
- $x' := z'$.
- A는 x'을 출력.

$\Pr[2PR_{\Pi,A}(n)=1] \geq \Pr[Vforge_{\Pi',B}(n)]$은 자명하다. 또한, $H^S(.)$가 제2 역상 저항성을 만족하기 때문에 $\Pr[2PR_{\Pi,A}(n)=1] \leq negl(n)$이 만족된다. 따라서, 위의 Experiment, 정리, 정의의 결과로 $\Pr[Vforge_{\Pi',B}(n)] \leq \Pr[2PR_{\Pi,A}(n)=1] \leq negl(n)$. 즉, 수식 (1)은 위조 공격에 대해 안전하다. □

V. 결 론

스마트폰의 보급과 핀테크 열풍으로 인해 모바일 스마트 결제의 비중이 나날이 높아져가고 있다. 그에 따라 편의성만큼이나 보안성도 향상되어야 할 필요성이 있다. 이에 따라 최근에는 신용카드 정보의 유출을 방지하기 위해 대체할 수 있는 값을 생성하여 사용하는 기법들이 많이 제안되고 있다. 특히 토큰화는 EMV, PCI-DSS 등에서 규격[14,15]을 제안하고 있으며 애플페이, 삼성페이를 비롯한 여러 서비스에 직접 구현되어 사용되는 등 많은 연구가 진행 중이다. 본 논문에서는 이러한 신용카드 대체기법 중 스마트기기를 기반으로 대면거래 환경에서 PKI와 인증서 없이 효율적으로 인증할 수 있는 가상카드번호 결제 기법을 제안하였다. 그리고 대면거래환경에서 표준으로 자리 잡고 있는 EMV 기법과 함께 어떠한 방식으로 보안을 제공하는지 비교·분석해 보았다. 향후에는 제안기법에 대한 구현 및 테스트를 통해 단점을 보완하고 신용카드 결제 서비스에서 필수로 자리 잡고 있는 토큰화를 접목시키는 방향의 연구가 필요할 것으로 보인다.

References

[1] EMV Spec. V4.3 Book1, Application Independence for ICC to Terminal Interface Requirements, Nov. 2011.

[2] EMV Spec. V4.3 Book2, Security and Key Management, Nov. 2011.

[3] EMV Spec. V4.3 Book3, Application Specification, Nov. 2011.

[4] EMV Spec. V4.3 Book4, Cardholder, Attendant, and Acquirer Interface Requirements, Nov. 2011.

[5] ISO 7816, Identification Cards - Integrated Circuit(s) Cards with

Contacts Part 1-15.
〔6〕 ISO 14443, Identification Cards - Contactless Integrated Circuit Cards - Proximity Cards Part 1-4.
〔7〕 Hak-Beom Kim, "Financial IC Card Security and EMV Certification," Review of KIISC, 16(5), p. 84-93, Oct. 2006.
〔8〕 Els Van Herreweghen, Uta Wille, "Using EMV Smartcards for Internet Payments," Proceedings of the 8th ECIS, p. 901-908, Jul. 2000.
〔9〕 Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond, "Chip and PIN is Broken," Proceedings of the IEEE Symposium on Security and Privacy, p. 433-446, May. 2010.
〔10〕 Ross Anderson, Mike Bond and Steven J. Murdoch, "Chip and Spin," Computer Security Journal, vol. 22, no. 2, p. 1-6, Mar. 2006.
〔11〕 Ross Anderson and Steven J. Murdoch, "EMV:Why Payment System Fail," Communications of the ACM, vol. 57, no. 6, p. 24-28, Jun. 2014.
〔12〕 Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov and Ross Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack," Proceedings of the 2014 IEEE Symposium on Security and Privacy, p. 49-64, May. 2014.
〔13〕 Steven J. Murdoch, Ross Anderson, "Security Protocols and Evidence: Where Many Payment Systems Fail," Proceedings of the 18th International Conference on Financial Cryptography and Data Security, p. 21-32, Mar. 2014.
〔14〕 EMV Spec. V1.0, EMV Payment Tokenisation Specification - Technical Framework, Mar. 2014.
〔15〕 PCI Data Security Standard V2.0, Information Supplement:PCI DSS Tokenization Guidelines, Aug. 2011.

〈저자소개〉

박 찬 호 (Chan-ho Park) 학생회원
2013년 8월: 단국대학교 멀티미디어공학과 졸업
2014년 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 소프트웨어학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 무선 인터넷 및 모바일 컴퓨팅 보안, 금융보안