Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.931

거래 인증 모드를 사용한 이동 결제 시스템 설계*

성 순 화,† 류 재 철‡
충남대학교 소프트웨어 연구소

Mobile Payment System Design with Transaction Certificate Mode*

Soon-hwa Sung,† Jae-cheol Ryou‡
Chungnam National University, Software Research Center(SOREC)

요 약

결제를 위한 이전의 웹 접근 인증 시스템의 웹 혹은 모바일 채널은 단지 사용자 인증만을 위한 것이며 사용자와 은행 및 금융 기관과의 인증은 이루어지지 않고 있다. 따라서 본 논문은 웹 기반 결제 시스템을 위한 사용자와 은행 및 금융 기관과의 상호 인증이 가능한 결제 거래 인증 모드를 제안한다.

제안한 시스템은 유선 전자 거래를 위한 안전한 전자 거래 (Secure Electronic Transaction : SET)를 무선 네트워크를 위한 결제 시스템으로 설계하였다. 또한 거래 인증 모드를 사용한 이 시스템은 SET 단점인 유선의 카드 기반 거래를 대신하여, 무선의 계좌 기반 거래를 지원 할 수 있다. 따라서 고객은 고객과 고객 은행 사이의 상호 인증으로 고객 은행 사이트에 다시 로그인할 필요 없이 잔고를 확인할 수 있다.

ABSTRACT

The Web or Mobile channel of previous Web access authentication system for a payment only provides the authentication of remote users, and does not provide the authentication between a user and a bank/financial institution. Therefore, this paper proposes the Transaction Certificate Mode(TCM) for a payment which can preserve the mutual authentication between a user and a bank/financial institution for Web-based payment systems.

The proposed system has designed for wireless network instead of Secure Electronic Transaction (SET) designed for wired electronic transaction. In addition, this system with TCM is able to support an account-based transaction for wireless networks instead of a disadvantage of SET such as a card-based transaction for wired networks. Therefore, customers can check their balances without logging on their bank's web site again due to mutual authentication between a customer and his bank/financial institution.

Keywords: mobile payment, transaction certificate, mutual authentication, user-based payment

I. 서 론

최근 전자 상거래와 이동 전자 상거래에서 사용자 인증 계획안이 중요한 보안 쟁점이 되고 있다. 하지만 원거리 사용자 인증 기법은 부주의한 비밀번호 관리와 정교한 공격 기술로 인해 심하게 노출되고 있다. 몇몇 기법[1-6]은 사용자 인증 기법에서 여러 가지 보안 문제를 향상시키기 위하여 제안 되었지만, 이동 결제 시스템에서 사용하기 위해서는 미숙한 보안 쟁점으로

접수일(2014년 6월 16일), 수정일(2014년 8월 21일), 게재확정일(2014년 10월1일)
* 이 논문은 2014년 정부재원(미래창조과학부 여성과학기술인 R&D 경력복귀지원 사업)으로 한국연구재단과 한국여성과학기술인지원센터의 지원을 받아 연구되었으며, 한국전자통신연구원-산업융합원천기술개발사업(No.10047528)의 지원을 일부 받아 수행된 연구임.
† 주저자, shsung@cnu.ac.kr
‡ 교신저자, jcryou@cnu.ac.kr(Corresponding author)

남아있다.

현재 이동 결제 시스템은 주로 두 가지 형식으로 나누어 볼 수 있다[7]. 첫 번째는 이동 전화, 스마트 카드 혹은 신용 카드를 기반으로 할 수 있는 계좌 기반 결제 시스템[8,9,10,11]이다. 두 번째는 고객이 자동 판매기 혹은 이동 장치가 있는 소매점에서 물건을 구입할 수 있는 이동 POS(Post of Sale) 결제 시스템이다. POS는 판매 시점 관리 단말기로 개인용 컴퓨터에 카드 결제 장치를 달아 판매 시점의 상품명이나 가격 등의 데이터를 저장하는 단말기로 종합적인 매출 관리를 해야 하는 대형 마트는 물론 소형 가맹점에서도 많이 사용하고 있다. 이러한 POS 시스템은 결제 시 고객 카드 정보 유출 경로로 이용되는 경우가 많아 그 해결 방안이 필요한 시점이다.

따라서 첫 번째, 두 번째 이동 결제 시스템 모두에서 안전한 웹 거래를 위한 사용자 인증과 이동 금융 거래의 사용자 신뢰를 증가시킬 수 있는 기술이 요구된다. 안전한 거래를 위한 제안된 다양한 인증 기술 중 [12]에서는 SMS(Short Message Service)를 제안하였고, [13]에서는 거래 식별 코드 TIC (Transaction Identification Code)와 SMS를 제안하였으나, [13]의 TIC는 사용자인 고객의 수가 많아지면 일회성 사용인 TIC를 유지 관리하는 서버 데이터베이스의 용량이 증가함으로써 이동 거래를 위한 효율적인 방법이 될 수 없다.

그러므로 본 논문에서는 [13]의 TIC 대신 TCM(Transaction Certificate Mode)을 제안함으로써 회사나 서비스 제공자는 금융 기관에 대한 사용자 인증과 함께 사용자에 인증된다. TCM은 고객을 위한 인증 모드 TCM1과 상인을 위한 TCM2로 구성되어 상호 인증을 지원한다. 이 제안은 유선 결제 거래를 위한 SET(Secure Electronic Transaction) 프로토콜을 무선 결제 거래를 위한 개선된 SET 프로토콜을 사용함으로써 전통적 SET 프로토콜의 결제 데이터 흐름인 단 방향 인증에서 상호 인증함으로써 계좌 기반 거래를 가능하게 한다.

본 논문 구성은 2장 관련 연구, 3장 거래 인증 모드, 4장 무선 네트워크를 위한 개선된 SET 프로토콜, 5장 안전한 상호 인증 프로토콜, 6장 공격 특징에 대한 보안 분석 및 암호 연산 분석, 7장 결론으로 구성된다.

II. 관련 연구

SET(Secure Electric Transaction)는 인터넷 상의 신용 카드 거래를 보호하기 위해 설계된 공개된 암호 및 보안 설명서이다. SET가 유선 기반[14,15,16]에서 작용하도록 설계되었지만 그 거래 흐름과 보안 실행은 무선 환경에서도 이용할 수 있다. SET 프로토콜은 현 신용 카드 기반 결제 시스템을 진화시켰고 등록과 인증에 의한 거래자의 신원 인증 뿐만 아니라 정보 전송을 위한 향상된 보안을 제공한다. SET는 고객이 웹 기반 서비스를 제공하는 상인에게 신용 카드 결제를 허락하는 반면, 고객은 온라인 은행 업무 시설을 사용하여 다른 형태의 서비스를 위한 결제 선택을 할 수 있다.

Fig.1.의 SET 거래 흐름을 살펴보면 다음과 같다.

1. 고객은 상인 웹 사이트에 접근하여 진열된 상품을 검색하여 그가 원하는 상품을 선택한 후, 선택된 상품의 세금과 운송비를 포함한 총액을 얻는다.
2. 시스템은 결제 방법을 묻고 고객은 SET를 사용한 신용 카드를 통한 결제를 선택한다.
3. 전자지갑(Digital Wallet)이라고 하는 고객 컴퓨터의 특별한 소프트웨어가 실시되어 그가 소유하고 있는 많은 신용 카드 중 하나를 선택한다.
4. 고객은 카드를 선택하여 SET를 사용한 전자 거래를 진행한다.
5. 고객 결제 항목을 얻은 후, 상인은 상인 인증과 결제를 위한 상인 은행과 연락한다.
6. 상인 은행은 고객 은행과 연락하여 결제 승인을 얻는다.
7. 거래가 성공적이면 상인은 확인한다.
8. 몇 초 후, 주문이 진행된 것을 고객에게 확인시킨다.

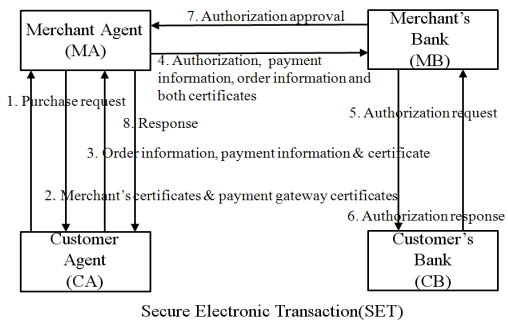

Fig. 1. Transaction Flow in Secure Electronic Transaction(SET)[13]

SET의 단점은 다음과 같다.

◉ SET는 유선을 위해 설계되어 무선의 장애를 고려하지 않는다.

◉ SET 프로토콜은 결제 데이터의 전통적 흐름으로 설계되어 단 대 단 보안 메커니즘이 요구된다.

◉ 거래 흐름은 고객에서 상인으로 진행되므로 사용자 신용 및 인출 카드의 모든 항목이 상인 측을 통해야만 한다. 이는 데이터가 복사되고 인증 없이 고객 계좌가 나중에 사용될 수 있기 때문에 사용자 정보 위험을 가중시킨다.

◉ 성공적 거래 후 고객 은행으로부터 고객에 대한 통지가 없다. 사용자는 다시 그의 은행 웹 사이트에 로그인 후 잔고 체크를 해야만 한다.

◉ SET는 카드 기반 거래만 하고 계좌 기반 거래는 포함하지 않는다[13].

III. 거래 인증 모드(Transaction Certificate Mode : TCM)

본 논문은 사용자와 진행 중인 거래를 검증하기 위한 TCM 인증 기술을 제시함으로써 이동 결제를 위한 웹 기반 인증을 제안한다. TCM 인증은 현재 거래가 정당한 사람으로 시작되며, 그의 계좌에 접근하려는 유효한 사람임을 확인시켜 준다. TCM은 TCM1과 TCM2로 구성되며, TCM1은 고객에 대한 은행 혹은 금융 기관에 의해 발행되며, TCM2는 상인에 대한 은행 혹은 금융 기관에 의해 발행된다. TCM1는 암호화된 계좌 정보를 포함한 고객 정보와 상인 에이전트에 대한 주문서 항목을 가진 인증서이며, TCM2는 암호화된 계좌 정보를 포함한 상인 정보와 고객 에이전트에 대한 청구서 항목을 가진 인증서로 구성된다. 이러한 형식의 TCM1은 고객의 비밀키로 서명함으로써 고객 주도의 결제 거래를 제공하며, TCM2는 상인의 비밀키로 서명함으로써 고객의 요구에 따라 상호 인증 결제 거래를 지원한다.

Fig.2.는 TCM의 구성으로서, TCM은 고객 은행의 인증서인 TCM1과 상인 은행의 인증서인 TCM2를 합한 거래 인증 모드이다. Fig.3.에서는 그 구성 흐름을 설명하고 있으며, TCM1은 고객 정보와 주문 정보를 이진수로 부호화한 후, 해시 함수로 길이를 단축함과 동시에 암호화하여 고객의 비밀키로 서명한다. 이러한 TCM은 공인인증서와 같은 역할로 금융 기관과 금융 기관을 관리하는 공인 기관에서 제어 감독한

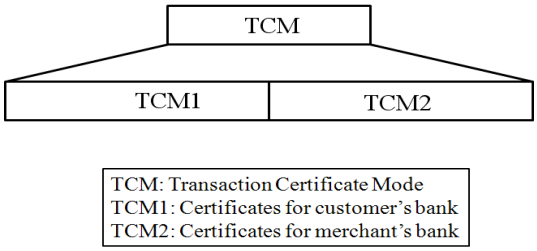

Fig. 2. Transaction Certificate Mode(TCM) Construction

다. TCM은 이동 결제를 위한 간단한 메시지 전달을 위한 SMS 인증을 지원한다.

금융 기관은 여러 요소 인증을 제공하기 위해 사용자 이동 전화 번호를 저장한다. 사용자는 일반적으로 이동 전화를 휴대함으로 간단한 메시지를 받을 수 있으므로 유효한 사용자만이 인증 서버로부터 SMS를 받을 수 있다. SMS를 받은 후 사용자는 선택을 인정하고, 인증 서버로부터 "예"를 받으면 사용자가 유효하므로 사용자가 최초 거래를 승인한다[12].

TCM은 안전한 결제 거래를 위해서 사용자와 상인, 사용자 은행과 상인 은행들과의 각 객체들과의 상호 거래 인증을 제공하며, 사용자 중심의 결제 거래를 유도할 수 있다.

다음 장에서는 TCM을 사용한 이동 결제 거래를 위한 프로토콜을 설계한 후, 고객 에이전트와 고객 은행 사이의 상호 인증 프로토콜과 SMS 지원을 설명한다.

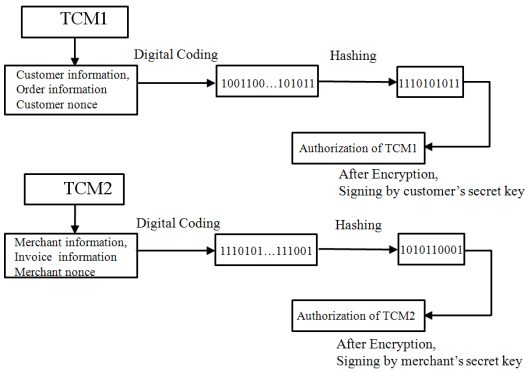

Fig. 3. Transaction Certificate Mode(TCM) Construction Flow

IV. 무선 네트워크를 위한 개선된 SET 프로토콜

본 논문은 유선의 카드 결제를 위한 SET를 무선

네트워크를 위한 SET 프로토콜을 제안함으로써, SET 단점인 카드 기반 거래를 계좌 기반 거래로 보완하기 위한 거래 인증 모드 TCM을 제안하여 계좌 이체가 가능한 결제 거래를 지원한다.

Fig.4.는 개선된 SET 프로토콜로서 고객 에이전트, 고객 은행, 상인 에이전트, 상인 은행 각 개체가 상호 인증 할 수 있도록 TCM 지원을 설명한다. 이전 SET의 단방향 인증을 사용자가 주체가 되어 상호 인증함으로써 사용자 기반의 이동 결제 거래를 제공한다.

Fig.4.의 거래 인증 모드를 사용한 무선 결제 프로토콜은 다음과 같이 진행된다.

1. 고객은 상인 에이전트인 상인 웹 사이트에 들어가서 상품을 검색한 후, 그가 원하는 상품을 선택한 후, 세금과 배송비를 포함한 총 금액을 얻는다.
2. 상인 웹 사이트는 지불 방법을 묻고, 청구서를 고객 에이전트에게 보낸다.
3. 고객은 신용카드 혹은 계좌 이체 결제를 선택한 후, 인증된 주문 정보를 상인 에이전트에게 보낸다.
4. 상인 에이전트는 상인 은행에게 고객 주문 정보에 대한 인가를 보낸다.
5. 고객 에이전트인 고객 웹 사이트는 상인 은행에 대한 인증모드인 TCM2를 상인 은행에게 요구한다.
6. 유효한 경우, 상인 은행은 고객 에이전트에게 긍정 응답을 보내고 다음 단계를 진행한다. 유효하지 않은 경우, 거래를 중단한다.
7. 상인 은행은 고객 은행에게 고객 은행에 대한 인증 모드인 TCM1을 요구한다.
8. 안전한 상호 인증 프로토콜은 상인을 인증 한 후, 결제 전 고객을 인증하기 위해 진행한다.
9. 유효한 경우, 고객 은행은 고객 에이전트와 상인 은행에게 결제 통보를 한다.
10. 상인 은행은 상인 에이전트에게 결제 승인을 한다.

Fig.4.의 8번인 안전한 상호 인증 프로토콜은 고객 에이전트와 고객 은행과의 상호 인증으로써 TCM을 사용한 무선 결제 거래를 완성시킨다. 그 인증 절차는 Fig.5.에서와 같다.

1. 사용자가 사용자 ID(Identification), 비밀번호, 그리고 고객 은행으로부터 TCM1을 얻는다.
2. 사용자는 사용자 ID와 비밀번호에 의해 고객 은행 웹 서버에 로그인한다.
3. 고객 은행 웹 서버는 사용자가 성공적으로 인증되었음을 알린다.
4. 사용자는 결제 모드를 선택한다.
5. 사용자는 사용자가 이체할 계좌 정보와 상인 정보가 들어 있는 결제 항목을 채운다.
6. 사용자는 거래를 인증하기 위한 TCM1을 고객 은행 웹 서버에게 보낸다.
7. 고객 은행 웹 서버에서는 사용자 거래를 검증하기 위해 사용자에게 SMS를 보내어 거래 및 은행 잔고를 확인시킨다.
8. 사용자는 SMS 응답에 따라 거래를 거부하거나 거래 확인을 보낸다.

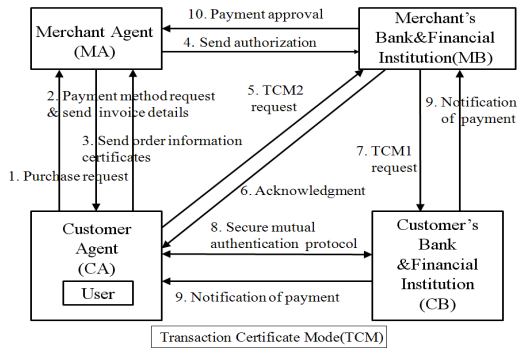

Fig. 4. Wireless Payment Protocol using Transaction Certificate Mode(TCM)

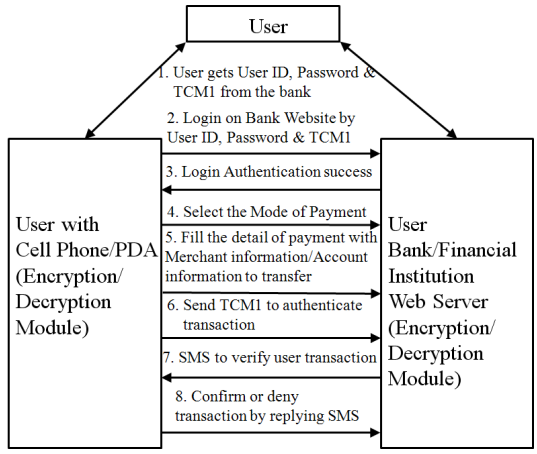

Fig. 5. Secure Mutual Authentication

V. 안전한 상호 인증 프로토콜

Fig.6.의 제안된 상호 인증 프로토콜은 고객 에이전트와 고객 은행, 상인 에이전트와 상인 은행과의 상호 인증을 위하여 등록, 로그인, 인증 3단계로 구성된다.

Table 1 에서의 N_c와 N_s은 반복 공격을 보호하기 위하여 사용함으로써 안전한 상호 인증을 지원한다.

등록단계: 사용자는 서버에게 사용자 아이디 ID_c, 비밀번호 Pw_c를 제시하면 서버는 다음과 같이 진행한다.

1) $Vc=H(ID_c, TSP, Pri_s)$를 계산한다.
2) $Ac=H(ID_c, TSP, Pri_s)\oplus Pw_c$를 계산한다.
3) TCM에 $(ID_c, Vc, Ac, H(.))$를 저장한다.

로그인단계: 사용자는 서버에 로그인하기 위하여 TCM에게 사용자 아이디 ID_c, 비밀번호 Pw_c를 제공한 후, 다음을 수행한다.

1) $Bc=Ac\oplus Pw_c$를 계산한다.
2) $Bc=Vc$ 인지를 체크한다. 만약 실패이면 요구는 거절된다.
3) $C_1=Bc\oplus N_c$를 계산한다.
4) 서버에게 (ID_c, C_1)를 보낸다.

인증단계: 서버가 로그인 요구 (ID_c, C_1)를 받을 때 다음을 수행한다.

1) ID_c 구성 방식을 테스트한 후, 구성 방식이 옳지 않으면 로그인 요구가 거절된다.
2) $Bs=H(ID_c, TSP, Pri_s)$를 계산한다.
3) $C_2=C_1\oplus B_s$를 계산한다.

Table 1. Notation

Symbol	Description
Uc	User
S	Server
IDc	Identity of the user
Pwc	Password
Pris	Server's Private key
TSP	Timestamp given by trusted time stamping
Nc	User's generated nonce
Ns	Server's generated nonce
TCM	Transaction Certificate Mode
Sk	TCM session key
H( )	Hash function
⊕	XOR
‖	Concatenation

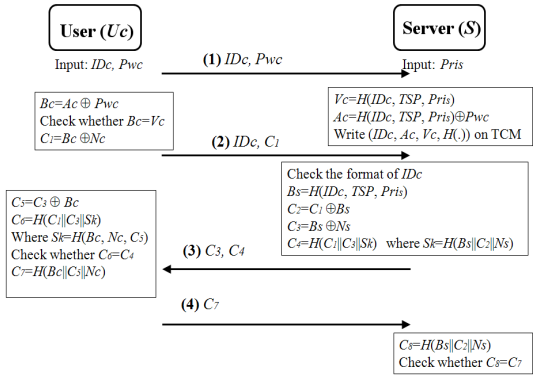

Fig. 6. Secure Mutual Authentication Protocol

4) $C_3=B_s\oplus N_c$를 계산한다.
5) $C_4=H(C_1\| C_3\| Sk)$를 계산한다.
   단, $Sk=H(B_s\| C_2\| N_s)$
6) 단방향 인증을 위하여 사용자에게 $\{C_3, C_4\}$를 보낸다.

사용자는 서버로부터 $\{C_3, C_4\}$를 받자마자, 다음을 수행한다.

7) $C_5=C_3\oplus B_c$와 $C_6=H(C_1\| C_3\| Sk)$를 계산한다.
   단, $Sk=H(B_c\| C_5\| N_c)$
8) $C_6=C_4$ 이면 사용자는 서버를 인증한 후, 단방향 인증이 이루어진다. 만약 그렇지 않으면 사용자는 요구를 거절한다.
9) $C_7=H(B_c\| C_5\| N_c)$를 계산한 후, C_7를 서버에게 보낸다.
   사용자로부터 C_7를 받은 서버는 다음을 수행한다.
10) $C_8=\mathrm{H}(B_s\| C_2\| N_s)$를 계산한다.
11) $C_8=C_7$ 이면 서버는 사용자를 인증함으로써, 상호 인증이 이루어진다.

VI. 분 석

본 논문은 제안된 기법의 보안을 분석하기 위하여, 공격자가 어떤 방법[17,18]으로 스마트카드에 저장된 비밀 값을 추출하고 사용자의 스마트카드에 접근할 수 있으며, 사용자와 서버 사이의 통신 메시지를 삽입할 수 있다고 가정한다. 그리고 Ayu et al.[13]기법과 제안된 기법의 상호 인증, 사용자 가장 공격, 서버 가장 공격, 재전송 공격을 Table 2에서 비교 분석한다.

상호 인증: 제안된 기법의 Fig.4.에서 무선 네트워크를 위한 개선된 SET 프로토콜은 고객과 상인, 고객 은행과 상인 은행, 고객과 고객은행, 상인과 상인

은행, 고객과 상인 은행과의 각 객체들과의 상호 거래 검증을 할 수 있다.

Ayu et al.[13]기법에서는 고객이 상인과 상인 은행과의 상호 인증이 직접 이루어지지 않고, 고객이 고객 은행을 통한 상인과 상인 은행 인증이 이루어지므로 불완전한 상호 인증이 이루어지고 있다.

사용자 가장 공격: Ayu et al.[13]기법은 사용자가 사용자 이름과 비밀번호만으로 웹 서버에 로그인하기 때문에 서버에는 사용자 이름과 비밀번호를 저장하여 거래할 때마다 이를 확인하여 사용자 인증한 후, 거래 식별 코드를 요구한다. 따라서 사용자가 웹서버에 로그인할 때 거래 식별 코드 안전성의 혜택을 받을 수 없으며, 공격자는 여러 방법으로 서버에 저장된 사용자 이름과 비밀번호를 공격할 수 있다. 또한 거래 식별 코드를 복호화하기 위한 서버에 의해 생성된 비밀 키의 반복 사용으로 서버 가장 공격을 받아, 사용자 이름과 비밀번호를 가장한 사용자 공격을 받을 수 있다.

제안된 기법은 사용자가 웹 서버에 로그인할 때, 사용자 이름, 비밀번호 그리고 거래 인증 모드인 TCM1으로 인증을 받는다. 거래 인증 모드 TCM1은 고객 정보와 주문 정보를 고객의 비밀 키로 서명한 것으로 사용자 가장 공격 시 고객의 비밀 키로 확인 할 수 있다.

서버 가장 공격: 제안된 기법은 상호 인증 프로토콜의 인증 단계에서 서버가 사용자를 인증하기 위해 사용자 N_C와 서버의 TCM 세션 키 S_K를 사용한다. 반면 사용자가 서버를 인증하기 위해 서버 논스 N_S와 사용자의 TCM 세션 키 S_K를 사용함으로써 안전한 거래를 완성한다. 따라서 TCM 거래 인증 모드의 세션 키를 가장하여 서버를 공격한다고 하더라도 사용자의 TCM 거래 인증 모드의 세션 키가 없으면 상호 인증이 이루어지지 않기 때문에 가장 공격의 목적을 이룰 수 없다.

Ayu et al.[13]기법은 거래 식별 코드 TIC가 서버에 제출되기 전에 고객의 모든 계좌 정보가 암호화되기 위해 사용된다. 이 거래 식별 코드는 서버에 의해 생성된 비밀 키로 암호화되어 서버에 성공적인 로그인 후, 사용자에게 전해진다. 거래 식별 코드를 복호화할 이 비밀 키는 서버에 저장되어 고객에게 발행한 거래 식별 코드와 일치하는지 확인한다. 만약 일치한다면 비밀 키는 동일한 거래 식별 코드에 의해 암호화될 다른 거래 항목을 복호화하기 위해 다시 사용된다. 이러한 비밀 키의 중복 사용은 공격자로부터 서버 공격이 가능할 수 있다.

재전송 공격: 제안된 기법은 상호 인증프로토콜에서 TCM에 타임스탬프 TSP를 저장하고, 특히 사용자와 서버의 논스 생성으로 공격자가 재전송 공격을 할 수 없도록 지원한다.

반면, Ayu et al.[13]기법에서는 웹 서버가 사용자 이름과 비밀번호를 사용하여 웹 사용자를 인증한 후, 웹 사용자로부터 거래 식별 코드를 요구한다. 거래 식별 코드는 거래의 안전성을 위해 비밀번호와 같은 역할을 하며, 일회성 사용으로 서버 데이터베이스에 저장된다. 서버 데이터베이스에 저장된 거래 식별 코드를 삭제하지 않는 한, 공격자가 서버를 공격하여 거래 식별 코드를 얻으면 일부 재전송 공격이 가능할 수 있다.

이동 결제 프로토콜 성능 분석으로 계산 비용인 암호 연산 횟수를 제안된 기법과 S. K. et al.[19]기법, T. S. et al.[20]기법, 그리고 J.T. et al.[21]기법을 Table 3에서 비교 분석하였다. 한 번의 이동 결제 거래 동안 사용자인 고객과 서버인 상인 측에서의 대칭키 암·복호화, 해시 함수, 키 해시 함수, 그리고 키 생성에 필요한 시간을 단위 시간으로 환산하여 그 횟수를 비교 하였다.

제안된 기법의 암호 연산 횟수를 살펴보면, 대칭키 암·복호화에서는 상호 인증 프로토콜의 사용자 등록과 로그인 단계에서 논스를 포함한 비밀 키의 XOR가 3

Table 2. Security comparison of Ayu et al.[13]scheme and the proposed scheme

Security Features	Ayu et al.[13] Scheme	The Proposed Scheme
Mutual Authentication	Part Provided	Full Provided
User Impersonation Attack	Possible	Impossible
Server Masquerading Attack	Possible	Impossible
Replay Attack	Partial Possible	Impossible

Table 3. Comparison of the Number of Cryptographic Operations

Cryptographic Operations		The Number of Cryptographic Operations			
		S. K. et al.[19] Scheme	T. S. et al.[20] Scheme	J.T. et l.[21] Scheme	The Proposed Scheme
Symmetric key encryption/decryptions	*Uc*	4	5	3	3
	S	5	6	4	3
Hash Functions	*Uc*	2	2	2	2
	S	-	1	1	5
Keyed-hash Functions	*Uc*	2	-	2	-
	S	2	-	1	2
Key Generation	*Uc*	2	-	2	2
	S	1	-	4	2

번, 인증 단계의 서버에서도 논스를 포함한 비밀 키의 XOR가 3번 이루어지므로 그 횟수가 각각 3이다. 해시 함수는 상호 인증 프로토콜의 사용자 등록단계에서 2번, 서버 인증 단계에서 5번, 키 해시 함수는 상호 인증 프로토콜의 인증 단계의 TCM 세션 키를 사용한 해쉬 함수가 2번 이루어진다. 키 생성에서는 사용자의 패스워드와 논스 생성으로 2번, 서버의 비밀 키와 논스 생성이 이루어지므로 2번 연산된다.

제안된 기법의 해시 함수 연산 횟수가 다른 연구보다 많은 이유는 상호 인증을 지원하기 때문이며, 그 외 연산에서는 이전 기법들보다 계산 효율이 향상되었다.

VII. 결 론

본 논문은 카드 사용을 위한 유선 전자 거래 SET 프로토콜을 카드와 계좌 이체가 가능한 무선 거래 프로토콜로 개선함으로써 고객 주체의 결제 거래를 가능하게 하였고, 제안된 시스템의 보안 분석을 하였다. 제안한 거래 인증 모드 TCM은 무선 거래 프로토콜의 각 개체를 상호 인증하는 역할을 하며, 무선 상호 인증 프로토콜은 안전한 결제 거래를 할 수 있도록 지원하므로 여러 종류의 공격을 막을 수 있다.

일회성 사용의 거래 식별 코드 TIC를 제시한 Ayu et al.[13]기법은 TIC를 관리하는 서버 데이터베이스 용량 증가로 사용자가 많을 경우, 무선 결제 거래의 유지 관리에 어려움이 있다. 하지만 제안한 거래 인증 모드 TCM은 고객과 상인이 쉽게 변경할 수 있는 각자 소유한 비밀 키로 서명하기 때문에 사용자 수에 상관없이 무선 결제 거래를 쉽게 유지 관리할 수 있다.

거래 인증 모드를 사용한 결제 거래는 결제 거래 흐름이 고객이 주체가 되어 거래 개체들의 상호 인증이 가능하다. 뿐만 아니라, 이전 연구들과 비교할 때 이동 결제 프로토콜의 연산 비용이 낮으며 연산 성능 효율성에서도 우수하다.

본 기법은 이동 결제 금융 시장의 한계인 송금이 결제보다 많다는 점을 해결하기 위하여 이전의 카드 결제를 위한 SET을 개선하므로 카드 결제와 송금 결제가 가능하게 되었다.

향후, 거래 인증 모드를 사용한 이동 결제 시스템의 다양한 성능 분석 연구가 필요하다.

References

[1] L. Lamport, "Password Authentication with Insecure Communication," Communication of the ACM, vol. 24, no. 11, pp.770-772, 1981.

[2] M. S. Hwang and L. H. Li, "A New Remote User Authentication Scheme using Smart Cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[3] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further Improvement of an Efficient Password based Remote User Authentication Scheme using Smart Cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 612-614, 2004.

[4] M. L. Das, A. Saxena, and V. P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme," IEEE Transactions on Consumer Electronics, vol. 50, no.2, pp.629-631, 2004

[5] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A New Strong-Password Authentication Scheme using One-way Hash Function," Journal of Computer and Systems Sciences International, vol. 45, no. 4, pp. 623-626, 2006.

[6] C. S. Bindu, P. Reddy, and B. Satyanarayana, "Improved Remote User Authentication Scheme Preserving User Anonymity," International Journal of Computer Science and Network Security, vol. 83, pp.62-66, 2008.

[7] J. Gao, J. Cai, K. Patel, and S.Shim, "Wireless Payment," Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), pp.367-374, 2005.

[8] S. Kungpisdan, B. Srinivasan and P.D. Le, "A Secure Account-Based Mobile Payment Protocol," Proceedings of the International Conference on Information

Technology: Coding and Computing, IEEE CS press, pp.35-39, 2004.

[9] Y.B. Lin, M.F.. Chang, H.C.H. Rao, "Mobile prepaid phone services," IEEE Personal Communications, Vol.7, pp.6-14, 2000.

[10] A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri, "A SET Based Approach to Secure the Payment in Mobile Commerce," In Proceedings of 27th Annual IEEE Conference on Local Computer Networks, pp.136-140, 2002.

[11] Huang Z., Chen K., "Electronic Payment in Mobile Environment," In Proceedings of 13th International Workshop on Database and Expert Systems Application (DEXA'02), pp.413-417, 2002.

[12] W. Adi, A. Mabrouk, A. Al-Qaye야, A. Zahro, "Combined Web/Mobile Authentication for Secure Web Access Control," Wireless Communications and Networking Conference, IEEE Communications Society, pp.667-681, 2004.

[13] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog, and Sugata Sanyal, "A Multi-Factor Security Protocol for Wireless payment Secure Web Authentication using Mobile Devices," IADIS International Conference Applied Computing 2007, pp.160-167, 2007.

[14] J. Hall, S. Kibank, M. Barbe며, E. Kranakis, "WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks," IEEE International Conference on Telecommunications (ICT), 2001.

[15] V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho, "Formal Analysis of Card-based Payment Systems in Mobile devices," Fourth Australasian Information Security Workshop, Conferences in Research and Practice in Information Technology, Vol.54, pp.213-220, 2006.

[16] L. Albert, K.C. Kaya, "CONSEPP: Convenient and Secure Electronic Payment Protocol Based on X9.59," 17th Annual Computer Security Applications Conference, IEEE press, pp.286-295, 2001.

[17] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proceedings of Advances in Cryptology, pp.388-397, 1999.

[18] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Transactions on Computers, vol. 51, no.5, pp. 541-552, 2002.

[19] S. Kungpisdan, B. Srinivasan, and P.D. Le, "Lightweight mobile credit-card payment protocol," The 4th International Conference on Cryptology in India (Progress in Cryptology - INDOCRYPT 2003), pp.295-308, 2003.

[20] T. S. Fun, L. Y. Beng, J. Likoh, and R. Roslan, "A lightweight and private mobile payment protocol by using mobile network operator," The International Conference on Computer and Communication Engineering, pp162-166, 2008.

[21] [21]Jesus Tellez Isaac and Sherali Zeadally, "An Anonymous Secure Payment Protocol in a payment Gateway Centric Model," The 9th International Conference on Mobile Web Information Systems (MobiWIS), Procedia Computer Science 10, pp758-765, 2012.

〈저자소개〉

성 순 화 (Soon-hwa Sung) 정회원
2005년 : 충남대학교 컴퓨터공학과 박사
2006년 ~2010년 : 충남대학교 차세대통신인력양성사업단 BK전임교수
2011년 : 충남대학교 공학교육혁신센터 초빙교수
2012년 : 충북대학교 소프트웨어학과 초빙교수
2014년 ~ 현재 : 충남대학교 소프트웨어 연구소
〈관심분야〉 사용자 인증, 이동 결제 시스템, IoT(Internet of Things) 보안

류 재 철 (Jae-cheol Ryou) 종신회원
1985년: 한양대학교 산업공학과 (학사)
1988년:Iowa State Univ. 전산학과 (석사)
1990년: Northwestern Univ. 전산학과 (박사)
1991년 ~ 현재: 충남대 전기정보통신공학부 교수
〈관심분야〉 인터넷 보안, 전자결제시스템