무선 인터넷을 위한 신용카드 기반의 인증 및 키 교환 프로토콜

이 현 주* · 이 충 세**

A Credit Card based Authentication and Key Exchange Protocol for Mobile Internet

Hyun-Ju Lee · Chung-Sei Rhee

요 약

무선 인터넷에서 신용카드 지불을 수행하는 WPP 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용한다. WTLS의 사용은 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 본 논문에서는 AIP 프로토콜에서 Mobile Gateway를 사용함으로서 무선 인터넷 플랫폼에 독립적이며 사용자와 VASP간에 보안이 제공되는 프로토콜을 제안한다. 또한, 타원곡선상에서 덧셈군 알고리즘인 Weil Diffie-Hellman 키 교환을 적용하여 인증과 지불 초기화 과정에 사용될 세션키를 생성함으로써 이동성이 많은 무선 인터넷 환경에 적합한 프로토콜을 제안한다.

키워드

Weil Diffie-Hellman, ID 기반 공개키 암호, 종단간 보안, 신용카드

ABSTRACT

WPP protocol based a Credit card payment in mobile Internet uses WTLS which is security protocol of WAP. WTLS can't provide End-to-End security in network. In this paper, we propose a protocol both independent in mobile Internet platform and allow a security between user and VASP using Mobile Gateway in AIP. In particular, our proposed protocol is suitable in mobile Internet, since session key for authentication and initial payment process is generated using Weil Diffie-Hellman key exchange method that use additive group algorithm on elliptic curve.

keyword

Weil Diffie-Hellman, ID-based Public Key Cryptosystem, End-to-End security, Credit Card

Ⅰ. 서 론

최근 무선 인터넷이 급성장하면서 멀티미디어 다운로드, 메일 송수신, 인터넷 뱅킹, 증권 거래에서 전자상거래까지 다양한 서비스가 제공되고 있다. 그러나 이 서비스들 중에서 인터넷 뱅킹이나 전자상거래의 경우는 사용자의 비밀 정보가 교환되는 민감한 서비스이므로, 비밀 정보들을 안전하게 전송하기 위한 보안 기술이 필수적이다. 반면, 무선 인터넷 환경은 낮은 대역폭, 단말기의 낮은 컴퓨팅 능력, 제한된 메모리와 전력 그리고 전송 지연등의 특징으로 보안 서비스를 제공하는데 많

* 정회원 : 충북대학교 전자계산학과
** 충북대학교 전기전자및컴퓨터공학부 교수
접수일자 : 2003. 10. 11

은 제약이 따른다. 그러므로 이러한 열악한 환경에서 보안 서비스를 제공하기 위하여 다양한 형태의 보안 프로토콜이 사용되고 있다. ME(Mobile Explore)와 I-mode는 무선 인터넷에서도 유선망에서 사용하는 SSL을 이용하여 보안 채널을 생성한다[1,2]. WAP은 초기 1.x 모델에서 연결 분리(split connection)기법을 사용하기 때문에 유선망은 SSL, 무선망에서는 WTLS를 보안 프로토콜로 적용하고 있다[3]. 2002년에 발표된 WAP2.0 모델에서는 ME나 I-mode와 같은 TLS 기반으로 보안 모델을 수정하였다[4]. 유선 환경에서 사용되는 지불 프로토콜 중에서 대표적인 신용카드 지불 프로토콜인 SET(Secure Electronic Transaction)는 지불에 사용되는 신용카드 정보가 안전하도록 프로토콜이 구성되어 있으며 시스템 또한 구축되어 있다. 그러나 제한적 요소가 많은 무선 인터넷에는 적합하지 않다[5]. 제한적 요소가 많은 무선 환경에서 신용카드를 사용하여 지불 수행을 하기 위해 제안된 WPP(Wireless Payment Protocol) 지불 프로토콜은 스마트 카드 기술과 WAP(Wireless Application Protocol)의 WTLS (Wireless Transport Layer Security)를 사용한다[6,3]. WTLS를 사용하는 WAP 프로토콜 스택은 인터넷 프로토콜과 서로 다르기 때문에 사용자가 직접 원하는 서버와 통신할 수 없다. 따라서 WAP에서는 무선 단말기와 유선상의 서버를 연결해 줄 수 있는 다리로써 WG(WAP Gateway)를 사용한다. 그러나 WG에서 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 메시지가 노출되는 위험성을 가지고 있다[7]. WAP의 WTLS를 사용하는 WPP 지불 프로토콜은 종단간 보안을 제공하지 못하기 때문에 사용자의 신용카드 정보를 보호할 수 없다. ASPeCT(Advanced Security for Personal Communications Telecommunications System)에서는 UMTS(Universal Mobile Telecommunications System)에서 사용자와 VASP(Value-Added Service Provider)간에 인증과 지불을 위한 AIP(Authentication and Initialization of Payment)프로토콜을 제안하였다[8,9].

본 논문에서는 Weil Pairing을 사용한 공개키 암호 시스템을 적용하여 종단간 보안이 제공되는 신용카드 기반의 인증 및 키 교환 프로토콜을 제안한다. 제안하는 프로토콜은 종단간 보안을 제공하는 AIP 프로토콜을 기초하여 참여자간의 인증을 수행하고 신용카드 지불을 수행하기 위해 타원곡선상에서 세션키(session key)를 생성한다. 또한 유선 구간에서는 인터넷에서 신용카드 지불을 수행하기 위해 구축되어 있는 시스템을 사용하며, WPP의 WG 문제점을 극복하기 위해 지불 프로토콜에 직접 참여하지 않고 무선 구간과 유선 구간의 연결 기능만을 수행하는 MG(Mobile Gateway)를 사용한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 소개하고, 3장에서는 제안하는 신용카드 기반의 인증 및 키 교환 프로토콜을 기술한다. 4장에서는 제안하는 프로토콜의 안전성 및 성능 평가를 하고, 5장에서는 결론을 제시한다.

II. 관련 연구

본 장에서는 WPP와 WPP에서 사용하는 WAP의 보안 프로토콜인 WTLS 및 AIP를 기술한다.

2.1 WPP

WPP는 SET을 기반으로 무선 인터넷 환경에서 신용카드 지불을 수행할 수 있도록 제안된 지불 프로토콜이다. WPP는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP의 WTLS를 사용한다. WPP의 참여자는 사용자와 사용자의 은행(신용카드사), 서비스 제공자(상점) 서버, 서비스 제공자의 은행으로 구성된다. 이때 사용자와 은행, 서비스 제공자 서버를 연결해주는 WG가 필요하다. WPP는 WAP의 WTLS를 사용하여 무선 구간의 보안을 제공한다. 이때 WAP에서는 무선 단말기와 유선환경에 존재하는 서버를 연결해 줄 수 있는 다리로써 WG를 사용한다. WG에서는 WTLS-SSL 프로토콜 변환 시 메시지의 암/복호화가 이루어지기 때문에 원본 메시지가 노출될 위험성을 가지고 있어 종단간 보안을 제공하지 못하는 단점을 가지고 있다[7].

2.2 WTLS

WTLS를 적용하기에 가장 큰 문제로 여겨지는 것은 무선 단말기와 사용자가 원하는 실제 데이터가 있는 서버 사이의 종단간 안전성(Ene-to-End security)의 문제이다. 왜냐하면 WAP이 사용하는 프로토콜 스택이 인터넷 프로토콜과 서로 다르기 때문에 사용자가 직접 원하는 서버와 통신할 수 없다. 따라서 WAP에서는 그림1과 같이 무선 단말기와 원래의 서버를 연결해 줄 수 있는 다리로서 WAP Gateway를 사용한다.

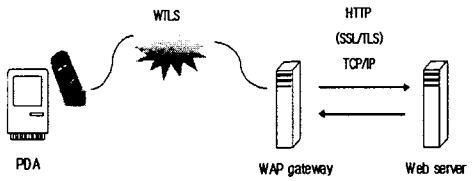

그림1. WAP gateway

즉, WTLS는 무선 단말기와 WG 사이의 통신을 보호할 뿐이다. 단말기로부터 전달된 메시지는 WG내에서 복호화된 후에 인터넷 프로토콜에 맞게 포맷팅되어 SSL/TLS로 다시 암호화되어 원래의 서버로 전달된다. 원래의 서버로부터 무선 단말기로의 데이터 전송도 같은 방법으로 WG를 거친다. 서버와 WG사이의 데이터 보호는 인터넷 프로토콜의 HTTP위에서 SSL/TLS등으로 보호할 수 있다. WTLS는 WAP의 보안 프로토콜로서 인터넷 프로토콜에서 TCP의 보안을 위해 사용하는 TLS를 무선 환경에 맞도록 최적화한 것이다. WTLS는 TLS와 마찬가지로 인증, 암/복호화, 무결성 검증등 보안을 제공한다. WAP 단말기와 서버가 WTLS를 이용해 메시지를 전송할 경우, 먼지 핸드쉐이크 프로토콜을 수행하여 메시지를 안전하게 전송하는데 사용되는 세션키, 암호 알고리즘, 인증서 등과 같은 암호 매개 변수를 공유하게 된다. 새로운 세션을 생성하기 위해 WAP 단말기와 서버가 서로 4번의 메시지 전송을 수행해야 한다. 또한 암/복호화에 사용할 키를 생성하기 위해 master_secret을 생성한다. master_secret은 키 교환 알고리즘으로 생성된 pre_master_secret과 난수를 사용하여 생성한다[3,10]. 핸드쉐이크 프로토콜에서 생성된 세션 정보는 레코드 프로토콜(Record Protocol)에서 안전한 메시지 전송을 하는데 이용된다.

2.3 AIP

ASPeCT의 AIP 프로토콜은 무선 이동 통신 환경에서 사용자와 VASP간에 인증과 지불 초기화를 수행하게 해주는 프로토콜이다. AIP 프로토콜은 사용자와 VASP가 상호 인증과 세션키를 설정하고 지불 초기화 정보를 교환한 후 Pederson의 소액 지불 기법을 사용하여 지불을 수행한다. 종단간 보안을 제공하는 AIP 프로토콜은 다음과 같은 조건을 만족시켜야 한다[8,11].

- 상호간의 새로운 키의 확신
- 사용자와 VASP간의 명확한 상호 인증
- 사용자와 VASP간의 함축적 키 인증성을 가진 세션키의 성립
- VASP에게 전송되는 사용자 데이터의 부인 방지
- 사용자와 VASP 인터페이스에서의 사용자신원의 기밀성
- 사용자의 신용카드 정보에 대한 안전성 제공

AIP 프로토콜은 참여자에게 인증서를 제공하는 온라인 TTP(Trusted Third Party)의 참여 여부에 따라 두 가지 종류의 프로토콜로 구분된다. 사용자와 서비스 제공자는 Diffie-Hellman 키 교환 방식에 의해 세션키를 생성하고 사용자와 TTP는 Elgamal 방식에 의해 세션키를 생성한다[12]. 생성한 세션키를 사용하여 인증을 수행한 후 지불을 수행하기 위한 초기화 정보를 교환한다.

III. 신용카드 기반의 인증 및 키 교환 프로토콜

본 논문에서 제안하는 인증 및 키 교환 프로토콜은 신용카드 지불을 안전하게 수행할 수 있도록

종단간 보안을 제공하는 AIP 프로토콜을 사용한다. 또한, 유한체 F_q에서 타원곡선(Elliptic Curve Cryptosystem)을 이용한 Weil Pairing에 의해 세션키를 생성하여 속도의 향상 및 안전성을 제공한다. 제안하는 프로토콜은 인증 과정에 온라인 인증기관이 참여하지 않는 경우와 참여하는 경우로 나누어 기술한다. 사용자 무선 단말기의 스마트카드에 저장되어 있는 신용카드 정보는 무선 환경에서 사용할 수 있도록 신용카드사와 미리 약속한 정보이다. 다음은 기존 프로토콜로부터 새롭게 제안하는 프로토콜의 향상된 내용이다.

- ECC를 이용한 Weil Pairing 에 의해 세션키를 생성한다.
- Weil Diffie-Hellman에 의해 보조세션키를 생성한다.
- 통신량(메시지 교환 횟수)을 감소시킨다.
- ID기반 ECC 알고리즘을 사용하여 안전성을 향상시킨다.

3.1 ID 기반 공개키 암호 시스템

본래의 PKC(Public Key Cryptosystem)는 공개키를 인증하고 관리하는 인프라 구축에 많은 비용이 든다. 반면, ID 기반 PKC는 이런 문제점을 해결하고 있다. ID 기반 PKC에서 모든 사람의 공개키는 사전에 이메일 주소와 같은 정보에 의해 결정된다. Shamir에 의해 제안된 이 개념은 원래 e-mail 시스템에서 인증 관리를 단순화 하기 위한 것이었다[13]. Alice가 Bob에게 bob@hotmail.com으로 메일을 보낼 때 보낼 때 공개키 스트링 bob@hotmail.com을 사용하여 메시지를 암호화한다. Alice는 Bob의 공개키 인증서를 획득할 필요가 없다. Bob은 메시지를 복호화하기 위해 KGC(Key Generation Center)에게 자신을 인증한 후 자신의 개인키를 얻는다. 기존의 e-mail 구조와 달리, Alice는 Bob이 사전에 공개키 인증을 설정하지 않아도 암호화된 메일을 보낼 수 있다. ID 기반 시스템에서는 KGC가 Bob의 개인키를 알고 있을때 key escrow는 고유하며 신뢰할 수 있는 KGC가 필요하다. KGC에서는 각 개체의 ID 기반 공개키를 사용하여 개인키를 생성한다.

3.2 Weil Pairing

Weil Pairing은 타원곡선 이산대수 문제의 공격에 사용되어왔으며 3자 키 공유 시스템의 구성도 가능하다[9]. Weil Pairing은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinear map)이다. G가 유한체 F_q상에서 초특이 타원곡선 위의 점으로 이루어진 군(group)이라 하자. G의 위수(order)를 l로 표기하고, l/q^k-1을 만족하는 가장 작은 정수 k를 정의하자. 쌍선형 사상 $\hat{e}$는 다음과 같이 정의된다[14].

$$\hat{e} : G \times G \rightarrow F_{q^k}^*$$

이때, 쌍선형 사상은 다음과 같은 성질을 만족한다.

- $\hat{e}(P_1+P_2, Q)=\hat{e}(P_1, Q)\cdot\hat{e}(P_2, Q)$,
- $\hat{e}(P, Q_1+Q_2)=\hat{e}(P, Q_1)\cdot\hat{e}(P, Q_2)$
- $\hat{e}(aP, bQ)=\hat{e}(P, Q)^{ab}$, $a, b \in Z_q^*$

3.3 시스템 설정

본 논문에서 인증기관은 ID 기반 시스템에서 KGC 역할을 한다고 가정한다. 사용자는 인증기관에게 자신의 인증서 암호화에 필요한 공개키 생성 요청을 위해 안전한 채널로 자신의 ID를 전송한다.

- $H' : F_q^* \rightarrow \{0,1\}^*$: 키 유도 함수(key derivation function)
- $H : \{0,1\}^* \rightarrow G$: 해쉬함수(hash function)

표1. 프로토콜에 필요한 알고리즘

알고리즘	설 명
$h(...)$	일 방향 해쉬 함수
$Sign_X\{data\}$	X의 개인키를 사용하여 메시지 서명
$\{data\}_{K_{XY}}$	X와 Y의 세션키K를 사용하여 암호화

표2. 시스템 설정에 필요한 파라메터

파라메터	설 명
U, V	사용자, 상품/서비스 제공자
PG, CA	지불 게이트웨이, 인증기관
Z	$Z \in \{U, V, PG, CA\}$
w_Z	Z의 개인키
W_Z	Z의 공개키
K_Z	Z의 세션키
k_Z	Z의 보조 세션키
id_Z	Z의 신원
cid_Z	Z의 인증서용 신원
$Cert_Z$	서명 확인용 Z의 공개키 인증서
$CertChain(X, Y)$	X가 Y의 인증서를 검증할 수 있도록 생성된 인증서 체인
T_Z	Z에 의해 생성된 타임스탬프
ch_data	지불 명세서(상품 명칭과 수량, 가격 포함)
$card\_data$	신용카드 정보

표2는 공개키/개인키, 세션키 생성에 필요한 파라메터를 나타낸다. 인증기관은 비밀키 $s \in \{1, ..., l-1\}$와 난수 $p \in G$을 선택한 후, $P_{CA} = [s]P$를 계산한다. 그리고 (P, P_{CA})는 공개한다.

3.3.1 세션키 생성

U, PG 그리고 CA는 세션키를 공유하길 원한다고 정의한다. U는 CA에게 자신의 아이디를 보낸다. 인증기관은 사용자의 공개키 $W_U = H(id_U)$를 생성하고 개인키 $w_U = [s]W_U$ 를 생성한다. 지불 게이트웨이의 공개키/개인키도 같은 방법으로 인증기관에 의해 생성된다. 사용자, 지불 게이트웨이, 인증기관은 각각 개인키 역할을 하는 난수 $a, b, c \in Z_q^*$를 생성한다. 세션키 생성 프로토콜은 다음과 같다.

- $U \rightarrow PG : [a]P, [a]W_{CA}$; $U \rightarrow CA : [a]P, [a]W_{PG}$
- $PG \rightarrow U : [b]P, [b]W_{CA}$; $PG \rightarrow CA : [b]P, [b]W_U$
- $CA \rightarrow U : [c]P, [c]W_{PG}$; $CA \rightarrow PG : [c]P, [c]W_U$

사용자, 지불 게이트웨이, 그리고 인증기관은 아래와 같이 세션키를 계산한다.

$$K_U = \hat{e}([a](W_{PG} + W_{CA}), P_{CA}) \cdot \hat{e}(w_U, ([b]P + [c]P)) \cdot \hat{e}([b]W_{CA}, P_{CA}) \cdot \hat{e}([c]W_{PG}, P_{CA})$$

$$K_{PG} = \hat{e}([b](W_U + W_{CA}), P_{CA}) \cdot \hat{e}(w_{PG}, ([a]P + [c]P)) \cdot \hat{e}([a]W_{CA}, P_{CA}) \cdot \hat{e}([c]W_U, P_{CA})$$

$$K_{CA} = \hat{e}([c](W_U + W_{PG}), P_{CA}) \cdot \hat{e}(w_{CA}, ([a]P + [b]P)) \cdot \hat{e}([a]W_{PG}, P_{CA}) \cdot \hat{e}([b]W_U, P_{CA})$$

따라서, 공통 세션키는 키유도함수(key derivation function) H의 값이 된다.

$$K_{UPGCA} = K_U = K_{PG} = K_{CA} = \hat{e}([a](W_{PG} + W_{CA}) + [b](W_U + W_{CA}) + [c](W_U + W_{PG}), [s]P))$$

세션키는 세 개체의 W_U, W_{PG}, W_{CA}와 인증기관의 비밀키 s, 그리고 개인키 a, b, c 에 의해 결정된다.

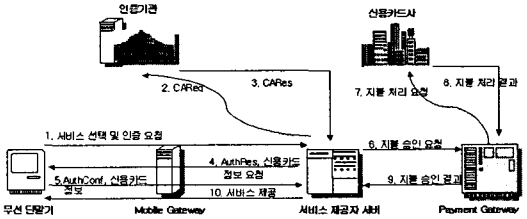

그림2. 제안하는 프로토콜 시스템의 구성도

3.3.2 보조세션키 생성

제안하는 프로토콜에서 사용자와 판매자는 두

개체만이 알고 있는 세션키가 필요하다. 인증과정에 온라인 인증기관이 참여하는 경우에는 판매자와 지불 게이트웨이 사이에도 보조 세션키가 필요하다. 이 각각의 경우, 두 개체를 각각 A, B로 하여 보조 세션키를 Weil Diffie-Hellman Assumption에 의해 생성한다[15].

A 개체의 공개키는 $W_A = H(id_A)$ 이고, 개인키는 $w_A = [s]W_A$ 이다. A, B는 일회용 개인키 a, b 를 생성하고 일회용 공개키 T_A, T_B 를 생성하여 교환한다.

표3. 키 교환 과정

A		B
a		b
$T_A = [a]P$	$\rightarrow$	T_A
T_B	$\leftarrow$	$T_B = [b]P$

A는 다음을 계산한다.

$k_A = \hat{e}([a]W_B, P_{CA}) \cdot \hat{e}(w_A, T_B)$

B도 다음을 계산한다.

$k_B = \hat{e}([b]W_A, P_{CA}) \cdot \hat{e}(w_B, T_A)$

다음에서 두 비밀키 k_A와 k_B가 같다는 것을 알 수 있고, 개체 A와 B는 비밀 세션키 k_{AB}를 공유할 수 있다.

$$
\begin{aligned}
k_A &= \hat{e}([a]W_B, P_{CA}) \cdot \hat{e}(w_A, T_B) \\
&= \hat{e}(W_B, P_{CA})^a \cdot \hat{e}(w_A, T_B) \\
&= \hat{e}(W_B, P)^{as} \cdot \hat{e}(W_A, P)^{bs} \\
&= \hat{e}(w_B, T_A) \cdot \hat{e}(W_A, [s]P)^b \\
&= \hat{e}(w_B, T_A) \cdot \hat{e}([b]W_A, [s]P) \\
&= \hat{e}([b]W_A, P_{CA}) \cdot \hat{e}(w_B, T_A) \\
&= k_B \\
\therefore\ k_{AB} &= k_A = k_B
\end{aligned}
$$

3.4 인증 과정에 온라인 인증기관이 참여하 지 않는 경우

사용자와 판매자가 인증서를 가지고 있고, 동일한 도메인에 존재하는 경우에 대한 프로토콜이다. 이 경우, U와 PG는 인증기관과의 세션키를 가지고 있다. U는 V의 신원 id_V, 선택한 상품에 대한 서비스 명칭, 수량, 가격이 포함된 정보 data, 그리고 난수 u를 생성하여 임시 공개키 $[u]P$를 생성한 후 V에게 전송한다.

V는 난수 r을 생성하고 U의 임시 공개키를 사용하여 U와의 보조 세션키 k_{UV}를 전송한다. 또한 지불 명세서 ch_data, 타임스탬프 T_V, 그리고 자신의 임시 공개키 $[v]P$를 전송한다.

메시지를 받은 U는 V의 공개키 $[v]P$에서 보조 세션키를 구한 후 해쉬값 $h(k_{UV}||r||id_V)$과 동일한지를 비교한다. 동일하면 인증 확인 메시지와 $Cert_U$를 전송한다. 이때 $[v]P$에 사용된 v는 V가 생성한 난수이다. 또한, 자신이 요청한 상품의 지불 명세서를 확인 한 후, 지불을 위한 신용카드 정보 $card_data$를 세션키로 암호화하여 V에게 전송한다.

V는 PG에게 지불 승인 요청을 위해 id_U, id_V, ch_data 를 PG와의 보조 세션키 k_{VP}로 암호화한 메시지와 U가 생성한 지불 정보 메시지를 다시 PG에게 전송한다. PG는 U와 V가 보낸 메시지를 확인하고 지불 명세서를 비교하여 동일하면 신용카드 정보 $card_data$를 사용하여 지불을 수행한다. 사용자의 신용카드 정보로 지불이 성공적으로 이루어지면 거래에 참

여한 참여자의 신원 id_U, id_V 와 지불이 수행된 시간 T_P, 지불 명세서 ch_data 의 해쉬값에 서명하여 V에게 전송하고 V를 통하여 U에게도 전송한다. 이 과정이 수행되면 U는 선택한 상품이나 서비스를 제공받게 된다.

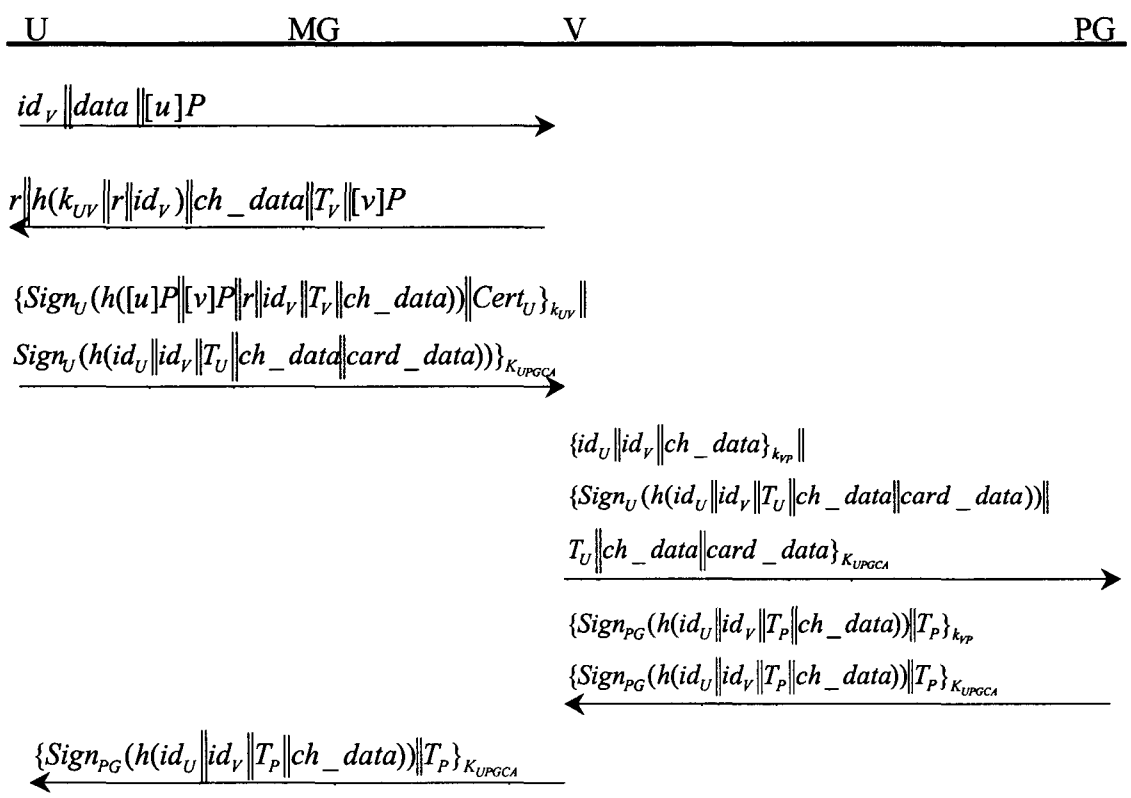

그림3. 인증과정에 온라인 인증기관이 참여하지 않는 경우의 인증 및 지불 프로토콜

3.5 인증 과정에 온라인 인증기관이 참여하는 경우

U가 인증서를 가지고 있지 않거나 V와 다른 도메인에 속하면 인증기관인 CA가 인증과정에 참여하여 프로토콜을 수행해야 한다. U, PG와 CA는 3.3.1에 의해 세션키를 생성한 후 지불을 수행하고 U와 V는 인증서 체인을 통해 서로의 인증서를 검증한다. 이 경우의 프로토콜은 그림4와 같다. U는 V와 연결하기 위해 자신의 신원 id_U를 세션키로 암호화하고, U의 CA의 신원 id_{U_CA}, 선택한 서비스 정보 $data$와 보조 세션키 생성에 필요한 임시 공개키 $[u]P$를 V에게 전송한다. V는 U가 전송한 메시지와 자신의 인증서 $Cert_V$를 온라인 인증기관인 CA에게 전송한다. CA는 V에게 받은 메시지에서 V의 신원을 확인하고 V가 U와 CA의 공개키를 확인할 수 있도록 $CertChain(V, U)$와 $CertChain(V, CA)$를 생성하여 V에게 전송한다. 이때, $CertChain(V, U)$는 세션키로 암호화하여 악의적인 VASP 재전송 공격을 막는다.

V는 난수 r을 생성한 후 U와의 보조 세션키 k_{UV}를 생성하여 지불 명세서와 인증서 체인 그리고 CA의 서명이 포함된 데이터를 U에게 전송한다. U는 $CertChain(U, V)$를 통해서 V의 인증서를 검증할 수 있다. 지불 명세서와 타임스탬프를 확인한 후 신용카드 정보가 포함되어 있는 메시지를 세션키로 암호화하여 전송한다. 이때 V가 $CertChain(U, V)$를 검증할 수 있도록 세션키 K_{UPGCA}를 U와 V의 세션키로 암호화하여 전송한

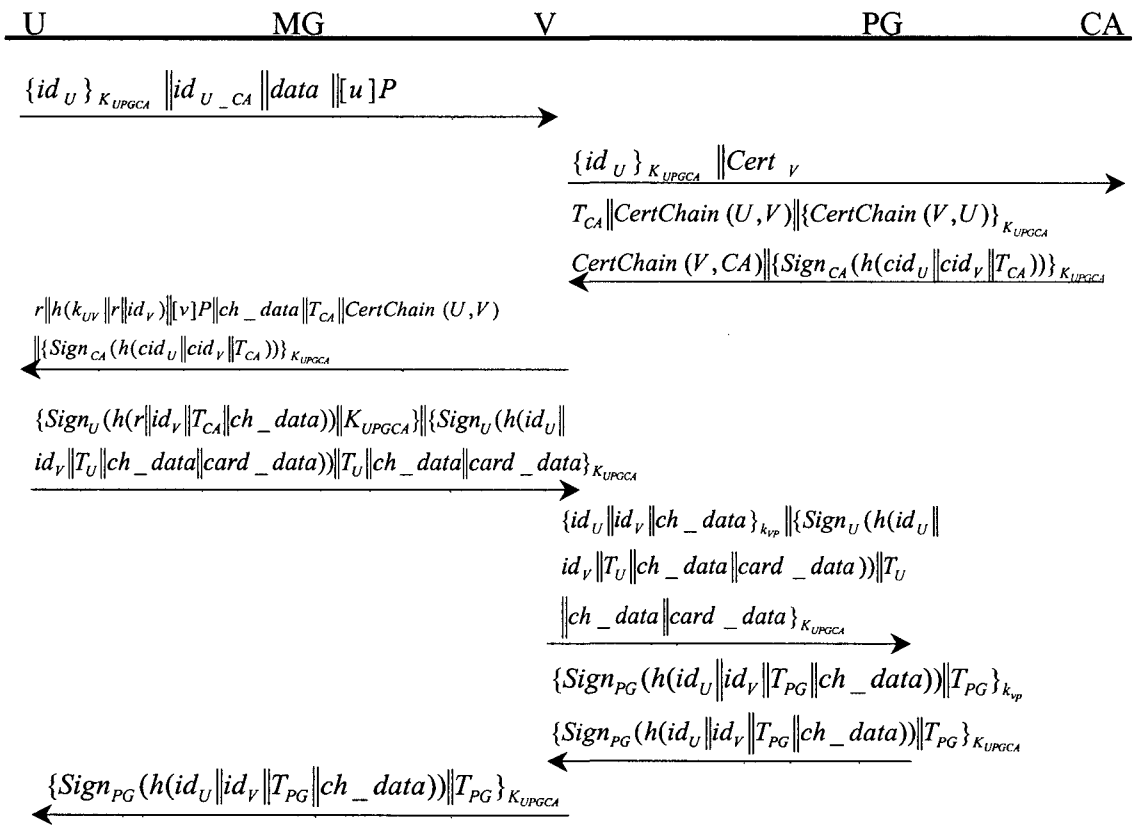

그림4. 인증과정에 온라인 인증기관이 참여하는 경우의 인증 및 지불 프로토콜

다. V는 U에게 받은 세션키 K_{UPGCA}로 $CertChain(U, V)$을 확인한다. 그리고 U가 서명한 메시지를 확인하고, PG에게 전송할 메시지 $\{id_U||id_V||ch\_data\}_{K_{VP}}$ 를 생성하여 신용카드 정보가 포함되어 있는 U가 서명한 메시지를 PG에게 함께 전송한다. PG는 U와 V 가 보낸 메시지를 확인하고 지불 명세서를 비교하여 동일하면 신용카드 정보 $card_data$를 사용하여 지불을 수행한다. 사용자의 신용카드 정보로 지불이 성공적으로 이루어지면 거래에 참여한 참여자의 신원 id_U, id_V 와 지불이 수행된 시간 T_{PG}, 지불 명세서 ch_data 의 해쉬값에 서명하여 V 에게 전송하고 V 를 통하여 U에게도 전송한다. 이 과정이 수행되면 U는 선택한 상품이나 서비스를 제공받게 된다.

IV. 안전성 및 성능 평가

제안한 신용카드 기반의 인증 및 키 교환 프로토콜이 무선 인터넷 환경에서 지불을 수행하기 위한 안전성에 대해 분석하고 알고리즘의 연산량과 통신량을 비교한다.

4.1 안전성 분석

- U의 신용카드 정보에 대한 안전성: U의 신용카드 정보는 PG와의 세션키로 암호화하

여 V는 신용카드 정보를 알 수 없다. $card_data$가 포함되어 있는 메시지에 id_U와 T_U를 첨가하여 신용카드 정보를 보호하고 $card_data$는 일정 기간 거래 후 신용카드사와 재 협약하기 때문에 신용카드 정보에 대한 안전성을 제공한다.

- V에 대한 키 확인과 인증: 그림4에서 세션키를 생성하여 $h(k_{UV}||r||id_V)$를 U에게 보내는 것은 V가 U에게 키 확인과 V의 함축적 키 인증과 개체 인증을 제공한다.
- U에 대한 키 확인과 인증: 그림3의 세 번째 과정에서 $Cert_U$를 보조 세션키 k_{UV}로 암호화하는 것은 키 확인을 제공한다. 또한, 해쉬함수에 $[u]P$ $||[v]P||r$ 의 첨가는 V에게 함축적 키 인증을 제공한다. 난수 r의 첨가는 U에 대한 개체 인증을 제공한다.
- 새로운 키 제공 : 세션키 K_{UPGCA}와 k_{UV}생성에 난수가 사용되기 때문에 세션키가 새로운 키(key freshness)임을 증명한다. 이는 이전에 사용되었던 세션키와 다르기 때문에 세션키 K_{UPGCA}와 k_{UV}를 알기 위한 code-book 공격에 안전하다.
- 근원지 대체 공격 방지: 그림4에서 V의 신원을 포함하는 것은 근원지 대체 공격(source-substitution attack)을 방지하기 위함이다.
- 악의적인 사용자의 경우: 타인의 신용카드 정보를 이용하거나 신용 불량자인 경우에 제안한 프로토콜은 다음과 같이 수행된다. V가 PG에게 악의적인 U의 신용카드 정보를 전송하고, PG가 신용카드사에게 지불 처리 요청을 하였을 때 신용카드사는 지불 처리 결과로 지불 처리 실패 메시지를 전송한다.
- 악의적인 서비스 제공자의 경우: V가 사용한 지불 정보를 다시 사용하려 하거나, U의 지불 금액보다 많은 금액을 요청할 때 악의적인 서비스 제공자의 경우에 속한다. 이 경우에 PG는 U가 생성한 메시지에 포함되어 있는 T_U를 확인하여 사용할 수 없는 데이터임을 알고 V에게 지불 처리 요청 실패 메시지를 전송한다. 또한 V가 거래 금액보다 많은 금액을 요청하였을 때는 PG가 V로부터 전송받은 메시지 중 U가 서명한 메시지와 V가 서명한 메시지를 비교함으로써 악의적인 서비스 제공자임을 알 수 있다.

4.2 성능 평가

표4는 SET, WPP, 제안한 프로토콜의 특성을 나타내고 있다. 무선 인터넷 환경에서 안전한 지불을 수행하기 위한 키 교환 알고리즘으로 전통적인 공개키 암호 기법에 의한 Diffie-Hellman 키 교환 대신 ID 기반 공개키 암호와 Weil Pairing을 이용한 Diffie-Hellman을 사용하여 보다 안전한 키 교환을 수행하였다. SET과 WPP는 인증 과정을 수행한 후 지불 과정을 수행하지만, 제안한 프로토콜은 인증 과정을 수행하면서 지불 정보를 전송함으로써 인증 과정과 지불 과정을 통합하였다. WPP는 WAP에만 제한적으로 사용되지만 제안한 프로토콜은 무선 인터넷 플랫폼에 독립적이며 SET과 같이 종단간 보안을 제공하지만 인증서를 받은 후 인증 과정을 수행하는 SET과는 달리 무선 인터넷의 이동성을 보장하기 위해 온라인 인증 기관이 제공하는 인증 체인을 사용한다. 또한 프로토콜 참여자만이 지불 정보를 볼 수 있어야 하기 때문에 제안한 프로토콜은 종단간 보안을 위해 상품/서비스 제공자와 안전한 세션을 생성한 후, 신용카드 정보를 PG와의 세션키를 사용해서 암호화하여 PG만이 지불 정보를 볼 수 있다. WPP의 WG 문제점을 극복하기 위해 유・무선 구간을 연결하는 역할만을 수행하는 MG를 사용하였다. 또한 유선구간은 인터넷에서 신용카드 지불을 위해 구축되어 있는 PG를 사용한다.

표4. 프로토콜의 특성 비교

	SET 프로토콜	WPP 프로토콜	제안한 프로토콜
키 교환 알고리즘	RSA/DES	RSA/Diffie-Hellman	ID 기반 공개키 암호 /Weil Diffie-Hellman
인증과 지불 통합 여부	×	×	○
지불 수행 체계	Payment Gateway	사용자와 서비스제공자의 은행	Payment Gateway
무선 인터넷 플랫폼	-	WAP	독립적
종단간 보안성	○	×	○
유무선 연결 수행 체계	-	WAP Gateway	Mobile Gateway

(○: 제공, ×: 제공하지 않음)

WPP와 제안한 프로토콜과의 성능 분석 결과는 표5와 표6에 나타나 있다. SET 프로토콜은 유선 환경에서 사용되므로 성능 분석 표에서는 제외하였다. 성능 분석은 무선 인터넷 환경에 많은 영향을 끼치는 통신량과 계산량을 비교하였다. 통신량은 전송되는 메시지 횟수이고, 계산량은 타원곡선상에서 세션키 생성 횟수를 계산하였다. WPP는 WAP 단말기와 서버가 안전하게 정보를 전송하기 위해 핸드쉐이크 프로토콜을 통해 암호 매개변수를 교환하고 세션키를 설정한다. 암호 매개변수를 교환하기 위해 WAP 단말기는 상품/서비스 제공자(상품/서비스 제공자측의 WG)와 4번, 사용자의 은행(사용자의 은행측의 WG)와 4번, application data 전송을 위해 각각 1번씩, 즉 10번의 메시지 교환을 수행한다. 또한 pre_master_secret와 공개키를 생성하기 위해 3번의 멱승을 수행한다[3,16]. WAP의 WTLS는 암호 매개변수를 교환할 때 많은 선택사항을 가지고 있다. 표5와 표6에서는 선택 사항에서 추가되는 멱승 횟수는 제외하였다. 표5는 제안한 프로토콜 중 온라인 인증기관이 인증 과정에 참여하는 경우와 WPP 프로토콜을 사용자 측면에서 비교하였고, 표6은 서비스 제공자 측면에서 비교하였다. 제안한 프로토콜과 WPP 프로토콜을 비교한 결과. 계산량에서 세션키 생성 횟수는 비슷하지만 연산법이 곱셈군에서 덧셈군으로 대치되었고, 통신량에서의 메시지 교환 횟수도 제안한 프로토콜에서 감소되었다. 따라서 무선 환경에 적합한 속도의 향상 및 안전성을 제공한다.

표5. 사용자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 프로토콜
메시지 교환 횟수	10	4
세션키 생성 횟수	3	2
세션키 생성 연산법	공개키 암호의 멱승(곱셈군)	타원곡선의 덧셈군

표6. 서비스 제공자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 프로토콜
메시지 교환 횟수	10	8
세션키 생성 횟수	3	2
세션키 생성 연산법	공개키 암호의 멱승(곱셈군)	타원곡선의 덧셈군

V. 결 론

WPP 프로토콜은 무선 인터넷 환경에서 신용카드 지불을 수행한다. 그러나 WPP 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용함으로써 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 본 논문에서는 MG와 타원곡선상의 Weil Pairing을 사용하여 AIP 프로토콜을 토대로 특정 무선 플랫폼에 독립적이며 사용자와 VASP간의 종단간 보안이 제공되는 지불 프로토콜을 제안하였다. 제안한 프로토콜은 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써 이동성이 많은 무선 단말기가 다른 도메인에 존재하는 서비스 제공자에게도 서비스를 받을 수 있다. 향후 신용카드 정보를 이용한 Mobile-Payment 설계 시 새로운 ID 기반 SignCryption 기법을 적용하여 효율성과 안전성을 높이는 방법을 연구할 것이다.

Reference

[1] i-mode, "DoCoMo i-mode", NTT, November 1999.

[2] Alan O.Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol version 3.0, Internet-Draft," 1996, http://home.netscape.com/eng/ssl3/.

[3] WAP Fourm, "Wireless Application Prot-

ocol Wireless Transport Layer Security Spectification version 18-FEB-2000,"2000
[4] WAP Fourm, "Wireless Application Protocol" WAP2.0, Technical White Paper, January 2002. T. Dierks, C. Allen, "The TLS Protocol," January 1999, http://www.ietf.org/rfc/rfc2246.txt.
[5] VISA & Mastercard, "SET Electronic Transaction Specification," 1997.
[6] J. Hall, S. Kilbank, M. Barbeau, and E. Kranakis, "WPP: A Secure Payment Protocol for Supporting Credit-card and Debit-card Transactions Over Wireless Networks," IEEE International Conference on Telecommunications(ICT), Bucharest, June, 2001.
[7] Eun-Kyeong Kwon; Yong-Gu Cho; Ki-Joon Chae, "Integrated transport layer security: end-to-end security model between WTLS and TLS, "Information Networking, 2001. Proceedings. 15th International Conference on, pp. 65-71, 2001.
[8] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems, " ESORICS, LNCS 1485,pp.277-293, 1998.
[9] K. M. Martin, B. Preneel, C. J. Mitchell, H. J. Hitz, G. Horn, A. Polickova, P.Howard, "Secure Billing for Mobile Information Services in UMTS," LNCS 1430, Springer-Verlag, IS$N May. 1998.
[10] A. Freier, P. Karlton, P. Kocher, "The SSL Protocol version 3.0," Internet Draft, Nov.1996.
[11] ACTS AC095, "ASPeCT Deliverable D20, Project final report and results of trials," Dec. 1998.
[12] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1997.
[13] Divya Nalla, and K.C.Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings" 2002.
[14] N.P.Smart, "An Identity based authenticated Key Agreement Protocol based on the Weil Pairing", Cryptology ePrint Archive, Report 2001/111,2001.http://eprint.iacr.org/.
[15] D.Boneh and M.Franklin. Identity-based encryption from the Weil Pairing. In Advances in Cryptology-CRYPTO2001, Springer-Verlag LNCS 2139, 213-229, 2001.
[16] T. Dierks, C. Allen, "The TLS Protocol version1.0," IETF RFC 2246,Jan.1996.

저자 소개

이현주(Hyun-Ju Lee)

1990년 2월 청주대학교 수학교육과 졸업(이학사)
1992년 2월 청주대학교 수학과 졸업(이학석사)
2000년 8월 청주대학교 수학과 졸업 (이학박사)
2001년-현재 충북대학교 대학원 전자계산학과 박사과정 수료
※ 관심분야 : 정보보안, 사용자 인증, 스마트카드, 전자지불

이충세(Chung-Sei Rhee)

1989년 University of South Carolina, 전산학 박사University of North Dakota 전산학과 조교수
1991년- 현재 : 충북대학교 전기전자 및 컴퓨터공학부 교수
※ 관심분야 : 결함허용, 알고리즘 및 전문가 시스템, 정보보안