무선인터넷에서의 안전한 신용카드기반의 소액 지불 프로토콜

김석매, 이영진, 이현주, 이충세
충북대학교 컴퓨터과학과
e-mail:lyz2003@just.chungbuk.ac.kr

Secure Credit Card based Micro-Payment Protocol in Wireless Internet

Shi-Mei JIN, Yong-Zhen Li, Hyun-Ju Lee,
Chung-se Rhee
Dept of Computer Science, Chungbuk National Universit

요 약

무선 환경에서의 전자상거래가 빠르게 성장함에 따라 종단간 보안이 필요하다. 기존 WTLS를 사용하는 WPP 프로토콜에서는 종단간 사용자 안전성을 보장하고 있지 않다. 이 논문에서는 AIP프로토콜에서 사용자와 서비스 제공자간에 종단간 안전성이 제공되는 무선 인터넷 플랫폼에 독립적인 소액지불 프로토콜을 제안한다. 또한 인증기관이 인증과정에 참여할 경우 ID 기반 공개키 암호 시스템을 적용한 세션키를 생성하여 제안 프로토콜의 안전성 및 효율성을 분석한다

1. 서론

최근 정보통신기술의 급속한 발달로 무선인터넷을 이용한 전자상거래 사용자가 폭발적으로 증가되고 있다. 원래의 유선에서 유-무선 혼합 환경으로 변화함에 따라 보안상의 많은 문제점이 제시도고 있다. 무선 환경에서의 전자상거래는 많은 편리함을 제공하긴 하지만 무선이 원래 신뢰도가 떨어지는 매체이기 때문에 새로운 문제들이 발생한다. 누군가가 공중을 오가는 메시지는 몰래 도청할 수도 있다. 즉 종단간 보안(end-toend security)이 필수적이다.

현재 유선환경에서 주로 사용되는 신용카드 기반 지불프로토콜은 SET(Secure Electronic Transaction)이고 이 프로토콜은 저장공간, 계산량 및 통신량의 제약성으로 무선 환경 사용에는 적합하지 않다[1]. 무선 인터넷에서는 주로 사용하는 신용카드기반의 지불 프로토콜은 WPP(Wireless Payment Protocol)와 ASPeCT에서는 제안한 인증과 지불을 위한 AIP(Authentication and Initialization of Payment)프로토콜이다.[1,2,3].

이 논문에서는 ID 기반 공개키 암호 시스템을 적용한 Weil Pairing 기법을 사용하여 AIP프로토콜에서 종단간 보안이 제공되는 새로운 지불 프로토콜을 제안한다. 또한 온라인 인증기관이 참여하는 경우에 기존 프로토콜과 제안프로토콜에 대한 비교분석을 통하여 제안 프로토콜의 안전성 및 효율성을 입증한다.

2. 관련연구

2.1 WPP 프로토콜

WPP 프로토콜은 SET을 기초하여 무선 인터넷에서 신용카드 지불을 할 수 있도록 제안된 지불 프로토콜이다. WPP는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP의 WTLS를 사용하였다. WPP는 사용자와 사용자의 은행(신용카드사),서비스제공자(상점),서비스 제공자의 은행으로 구성된며 사용자와 은행, 서비스제공자를 연결해주는 WG(WAP Gateway)가 필요하다. 그림1은 WPP의 구성도 및 지불 흐름도를 나타낸 것으로써 WAP 프로

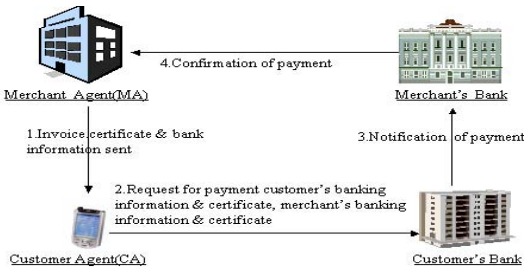

그림 1 WPP의 구성도 및 지불 흐름도

토콜 스택을 인터넷 프로토콜로 변환하는 WG를 생

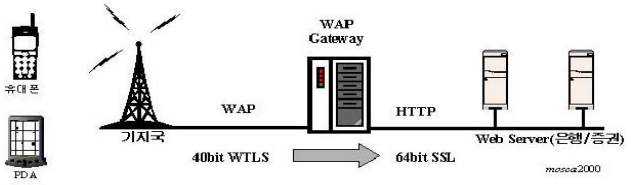

그림 2 WAP에서 WTLS-SSL프로토콜 변환

략하였다. 그림2에서 보는 바와 같이 WG에서는 WTLS-SSL프로토콜 변환 시 암호화된 메시지가 복호화되어 원본 메시지가 노출될 위험성을 가지고 있어 종단간 보안을 제공하지 못한다는 단점을 가지고 있다. 또한 WTLS를 사용하는 WAP 프로토콜 스택은 인터넷 프로토콜과 서로 다르기 때문에 WG에서 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 메시지가 노출되는 위험성을 가지고 있다[1,2].

2.2 AIP 프로토콜

ASPeCT의 AIP 프로토콜은 무선 이동 통신 환경에서 사용자와 VASP간에 인증과 지불 초기화를 수행 가능하게 해주는 프로토콜이다. AIP프로토콜에서 종단간 보안을 제공하려면 다음과 같은 조건은 만족시켜야 한다.

① 사용자와 VASP간의 명확한 상호인증
② 사용자와 VASP간의 인증된 세션키의 성립
③ 사용자와 VASP가의 상호 키 동의
④ 상호간의 새로운 키의 확신
⑤ VASP에게 전송되는 사용자 데이터의 부인방지
⑥ VASP인터페이스에서의 사용자 신원의 기밀성

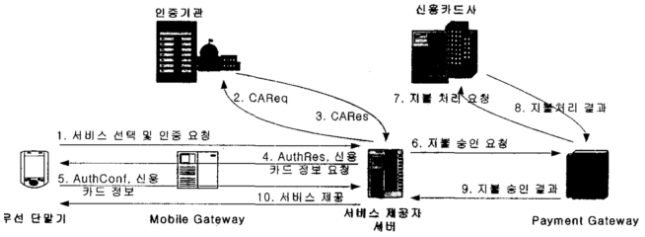

그림 3 제안 프로토콜을 위한 시스템 구성도 및 데이터 흐름도

AIP프로토콜은 온라인 인증기관이 참여여부에 따라 두 가지로 구분된다. 그림3 기존 인증기관이 참여한 AIP프로토콜 사용을 위한 시스템 구성도 및 데이터 흐름도이다. 여기서 사용자는 VASP와 Diffie-Hellman 키 설정 기법을 사용하여 세션키를 생성하고 사용자와 인증기관은 Elgamal기법을 사용하여 세션키를 만든다. 생성된 세션키로 인증과정을 거치고 지불을 위한 초기화 정보를 교환한다[7,8].

2.3 ID 기반 공개키 암호 시스템 및 Weil Pairing

2.3.1 ID 기반 공개키 암호 시스템

Shamir에 의해 제안된 이 개념은 원래 e-mail 시스템에서 인증 관리를 단순화하기 위한 것이었다. Alice가 Bob(bob@hotmail.com)에게 메일를 보낼 때 공개키 스트링 bob@hotmail.com을 사용하여 메시지를 암호화한다. Alice는 Bob의 공개키 인증서를 획득할 필요 없지만 Bob는 메시지를 복호화 하기 위해 KGC(Key Generation Center)에게 자신을 인증한 후 자신의 개인키를 얻어야 한다. 기존의 e-mail 구조와 달리, ID-based 시스템에서는 신뢰할 수 있는 KGC가 필요하다. KGC에서는 각 개체의 ID 기반 공개키를 사용하여 개인키를 생성한다[4].

2.3.2 Weil Pairing

Weil pariring은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinearmap)이다. G가 유한체 F_q 상에서 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[5].

쌍선형 사상 $\hat{e}: G\times G\rightarrow F_{q^k}^*$의 함수 e는 다음과 같은 조건을 만족할 때 Weil Pairing으로 정의 된다

임이의 $P, P_1, P_2, Q, Q_1, Q_2 \in G$와 $a, b \in Z/l$일때

$$\hat{e}(P_1+P_2, Q)=\hat{e}(P_1, Q)\cdot\hat{e}(P_2, Q)$$

$$\hat{e}(P, Q_1+Q_2)=\hat{e}(P, Q_1)\cdot\hat{e}(P, Q_2)$$

또는 $\hat{e}(aP, bQ)=\hat{e}(P, Q)^{ab}, a, b \in Z_q^*$

Weil Pairing의 기법을 이용한 ID기반 암호화 및 서명은 그의 독특한 효율성으로 최근에 연구가 활발히 진행되고 있다[5].

3. 제안하는 소액 지불 프로토콜

이 논문에서는 AIP 프로토콜을 이용하여 인증과정에 온라인 인증기관이 참여한 ID기반 소액 지불을 안전하게 수행할 수 있는 프로토콜을 제안한다.

3.1 세션키 생성

이 논문에서 인증기관는 ID 기반 시스템에 KGC 역할을 한다고 가정한다. 사용자는 인증기관에게 자

신의 인증서 암호화에 필요한 공개키 생성 요청을 위해 안전한 채널로 자신의 ID를 전송한다.

표1. 시스템 설정에 필요한 파라메터

데이터 요소	설명
U, V	사용자, 서비스 제공자
PG, CA	지불게이트웨이, 인증기관
id_X	X의 신원
cid_X	X의 인증서용 신원
W_X	X의 공개키
w_X	X의 개인키
k_{XY}	X, Y의 보조세션키
C_X	X의 인증서
K_{XY}	X, Y의 세션키
$CertU$	서명 확인 U의 공개키 인증서
$CertV$	세션키 생생용 V의 공개키 인증서
$CertChain(X, Y)$	X가 Y의 인증서를 검증용 인증서 체인
T_X	X에 의해 생성된 타임스템프
ch_data	지불 명세서를 의미하며, 상품이나 서비스 명칭과 수량, 가격이 포함된다.
$card\_data$	신용카드 정보를 의미한다.
$h(\dots)$	일방향 해쉬 함수
$Sign_X\{data\}$	X의 개인키를 사용하여 메시지 서명

표1은 공개키, 개인키, 세션키 생성에 필요한 파라미터를 나타낸다. 인증기관는 비밀키 $s \in \{1, \cdots l-1\}$와 난수 $p \in G$을 선택한 후 $P_C = [s]P$를 계산한다. 그리고 (P, P_C)는 공개한다. 사용자, 지불게이트웨이, 그리고 인증기관은 세셜키를 공유하길 원한다고 정의한다. 사용자는 인증기관에게 자신의 ID를 보낸다. 인증기관은 사용자의 공개키 $W_U = H(U_{ID})$를 생선하고 개인키 $w_U = [s]W_U$를 생성한다. 지불 게이트웨이의 공개키/개인키도 같은 방법으로 인증기관에 의해 생성된다. 사용자, 지불게이트웨이, 인증기관은 각각 개인키 역할을 하는 난수 $a, b, c \in Z_q^*$를 생성한다. 세션키 생성 프로토콜은 다음과 같다.

- $U \rightarrow PG, CA : [a]P_c$
- $PG \rightarrow U, CA : [b]P_c$
- $CA \rightarrow PG, PG : [c]P_c$

사용자는 세션키를 계산한다. 지불게이트웨이와 인증기관도 동일한 방법으로 세션키를 생성한다.

$$k_U = \hat{e}(w_U, P) \cdot \hat{e}(W_{PG}, [b]P_C) \cdot \hat{e}(W_{CA}, [c]P_C)$$
$$= \hat{e}([a]W_V + [b]W_{PG} + [c]W_{CA}, [s]P)$$

따라서 공통 세션키는 다음과 같다.

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

3.2 인증과정에 온라인 인증기관이 참여하는 경우

인증 과정에 온라인 인증기관이 참여 시 사용자와 서비스제공자 그리고 서비스 제공자와 지불게이트웨이사이에 두 개체만이 알고 있는 보조 세션키 k_{XY}가 필요하다. 이 경우에는 Diffie-Hellman Assumption에 의해 세션키를 생성한다[6].

U가 인증서를 가지고 있지 않거나 V와 다른 도메인에 속하면 인증기관인 CA가 인증과정에 참여하여 프로토콜을 수행해야 한다.

1) 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.
$\{id_U\}_{K_{UPGCA}} \mid id_{U-CA} \mid data \mid [u]P$
2) V는 U가 전송한 메시지와 자신의 인증서 $Cert_V$를 온라인 인증기관인 CA에게 전송한다.
$\{id_U\}_{K_{UPGCA}} \mid Cert_V$
3) 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.
$T_{CA} \mid CertChain(U, V) \mid \{CertChain(V, U)\}_{K_{UPGCA}} \mid$
$CertChain(V, CA) \mid \{Sign_{CA}(h(cid_U \mid cid_V \mid T_{CA}))\}_{K_{UPGCA}}$
4) 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.
$r \mid h(k_{UV} \mid r \mid id_V) \mid [v]P \mid ch\_data \mid T_{CA} \mid$
$CertChain(U, V) \mid \{Sign_{CA}(h(cid_U \mid cid_V \mid T_{CA}))\}_{K_{UPGCA}}$
5) U는 $CertChain(U, V)$를 통해서 V의 인증서를 검증할 수 있다. 지불 명세서와 타임스탬프를 확인한 후 신용카드 정보가 포함되어 있는 메시지를 세션키로 암호화하여 전송한다.
$\{Sign_U(h(r \mid id_V \mid T_{CA} \mid ch\_data)) \mid K_{UPGCA}\}_{k_{UV}} \mid$
$\{Sign_U(h(id_U \mid id_V \mid T_U \mid ch\_data \mid card\_data))$
$\mid T_U \mid ch\_data \mid card\_data\}_{K_{UPGCA}}$
6) 이때 V가 $CertChain(U, V)$를 검증할 수 있도록 세션키 K_{UPGCA}를 U와 V의 세션키로 암호화하여 전송한다.
$\{id_U \mid id_V \mid ch\_data\}_{k_{VPG}} \mid \{Sign_U(h(id_U \mid id_V \mid T_U \mid$
$ch\_data \mid card\_data)) \mid T_U \mid ch\_data \mid card\_data\}_{K_{UPGCA}}$
7) V는 U에게서 받은 세션키 K_{UPGCA}로 $CertChain(U, V)$을 확인한다. 그리고 U가 서명한 메시지를 확인하고, PG에게 전송할 메시지 $\{id_U \mid id_V \mid ch_data\}_{k_{VPG}}$를 생성하여 신용카드 정보가 포함되어 있는 U가 서명한 메시지를 PG에게 함께 전송한다.
$\{Sign_{PG}(h(id_U \mid id_V \mid T_{PG} \mid ch\_data)) \mid T_{PG}\}_{k_{VPG}}$
8) PG는 U와 V가 보낸 메시지를 확인하고 지불 명세서를 비교하여 동일하면 신용카드 정보 $card_data$를 사용하여 지불을 수행한다. 사용자

의 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.

$$\{Sign_{PG}(h(id_U \mid id_V \mid T_{PG} \mid ch\_data)) \mid T_{PG}\}_{K_{UPGCA}}$$

$$\{Sign_{PG}(h(id_U \mid id_V \mid T_{PG} \mid ch\_data)) \mid T_{PG}\}_{K_{UPGCA}}$$

4. 안전성 및 효율성 분 석

4.1 안전성 분석

- V에 대한 키 확인과 인증: 제안한 프로토콜에서 세션키를 생성하여 $h(k_{UV} \mid r \mid id_V)$를 U에게 보내는 것은 V가 U에게 키 확인과 V의 함축적 키 인증과 개체 인증을 제공한다.
- U에 대한 키 확인과 인증: 세 번째 과정에서 $Cert_U$를 보조 세션키 k_{UV} 로 암호화하는 것은 키 확인을 제공한다. 또한, 해쉬함수에 $[u]P \mid [v]P \mid r$ 의 첨가는 V에게 함축적 키 인증을 제공한다. 난수 r의 첨가는 U에 대한 개체 인증을 제공한다.
- U의 신용카드 정보에 대한 안전성: U의 신용카드 정보는 PG와의 세션키로 암호화하여 V는 신용카드 정보를 알 수 없다. $card_data$가 포함되어 있는 메시지에 id_U와 T_U를 첨가하여 신용카드 정보를 보호한다. $card_data$는 일정 기간 거래 후 신용카드사와 재 협약한다.

4.2 성능 평가

WPP와 제안한 프로토콜과의 성능 분석 결과는 표2에 나타나있다. 성능 분석은 무선 인터넷 환경에 많은 영향을 끼치는 통신량과 계산량을 비교하였다.

표2. 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

통신량은 전송되는 메시지 횟수이고, 계산량은 ID기반 공개키 암호에서 세션키 생성 횟수를 계산하였다. 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.

5. 결 론

WPP 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용함으로써 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 이 논문에서는 ID 기반 공개키 암호를 적용한 Weil Pairing을 사용하여 AIP 프로토콜을 토대로 종단간 보안이 제공되는 특정 무선 플랫폼에 독립적인 지불 프로토콜을 제안하였다. 이 제안한 프로토콜은 사용자와 서비스 제공자간의 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써 다른 도메인에 존재하는 서비스 제공자에게서도 효율적이고 안전한 서비스를 받을 수 있다.

참고문헌

[1] 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.

[2] WAP Fourm, "Wireless Application Protocol Wireless Transport Layer Security Spectification version 18-FEB-2000,"2000

[3] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems, " ESORICS, LNCS 1485,pp.277-293, 1998.

[4] Divya Nalla, and K.C.Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings" 2002.

[5] 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/.

[6] D.Boneh and M.Franklin. "Identity-based encryption from the Weil Pairing". In Advances in Cryptology-CRYPTO2001, Springer-Verlag LNCS 2139, 213-229, 2000

[7] W. Diffie, M. Hellman, "New Directions in Cryptography" IEEE Transactions on Informations Theory, Vol, IT-22, No 6, pp.472-492, Nov,1976.

[8] A. Menezes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography" CRC Press, Boca Raton,1997