이동 통신 시스템에서의 종단간 인증 및 지불 프로토콜

김선형[0], 김태윤
고려대학교 컴퓨터학과
{shaklim[0], tykim}@netlab.korea.ac.kr

End-to-End Authentication and Payment Protocol in Mobile Telecommunication System

Sun-Hyoung Kim[0], Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

UMTS와 같은 제 3세대 이동 통신 시스템에서 공개키 기반 구조의 이용이 가능해짐에 따라 공개키 인증서를 획득한 각 이동 단말들 사이의 암호 통신에 대한 연구가 활발해지고 있다. 본 논문에서는 이동 단말기를 소유한 사용자와 디지털 정보 서비스를 운영하는 VASP 사이에서의 인증과 지불에 관련된 메커니즘을 제안한다. 이동 사용자는 브로커로부터 획득한 공개키 인증서를 사용하여 다른 도메인에서도 온라인 TTP(Trusted Third Party)의 통신을 거치지 않고도 효율적인 인증 서비스 및 디지털 정보 서비스를 받을 수 있다. 본 논문은 사용자 단말기의 제한된 성능과 이동 통신 환경이라는 제약적인 조건을 고려하여 이에 적합한 소액지불 프로토콜을 제시한다.

1. 서론

UMTS(Universal Mobile Telecommunications System)[1]와 같은 제 3세대 이동 통신 시스템에서는 GSM(Global System for Mobile Communications)과 같은 제 2세대 이동 통신 시스템에서 제공되지 못했던 공개키 기반 구조(PKI; Public Key Infrastructure)의 이용이 가능하게 되었다. 제 3세대 이동 통신 환경에는 디지털 서비스를 제공하는 수많은 VASP(Value-Added Service Provider)들이 존재한다. 이동 단말기를 소유한 사용자는 VASP들로부터 시간과 장소에 구애받지 않고 원하는 서비스를 제공받을 수 있다.

이러한 제 3세대 무선 인터넷 기반의 전자상거래에서 공개키 암호 시스템을 제공하기 위해서는 사용자의 효율적인 이동성이 보장받을 수 있도록 이동 단말기의 제한된 성능과 저장 공간이 고려되어야 한다.

ACTS 프로젝트인 ASPeCT(Advanced Security for Personal Communications Technologies)에서 개발된 AIP(Authentication and Initialisation of Payments) 프로토콜[2]은 제 3세대 이동 통신 시스템에서 공개키 암호 시스템을 기반으로 사용자와 VASP간의 인증과 지불에 관련된 메커니즘을 제시하고 있다.

AIP 프로토콜은 사용자가 온라인 TTP를 거치지 않고, 자신이 생성한 지불 정보를 VASP에게 사용함으로써 이동 통신 시스템에서의 적절한 소액지불 기법을 제공하고 있지만 지불 정보들이 다른 VASP와 거래할 때마다 새롭게 생성되어야 하는 문제점이 있다.

본 논문에서는 이러한 점을 개선하여 제 3세대 이동 통신 시스템에 적합한 소액지불 프로토콜을 제안한다. 제안한 프로토콜은 공개키 암호 시스템을 사용하는 PayWord 기법[3]을 기반으로 하여 이동 사용자가 한 번 생성한 지불 정보를 여러 VASP에게 사용할 수 있는 효율적인 방법을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 ASPeCT에서 개발된 AIP 프로토콜에 대하여 살펴본다. 3장에서는 본 논문에서 제안하는 지불 프로토콜에 대하여 설명한다. 4장에서는 제안한 프로토콜에 대한 안전성을 분석하고, AIP 프로토콜과의 효율성을 비교한다. 5장에서 결론을 맺고 향후 연구 과제를 제시한다.

2. AIP 프로토콜

AIP 프로토콜은 사용자와 VASP간의 상호 인증과 세션키 설정을 위한 단계와 Pederson[4]의 "tick"을 사용하는 지불 단계로 구분된다. 표 1은 본 논문의 프로토콜에 사용되는 기호를 나타낸다.

표 1. 프로토콜에 사용되는 기호

기호	설명
U, V, B	이동 사용자, VASP, 브로커
id_X	참여자 X의 신원
g^u	사용자의 키 설정용 공개키
r_X	X에 의해 생성된 난수
TS_X	X가 생성한 타임스탬프
PK_U	사용자의 공인된 서명 검증 공개키
SK_U	사용자의 비밀 서명키
$h(x)$	x에 대하여 일방향 해수 함수를 적용
$\{M\}_K$	메시지 M을 키 K를 사용하여 암호화
$Sig_X\{M\}$	메시지 M을 X가 서명

U는 VASP와의 통신을 개시하기 위해 난수 u를 생성하고 g^u를 계산하여 이를 자신의 인증기관 신원인 id_{CA}와 함께 V에게 전송한다.

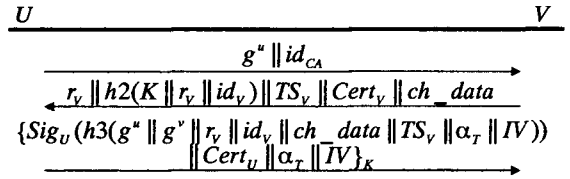

그림 1. AIP 프로토콜

메시지를 수신한 V는 난수 r_V를 생성하고, U와 비밀 세션키 $K = h1(g^{uv} \| r)$을 계산한다. 그런 후에 $CertV$와 지불 관련 정보 ch_data, TS_V, 난수 r_V와 id_V를 K와 함께 해쉬 함수를 수행하고 이를 전송한다. 이로써 U는 V가 K를 수립하고 있음을 알게 된다.

두 번째 메시지를 전달받은 U는 V의 인증서 $CertV$를 검증하고 V와 동일한 K를 계산한다. 그런 후에 ch_data, g^u, g^v, r을 idV와 TS_V, α_T, 지불 초기화 벡터 IV를 함께 서명한 후 K로 암호화하여 V에게 전송한다.

마지막 메시지를 수신한 V는 U의 인증서를 이용하여 서명을 검증하고 지불 관련 요소을 얻는다. 검증이 완료되면 V는 U에게 서비스를 제공한다. U는 제공받은 서비스에 대하여 tick 지불 프로토콜을 사용하여 지불한다.

3. 이동 통신 서비스를 위한 지불 프로토콜

본 논문에서는 제안하는 시스템은 기본적으로 이동 사용자, VASP, 그리고 브로커로 구성되어 있다. 이들은 다음과 같은 단계를 거쳐 이동 통신 시스템에서의 전자상거래를 실현한다.

- 인증서 발급 단계 : 이동 사용자와 브로커
- 지불/정보 교환 단계 : 이동 사용자와 VASP
- 결제 단계 : VASP와 브로커

3.1 인증서 발급 단계

U는 키 설정 공개키 g^u, 서명 관련 키 쌍인 PK_U, SK_U를 생성하여 B에게 상호 인증된 안전한 채널로 전송한다. B는 U에게 지불 생성의 권한을 부여하는 인증서 $PayCert$를 발급한다.

$$PayCert = \{Sig_U(h(id_B \| TN_U \| g^u \| PK_U)) \| id_B \| TN_U \| TS_B \| g^u \| PK_U\}$$

B는 U와 수립하고 있는 비밀 세션키 L을 이용하여 $TN_U = h(L \| r_B \| id_V)$를 계산하고 아래와 같이 임의의 T_N을 선택하여 $i = N-1, \ldots, 0$에 대한 해쉬 체인을 수행한다. 이와 같이 생성된 $PayRoot$는 U가 생성한 지불되지 않은 첫 번째 해쉬 체인 값과 연동하여 root 값으로 사용함으로써 $PayRoot$의 수 만큼 다중 지불을 할 수 있게 한다.

$$T_i = h(T_{i+1}, TN_U)$$

3.2 지불/정보 교환 단계

U는 B로부터 $PayCert$를 발급받고 이를 VASP에게 전송하여 정보 서비스의 구매 의사를 밝힌다. V는 사용자와의 비밀 세션키 $K = h(g^{uv} \| r_V)$를 계산하고 r_V, K, id_V를 해쉬 함수로 처리하여 이를 TS_V와 공개키 인증서 $Cert_V$와 함께 U에게 전송한다.

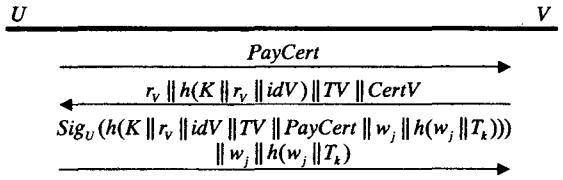

그림 2. 제안하는 지불 프로토콜

메시지를 수신한 U는 V의 인증서를 검증하고 V와의 비밀 세션키 K를 계산한다. U가 이전까지 거래한 $k-1$

번째 V에게 지불한 전자 화폐가 w_{j-1}이라고 가정하면 현재 거래 중인 k 번째 V와의 거래에서 지불되지 않은 첫 번째 해쉬 값인 w_j가 새로운 root 값으로 설정된다. *PayRoot*와 해쉬 함수를 수행한 $h(w_j \| T_k)$는 w_j가 k 번째 VASP에게 사용되는 root 값임을 나타낸다. U는 이러한 지불 요소들과 *PayCert*, r_V, K, id_V가 포함된 메시지를 비밀 서명키 SK_U로 서명하여 V에게 전송한다.

메시지를 전달받은 V는 *PayCert*를 검증하고, PK_U로 U의 서명을 검증하여 이후에 U가 지불할 전자 화폐에 대한 정당성을 확보하고, 해쉬 함수를 통해 이를 인증한다.

3.3 결제 단계

V는 마지막 지불 값인 $P_{j+l}=(w_{j+l}, j+l)$과 *PayCert*, w_j, $h(w_j \| T_k)$를 저장하고 결제 단계에서 브로커에 이를 제출하여 지불 요구한다.

4. 성능 평가

4.1 안전성 평가

- 상호 인증 : U에게 전송되는 $h(K \| r_V \| id_V)$는 V에 대한 함축적 키 인증(implicit key authentication)과 개체 인증(entity authentication)을 제공한다[5].
- 기밀성 : 사용자와 VASP 사이에 수립된 비밀 세션 키는 이들 사이에 교환되는 통신 메시지에 대한 기밀성을 보장한다.
- 부인 방지 : 사용자는 공개키 인증서에 자신의 서명을 증명할 수 있는 공개키 PK_U를 삽입하고 이를 전자 화폐의 root 값과 함께 전송하기 때문에 사용자는 제공받은 서비스에 대한 부인을 할 수 없다.
- 익명성 : *PayCert*의 TN_U는 사용자의 익명성을 제공한다. 이는 브로커만이 알고 있기 때문에 제 3자가 이를 획득한다 할지라도 사용자의 신원을 확인할 수 없다. VASP는 단지 PK_U로 사용자의 서명을 검증할 뿐이다.
- 이중 지불 탐지 :사용자가 생성하는 전자 화폐의 root 값으로서 w_j가 사용되며 이는 거래 중인 VASP에 대한 *PayRoot*와 연동되어 있기 때문에 사용자가 이를 이중으로 지불하게 된다면 브로커가 이를 탐지할 수 있다.
- 위조 방지 : 사용자가 생성하는 전자 화폐는 오직 브로커만이 생성할 수 있는 *PayCert*로부터 인증받기 때문에 이를 위조하는 것이 불가능하다.

4.2 효율성 평가

표 2는 제시된 프로토콜들의 사용자와 VASP간에 수행되는 지수 연산의 횟수를 측정한 것이다. 제안한 프로토콜은 *PayCert*를 사용하므로 키 설정 공개키 g^{α}에 대한 계산이 필요하지 않으며 프로토콜에서 V에게 마지막으로 전송되는 메시지를 암호화할 필요가 없으므로 이에 대한 공개키 암호화/복호화 연산이 한 번씩 줄어든다.

표 2. 제시된 프로토콜들의 계산량 비교

구분	제안한 프로토콜		계산한 프로토콜	
연산	U	V	U	V
사전 계산	1	0	0	0
온라인 계산	1	1	1	1
공개키 암호화	1	0	0	0
공개키 복호화	0	1	0	0
서명 생성	1	0	1	0
검증	1	2	1	2

5. 결론 및 향후 연구 과제

본 논문에서는 이동 통신 시스템에서 종단간의 상호 인증과 지불을 수행할 수 있는 프로토콜을 제안하였다. 본 연구는 대표적인 소액지불 프로토콜 중의 하나인 PayWord 시스템을 이동 통신 환경에 적합하도록 설계하였으며, 한 번 생성된 해쉬 체인이 하나의 VASP에게만 지불되었던 문제점을 해결한 효율적인 지불 메커니즘을 제안하고 있다.

향후에는 각 통신 개체들이 수립하고 있는 키의 관리 문제와 적법한 절차를 거치는 키 복구 시스템에 관한 연구가 이루어져야 할 것이다.

참고 문헌

[1] UMTS Forum, "A Regulatory Framework for UMTS," Report No.1, 1997.

[2] ACTS AC095, ASPeCT Deliverable D20, Project final report and results of trials, Dec. 1998.

[3] R.Rivest, A.Shamir, "PayWord and MicroMint: two simple micropayment schemes," LNCS, Vol.1189, pp.69-87 Springer-Verlag, 1996.

[4] T.P.Pederson, "Electronic payments of small amounts," Security Protocols, LNCS Vol.1351, pp.59-68, Springer-Verlag, 1997.

[5] G.Horn, B.Preneel, "Authentication and payment in future mobiel systems," In Computer Security - ESORICS '98, LNCS, Vol.1485, pp.277-293, 1998.