임시 이동 사용자 인증서에 기반한 효율적인 인증 기법

이병래*, 고찬**, 김태윤*
*고려대학교 컴퓨터학과
**서울 산업대학교 전자계산학과
brlee@netlab.korea.ac.kr

Efficient Authentication Scheme based on Temporary Mobile User Certificate

Byung-Rae Lee*, Chan Koh**, Tai-Yun Kim*
*Dept. of Computer Science & Engineering, Korea University.
**Dept. of Computer Science, Seoul National Univ. of Technology

요 약

본 논문에서는 미래 이동 통신 환경에서의 공개키 암호시스템에 기반한 VASP 와의 효율적인 상호 인증과 키 교환 프로토콜을 제안한다. 제안된 프로토콜은 임시적으로 생성한 서명용 비밀키에 대한 인증서인 임시 이동 사용자 인증서를 기반으로 한다. 본 논문에서는 이동 통신 환경에 임시 이동 사용자 인증서(Temporary Mobile User Certificate)를 도입하기 위하여 새로운 등록 프로토콜을 제시하였으며 제안된 임시 이동 사용자 인증서를 이용하여 VASP 와의 효율적인 인증 및 키 교환 프로토콜을 제안한다. 또한 임시 이동 사용자 인증서는 이동 사용자의 익명 서비스 사용을 보장할 수 있다.

1. 서론

UMTS[1]와 같은 제 3 세대 이동 통신 환경으로 나아가면서 이동 사용자는 다양하고 수 많은 VASP 들로부터 서비스를 제공받고 지불을 하게 될 것이다. 다양한 VASP 들과 인증 및 세션키 성립을 위해서 사용자와 VASP 는 서로간의 인증서를 검증할 수 있어야 한다. 그러나 수많은 사용자와 VASP 가 존재할 미래의 이동 통신 환경에서 서로간의 인증서를 검증할 수 있는 공개키를 가지고 있을 가능성은 적다.

본 논문에서는 사용자와 VASP 간의 효율적인 인증과 키 교환을 위하여 임시 인증서를 제안한다. 제안한 임시 이동 사용자 인증서는 다음과 같은 특징을 가진다.

1. 사용자가 임시적으로 생성한 서명용 비밀키에 대한 인증서이다.
2. 인증서안의 신원 정보는 임시적으로 사용할 수 있어서 익명 서비스 사용이 가능하다.
3. 사용자가 방문하고 있는 도메인에 존재하는 신뢰할 수 있는 제 3 기관인 TTP(Trusted Third Party)의 비밀키로 전자 서명이 되어 사용자에게 발행이 되므로 방문 도메인의 VASP 는 효율적으로 사용자의 인증서를 검증할 수 있다.

제안된 등록 프로토콜을 통하여 발급된 임시 인증서를 이용하여 검증 시 필요한 공개키 분배 문제를 해결할 수 있으며 따라서 개선된 효율성을 제공할 수 있다.

제안한 임시 인증서를 UMTS 에서 VASP 와의 인증 및 지불 초기화 프로토콜로 제시된 AIP(Authentication and Initialization of Payment) 프로토콜[2,3,4]에 적용하여 그 효율성을 검증하고 성능 비교를 하였다. 사용자는 자신의 홈 도메인 인증 기관의 서명 검증용 공개키를 소유하고 있다는 가정에서 임시 이동 사용자 인증서 발급 과정이 들어가는 등록 프로토콜을 제안하였다. 임시 인증서를 기반으로 한 AIP 프로토콜을 제안하고 동일한 가정에서 수행되는 온-라인 TTP 를 이용하는 AIP 프로토콜과 성능을 비교하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 인증 및 지불 초기화 프로토콜에 대하여 알아본다..3 장에서는 제안하는 모델에 대해서 설명하고 4 장에서는 새로운 등록 프로토콜을 제안한다. 5 장에서는 임시 이동 사용자 인증서를 이용한 효율적인 AIP 프로토콜을 제안한다. 6 장에서는 성능 평가를 하고 7 장에서는 결론을 제시한다.

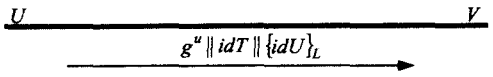
2. 인증 및 지불 초기화 프로토콜

UMTS 에서의 이동 정보 서비스를 위하여 제시된 AIP 프로토콜은 그림 1-3 과 같이 수행이 된다. 아래의 프로토콜의 가정은 사용자는 VASP 의 인증서 검증에 필요한 공개키를 가지고 있지 않다는 것이다.

프로토콜의 표기 형식은 다른 암호 시스템으로의 응용을 위하여 일반적인 방식을 이용하였다. 프로토콜의 참여자는 사용자 U, 서비스 제공자 V, 신뢰기관 T 이다. idX 는 X 의 신원을 의미하며, $CertX$ 는 X 의 인증서를 뜻한다. U, T 의 메시지 M 에 대한 전자서명 알고리즘은 각각 $Sig_U(M)$, $Sig_T(M)$ 로 표기된다. 세션키 K 로 암호화된 메시지 M 은 $\{M\}_K$ 로 나타내어진다. h 는 해쉬 함수이다.

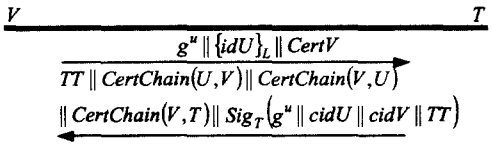
U 는 T 와 같이 ElGamal 키 설정 방식[5]으로 세션키를 성립하고, V 와는 Diffie-Hellman 방식[6]에 의하여 세

션키를 설정한다.



<그림 1> AIP 프로토콜 - 1

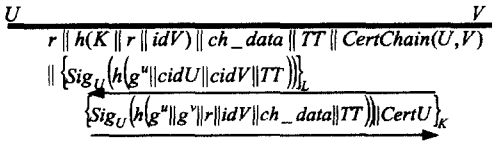
프로토콜(<그림 1>)이 시작되면 U 는 난수 u 를 생성하여 키 설정용 공개키 g^u 를 생성하고 T 의 공개키 g^w 와 같이 세션키 $L = g^{uw}$ 을 계산한다. 이와 같이 자신의 T 의 신원 idT, 그리고 자신의 신원 idU 를 세션키 L 을 이용해서 암호화해서 V 에게 보낸다.



<그림 2> AIP 프로토콜 - 2

<그림 2>에서 V 는 U 로 부터 전송 받은 g^u, $\{idU\}_L$ 를 자신의 인증서 $CertV$ 와 같이 T 에게로 보낸다.

T 는 U 의 공개키 g^u 와 같이 세션키 $L = g^{uw}$ 을 계산한다. T 는 V 로부터 전송 받은 idU 를 이용하여 U 의 인증서를 찾아내고 인증서 체인 $CertChain(V,U)$ 을 생성한다. 마찬가지로 T 는 $CertV$ 에 기반해서 $CertChain(U,V)$ 을 만들어내고 g^u 를 이용하여 $CertChain(V,T)$ 를 계산한다. T 는 타임스탬프 TT 를 생성하고 U 의 공개키 g^u 와 인증서 식별 번호 $cidU, cidV$ 에 전자서명을 수행하여 V 에게 전송한다.



<그림 3> AIP 프로토콜 - 4

<그림 3>을 보면 V 는 $CertChain(V,T)$ 를 검증하여 T 의 서명을 검증할 수 있는 공개키를 얻고 $CertChain(V,U)$ 을 이용하여 U 의 전자서명을 검증할 수 있는 공개키를 얻는다. V 는 U 의 공개키 g^u 를 이용하여 세션키 $K = h(g^{uv} \| r)$ 를 계산해 낸다.

U 는 V 로부터 받은 $CertChain(U,V)$ 를 이용하여 V 의 전자서명을 검증할 수 있도록 공개키를 복구해낸다. 그리고 V 의 g^s 를 이용하여 세션키 $K = h(g^{vu} \| r)$ 를 계산해 낸다.

3. 임시 이동 사용자 인증서

이동 사용자는 외부 도메인에서의 **VASP** 의 인증서를 검증할 공개키를 가지고 있는 확률이 적다는 경우에서 임시 이동 사용자 인증서는 시작된다. 임시 이동 사용자 인증서는 방문하고 있는 도메인의 **TTP** 에 의해서 전자서명이 이루어져서 사용자에게 발급된다.

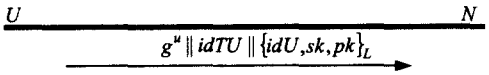
ASPeCT 인증서 형식[2]에서 다음과 같은 수정이 요구된다.

1. 사용자가 임시로 생성한 비밀 서명키의 공개키에 대한 정보를 가지고 있다.
2. 사용자의 신원은 방문하고 있는 도메인에서의 익명 서비스 사용을 보장하기 위하여 임시 번호가 될 수 있다.
3. 유효 기간은 사용자의 신용 정보에 따라서 방문하고 있는 **TTP** 가 생성을 한다.
4. 발급자의 신원은 방문 도메인의 **TTP** 가 되어야 한다.

임시 이동 사용자를 사용자에게 발급하는 과정을 포함하는 새로운 등록 프로토콜을 4 장에서 제안한다. 사용자는 등록 프로토콜의 결과로 발급된 임시 이동 사용자 인증서를 이용하여 **VASP** 와의 인증 및 지불 초기화 프로토콜을 효율적으로 수행할 수 있다.

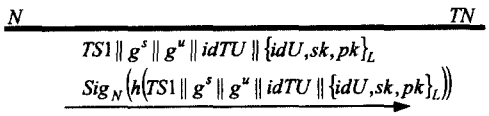
4. 제안한 등록 프로토콜

제안한 등록 프로토콜은 사용자 U, 네트워크 오퍼레이터 N, 네트워크 오퍼레이터의 신뢰기관 TN 그리고 사용자의 신뢰기관 TU 가 참여한다.



<그림 4> 제안한 등록 프로토콜 - 1

프로토콜(<그림 4>)이 시작되면 U 는 난수 u 를 생성하여 공개키 g^u 를 생성하고 TU 의 공개키 g^w 와 같이 세션키 $L = g^{uw}$ 을 계산한다. 이와 같이 자신의 TU 의 신원 $idTU$, 그리고 자신의 신원 idU 를 세션키 L 을 이용해서 암호화해서 N 에게 보낸다 idU 를 암호화해서 보내는 이유는 사용자의 익명성을 보장하기 위해서이다.

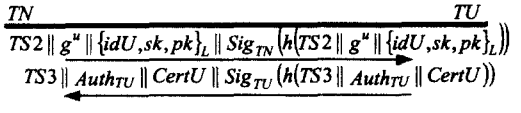


<그림 5> 제안한 등록 프로토콜 - 2

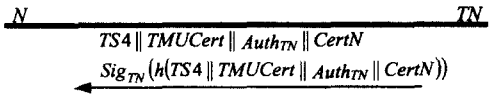
<그림 5>에서 N 은 TN 로 부터 전송 받은 g^u, $\{idU,sk,pk\}_L$ 를 자신의 키 설정용 공개키 g^s 와 같이 서명을 하여 TN 에게로 보낸다.

<그림 6>을 보면 TU 는 U 의 공개키 g^u 와 같이 세션키 $L = g^{uw}$ 을 계산한다. TU 는 pk 에 대한 인증서를 생

성하고 U 가 TN 의 공개키를 검증하는데 필요한 $Auth_{TU}$ 를 생성한다. TU 는 U 의 인증서와 $Auth_{TU}$, 타임스탬프 $TS3$에 전자 서명을 하여 TN 에게 전송한다.

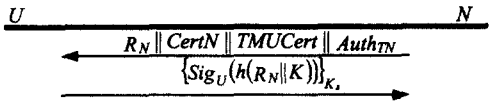


<그림 6> 제안한 등록 프로토콜 - 3



<그림 7> 제안한 등록 프로토콜 - 4

<그림 7>을 보면 N 는 $TMUCert$ 를 이용하여 U 의 공개키를 검증할 수 있다. N 은 자신이 받은 메시지와 난수 R_N 을 생성하여 U 에게 전송하고 g^u 를 이용하여 세션키 $K_s=(g^{us} \| R_N)$ 를 계산해 낸다.

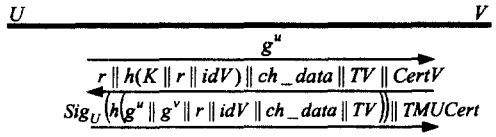


<그림 8> 제안한 등록 프로토콜 - 5

U 는 N 로부터 받은 $CertN$ 를 이용하여 N 의 전자서명을 검증할 수 있도록 공개키를 얻고 N 의 공개키 g^s 를 이용하여 N 과의 세션키 $K_s=(g^{su} \| R_N)$ 를 계산해낸다.

5. 제안한 인증 및 키 교환 프로토콜

U 는 사용자, V 는 서비스 제공자를 나타낸다. U 는 등록 프로토콜의 수행 결과로 $TMUCert$ 와 $CertV$ 를 검증할 수 있는 공개키를 가지고 있다.



<그림 9> 제안한 AIP 프로토콜

프로토콜(<그림 9>)이 시작되면 U 는 세션키 설정을 위한 공개키 g^u 를 V 에게 보낸다.

V 는 난수 r 을 생성하고 g^u 와 자신의 공개키 g^v 를 이용하여 세션키 $K=h(g^{uv} \| r)$ 를 계산해 낸다. V 는 K, r, idV 를 해쉬화 하고 지불 데이터 ch_data, 타임스탬프 TV, 인증서 $CertV$ 를 U 에게 전송한다.

U 는 세션키 $K=h(g^{vu} \| r)$ 를 생성하고 g^u, g^v, r 과 V 의 신원 idV 와 지불 데이터 ch_data, 타임스탬프 TV 를 해쉬 함수 h 로 처리하고 서명을 구한 후 자신의 인증서 $TMUCert$ 와 같이 V 에게 전송한다.

6. 성능 평가 및 분석

외부 도메인에 접근했을 때 수행되는 등록 프로토콜의 결과로 임시 이동 사용자 인증서를 이용한 제안된 AIP 프로토콜과 온라인 TTP 를 이용하는 AIP 프로토콜과의 성능 평가는 표 1 에 나와 있다. 제안된 프로토콜은 인증서 체인의 사용을 제거하였으며 메시지의 교환 횟수를 감소하였다. 암호화와 서명 생성 등에서 개선된 효율성을 보여준다.

<표 1> 제안한 AIP 프로토콜과의 성능 평가

	×	○
	ElGamal, Diffie-Hellman	Diffie-Hellman
	3	2
	5	3
	3	0
	2	1
	1	1
	1	0
	2	0

○: Yes(possible) ×: No(impossible)

7. 결론 및 향후 연구 과제

본 논문에서는 임시 이동 사용자 인증서를 제안하였다. 이를 위하여 새로운 등록 프로토콜과 이동 사용자가 방문하고 있는 도메인의 VASP 와의 효율적인 인증 프로토콜을 제시하였다.

참고문헌

[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, 1998.

[3] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," *ESORICS, LNCS*, vol.1488, pp. 469-472 1998.

[4] K.M. Martin, B. Preneel, C. Mitchell, H.J. Hitz, G. Horn, A. Poliakova and P. Howard, "Secure billing for mobile information services in UMTS," *IS&98, LNCS* vol.1430, pp. 535-548, 1998.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Informatio Theory*, Vol. IT-31, No.4, pp.469-472, 1985.

[6] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976.