이동 통신을 위한 티켓 기반 서비스 접근 프로토콜

이병래°, 장경아, 김태윤
고려대학교 컴퓨터학과
{brlee, tykim}@netlab.korea.ac.kr

Ticket Based Service Access Protocol for Mobile Communications

Byung-Rae Lee°, Kyung-Ah Chang, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University.

요 약

다양한 도메인에 있어서 이동 호스트의 서비스 접근은 이동성 계약에 의한 홈 도메인과 도메인간 인증에 의하여 이루어지고 있다. 그러나 다양한 서비스 제공자와 서비스들 그리고 수많은 이동 사용자들에게 있어서 홈 도메인에 의존 한 이동성 계약은 비 효율적이며 실용적이지 못한다. 본 논문에서는 티켓에 기반 한 새로운 지불 프로토콜을 제안한다. 공개키 암호 시스템에 기반 한 제안된 티켓 기반 지불 프로토콜은 기존의 연구[1,2]와 비교하여 개선된 안전성과 확장성을 제공한다.

1. 서론

사용자의 이동성을 지원해주기 위한 전통적인 접근 방식은 도메인간의 인증(cross-domain authentication)과 이동성 계약(roaming agreement)에 의한 것이었다. 외부 도메인을 접근해서 서비스를 제공받기 위해서는 사용자는 자신의 홈 도메인의 도움을 받아서 외부 도메인이 인증하도록 하여야 한다. 이러한 방식은 근본적으로 거리상에 있어서 시간을 소모하며 비 효율적이다. 또한 도메인간의 인증은 외부 서비스 제공자가 사용자의 홈 도메인을 신뢰하여야 한다는 요구 조건이 존재한다. 현재 이러한 신뢰는 이동성 계약에 의해서 이루어진다. 그러나 증가하고 있는 서비스 제공자들을 볼 때 이러한 이동성 계약은 적용하기 어려우며 효율적이지 못하다.

본 논문에서는 공개키 암호 시스템에 기반한 티켓 기반 서비스 접근 프로토콜을 제안한다. 티켓에 기반한 서비스는 도메인간의 인증 문제를 해결할 수 있는 기법으로 [1,2]에서 제시되었다. 제안한 티켓 기반 프로토콜은 티켓 획득 프로토콜과 티켓 이용 프로토콜로 구성되어진다. 대칭 키 암호 시스템에 의존하는 기존의 연구[1,2]와는 달리 제안된 티켓 획득 프로토콜은 공개키 암호 시스템에 기반하기 때문에 티켓 서버가 공격을 당하여도 사용자의 안전성과 권익은 보호 될 수 있다. 또한 제안된 티켓 사용 프로토콜은 Diffie-Hellman 키 설정 프로토콜을 이용하여 다양한 서비스 제공자와의 상호 인증과 세션 키 설정, 티켓 사용이 가능하다.

본 논문의 구성은 다음과 같다. 2 장에서는 티켓의 기본적인 요구 사항에 대하여 설명한다. 3 장에서는 이동통신에서의 보안에 관하여 기술하고 4 장에서는 티켓 기반 지불 모델을 제시한다. 5 장에서는 새로운 공개키 기반 티켓 획득 프로토콜과 티켓 사용 프로토콜을 제안하며 6 장에서는 제안된 프로토콜에 대한 분석을 한다. 7 장에서는 기존의 연구에 대하여 설명하고 8 장에서는 결론을 제시한다.

2. 관련 연구

티켓 기반의 지불 프로토콜은 [1,2]에 의하여 연구되어 있다. [1]은 대칭키에 의한 티켓 획득 프로토콜과 티켓 지불 프로토콜을 기술하고 있다. [2]에서는 대칭키 방식에 의한 티켓 획득 프로토콜과 공개키에 기반한 티켓 사용 프로토콜을 제시하고 있다. 대칭키 기반의 티켓 관리 기법에 있어서는 키 관리의 문제와 더불어 티켓 서버가 공격을 당할 경우 사용자들의 키가 노출이 되어 티켓의 부정한 사용이 이루어 질 수 있는 문제점들이 존재한다.

본 논문에서 제안된 공개키 방식의 티켓 획득 프로토콜은 티켓 서버가 공격을 당하여도 모든 사용자의 암호키가 노출될 위험이 적으며 키 관리의 문제점도 줄어든

다. 따라서 정당한 사용자의 티켓 사용을 보호할 수 있다. 그러나 공개키 기법의 경우에 있어서도 티켓 서버가 공격을 당하면 옳지 않은 티켓의 발행이 이루어질 수 있다.

3. 티켓 요구 사항

티켓을 이용한 서비스 접근 기법에서 고려해야 할 티켓의 사항으로는 아래와 같은 문제들이 있다.

복제 (Duplication): 티켓은 원본만이 존재하여야 하며 복제되어서 사용되어서는 안 된다. 이 문제는 전자 화폐에 있어서 이중 사용 문제와 유사하다.

수정 (Modification): 티켓의 내용을 불법적으로 수정해서 허가 받은 이상의 서비스를 제공 받아서는 안 된다.

위조 (Forgery): 위조를 통하여 네트워크가 올바르게 인정하는 티켓이 생성되어서는 안 된다.

재판매 (Re-sale): 티켓이 다른 사용자에게 양도할 수 있는 여부를 의미한다. 특정 기관에서는 자신이 발행한 티켓이 원 소유주 이외의 다른 사용자가 사용하는 것을 원하지 않을 수 있다.

4. 이동 통신 보안

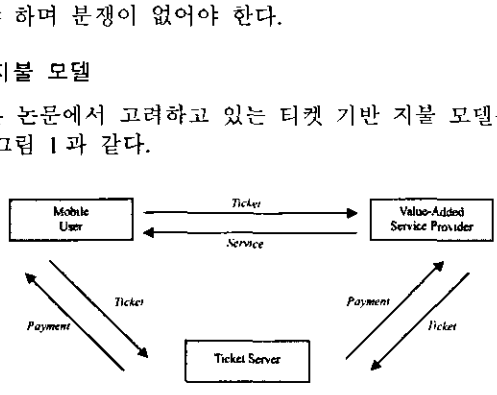
제 3 세대 이동 통신 시스템 [3,4] 보안 요소는 기존의 유선 망과 대등한 수준의 보안을 제공하는 것이다. 이 같은 요구에 대응하는 요소들은 다음과 같다. 무선 인터페이스에서의 기밀성, 사용자 신원의 익명성 그리고 가장 중요한 것은 사용자의 네트워크로의 인증이다 [5,6].

공개키 암호 시스템은 기존의 2 세대 이동 통신 시스템에서는 메시지의 길이와 계산량의 문제 때문에 사용되지 못하였다. 그러나 타원 곡선 암호 시스템의 출현과 단말기의 계산 능력 개선으로 인하여 제 3 세대 이동 통신 시스템에 있어서는 공개키 암호 시스템의 사용이 가능하게 되었다 [5,6].

다양한 서비스 제공자의 증가로 인하여 이동 사용자와 서비스 제공자간의 상호 인증은 중요한 문제로 부가되었다. 또한 사용자와 서비스 제공자간의 지불 기법은 안전해야 하며 분쟁이 없어야 한다.

5. 지불 모델

본 논문에서 고려하고 있는 티켓 기반 지불 모델은 아래 그림 1 과 같다.



<그림 1> 티켓 기반 지불 모델

우선 사용자는 티켓 서비로부터 적절한 지불 방법을 통하여 티켓을 구입한다. 사용자는 티켓을 이용하여 서비스 제공자로부터 원하는 서비스를 얻는다. 서비스 제공자는 사용자로부터 얻은 티켓을 티켓 서버에게 제시하고 돈을 지불 받는다.

6. 제안한 티켓 기반 지불 프로토콜

본 장에서는 새로운 공개키 기반 티켓 획득 프로토콜과 티켓 사용 프로토콜을 제시한다. 제안된 티켓 획득 프로토콜에서는 사용자는 티켓 서버와 ElGamal 키 공유 [7] 기법으로 세션 키를 계산해낸다. 티켓 사용 프로토콜에서는 서비스 제공자와 Diffie-Hellman [8] 기법으로 세션 키를 생성해낸다.

6.1 티켓 구조

티켓은 일련 번호 sn, U 의 Diffie-Hellman 공개 키 g^u, U 의 서명을 검증할 수 있는 공개 키 P_u, 기타 정보에 대한 $options$, 그리고 티켓 서버의 서명으로 이루어진다.

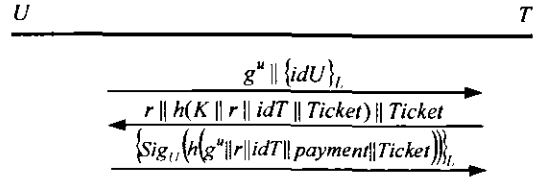
$$Ticket = \{sn, idT, g^u, P_u, option, Sig_t\{sn, idT, g^u, P_u, option\}\}$$

티켓 서버의 서명은 불법적인 수정과 위조로부터 티켓을 보호한다.

6.2 티켓 획득 프로토콜

U 는 이동 사용자를 나타내고 TS 는 티켓 서버를 지칭한다. $certX$ 는 X 의 인증서를 뜻한다. U 의 메시지 M 에 대한 전자서명 알고리즘은 각각 $Sig_U(M)$로 표기된다. 세션 키 K 로 암호화된 메시지 M 은 $\{M\}_K$ 로 나타내어진다.

프로토콜이 시작되기 전에 우리는 다음과 같은 사항을 가정한다. U 는 T 의 서명을 검증할 수 있는 서명 검증용 공개 키와 ElGamal 공개키 설정 키 g^t 를 가지고 있다. T 는 U 의 서명을 검증할 수 있는 서명 검증용 공개키를 가지고 있다.



<그림 2> 티켓 획득 프로토콜

프로토콜(<그림 2>)이 시작되면 U 는 난수 u 를 생성하고 ElGamal 공개키 g^u 를 계산하고 T 의 공개키 g^v 와 같이 세션 키 L 를 생성한다. U 는 자신의 신원 idU 를 생성한 세션 키 L 로 암호화하여 T 에게 보낸다.

T 는 g^u 와 자신의 Diffie-Hellman 공개키 g^v 를 이용하여 세션키 K 를 계산해 낸다. T 는 난수 r

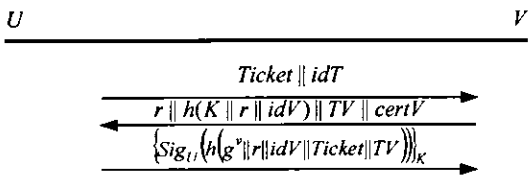
U 는 g^u, g^v, r 과 T 의 신원 idV 와 티켓의 일련 번호 sn 과 타임스탬프 TV 를 해쉬 함수 h 로 처리하고 시

명을 구한 후 자신의 인증서 $certU$ 와 같이 세션키 K 로 암호화를 하여 T 에게 전송한다.

6.3 티켓 사용 프로토콜

사용자는 서비스 제공자에게 티켓을 전달하고 원하는 서비스를 제공받을 수 있다.

V 는 서비스 제공자를 나타내고, $certV$ 는 V 의 인증서, $certV$ 는 V 의 인증서를 나타낸다. V 는 티켓 서버의 서명을 검증할 수 있는 공개 키를 가지고 있으며 U 는 $certV$ 를 검증할 수 있는 공개 키를 가지고 있다.



<그림 3> 티켓 사용 프로토콜

프로토콜(<그림 3>)이 시작되면 U 는 $Ticket$ 과 티켓 서버의 신원 idT 를 V 에게 보낸다.

V 는 g^u 와 자신의 Diffie-Hellman 공개키 g^v 를 이용하여 세션키 K 를 계산해 낸다. V 는 난수 r

U 는 g^u, g^v, r 과 V 의 신원 idV 와 티켓의 일련 번호 sn 과 타임스탬프 TV 를 해쉬 함수 h 로 처리하고 서명을 구한 후 자신의 인증서 $certU$ 와 같이 세션키 K 로 암호화를 하여 V 에게 전송한다.

7. 성능 분석 및 고찰

7.1 티켓

복제 (Duplication): 정당하지 못한 사용자는 티켓을 복제하여 사용할 수 있다. 그러나 티켓 사용 프로토콜에서의 서명을 생성해낼 수가 없으므로 티켓의 복제 사용은 방지될 수 있다.

수정 (Modification)과 위조(Forgery): 티켓 서버이외의 엔티티로 부터의 티켓의 수정은 가능하지 않다. 왜냐하면 사용자나 정당하지 못한 티켓의 사용은 티켓 서버의 서명을 생성해낼 수 없기 때문이다.

재판매 (Re-sale): 제안된 프로토콜에서는 사용자가 자신의 비밀키를 제공해야만 티켓의 재판매가 이루어진다.

7.2 티켓 획득 프로토콜

제안된 공개키 기반 티켓 획득 프로토콜은 기존의 대칭 키 기반 티켓 획득 과정에 비교하여 티켓 서버가 공격을 당하여도 사용자의 비밀 키의 노출 위험이 없다.

익명성을 보장하기 위하여 사용자의 신원 idU 는 세션 키 L 에 의하여 암호화되어 티켓 서버에게 전송이 된다.

U 의 서명은 U 가 티켓을 획득했다는 부인방지의 기능이 있다.

7.3 티켓 사용 프로토콜

두 번째 메시지의 해쉬 값 $h(K \| r \| idV)$ 은 V 의 신원 인증을 가능하게 된다.

세 번째 메시지의 서명에 포함되어 있는 r 을 통하여 V 는 U 의 신원을 확인할 수 있다.

세션 키 K 의 재사용을 막기 위하여 V 로부터 생성된 난수 r 와 $Ticket$ 이 가지고 있는 g^u 를 이용하여 세션 키가 계산되어진다.

사용자는 마지막 메시지에서 자신의 비밀키로 티켓의 일련 번호인 sn 과 난수 r 을 서명을 하여 세션키 K 로 암호화를 한 후 전송한다. 서비스 제공자 V 는 사용자의 서비스 제공의 증거로 이 서명을 티켓 서버에게 제공할 수 있다. 따라서 사용자는 자신이 서비스를 제공 받은 사실을 부인할 수 없다.

8. 결론

본 논문에서는 이동 사용자의 지불 프로토콜에 있어서 홈 도메인과의 인증을 제거하고 효율적인 인증과 지불 과정을 보여주는 공개키 암호 시스템 기반 티켓 기반 지불 프로토콜을 제안하였다. 제안된 프로토콜은 제 3 세대 이동 통신을 대비하여 티켓 획득 과정과 티켓 사용 프로토콜이 공개키 기반이다.

참고문헌

[1] B. Patel and J. Crowcroft, "Ticket Based Service Access for the Mobile User," Mobicom, 1997.

[2] L. Buttyan and J-P. Hubaux, Accountable and anonymous service usage in mobile communication systems. EPFL SSC Technical Report No. SSC/1999/016, 1999.

[3] UMTS Forum, "A regulatory framework for UMTS," Report no. 1, 1997.

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

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

[6] 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.

[7] 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.

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