

이동 사용자 사이의 안전한 통신을 위한 인증 프로토콜

김선형⁰, 이병래, 김태윤
고려대학교 컴퓨터학과

{shaklim, brlee, tykim}@netlab.korea.ac.kr

An Authentication Protocol for Secure Communication Between Mobile Users

Sun-Hyoung Kim⁰, Tai-Yun Kim

Dept. of Computer Science & Engineering, Korea University

요 약

무선 통신 시스템에서 이동 사용자들의 안전성에 대한 문제는 끊임없이 제기되어 왔고, 더 안전한 통신을 위한 방안들이 강구되고 있다. 무선 통신 환경에서는 전달하고자 하는 메시지들이 공중파를 매체로 하여 전송되기 때문에 안전성에 대한 철저한 고려가 수반되어야 한다. 본 논문에서는 무선 이동 네트워크 환경에서 인증서를 기반으로 한 안전한 프로토콜을 제안하고자 한다. 특히 이동 사용자들이 각기 다른 도메인으로부터 서비스를 받고 있는 상황 하에서 종단간에 위치한 이동 사용자들이 서로를 인증하고 통신을 위한 비밀키를 공유할 수 있는 프로토콜을 제안한다.

1. 서론

기존의 유선 네트워크에 무선 이동 네트워크를 접목시키는 작업은 단순히 유선 상에서의 기술들을 옮겨놓는 것만으로 끝나지 않는다. 무선 네트워크 기술은 새로운 기술력을 필요로 하는 독립적인 네트워크 시스템이라 할 수 있다. 대부분의 이동 사용자는 이동 단말기를 통해 자신이 원하는 서비스를 받기를 원하며 앞으로도 사용자들의 요구는 끊임없이 늘어날 것이다. 그러나 이러한 이동 사용자에 대한 서비스의 질과 양적인 측면을 논하기 이전에 이동 사용자들로 하여금 안전하고 신뢰성 있는 통신의 보장이 필수적으로 이루어져야 할 것이다.

본 논문에서는 무선 이동 네트워크 환경에서 인증서를 기반으로 한 안전한 프로토콜을 제안하고자 한다. 특히 이동 사용자들이 각기 다른 도메인으로부터 서비스를 받고 있는 상황 하에서 종단간에 위치한 이동 사용자들이 서로를 인증하고 통신을 위한 비밀키를 공유할 수 있는 프로토콜을 제안한다.

본 논문은 다음과 같이 구성되어 있다. 2절에서는 이동 네트워크 시스템의 환경에 대해 설명한다. 3절에서는 종단간 이동 사용자 사이의 프로토콜에 대해 살펴보고 이 프로토콜의 취약점을 고찰한다. 4절에서는 두 사용자가 서로를 인증하고 공통의 비밀키를 확립할 수 있는 안전한 종단간 프로토콜을 제시하

고 5절에서 이에 대한 성능 평가를 한다. 6절에서 본 논문의 결론을 맺는다.

2. 이동 네트워크 환경

무선 이동 통신 시스템은 단말기를 소유한 이동 스테이션(MS)과 이동 네트워크 시스템(MNS)의 두 가지로 분류할 수 있다. 네트워크 시스템은 이러한 이동 스테이션에 대한 제반 사항에 대한 기록을 관리하고 있으며 <그림 1>과 같이 기지국(BS), 위치 레지스터, 이동 스위칭 센터(MSC)의 세 가지로 구분할 수 있다. 이동 스테이션은 기지국을 통하여 네트워크 시스템에 접속할 수 있고 하나의 기지국은 해당 네트워크의 위치 레지스터에 의해서 제어된다. MSC는 다른 모든 이동 네트워크 혹은 유선망과 연결되는 접속점의 역할을 하며 MS의 이동 정보에 대한 데이터베이스를 수반하고 있다. 또한 각각의 네트워크에는 인증 서버(AS)가 존재하며 이는 위치 레지스터와 같은 도메인 상에 위치하고 있다. AS는 이동 사용자의 비밀키와 같은 보안과 관련된 정보를 저장하고 있으며 위치 레지스터는 자신의 네트워크에 등록된 이동 사용자의 현재 위치와 가입 정보를 가지고 있다. 각각의 이동 사용자는 이동 네트워크에 가입할 때 자신의 홈 네트워크(HN)를 가지게 된다. 이동 사용자는

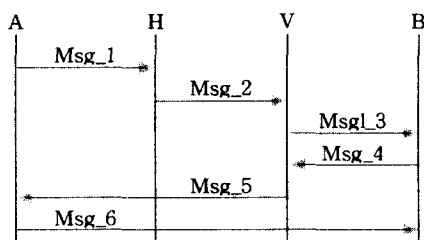
4.1. 가정 및 기호

- 이동 사용자 A, B : 각각의 사용자는 CA 로부터 서명된 공개키 인증서를 가지고 있다. 또한 각 사용자는 자신이 속한 네트워크와 공통의 비밀키를 공유하고 있다.
- 이동 네트워크 H, V : 각각의 네트워크는 CA 로부터 서명된 공개키 인증서를 가지고 있다. 서로 분리되어 있는 각 네트워크 사이에 공통의 비밀키를 공유하고 있다.

다음은 프로토콜에 사용되는 기호들이다.

- h_1, h_2, h_3 : 일방향 해쉬 함수 ([5] 참조)
- $Sig_A(X)$: 메시지 X 에 대한 A 의 서명
- $cert_A$: 이동 사용자 A 의 인증된 공개 서명키
- $cert_B$: 이동 사용자 B 의 인증된 공개키 (g^{x_B})
- K_{AB} : A 와 B 사이의 공통의 비밀 세션키

4.2. 제안한 새로운 종단간 인증 프로토콜



<그림 3> 새로운 종단간 인증 프로토콜

[프로토콜 II]

1. Msg_1 : $[ID_A, ID_B, g^r, ID_{CA}]_{K_{AH}}$
2. Msg_2 : $[g^r, ID_H, ID_{CA}]_{K_{HV}}$
3. Msg_3 : $[g^r, ID_V, ID_{CA}]_{K_{VW}}$
4. Msg_4 : $[r_B, h_2(K_{AB}, r_B, ID_B), T_B, cert_B]_{K_{BV}}$
5. Msg_5 : $r_B, h_2(K_{AB}, r_B, ID_B), T_B, cert_B$
6. Msg_6 : $[Sig_A(h_3(g^r, g^{x_B}, r_B, ID_B, T_A), cert_A)]_{K_{AH}}$

Msg_1 에서 A 는 B 를 호출하기 위해 B 의 신원을 포함시킨다. Msg_2 와 Msg_3 에서 H 와 V 는 B 에게 A 의 정보를 전달하게 되고, B 는 자신의 비밀키 x_B 와 A 의 임시 비밀키 r_A 를 기반으로 공통의 비밀키 $K_{AB} = h_1(r_B, g^{x_B})$ 를 확립한다. Msg_4 와 Msg_5 를 통해 A 는 공통의 비밀키를 확립함으로써 B 를 인증할 수 있다. Msg_6 에서 B 는 A 로부터 비밀 세션키 K_{AB} 로 암호화한 메시지를 해독함으로써 A 를 인증할 수 있다.

5. 성능 평가

본 논문에서 제시한 프로토콜은 종단간의 두 이동 사용자들 사이에서 인증과 공통의 비밀키의 확립을 주요 목표로 하고 있다. 여기서는 앞서 제시한 두 개의 프로토콜을 비교한다.

<표 1> 프로토콜의 안전성 비교

상호 실체 인증	×	○
상호 키 합의	○	○
상호 합축적 키 인증	×	○
상호 키 확증	×	○
사용자 신원의 기밀성	○	○

[○ : 만족, × : 불만족]

프로토콜 I은 이동 사용자와 네트워크 사이에서 서로에 대한 인증을 못하기 때문에 공격자는 자신의 실체를 드러내지 않고서도 다른 실체의 역할을 할 수 있다. 제안한 프로토콜 II는 서명의 암호화를 통해 서명자 인증 공격과 콘텐츠 인증 공격을 방지하고 있으며 메시지의 해쉬 함수에 네트워크 식별자와 난수를 포함함으로써 근원지 대체 공격과 타임-메모리 교환 공격을 방지할 수 있다. 또한 서로 다른 프로토콜의 세션키 값이 같을 때, 이를 찾기 위한 코드북 공격을 방지할 수 있다[5].

6. 결론

본 논문에서 제시된 종단간의 인증 프로토콜에서는 이동 사용자의 어떠한 비밀 정보도 다른 네트워크 상으로 전송되지 않으며, 이는 어느 누구도 이동 사용자로 위장할 수 없음을 의미한다. 따라서 두 이동 사용자의 비밀 통신이 보장될 수 있다. 또한 안전한 통신 채널이 사용자와 네트워크 사이에 설정되면 어떠한 암호학적 동작도 수행되지 않기 때문에 네트워크에서의 작업량이 경감될 수 있다.

참고 문헌

- [1] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users," IEEE Network, pp. 26-34, 1994.
- [2] Y. Yacobi, Z. Shmuley, "On Key Distribution Systems," in Advances in Cryptology - Crypto'89, LNCS 435, pp. 344-355, Springer Verlag, 1989.
- [3] C. Park, "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems," IEEE Network, pp. 50-55, September/October 1997.
- [4] C. Boyd, D.-G. Park, "Public Key Protocols for Wireless Communications," in The 1st International Conference on Information Security and Cryptology(ICISC'98), pp. 47-57, 1998.
- [5] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," In Computer Security - ESORICS '98 Proceedings, pp. 277-293, Lecture Notes in Computer Science Vol. 1485, Springer Verlag, Berlin, 1998.