타원 곡선 기반의 무선 인터넷에서의 인증 및 키 합의 프로토콜

문준선, 반용호, 김종훈
동아대학교 컴퓨터공학과

Authentication and Key Agreement Protocol based on ECC in the Wireless Internet

Joon-Sun Moon, Yong-Ho Ban, Jong-Hoon Kim
Dept. of Computer Engineering, Donga University

요 약

무선 인터넷 사용의 증가와 함께 PDA 또는 무선단말기와 같은 제한된 시스템 환경에 적합한 보안 서비스의 필요성이 증가되고 있다. 무선환경을 위해 제공되어야 할 다양한 보안 서비스 중 인증 및 키 합의를 위한 과정은 보안상 매우 민감한 부분이다. 안전한 프로토콜 설계에서 통신에 참여하는 개체들에 대한 인증 및 이후 진행되는 해당 세션의 안전성 확보를 위한 세션키 설정, 서비스 사용자에 대한 익명성 보장 등이 고려되어야 한다. 본 논문에서는 무선 인터넷의 한정된 시스템 환경을 고려한 타원 곡선 암호시스템(ECC) 기반의 인증 및 키 합의 프로토콜을 제안한다.

1. 서론

이동 통신 기술의 발달로 무선 인터넷뿐만 아니라 이동 컴퓨팅, 이동 멀티미디어 서비스 등 이동 통신 시스템을 이용한 응용 서비스 개발과 서비스 제공이 급증하면서 이용자 신분 및 위치 정보의 노출, 송수신 데이터의 도청 및 변조, 불법적인 서비스 이용 등 무선 인터넷에서의 보안 문제 해결이 급선무이다. 무선 인터넷을 이용한 전자상거래 서비스에서는 사용자의 익명성을 보장하면서 인증 및 키 합의 문제를 해결해야 한다. 설계 시에 이동 통신이 갖는 제약점, 즉 제한된 메모리, 자원, 계산력, 대역폭을 고려해야 한다. 따라서 빠른 키 생성, 빠른 계산 속도, 적은 양의 메모리를 사용하면서도 보안이 보장되어야 한다.

지금까지 이동 통신 환경에서의 인증 및 키 합의 프로토콜이 많이 제안되었다. 특히 공개키 암호기반[1,2] ASPeCT프로토콜과 대칭키 암호와 공개키 암호를 결합한 혼합형 방식으로 분류할 수 있다. 본 논문에서는 공개키 암호 알고리즘 중에 하나인 타원 곡선 암호시스템[3] 이용하여 인증 및 키 합의 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 무선 인터넷에서 요구되는 보안 특성들에 대해서 기술하고 3장에서는 타원곡선 암호시스템 이용한 무선 인터넷에서의 인증 및 키 합의 프로토콜을 제안한다. 그리고, 4장에서는 제안한 프로토콜에 대하여 기존의 방식과 보안 특성을 비교한다. 마지막으로 5장의 결론에서는 향후의 연구과제를 제시한다.

2. 무선 인터넷에서 요구되는 보안 특성

무선 인터넷 사용자는 서비스 제공자가 제공하는 서비스를 언제 어디서나 보다 편리하고 안전하게 이용하고자 한다. 이를 위한 이동 통신 환경에서 요구되는 보안 특성은 아래와 같다.[1,4,5]

- 묵시적 키 인증성(implicit key authentication)

실체 A와 B 이외에 어느 누구도 공유키를 생성할 수 없다는 확신할 수 있다. 이 경우를 A는 B에 대한 묵시적 키 인증성이라 한다. 반대로, B는 A 이외에 다른 어느 누구도 공유키를 생성할 수 없음을 확신할 수 있다. 이 경우를 B는 A에 대한 함축적 키 인증성을 갖는다고 한다. 이 두 조건을 만족하는 경우에 인증된 키 합의 프로토콜(authenticated key agreement)이라한다.

- 명시적 키 인증성(explicit key authenticaiton)

실체 A와 B 는 공유키를 생성한다. 이때, A는 B가 실제로 공유키를 계산해 가지고 있음을 확인할 수 있을 때, B에 대한 명시적 키 인증성을 갖는다. 반대로 B는 A가 실제로 공유키를 계산해 가지고 있음을 확인할 수 있을 경우에 A에 대한 명시적 키 인증성을 갖는다.

- 알려진 키에 대한 안전성(known-key security)

실체 A와 B는 인증 및 키 합의 프로토콜에 참여할 때, 세션마다 유일한 세션키를 생성한다. 이전에 세션에서 공격자로부터 세션키를 공격당해 노출되더라도 현제 세션이 안전함이 보장되는 것을 알려진 키에 대한 안전성이라 한다.

- 전향적 보안성(forward security)

하나 또는 둘 이상의 실체들의 장기적인 개인키가 노출되었을 경우에도 이전에 합의한 세션키의 안전성이 제공된다.

- 키 위장에 대한 안전성

실체 A의 장기적인 개인키가 노출되었을 경우 공격자가 A에 대한 다른 실체 B인 것처럼 위장 할 수 없는 안전성을 말한다.

- 미지의 키 공유에 대한

실체 A는 실체 B와 공유하고 있다고 믿고 있지만, B는 공격자 E와 키를 공유하고 있다고 믿게 하는 공격에 대해 안전할 경우를 말한다.

- 이동 사용자의 익명성

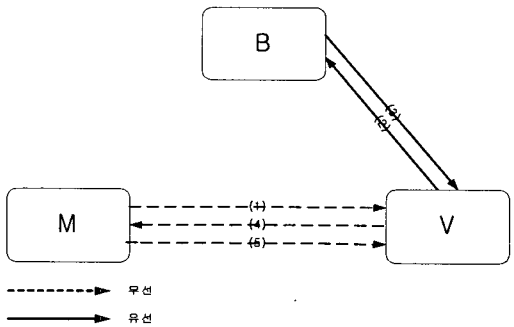
사용자의 위치가 고정된 유선 환경에서는 위치 정보가 그다지 중요하지 않지만, 휴대성과 편리함을 특징으로 갖는 무선 통신 환경에서는 사용자의 위치 및 정보에 대한 보안이 중요하다. 만일 정보가 노출되게 되면, 사용자의 프라이버시를 침해받게 된다. 그러므로 무선 통신 환경에서 사용자의 익명성(anonymity of mobile user)이 제공되어야 한다. 이는 통신에 참여한 개체 중에서 정보를 전송하는 상대의 공개키 또는 세션키를 이용하여 사용자 인증 정보를 암호화함으로써 이동 사용자의 익명성을 제공할 수 있다.

3. 제안한 프로토콜

무선 인터넷에서의 인증 및 키 합의 프로토콜은 무엇보다 높은 효율성과 보안성이 중요하다. 이는 단말기와 무선 통신 환경이 갖는 제약점을 극복해야하기 때문이다. 이 장에서는 이런 제약적인 환경에 적합한 프로토콜을 제안하며 무엇보다 타원곡선 암호시스템을 이용한 세션키를 생성한다. 이는 보다 빠르고 안전한 인증 및 키 합의 프로토콜을 제안한다. 다음 <표 1>은 프로토콜 설명에 사용하는 기호이고, <그림 1>은 제안한 프로토콜의 전체 수행과정을 나타낸다.

<표 1> 기호 정의

기호	설명
M	이동 사용자
V	서비스/컨텐츠 제공자
B	M의 신분을 보증해주는 신뢰 서버
p	사용되는 기반 필드 GF(p)의 크기
E	a와 b에 의해서 정의된 F_q 상의 타원곡선 (E : $y^2=x^3+ax+b$)
a, b	GF(p)의 타원 곡선 상의 임의의 원소 ($4a^3+27b^2\neq 0$)
n	G의 위수(order)
P	타원곡선 상의 한 점
점 Q	$(x_Q, y_Q)=dG$ (d : 비밀키, Q : 공개키)
$d_{e,m}$, $Q_{e,m}$	M의 일회용 키쌍
$d_{s,m}$, $Q_{s,m}$	M의 고정된 키쌍
$d_{s,v}$, $Q_{s,v}$	V의 고정된 키쌍
$d_{s,b}$, $Q_{s,b}$	B의 고정된 키쌍
K_{AB}	A와 B 사이의 세션키
{ }K	키 K를 사용하여 암호화
h()	해쉬 함수



<그림 1> 제안한 프로토콜의 전체 동작 방식

<그림 1>에서 보는 것처럼 제안한 프로토콜은 크게 5단계로 나눌 수 있다. 다음은 각 단계에 대해 설명이다.

(1) M이 V의 서비스를 요구하기 위해 연결을 시도한다.

- M은 일회용 키쌍($d_{e,m}$, $Q_{e,m}$)을 생성한다.
- M은 자신의 정보와 일회용 공개키를 B의 공개키

($Q_{s,b}$)로 암호화한다. 다음 정보 {h(M)||$Q_{e,m}$}$Q_{s,b}$는 M과 B 사이에서 사용자 식별을 위해 사용된다.
- M은 V에게 {h(M)||$Q_{e,m}$}$Q_{s,b}$, B을보낸다.

(2) V는 M을 식별하기 위해 M으로부터 받은 메시지를 다음과 같이 처리한다.
- V는 자신의 TS_v를 생성한다.
- M에게서 받은 메시지({h(M)||$Q_{e,m}$}$Q_{s,b}$)와 V의 TS_v 그리고 $Cert_v$를 B에게 보낸다.

(3) B는 V로부터 받은 메시지 중에 TS_v 값과 $Cert_v$가 유효한지 검사한다. 만약 그 메시지들이 유효하다면, B는 다음과 같은 일을 한다.
- B는 {h(M)||$Q_{e,m}$}$Q_{s,b}$를 복호화 한 다음 h(M)로 M을 식별한다.
- M이 정당한 사용자라면, B는 자신의 정보(B)와 M의 일회용 공개키를 B의 고정된 개인키로 서명한 값({h($Q_{e,m}$||B)}$d_{s,b}$)을 생성한다.
- B는 자신의 TS_b를 생성한다.
- B는 {h($Q_{e,m}$||B)}$d_{s,b}$, $Q_{e,m}$, $Cert_b$, TS_b를 V에게 보낸다.

(4) V는 B로부터 받은 $Cert_b$와 TS_b가 유효한지 검사한다. 만약 그 메시지들이 유효하다면, V는 다음과 같은 일을 한다.
- V는 B로부터 받은 서명값({h($Q_{e,m}$||B)}$d_{s,b}$)을 검증한다.
- B를 신뢰할 수 있다면, M의 일회용 공개키를 이용하여 <표 2>에서처럼 세션키(K_{mv})를 생성한다.[3]

<표 2> M과 V 사이의 세션키 생성방법

M		V
일회용 키 쌍($d_{e,v}$, $Q_{e,m}$) 생성	$Q_{e,m}$ →	$K_e = DH(d_{s,v}, Q_{e,m})$ $K_s = DH(d_{s,v}, Q_{s,m})$ $K_{mv} = K_e \| K_s$
$K_e = DH(d_{e,m}, Q_{s,v})$ $Ks = DH(d_{s,m}, Q_{s,v})$ $K_{mv} = K_e \| K_s$		
KeyData = kdf(K_{mv}, [SharedInfo])		KeyData = kdf(K_{mv}, [SharedInfo])

- V는 세션키로 h(V)||TS_b를 암호화한다.
- V는 자신의 생성한 타임스탬프(TS'_v)인증서($Cert_v$)와 암호메시지({h(V)||TS_b}$K_{m,v}$)와 함께 M에게 보낸다.

(5) M은 자신의 일회용 공개키와 V의 공개키를 이용하여 <표 2>에서처럼 세션키(K_{mv})를 생성하고 아래의 일을 한다.
- M은 V로부터 받은 암호메시지({h(V)||TS_b}$K_{m,v}$)를 자신이 생성한 세션키로 복호화하고. TS'_v와 $Cert_v$가 유효한지 검사한다. 만약 그 메시지들이 유효하다면, M은 다음과 같은 일을 한다.
- M은 V로부터 받은 복호화 한 메시지(h(V)||TS_b)를 자신의 개인키로 서명을 한다.
- 서명한 값과 TS'_v를 M이 생성한 세션키로 암호화한다.
- M은 {(h(h(V)||$Cert_m$||TS_b)$d_{s,m}$||TS'_v}$K_{m,v}$를 V에게 보낸다.

4. 제안한 프로토콜 보안 특성 비교

무선 인터넷에서 인증 및 키 합의 프로토콜의 여러 가지 보안 특성 중 이동 사용자와 서비스 제공자간 상호 신분 확인 및 익명성의 관점에서 GSM 인증 프로토콜[6,7], 혼합형 프로토콜, ASPeCT프로토콜[1]과 제안한 프로토콜에 대한 비교 내용을 <표 3>에 나타내었다.[8,9,10]

<표 3> 인증 및 키 합의 프로토콜 비교

보안 특성	GSM	혼합형 프로토콜	ASPeCT	제안한 프로토콜
묵시적 키 인증성	○	○	○	○
명시적 키 인증성	×	×	△	△
알려진 키에 대한 안전성	×	△	○	○
전향적 보안성	×	×	×	△
키 위장에 대한 안전성	×	×	×	○
미지의 키 공유	×	×	×	○
사용자 익명성	×	△	○	○

※ ○ : 좋음 △ : 보통 × : 나쁨

제안한 프로토콜에서 임시 신분의 세션별 갱신은 동일한 서비스 지역에서 세션이 빈번하게 발생하는 무선 인터넷에서 이용자 익명성의 보안 특성이 더욱

강화된다. 또한 제안한 프로토콜은 일회용 키쌍을 이용하여, 네트워크가 프로토콜 실행 초기에 이용자의 신분을 잠정적으로 확인할 수 있다는 점에서 프로토콜의 마지막에서 신분정보를 암호화하여 익명성을 유지하는 ASPeCT프로토콜과 차이가 있다.

5. 결론

무선 인터넷의 사용이 음성 위주에서부터 증권이나 뱅킹같은 데이터 서비스까지 폭 넓게 사용됨에 따라 사용자의 익명성과 인증 및 키 합의는 무선 인터넷에서 가장 중요한 보안 요소가 될 것이다. 본 논문에서는 이런 보안 요소를 해결하기 위해 프로토콜을 제안했다. 제안한 프로토콜은 통신 실체간 상호 인증 및 신분확인, 안전한 세션키 합의 그리고 이용자의 익명성 등이 기존의 프로토콜보다 안전하다.

이동 통신 환경에서의 보안은 무선 인터넷을 충분히 고려하여 이루어져야 하며 또한 단순히 무선 인터넷에서만 그치는 것이 아니라 유선 인터넷과의 연동을 반드시 고려해야 한다.

[참고문헌]

[1] G. Horn and B. Preneel. "Authentication protocols for personal communication systems," Computer Security - ESORICS'98, Lecture Notes in Computer Science, 1485, pp277-293, Springer Verlag, 1998.

[2] D. G. Park, C. Boyd and S. J. Moon, "Forward Security and Its Application to Future Mobile Communications Security," PKC 2000, Springer-Verlag, pp. 433-455

[3] ANSI X9.63, "Public Key Cryptography for the financial services industry : key agreement and key transport using elliptic curve cryptography," 2001.

[4] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, "An Efficient Protocol for Authenticated Key Agreement Protocol," Technical report CORR 98-05, University of Waterloo, Canada, March, 1998.

[5] C. J. Mitchell, "Security in Future Mobile Network," in Proceedings of the Second International Workshop on Mobile Multi-Media Communication(MoMuC-2), Bristol, April 1995

[6] A. Mehrotra, L. S. Golding, "Mobility and security management in the GSM system and some proposed future improvements," Proceedings of the IEEE, Vol: 86 Issue: 7, pp1480-1497, July 1998.

[7] GSM 03.20 version 6.01, Digital cellular telecommunication system(Phase 2+); Security related network functions, release 1997.

[8] 조동욱, 최연이, 김희도, 원동호, "이동 통신 환경에 적합한 상호 인증을 제공하는 키 분배 프로토콜의 설계," 한국정보보호학회 논문지, 제 10권 제 2호, 2000.

[9] 최영근, 김순자, "이동시스템에서의 효율적인 인증 및 키교환 프로토콜," 한국정보보호학회 논문지, Vol. 11, No. 2, pp.73-82, Apr. 2001.

[10] J. S. Go, K. J. Ko, "Wireless Authentication Protocol Preserving User Anonymity," SCIS, 2001.