무선통신 환경에서 타원 곡선을 이용한 SRP 프로토콜

유수정, 박영만, 박상규

한양대학교 전자전기컴퓨터공학부

Elliptic Curve Secure Remote Password Protocol in Wireless Communication

Su Jung Yu, Young Man Park, Sang Kyu Park

Division of Electrical and Computer Eng., Hanyang Univ.

요 약

본 논문에서는 확인자 기반의 SRP 프로토콜을 이용하여 무선통신 환경에서 상호 인증 프로토콜을 설계하는 것이다. 본 논문에서 제안한 타원 곡선 SRP 프로토콜은 타원 곡선 이산 대수 문제를 SRP에 적용시켜, 타원곡선의 높은 효율성과 보안성을 갖고, 스칼라 연산을 하게 됨으로써, 이동통신 시스템에 효율적인 인증 프로토콜을 제안한다.

I. 서 론

사용자 인증 프로토콜은 그 인증에 기반이 되는 요소에 따라 사용자 자체가 가지고 있는 물리적인 특징을 이용한 인증, 사용자가 소유한 물건을 통한 인증, 사용자가 알고 있는 지식을 통한 인증등으로 나눌 수 있다. 이러한 인증 방법 중 별도의 장비가 요구되지 않고, 쉽게 사용할 수 있는 방법 중 패스워드 프로토콜을 들 수 있다.

패스워드를 이용한 인증 프로토콜은 사용자의 패스워드를 서버에 저장하고 있는 평문등가(plaintext-equivalent) 프로토콜과 사용자의 패스워드가 서버에 존재하지 않고 다만 확인자만을 저장하고 있는 확인자 기반(verifier-based) 프로토콜이 있다. 확인자 기반 프로콜은 영지식(zero-knowledge)을 이용하고 있기 때문에 인증과정에서 사용자가 패스워드를 제공하지 않는다.

1997년 Thomas Wu는 이산 대수 문제를 기반으로 한 SRP (Secure Remote Password) 프로토콜을 제안하였다[1,2]. SRP 프로토콜은 사용자가 안전한 확인자 기반 방식을 위해 키의 크기를 크게 하거나 따로 저장 장소 (예를 들어, 스마트 카드)에 저장해 둘 필요가 없다. 또한 제 3의 인증기관도 필요하지 않다.

본 논문에서 제안하는 타원 곡선을 이용한 SRP 프로토콜은 SRP 프로토콜에서 제안하는 것과 달리 타원 곡선 이산 대수 문제를 기반으로 하고 있기 때문에 타원 곡선이 갖는 보안성과 효율성 이점을 갖는다. 이는 단말기에서 지수승을 계산하는

대신 스칼라 곱을 계산함으로써, 계산의 효율성을 극대화하고, 패스의 최적화를 한다.

또한 이 타원 곡선 SRP 프로토콜을 무선 통신 방법 중 WTLS에 적용시켜, 이동통신에서 효율적인 패스워드 방식을 이용한 인증 프로토콜을 설계한다.

II장에서는 인증 보안 프로토콜의 보안 요구사항을 알아보고, III장에서는 타원 곡선을 이용한 SRP 프로토콜을 제안하고, IV장에서 WTLS에서 이 타원곡선 SRP 프로토콜이 어떻게 동작하는지 보이고, 효율성에 대해 분석하며, V장에서 결론을 내린다.

II. 패스워드를 이용한 인증 프로토콜의 보안 요구 사항

패스워드를 이용하는 인증 프로토콜을 위해 다음 3가지 요구사항이 필요하다.

(1) 패스워드 프로토콜 설계시 가장 제약이 되는 부분이 패스워드를 넣는 키 공간이 작기 때문에 랜덤으로 선택된 키를 이용하는 방식에 비해 공격이 쉽다는 것이다. 패스워드를 암호화하는 키로 이용하게 되면 안전한 암호화 함수까지도 취약하게 만들 수 있다[3].

(2) 한 세션에 협상된 세션키는 패스워드에 대한 어떠한 정보도 가지고 있지 않아야 한다. 만약 이런 정보를 세션키가 가지고 있다면, 공격자에 의해 세션키 누출시 패스워드도 역시 누출 될 수 있다.

(3) 프로토콜은 Perfect forward secrecy 특성을 가지고 있어야 한다. 이는 패스워드가 만약 공격당하더라도 이전에 사용되었던 세션키가 누출되지 않아야 한다는 것이다[4].

III. 타원 곡선을 이용한 SRP 프로토콜

1. Asymmetric Key Exchange (AKE)

AKE나 EKE(Encrypted Key Exchange)는 키를 공유하여 인증하는 방식은 같지만 EKE 방식의 경우 두 객체가 같은 비밀키를 가지고 있어서 객체를 인증하지만, AKE 방식의 경우에는 공개키 방식을 사용하여 객체들의 공유키를 설정한다.

다음 나오는 표 1은 AKE에 쓰이는 매개 변수들과 함수의 정의이다.

표 1. AKE를 위한 매개변수와 함수

a, b, x, y	임의의 매개 변수
$H(\cdot)$	일 방향 확인자 생성 함수
$Q(\cdot, \cdot)$	개인 매개변수 조합 함수
$R(\cdot, \cdot)$	공개 매개변수 조합 함수
$S(\cdot, \cdot)$	세션키 생성 함수
K	세션키

AKE가 동작하는 방정식이 식 (1)에 나와 있다. 이 식은 자체로서는 보안성의 의미가 전혀 없고, 방정식에 쓰이는 함수로써 보안성을 갖게 된다.

$$S(R(H(a), H(x)), Q(b, y)) = S(R(H(b), H(y)), Q(a, x)) \quad (1)$$

(모든 a, b, x, y에 대하여)

2. 타원 곡선 SRP

SRP 프로토콜은 클라이언트와 서버간의 인증이 이루어지는 비대칭형 프로토콜이다. 프로토콜의 시작 개체는 항상 클라이언트이다.

본 논문에서는 타원 곡선 이산 대수 문제를 이용한 타원 곡선 SRP를 제안한다.

표 2. 타원곡선 SRP에서 쓰이는 기호

P	타원 곡선 군의 생성자
s	사용자의 랜덤 salt
Pwd	사용자의 패스워드
x	패스워드와 salt로부터 유도된 개인키
v	패스워드 확인자
u	공개적으로 알려지는 랜덤 스크램블링 매개 변수(Random scrambling parameter)
a, b	랜덤하게 생성되는 임시의 개인키 (공개적인 요소가 아니다)
A, B	a, b에 대응되는 공개키
$h()$	강력한 일방향 해쉬 함수
K	세션키

표 2는 타원 곡선 SRP 프로토콜에서 쓰이는 기호들을 나열한 것이다.

a, x, b, y는 인증 프로토콜 진행과정 중에서 개인키로 쓰이게 되는 매개변수로서 타원곡선 군의 위수 n에 대해 [1, n-1]의 값을 가져야 한다. 함수들은 AKE 방식을 따른다.

$H(x)$는 타원곡선 위의 점 P를 x번 더하는 계산을 하는 함수[5]이고, $Q(a, x)$은 개인 매개변수 조합 함수, 공개 매개변수 조합 함수 $R(A, v)$, 세션키 생성함수 $S(a, x)$의 표현이 다음 식 (2)에 정의되어 있다.

$$\begin{aligned} H(x) &= xP \\ Q(a, x) &= a + ux \\ R(A, v) &= A + u \cdot v \\ S(a, x) &= a \cdot x \end{aligned} \tag{2}$$

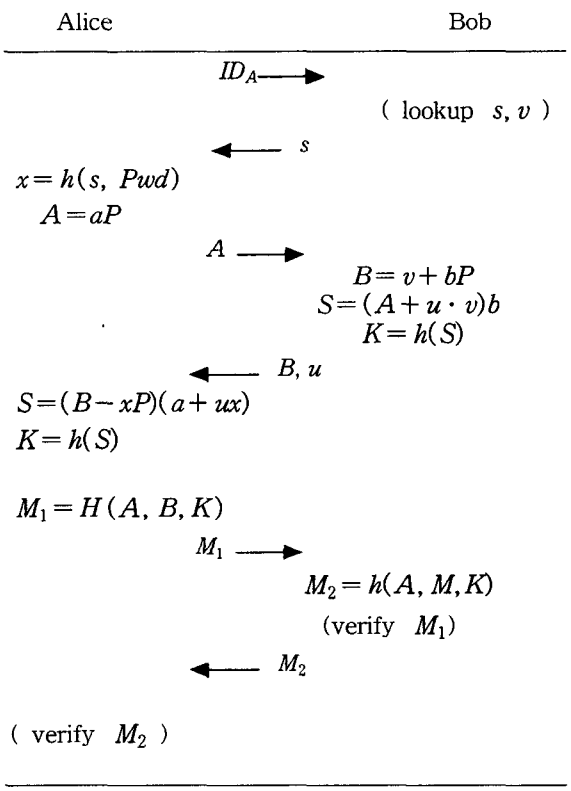

그림1. Alice와 Bob 간에 타원곡선 SRP 프로토콜

그림 1은 Alice와 Bob 사이에 타원 곡선을 이용한 SRP 프로토콜 설명하고 있다.

(1) Alice는 자신의 identity를 Bob에게 전달한다.

(2) Bob은 Alice의 확인자 $v(v=xP)$와 salt s를 찾은 후 s를 Alice에게 전달한다. Alice는 Bob에게서 받은 s와 자신의 패스워드 Pwd를 이용하여 확인자 x를 계산한다.

(3) Alice는 랜덤하게 자신의 임시 개인키 a를 선택하여, $A=aP$를 계산하여 Bob에게 보낸다.

(4) Bob 역시 랜덤하게 자신의 임시 개인키 b를 선택하고, $B=v+bP$를 계산한다. 그리고, 랜덤수 u를 택하여, Alice에게 받은 값 A와 함께, $S=(A+u\cdot v)b$를 계산한다. S에 강력한 일방향 해쉬함수를 이용하여 세션키 K값을 생성한다. 계산 값들이 다 정해지면, Bob은 계산에서 쓰였던 값들중 B와 u를 Alice에게 보내게 된다.

(5) Alice는 Bob에게서 받은 B와 u를 자신이 랜덤하게 선택했던 임시의 개인키 a와 함께 $S=(B-xP)(a+ux)$를 계산한다. S에 강력한 일방향 해쉬함수를 이용하여 세션키 K값을 생성한다.

(6) 세션키 값이 계산되면 Alice는 자신이 계산한 키 A와 Bob에게서 받은 B, 계산된 세션키 값 S를 해쉬함수를 이용한 M_1을 Bob에게 보내게 된다.

(7) Bob은 M_1을 검증한 후, Alice가 인증되었다는 M_2메시지를 보내게 된다. M_2는 Alice에게서 받은 키 A, M_1, 자신이 계산한 세션키 값 K에 해쉬함수를 이용한 값이다.

(8) Alice는 M_2를 검증하고 Bob을 인증한다.

3. 타원 곡선 SRP 프로토콜 분석

공격자가 세션키 K 를 알아냈다 하더라도 K, M_1, M_2 만 누출되고, 이 정보로부터 새로운 정보를 얻는 것은 힘들다. 그리고 세션키 K는 패스워드 Pwd에 대한 어떤 정보도 가지고 있지 않기 때문에 패스워드가 누출되지 않는 보안성을 가진다. 또한 타원 곡선 이산 대수 문제를 프로토콜에

적용시키므로서, 지수승을 계산하는 대신 군 연산을 함으로써, 계산의 효율성도 가져왔다.

IV. 무선통신 환경에서 타원곡선 SRP 프로토콜을 이용한 인증

무선 통신 환경에서 타원 곡선 SRP 프로토콜을 적용하였다. 여기서는 WTLS[6,7,8]의 경우를 고려하였다. 타원 곡선 SRP 프로토콜의 패스를 최적화하였고, WTLS에서 클라이언트와 서버간에 인증이 프로토콜을 설계하고 분석한다.

1. WTLS에서 타원 곡선 SRP

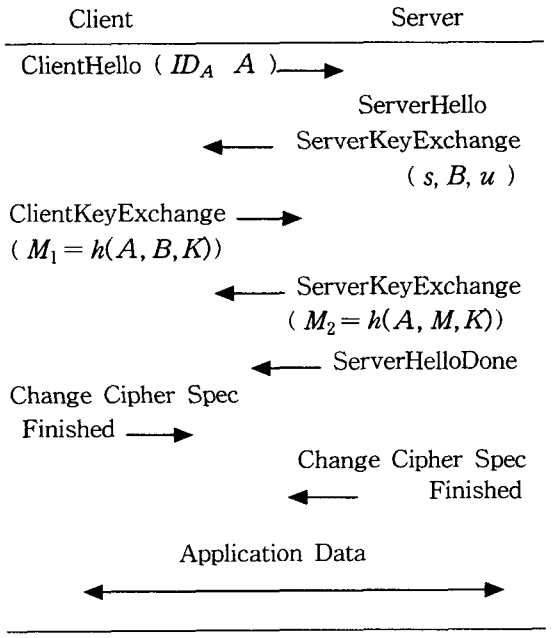

그림 2. WTLS에서 타원 곡선 SRP

그림 2는 WAP 프로토콜 중 WTLS 프로토콜에서 Handshake 프로토콜의 흐름도를 보여주고 있다. 보안과 관련된 모든 인자들은 handshake 동안에 정해진다. 이 인자들은 사용되는 프로토콜의 버전, 사용되는 암호화 알고리즘, shared secret을 생성하기 위한 공개키 기술과 인증에 대한 정보와 같은 속성들을 포함한다.

(1) Handshake는 Hello 메시지로부터 시작된다. 클라이언트가 서버에게 Client Hello 메시지를 보내면서 자신의 ID_A 와 임의로 임시 개인키 a를 선택하여 임시 공개키 A를 $H(x)$함수에 의해 계산하여 서버에게 보낸다.

(2) 서버는 Server Hello 메시지로 응답해야 한다. 서버는 확인자 v와 salt s를 찾은 후, 서버 자신이 선택한 임시 개인키 b를 이용하여 계산된 공개키 B, A를 사용해서 S를 계산하고, 일방향 해쉬 함수를 적용하여 세션키 K를 계산한다. 그리고 이때 선택하여 사용된 값 s, B, u 과 Server Hello 메시지를 클라이언트에게 보낸다. 이 Hello 메시지를 통해 클라이언트와 서버는 세션 capabilities에 합의한다.

(3) 클라이언트는 양측이 키 교환을 완료 할 수 있는 정보를 포함한 Client Key Exchange에 자신의 공개키 A와 서버에게 받은 공개키 B, 그리고 세션키를 해쉬함수로 서명(M_1) 하여 보내게 된다. 이때 서버는 클라이언트에게 받은 공개키 A와 자신이 계산한 공개키 B 를 사용하여 메시지 M_1을 검증하여 클라이언트를 인증한다.

클라이언트나 서버는 이전에 Change Cipher Spec 메시지를 사용하여 사로 조정한 세션 인자 값들을 사용하기 시작할지를 결정하게 된다.

(4) 클라이언트는 모든 데이터 검증을 포함한 메시지 Finished 메시지를 보낸다. 서버 역시 검증 결과인 Finished 메시지로 응답한다.

2. 무선 통신 환경하에서의 타원 곡선 SRP 프로토콜 분석

클라이언트와 서버간에 상호 인증을 한다. 서버의 identity는 제공되지 않고, 오직 클라이언트 identity만 제공된다.

만약 공격자가 과거에 사용된 세션키를 알았다 하더라도 각 세션마다 객체들의 임시 개인키가 다시 설정되므로 현재의 세션키를 알아내기는 힘들다. 또한 현재 설정된 개인키를 알았다 하더라도 x값을 유추할 수 없으므로, 현재의 세션키를 계산할 수 없으므로, 마지막 패스에서 세션에 참가는 객체나 서버에게 인증 받을 수 없다.

V. 결 론

본 논문에서 타원 곡선을 이용한 SRP 프로토콜은 타원곡선 암호 알고리즘의 이산 대수 문제를

기반으로 하여, 안전성과 효율성을 높은 프로토콜을 설계하였다. 또한, 이를 무선 통신 환경인 WTLS에 적용시켜 무선통신 환경에서 최적화된 패스로, 인증할 수 있음을 보였다.

VI. 참고문헌

[1] T .Wu, , "The SRP Authentication and Key Exchange System", *RFC 2945,* September 2000.

[2] T. Wu, "The Secure Remote Password Protocol", *in Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, CA,* Mar 1998, pp. 97-111

[3] D. P. Jablon, *"Strong Password Only Authenticated Key Exchange".* ACM SIGCOMM, vol. 26, no. 5, PP. 5-26, 1996

[4] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1996.

[5] A. Menezes, *Elliptic Curve Public Key Cryptosystems,* Kluwer Academic Publishers, 1993.

[6] Wireless Application Protocol Wireless Transport Layer Security Specification, Wireless Application Forum,

[7] Dierks, T. and C. Allen, "The TLS Protocol", *RFC 2246*, January 1999.

[8] Newman, C., "Using TLS with IMAP, POP3 and ACAP", *RFC 2595*, June1999.