M-Commerce 사용자를 위한 인증 및 키교환 프로토콜의 설계

박수진° · 서승현 · 이상호
이화여자대학교 컴퓨터학과
{moviefree°, happyday, shlee}@ewha.ac.kr

Design of an Authentication and Key Exchange Protocol for M-Commerce Users

Soo-Jin Park°, Seung-Hyun Seo and Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

M-Commerce 환경에서 이동통신 사용자가 다양한 서비스를 안전하게 제공받으려면 전송되는 메시지들을 암호화해야 하고, 이를 위해서 통신하는 개체들 사이에 세션키의 설정이 요구된다. 그러나 M-Commerce 환경은 유선환경에 비해 제약점이 있으므로 이를 고려한 보다 안전한 인증 및 키교환 프로토콜이 필요하다. 본 논문에서는 타원곡선 암호시스템을 사용한 효율적인 인증 및 키교환 프로토콜을 제안한다. 제안하는 프로토콜은 이동통신 사용자의 계산량을 줄여주고, 사용자의 신원을 M-Commerce 호스트에게 직접 드러내지 않음으로써 이동통신 사용자의 익명성을 보장하며, 사용자와 호스트 사이의 통신내용을 무선통신 사업자를 포함한 제 3자가 알지 못하도록 함으로써 통신정보의 기밀성을 보장한다.

1. 서론

최근 이동통신 사용자 수의 증가로 정보제공업자들은 M-Commerce 환경에서 게임, 금융 거래, 전자 지불, 온라인 예약 등 다양한 서비스를 제공하고 있다. 이러한 무선통신 환경에서 제공되는 서비스는 사용자에게 이동성 및 편리성을 제공하는 장점이 있으나, 유선에 비해 저속의 서비스를 제공하고 불안정한 통신품질을 가지기 때문에 실시간 공격, 도청으로 인한 평문의 노출, 다양한 사용자의 인증방식의 부족 등 보안상 많은 문제점들이 발생한다.[2] 그러므로 무선환경에서 안전한 통신을 보장하려면 통신하는 개체들이 주고받는 메시지가 암호화되어 전송되어야 하며, 전송되는 메시지를 암호화하기 위해서 통신하는 두 개체간의 세션키의 설정이 요구된다. 따라서 무선통신 환경의 문제점들을 해결하고 M-Commerce 환경에 적합한 효율적이고 안전한 키교환 프로토콜이 필요하다.

본 논문에서는 타원곡선 암호시스템을 사용한 인증 및 키교환 프로토콜을 제안한다. 타원곡선 암호시스템은 다른 암호시스템에 비해 비교적 짧은 키 길이로 동일한 보안강도를 제공하기 때문에 무선환경에 적합하다.[1][3] 본 논문에서 제안하는 프로토콜은 기존의 키교환 프로토콜들과 달리 무선통신 사업자가 M-Commerce 호스트와 이동통신 사용자 사이에 존재하므로 사용자의 계산과정의 일부분을 무선통신 사업자가 대신 수행하여 사용자의 계산량을 줄여줄 수 있고, 사용자와 호스트가 설정하는 세션키는 계산할 수 없기 때문에 둘 사이의 통신내용을 무선통신 사업자를 포함한 제3자가 알지 못하므로 통신정보의 기밀성이 보장된다. 또한, 이동통신 사용자는 무선통신 사업자를 통하여 M-Commerce 호스트에게 간접적으로 인증되므로 사용자의 익명성이 보장된다.

본 논문의 구성은 다음과 같다. 2장에서 용어 및 프로토콜의 환경, 보안 요구사항을 기술하고, 3장에서 제안하는 프로토콜을 제시한다. 4장에서 안전성 및 효율성을 분석한 후, 5장에서 결론을 맺는다.

2. 개요

이 장에서는 용어 정의와 제안하는 프로토콜의 환경, 보안 요구사항들을 기술한다.

용어 정의

- p : 사용되는 기반 필드 F_p의 크기(p는 소수)
- E : a와 b ($a, b \in F_p$)에 의해 정의된 F_p상의 타원 곡선
  ($E : y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0 \pmod{p}$)
- G : 타원 곡선 위의 기본점
- n : G의 위수
- U : 이동통신 사용자(mobile user)
- M : M-Commerce 호스트(contents provider)
- S : U와 M의 통신을 연결시켜주는 무선통신 사업자
- ID_M : 사용자 M의 식별자(identifier)
- pwd : U와 S사이에 미리 공유된 패스워드
- Q, Q^{-1} :, 패스워드 pwd로부터 계산하는 정수와 Q의 역수
- $H(\ )$: 강한 일방향(strong one-way) 해쉬 함수
- r_U : U가 구간 [2, n-2]에서 선택한 랜덤수
- R_U : r_U의 공개값, $R_U = r_U * G$
- c : 구간 [2, n-2]에서 선택한 랜덤수
- K : U와 M이 설정하는 세션키(session key)

· $E_K[\ ]$: 키 K를 사용한 대칭키 암호 알고리즘

· PK_M , SK_M : M의 공개키와 그에 대응하는 비밀키

· $\{\ \}_{PK_M}$: 키 PK_M을 사용한 공개키 암호 알고리즘

프로토콜 환경

이동통신 사용자가 M-Commerce 호스트로부터 서비스를 제공받기 위해서 무선통신 사업자를 통하여 M-Commerce 호스트 사이트에 접속한다. 이동통신 사용자와 무선통신 사업자 사이는 무선 네트워크(wireless network)로 연결되어 있고, 무선통신 사업자와 M-Commerce 호스트는 유선 네트워크(wired network)로 연결되어 있다. 본 논문에서는 이동통신 사용자와 무선통신 사업자 사이에 미리 공유된 패스워드가 있음을 가정하고 이를 사용하여 서로를 인증하도록 하고, 이 패스워드는 일정기간 후 무선통신 사업자가 사용자에게 패스워드의 갱신을 알리는 메시지를 전송하여 갱신하도록 한다. 또한 무선통신 사업자와 M-Commerce 호스트는 서로의 공개키를 포함한 인증서(certificate)를 가지고 있다고 가정한다. 제안하는 프로토콜 모델의 환경은 그림 1과 같다.

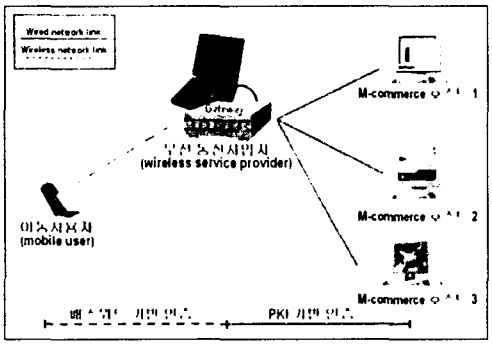

그림 1 프로토콜 환경

보안 요구사항

인증 및 키교환 프로토콜에 필요한 보안 요구사항들은 다음과 같다.[1]

① 개체 인증(entity authentication) : 프로토콜에 참여하고 있는 상대방의 신원이 확인 가능해야 한다.

② 키 확인(key confirmation) : 정당한 사용자가 자신이 의도한 상대방과 세션키가 공유되었음을 확인 가능해야 한다.

③ 묵시적 키 인증(implicit key authentication) : 상대방만이 세션키를 계산할 수 있음을 보장해야 한다.

④ 키 신규성(key freshness)을 제공해야 한다.

⑤ 능동적 위장 공격(active impersonation attack) : 공격자가 자신을 정당한 사용자로 위장하여 합법적인 사용자와 키교환을 수행하는 공격에 안전해야 한다.

⑥ 완전한 전향적 보안성(perfect forward secrecy) : 장기간(long term) 비밀키의 노출 및 분실이 있어도 현재의 세션키를 유추할 수 없어야 한다.

⑦ 알려진 키에 대한 안전성(known key security) : 사용자들 사이의 과거 세션키가 노출되어도 현재 세션키의 안전성에는 영향을 미치지 않아야 한다.

제안하는 프로토콜에 추가적으로 제공되는 요구사항은 다음과 같다.

⑧ 이동통신 사용자의 익명성(anonymity of mobile user) : M-Commerce 호스트가 무선통신 사업자를 통해 간접적으로 이동통신 사용자의 신원을 확인하게 함으로써 직접적으로 사용자의 신원을 알지 못하게 한다.

⑨ 통신정보의 기밀성(confidentiality of communication data) : 무선통신 사업자를 포함한 제 3자가 M-Commerce 호스트와 이동통신 사용자 사이의 통신내용을 알지 못하게 한다.

3. 제안하는 프로토콜 (Proposed protocol)

이동통신 사용자 U와 무선통신 사업자 S는 미리 공유된 패스워드 pwd와 pwd로부터 계산된 정수값 Q를 공유하고 있다. 모든 연산은 유한체 F_p에서의 연산이므로 mod p는 생략한다.

[이동통신 사용자 U => 무선통신 사업자 S]

Step 1. U는 구간 [*2, n-2*]에서 랜덤수 c와 r_U를 선택한다. 패스워드 인증을 위해 $x_U = r_U * Q$를 계산하고, 이의 공개값 $P_U = x_U * G$를 계산한다.

Step 2. U는 통신하려는 M-Commerce 호스트의 URL을 담은 req와 P_U, c값을 S에게 전송한다.

[무선통신 사업자 S => M-Commerce 호스트 M]

Step 3. U로부터 받은 값 P_U에 U와 미리 공유한 값인 Q의 역수 Q^{-1}을 사용하여 $Val_1 = Q^{-1} * P_U$ 를 계산한다.

Step 4. req로부터 M의 URL을 확인하고 { ID_S, Val_1, c }를 M의 공개키 PK_M으로 암호화하여 M에게 전송한다.

[M-Commerce 호스트 M => 무선통신 사업자 S]

Step 5. M은 구간 [*2, n-2*]에서 랜덤수 r_M을 선택하여 공개값 $R_M = r_M * G$를 계산하고, 전송 받은 암호문을 자신의 비밀키 SK_M으로 복호화한 후 U와의 세션키 $K = r_M * Val_1$을 계산한다. 그리고 나서 S에게 자신이 S로부터 전송 받은 Val_1값을 사용하였음을 알려주는 동시에, 자신이 전송한 R_M이 정당한지 확인시켜주는 $v = H(Val_1 \| R_M)$를 계산한다.

Step 6. 전송 받은 c를 세션키 K로 암호화하여 $E_K[c]$를 계산하고, $\{ID_M, E_K[c], v, R_M\}$을 S의 공개키 PK_S로 암호화하여 S에게 전송한다.

[무선통신 사업자 S => 이동통신 사용자 U]

Step 7. S의 개인키 SK_S로 암호문을 복호화한 후, M이 Step 3의 Val_1을 사용하였는지 확인하고 M이 전송한 R_M이 정당한지 검증하기 위해 $v' = H(A \| R_M)$을 계산하여 전송받은 v와 비교한다. $v' = v$ 인 경우, M이 Val_1을 사용하여 U와의 세션키 K를 계산하였고 전송 받은 R_M은 M이 생성한 올바른 값임을 확인할 수 있으므로 Step 8을 수행한다. $v' \neq v$ 인 경우 수행을 종료한다.

Step 8. S는 R_M을 패스워드 인증을 사용하여 전송하기 위해 $Val_2 = Q^{-1} * R_M$를 계산한 후 M에게 받은 $E_K[c]$와 함께 U에게 전송한다.

[이동통신 사용자 U]

Step 9. U는 Val_2를 사용하여 계산한 키 $K = x_U * Val_2$로 $E_K[c]$를 복호화하고, 복호화된 메시지가 자신이 생성한 c와 맞는지 검증함으로써 세션키 K가 올바른지 확인한다.

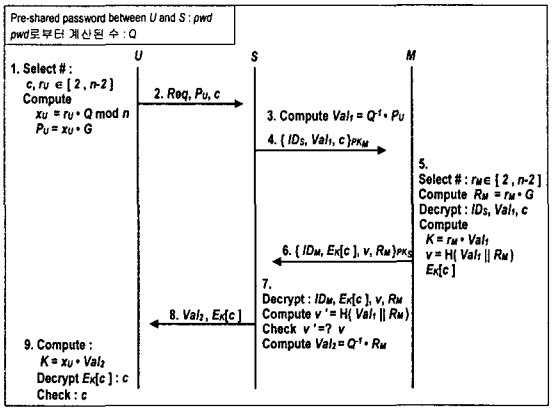

그림 2 프로토콜 흐름도

4. 안전성 및 효율성 분석

안전성 분석

① 개체 인증 : 이동통신 사용자와 무선통신 사업자는 미리 설정한 패스워드 pwd를 사용하여 서로를 인증하며, 각각 ID_S와 ID_M을 확인함으로써 M-Commerce 호스트와 무선통신 사업자는 서로를 인증한다. M-Commerce 호스트는 이동통신 사용자를 직접 인증하지 못하고 무선통신 사업자를 통해 간접적으로 인증한다.

② 키 확인 : 이동통신 사용자는 전송받은 암호문 $E_K[c]$을 복호화 하였을 때 얻은 메시지가 자신이 생성한 랜덤값 c임을 검증함으로써 M-Commerce 호스트와 이동통신 사용자 사이의 공유된 세션키 K가 존재함을 확인할 수 있다.

③ 묵시적 키 인증 : 비밀 랜덤값 r_U 또는 r_M을 아는 사람만이 세션키 K를 계산할 수 있음을 확신하므로 묵시적인 키 인증을 제공한다.

④ 키 신규성 : 매 세션마다 r_M과 r_U가 바뀌므로 매번 새로운 세션키가 설정되므로 키 신규성을 제공한다.

⑤ 능동적 위장 공격 : 이동통신 사용자는 무선통신 사업자와 패드워드 pwd를 공유하고 이로부터 계산된 Q^{-1}을 사용하여 통신값을 전달하므로 패스워드를 모르는 다른 사람이 해당 이동통신 사용자로 위장할 수 없다. 또한, M-Commerce 호스트와 무선통신 사업자 사이는 공개키 인증 기반 통신을 하기 때문에, 비밀키 SK_S 또는 SK_M을 모르는 다른 사람이 무선통신 사업자나 해당 M-Commerce 호스트로 위장할 수 없다. 따라서 본 프로토콜은 능동적 위장공격에 안전하다.

⑥ 완전한 전향적 보안성 : 공격자가 장기간(long term) 키인 패스워드 pwd를 알아냈을 경우라도 ECDH(Elliptic Curve Diffie-Hellman) 문제의 어려움[1]에 근거하여 세션키를 계산할 수 없으며, M-Commerce 호스트의 비밀키 SK_M과 무선통신 사업자의 비밀키 SK_S를 알아냈을 경우라도 통신내용은 노출되지만 ECDH 문제의 어려움에 근거하여 세션키 K는 계산할 수 없다.

⑦ 알려진 키에 대한 안전성 : 세션마다 새로운 랜덤값을 사용하여 세션키를 생성하므로, 과거 세션키의 노출이 현재 세션키의 안전성에는 아무런 영향을 미치지 않는다.

⑧ 이동통신 사용자의 익명성 : M-Commerce 호스트는 이동통신 사용자를 직접 인증하지 않고 무선통신 사업자를 통해 간접적으로 인증하여 세션키 K를 설정하기 때문에 M-Commerce 호스트에게 사용자의 신원이 노출되지 않으므로 이동통신 사용자의 익명성이 보장된다.

⑨ 통신정보의 기밀성 : 무선통신 사업자는 M-Commerce 호스트와 이동통신 사용자 사이의 세션키 K를 계산할 수 없으므로 무선통신 사업자를 포함한 제 3자로부터 사용자와 호스트 사이의 통신내용의 기밀성이 보장된다.

효율성 분석

M-Commerce 환경에서 이동통신 사용자의 계산량은 한계가 있기 때문에 키교환 프로토콜의 효율성은 이동통신 사용자의 계산량을 줄이는 것에 있다. 이동통신 사용자의 계산량을 고려해볼 때, 제안하는 프로토콜에서 많은 계산량이 요구되는 스칼라 곱셈 연산의 횟수는 P_U와 K를 계산할 때 2회이다. 이때 P_U는 오프라인 상에서 계산이 가능하기 때문에 온라인 상에서는 사용자가 K를 계산할 때 1회만 스칼라 곱셈 연산을 수행하면 되므로 무선환경에 적합하다. 또한, 무선통신 사업자가 이동통신 사용자를 대신하여 ID_M을 확인하고, v와 v'의 비교를 통해 호스트 M이 전송한 값이 정당한지 검증하기 때문에 사용자 U의 계산량을 줄일 수 있어서 효율적이다.

5. 결론 및 향후 연구

본 논문에서는 M-Commerce 환경에 적합하고 이동통신 사용자의 익명성을 보장하는 효율적인 인증 및 키교환 프로토콜을 제안하였다. 제안한 프로토콜은 이동통신 사용자의 계산량을 최소화함으로써 무선단말기의 한계점을 보완하고, M-Commerce 호스트가 무선통신 사업자를 통하여 이동통신 사용자를 간접 인증하는 형태로 사용자의 익명성을 제공하였다.

향후에는 제안한 프로토콜을 시스템으로 구현하고자 한다.

6. 참고문헌

[1] ANSI X9.63, "ANSI X9.63 : Public Key Cryptography for the Financial Services Industry : Key Agreement and Key Transport using Elliptic Curve Cryptography," ANSI Working Draft, 2000.

[2] B. Cho, Y. Ha, "Analysis of Wireless Internet Industry Trend in Korea," ETRI, 2002.

[3] L. Jacobs, "Elliptic Curve Cryptosystems An Overview," SANS, 2001.

[4] Y. Tseng, "Weakness in a Simple Authenticated Key Agreement Protocol," IEE Electronics Letters, Vol.36, No.1, pp.48-49, 2000.