Man-in-the-middle attack에 강한 변형된 AKE 프로토콜

장성렬*, 조현호**, 이경현***
*부경대학교 정보보호학과
**동부산대학 인터넷보안과
***부경대학교 전자컴퓨터정보통신공학부
e-mail : jiya686@lisia21.net*, chohh@dpc.ac.kr**, khrhee@pknu.ac.kr***

Secure modified AKE protocol against man-in-the-middle attack

Sung-Ryul Chang*, Hyun-Ho Cho**, Kyung-Hyune Rhee***
*Interdisciplinary Program of Information Security,
Pukyung Nat'l University
**Dept of Internet Security, Dong-Pusan College
***Division of Electronic, Computer, Telecommunication Engineering,
Pukyung Nat'l University

요 약

인터넷의 발전과 함께 사용자 인증 기술도 발전하였다. 이러한 사용자 인증 기술 중 패스워드 인증 기술이 특정 컴퓨터 또는 통신 시스템 서버의 서비스를 요구하는 클라이언트의 신분을 확인하는 기술로 가장 널리 사용되고 있다. 그러나 일반적으로 사용되는 패스워드 인증의 약한 안전성으로 인한 보안 사고는 매년 증가하고 있고, 그 피해 또한 상당하다. 본 논문은 이런 패스워드 인증 방식 중 강한 인증으로 분류되는 AKE 프로토콜에 대해 분석하고, man-in-the-middle attack이 가능하다는 것을 보인 후, 이 취약점을 보완하여 제 3의 신뢰기관을 두지 않고 두 파티간의 상호인증이 가능한 변형된 AKE 프로토콜을 제안한다.

1. 서론

요즘과 같은 정보화 시대에 인터넷상으로 데이터의 전송과 같은 정보의 유통이 급격히 증가함과 동시에 악의적인 목적을 가진 공격자에 의한 피해도 상당히 증가하고 있다. 그러므로 인터넷상에서 사용자와 정보 제공자(Client와 Server)간의 신뢰를 위한 상호간의 인증(Authentication)이 중요한 문제로 대두되고 있다.

패스워드 기반 인증 방식은 특정 사용자가 자신만이 알고 있는 비밀정보에 해당하는 패스워드와 자신의 이름(user name)을 시스템 서버에 제공하면 서버는 자신이 보유하고 있는 패스워드 파일에서 해당 사용자에 해당하는 패스워드와 비교해 봄으로써 인증을 하는 패스워드 기반의 인증 방식이다. 패스워드를 이용한 인증은 그 운영 메커니즘이 매우 단순하고 사용자들도 단지 패스워드만을 기억하면 되기 때문에 가장 편리하고 보편적인 인증방식으로 인식되고 있지만, 패스워드에 대한 불법적인 도청, 사전공격(dictionary attack)에 의한 패스워드 추측, 재생공격(replay attack), man-in-the-middle attack 등과 같은 보안상 문제점을 내포하고 있다[1]. 그러므로 패스워드 기반 프로토콜들은 악의적인 공격자에 의해 이루어지는 다양한 형태의 공격들로부터 대응할 수 있도록 구성되어야 한다.

이와 같은 보안상 강한 상호 인증 프로토콜에 대한 연구로는 패스워드 인증 수행을 위해 대칭 암호 방식과 공개키 암호 방식을 결합한 EKE(Encrypted Key Exchange)[2] 프로토콜을 들 수 있다. EKE 프로토콜은 사전 공격에 견디고 신뢰 기관이나 키 관리 없이 전향적 안전성(forward secrecy)을 제공하

는 최초의 프로토콜이다. 이런 EKE를 변형한 프로토콜로서 DH-EKE (Diffie-Hellman Encrypted Key Exchange)[3] 프로토콜과 SPEKE(Simple Passward Exponential Key Exchange)[3] 프로토콜이 있지만 이들의 가장 큰 단점은 평문 동등(plaintext-equivalent) 메커니즘[1]을 사용한다는 것으로 클라이언트나 서버가 동일한 비밀 패스워드나 해쉬값을 사용하는 문제점을 가진다. 그리고, EKE의 강화된 버전인 A-EKE(Augmented EKE) 프로토콜[5]은 사전 공격과 평문 동등성 문제는 해결하였지만, 전향적 안전성을 제공하지 못하는 문제점을 가지고 있다. 이러한 EKE 관련 프로토콜의 문제점을 해결하면서도 매우 효율적인 AKE (Asymmetric Key Exchange) 프로토콜[6]이 제안되었으나, 이 또한 man-in-the-middle attack에 취약한 단점을 가지고 있다. 본 논문에서는 AKE 프로토콜이 가지는 단점을 보완하면서도 거의 비슷한 계산량을 가지는 변형된 AKE 프로토콜을 제안하고자 한다.

본문의 구성은 다음과 같다. 2장에서는 AKE 프로토콜에 대한 분석과 함께 man-in-the-middle attack이 가능함을 보인 후, 3장에서는 man-in-the-middle attack에 강한 변형된 AKE 프로토콜을 제안하고, 4장에서는 본 논문에서 제시한 변형된 AKE 프로토콜의 안전성 분석을 한 후, 5장에서 결론을 맺는다.

2. AKE 프로토콜

2.1 개요

AKE 프로토콜 또한 두 파티(party)간 그들의 패스워드를 확인하기 위한 키를 교환한다는 점은 EKE 프로토콜과 동일하다. 하지만 프로토콜 흐름의 모두를 암호화하지 않는다는 것이 EKE 프로토콜과의 차이점이다. AKE 프로토콜은 초기에 설립된 패스워드와 이후 두 파티간 서로 교환한 임시값과의 결합을 위해 사전에 정의된 수학적 관계식을 이용하여, Client와 Server는 동일한 패스워드나 해쉬값을 사용하지 않고도 같은 세션키를 유도해 냄으로서 평문 동등성 문제를 해결하고 있다.

AKE 프로토콜 동작과정을 간단히 수식으로 표현해보면 다음과 같다. 한 파티에서 사용한 비밀값은 다른 파티에서는 공개값으로 사용되었다.

$$(\forall w,x,y,z)\quad S(R(R(P(w),P(x)),Q(y,z))) = S(R(R(P(y),P(z)),Q(w,x)))$$

2.2 AKE 프로토콜의 수학적 표기법

- w, x, y, z : 임의의 파라미터
- P(x) : 검증자가 생성한 일방향 함수 ($P(x)=g^x$)
- Q(w,x), R(w,x) : 공개 파라미터와 비밀 파라미터들의 결합 함수

  ($Q(w,x)=w+ux$, $R(w,x)=wx^u$,

  u : *random scrambling parameter, publicly revealed*)
- S(w,x) : 세션키 생성 함수 ($S(w,x)=w^x$)
- K : 세션키

2.3 AKE 프로토콜의 수행과정

① Client와 Server는 각각 long term secrets, x와 z를 생성한다.

② Client와 Server는 각각 x와 z를 일방향 함수 P( )로부터 산출된 값, P(x), P(z)를 서로 교환한다.

③ Client와 Server는 각각 long term secrets와 결합하기 위한 ephemeral 파라미터 w, y 값을 생성 후, 서로의 세션키를 확인하기 위한 값으로 P(w), P(y)를 생성해서 교환한다. ephemeral 파라미터는 매 세션마다 값이 바뀐다.

④ Client와 Server는 ①~③까지 서로 교환한 파라미터를 가지고 함수, Q( ), R( ), S( )를 통해 상호 인증을 위한 세션키를 생성한다.

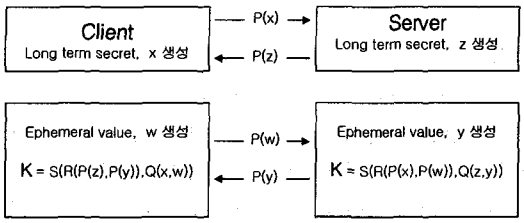

그림 1 AKE 프로토콜 수행과정

2.3 AKE 프로토콜의 취약점

AKE 프로토콜은 Client와 Server가 동일한 패스워드나 해쉬값을 사용하지 않으므로 평문 동등성 문제를 해결하고 있다. 그리고 매 세션마다 ephemeral 파라미터를 사용함으로써 전향적 안전성과 사전 공격으로부터 안전성을 모두 제공하고 있다.

그러나 AKE 프로토콜은 초기 long term secret을 설정할 때 DH 키 설정 방식을 사용하고 있으므로,

1) 어떤 데이터가 실제 패스워드를 통한 접속과 동일한 수준의 접속을 위해 사용된다면, 이러한 데이터를 특정 패스워드에 대한 "평문 동등하다"라고 정의한다. 평문 동등성을 피하기 위해서는 클라이어트/서버 양측에서 각각 비대칭적으로 동작하는 수학적 연산들을 선택해야 한다. [4]

DH 키 설정 방식의 알려진 문제점인 man-in-the-middle attack이 가능하게 됨을 그림 2에서 보여주고 있다.

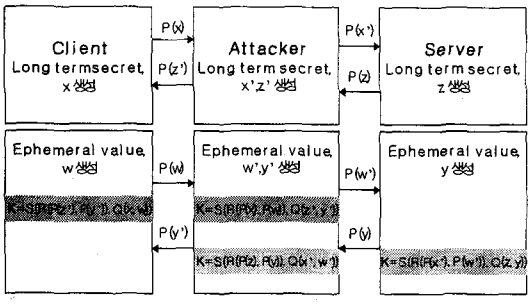

그림 2 AKE 프로토콜에 대한 man-in-the-middle attack

3. Modified-AKE 프로토콜

3.1 개요

2장에서 기술한 AKE 프로토콜은 [6]에서 제안되었으며, 이는 SRP(Secure Remote Passwod) 프로토콜을 구성하기 위한 근간을 이루는 프로토콜이다. 그러므로 AKE 프로토콜의 응용인 SRP 프로토콜 역시 man-in-the-middle attack 가능성을 완전히 배제하진 못한다. 따라서 본 절에서는 이러한 문제점을 보완하기 위한 방법으로 Interlock 프로토콜을 응용하고 있으므로 Interlock 프로토콜에 대해 기술하고 또한 man-in-the-middle attack에 강한 변형된 프로토콜을 제안한다.

3.2 Interlock 프로토콜

Man-in-the-middle attack으로부터 AKE 프로토콜을 보호하기 위한 방안으로 본 논문에서는 R. L. Rivest와 A. Shamir가 제안한 Interlock 프로토콜[7]을 응용한다. 이 프로토콜은 man-in-the-middle attack에 대한 방어와 동시에 제 3의 신뢰기관 없이 두 파티간의 상호인증이 가능하게끔 한다.

3.3 Interlock 프로토콜의 수행과정

Interlock 프로토콜의 수행과정은 그림 3과 같고, 이런 수행과정을 거쳐서 Client와 Server는 상호인증을 하게 된다. 수행과정 ①과 ②에서 공격자는 여전히 Client와 Server의 공개키를 자신이 만든 공개키로 대체하여 전송하는 man-in-the-middle attack을 취할 수 있다. 그러나, Client와 Server는 상대방의 공개키를 가지고 암호화한 값을 다시 반씩 나누어 전송하기에 ③과 ④에서 서로 전송한 메시지만 가지고서는 공격자가 메시지를 복호할 수 없고, ⑤와 ⑥에서도 마찬가지로 반만 가지고 있으므로 새로운 메시지로 복호할 수 없다. 그래서 ⑥과 ⑦에서 정당한 두 파티사이에 man-in-the-middle attack이 일어나면 두 파티는 상호인증을 할 수 없게 된다.

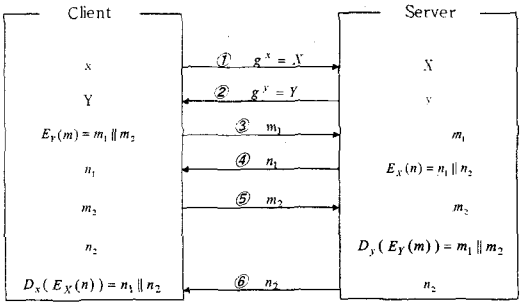

그림 3 Interlock 프로토콜의 수행과정

3.4 Modified-AKE 프로토콜

본 절에서는 기존의 AKE 프로토콜과 Interlock 프로토콜을 응용하여 man-in-the-middle attack에 강한 변형된 AKE 프로토콜 제안한다. AKE 프로토콜에서 사용한 수학적 표기법은 그대로 모두 사용하고, DH 방식의 세션키 k와 Client에서 보내는 메시지 m, Server에서 보내는 메시지 n을 추가한다.

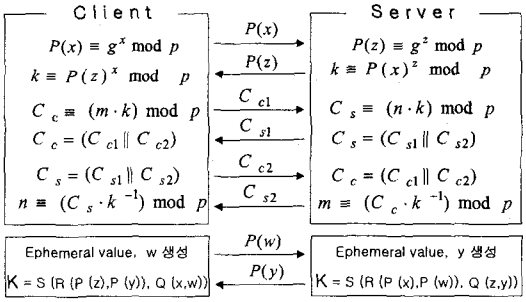

그림 4 Modified-AKE 프로토콜 수행과정

· m : Client에서 생성한 메시지
m = Client_ID|| $P(x)$||Timestamp||Random_Number
· 메시지 n : Server에서 생성한 메시지
n = Server_ID|| $P(z)$||Timestamp||Random_Number

Interlock 프로토콜에서의 암호화 함수 $E(\cdot)$는 공개키 암호화 알고리즘으로 이를 그대로 응용할 경우 그로 인한 계산량 측면의 오버헤드가 상당히 증가하여 제공되는 보안 서비스에 비해 비효율적으로 될 것이므로, 제안하는 Modified-AKE 프로토콜에서는

Client와 Server간의 DH 협상키인 k를 법 p상에서 메시지 m과 곱셈을 수행하는 것으로 적용하였다.

또한 메시지 m과 n의 구성상에서, man-in-the-middle attack은 통신로상의 두 파티간의 공개키 교환 시 그 공개키를 위조함으로써 발생된다는 점을 감안하여, 서로의 공개키에 대한 신뢰성을 부여하는 의미로 공개키를 사용하였으며, 그리고 Replay attack을 방지하기 위해 Timestamp를 추가하였으며, 프로토콜이 반복될수록 공격자가 Timestamp의 유효범위(threshold)를 유추할 가능성이 있기에 이를 보완하기 위해 Random_Number를 추가하였다.

그리고, 정당한 사용자라면 메시지 m과 n을 재구성할 수 있으며, User_ID 및 공개키의 일치여부를 확인함으로써 상호인증을 수행하게 된다. 그 이후의 수행과정은 AKE 프로토콜의 수행과정과 동일하다.

4. Modified-AKE 프로토콜 안전성 분석

Modified-AKE 프로토콜은 키 설정 부분에서 Interlock 프로토콜을 응용하여 만약 정당한 두 파티 사이에서 man-in-the-middle attack이 발생하였다고 가정할 경우, 그림 5와 같이 공격자는 각각의 DH 협상키 k_1, k_2 를 소유하고 있다 하더라도 Client 및 Server가 최초로 보내는 메시지 c_{c1}' 과 c_{s1}'으로부터 원 메시지 m, n의 구성 내용을 알지 못하므로 위조할 수 없고, c_{c2}'와 c_{s2}'도 위조할 수 없게 되므로 그대로 상대측으로 전송하게 되고, 따라서 최종 메시지를 받은 Client와 Server는 상호 전송한 메시지 m과 n을 재구성할 수가 없으므로 상호인증을 할 수가 없게 된다.

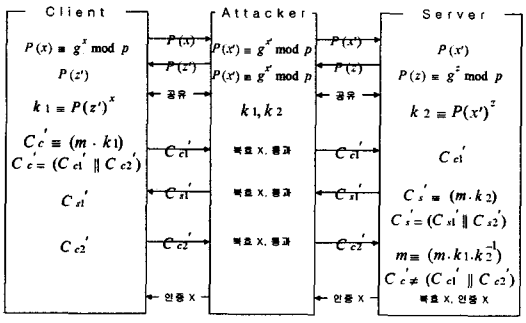

그림 5 Man-in-the-middle attack으로부터 보호

물론, c_{c2}', c_{s2}' 메시지가 전송이 된 후 공격자는 메시지 m, n을 재구성할 수 있으나, 이미 Modified-AKE 프로토콜은 인증이 실패하여 중단되었기에 공격자는 더 이상 공격할 수 없다. 또한 메시지 m, n의 구성 내용은 공개되어도 무방한 정보들과 매 프로토콜 수행 시마다 변하는 random number로 구성되어 있으므로 차후 공격에 있어서도 제안된 변형 프로토콜은 안전하다 할 수 있다.

5. 결론 및 향후과제

본 논문에서 제안한 Modified-AKE 프로토콜은 거의 유사한 계산량으로 기존 AKE 프로토콜의 문제점이었던 man-in-the-middle attack에 취약하다는 단점을 보완하여 제 3의 신뢰기관 없이 두 파티간의 안전한 상호 인증을 제공하고 있다. 그러나, 기존 AKE 프로토콜에 비해 메시지 교환 횟수가 상당히 증가하여 효율성은 오히려 감소하였다.

앞으로의 연구 과제로는 안전성은 그대로 유지하면서 AKE 프로토콜과 메시지 교환 횟수가 거의 비슷한 수준으로 감소시켜 효율성을 증대시키는 방향에 초점을 맞추어야 할 것이다.

참고문헌

[1] 박창섭, "암호이론과 보안", 대영사, pp.191~193, 2001

[2] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange : Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy, pp.72~84, 1992

[3] D. Jablon "Strong password-only authenticated key exchange", Computer Communication Review, 26(5), pp.5~26, 1996

[4] 김영수, 나중찬, 손승원, "패스워드 인증 프로토콜 동향", 전자통신동향분석 제16권 제6호, 2001

[5] S.M Bellovin and M. Merritt, "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise", TR, AT&T Bell Lab, 1994

[6] T. Wu, "The Secure Remote Password Protocol", NDSS '98, 1998 Internet Society Symposium on Network and Distributed System Security, 1998

[7] R. L. Rivest and A. Shamir, "How to Expose an Eavesdropper", Communications of the ACM, v.27, n.4, pp.393~395, 1984