안전하고 효율적으로 인증된 키 교환 프로토콜

박종민* · 박병전**

Authenticated Key Exchange Protocol for the Secure and Efficient

Jong-Min Park* · Byung-Jun Park**

요 약

키 교환 방식은 안전한 암호 통신을 위하여 매우 중요하다. 키 교환 프로토콜은 안전성, 키 확신, 키 신선도 등의 요구사항을 만족해야 한다. 본 논문에서는 두 개의 인증된 키 교환 프로토콜로 EKE-E 와 EKE-S를 제안한다. 프로토콜들의 기본적인 생각은 암호가 단위 추가 N에 의하여 나타내어질 수 있는 것이고, 암호를 나타내는 가능한 단위 추가 N 수는 2^N 이다.

EKE-E는 main-in-the-middle 공격과 오프라인 사전 공격을 포함하고, 실행은 또 다른 것과 비교해서 우수하며 중요한 교환 프로토콜들의 신임도를 인증한다. EKE-S는 EKE-E에 대한 약간의 변형이다. EKE-S는 EKE-E의 공격을 보존하는 동안에 오프라인 사전 공격을 하지 못하고 암호를 습득하기 위하여 평가 실행 불가를 제공한다.

ABSTRACT

The Key exchange protocols are very crucial tools to provide the secure communication in the broadband satellite access network. They should be required to satisfy various requirements such as security, Key confirmation, and Key freshness. In this paper, we propose Two authenticated key exchange protocols Two Pass EKE-E(Encrypted Key Exchange-Efficient) and Two Pass EKE-S(Encrypted Key Exchange-Secure) are introduced. A basic idea of the protocols is that a password can be represented by modular addition N, and the number of possible modular addition N representing the password is 2^N.

The Two Pass EKE-E is secure against the attacks including main-in-the-middle attack and off-line dictionary attack, and the performance is excellent so as beyond to comparison with other authenticated key exchange protocols. The Two Pass EKE-S is a slight modification of the Two Pass EKE-E. The Two Pass EKE-S provides computational in feasibility for learning the password without having performed off line dictionary attack while preserving the performance of the Two Pass EKE-E.

키워드

EKE-E, EKE-S, 프로토콜, 알고리즘

Key words

Encrypted Key Exchange-Efficient, Encrypted Key Exchange-Secure, protocol, algorithm

* 조선이공대학 사이버보안과 (pjm5234@lycos.co.kr)

** 조선대학교 (교신저자)

접수일자 : 2010. 04. 28

심사완료일자 : 2010. 05. 27

Ⅰ. 서 론

두 개의 존재, 어느 누군가 패스워드를 공유하고, 어느 누군가 존재하는 것을 기대할 수 없는 계통으로 통신하며, 서로의 신임도를 인증하는 것을 원하고 그들의 다음 의사소통을 막기 위하여 긴키에 대하여 동의한다.

짧은 암호라 불리는 키 교환 문제의 신임도를 인증하는데 EKE(Encrypted Key Exchange) 프로토콜은 신임이 인증된 첫 번째 암호이며, 키 교환은 프로토콜을 작성한다[1,2]. EKE의 생각은 암호가 암호해독의 키의 프로토콜 메시지들을 암호화하도록 사용한다. 그 다음에 암호를 추측하는 공격자는 대칭암호는 해독할 수 있으나, 메시지들에 비대칭적 암호는 중단할 수 없었고, 추측이 이처럼 진실임을 증명할 수 없다. EKE 지역에 다음 작업들의 다수를 위해 기초가 된다[3-5].

신임도가 인증된 키 교환 프로토콜은 재 발송, 페어플레이, 엿보기, man-in-the-middle 공격, 분할공격 그리고 오프라인 사전공격과 같은 공격들에 대해서 억제된다[6-10]. 공격자는 책임자등에게 비밀을 유지하기 위해 추측된 감지가능 데이터에 접근을 할지도 모른다. 신청한 사람의 약간은 프로토콜이 제거되었던 중요한 교환의 신임도를 인증한다[11]. 사용자로부터 데이터를 훔칠 수 있었던 공격자가 사전공격을 하지 않고 사용자로서 나중에 몰래 참가할 수 없기 위해서는 중요한 교환 프로토콜들의 신임을 인증하였던 신청한 사람의 약간의 암호파일 타협에 대해서 보호되기를 의도한다[12].

프로토콜이 적어도 세 개의 통행을 요구하였고, 적어도 두 번 단위 지수화를 수행하였던 것을 신청한다. 본 논문에서는 두 개의 신임이 인증된 키 교환 프로토콜들 EKE-E(Encrypted Key Exchange-Efficient)와 EKE-S (Encrypted Key Exchange-Secure)를 소개한다. 프로토콜들의 기본적인 생각은 암호가 단위 추가 N 에 의해서 나타내어질 수 있는 것이며, 그리고 암호를 나타내는 가능한 단위 추가 N 수는 2^N 이다.

EKE-E는 재 발송, 페어플레이, 엿보기, man-in-the-middle 공격, 분할공격 그리고 오프라인 사전공격과 같은 공격들에 대해서 안전하다. 그러나 약점이 있으므로 파일에 암호를 성립한다. EKE-E의 통행 수는 두 개이고 EKE-E는 모듈 지수화를 다시 요구하지 않는다. EKE-S는 EKE-E의 약간의 변형을 위해서 EKE-E의 공격을 보존하는 동안에 오프라인 사전 공격을 하지 않고 암호를 습득하기 위하여 암호 파일 타협에 대해 안전하기 위해서 공격들에 대한 안전은 EKE-E에서 보호된다[13].

Ⅱ. 관련 연구

2.1 안전하게 인증된 키 교환

키 교환 프로토콜이 보호 대비하여 필요로 하는 현재의 기본적인 공격의 목록이다.

- Replay attack: 공격자는 과거에 이루어졌던 통신상에서 보내진 메시지를 기록하고, 그것을 후에 다시 그들에게 보낸다.
- Pre-play attack : 공격자는 과거에 이루어졌던 통신상에서 보내진 메시지를 기록하고, 기록된 메시지들 중 특정 메시지를 현행 통신을 위해 결정한다.
- Eavesdropping : 공격자는 라인 상에 메시지를 듣고 통신 진행 중에 중요한 정보를 얻으려고 노력한다.
- Man-in-the-middle : 공격자는 집단들 사이에 보내진 메시지를 차단하고 그것을 공격자들의 메시지로 대신한다.
- Password guessing attacks : 공격자들은 패스워드의 일반적인 선택사항을 포함하고 있는 상대적으로 작은 사전에 대해 접속할 수 있는 것으로 간주된다. 기본적으로 공격자들이 사전을 사용할 수 있는 두 가지 방법이 있다. 즉 온라인과 오프라인 사전 공격이다.
- Off-line dictionary attack : 공격자들은 과거의 통신을 기록하고, 사전에 대충 보고, 기록된 통신과 일치하는 패스워드를 찾는다. 만약에 패스워드가 발견되면, 공격자는 이것을 공격의 패스워드라고 결론짓는다.
- On-line dictionary attack : 공격자들은 반복적으로 사전에 있는 패스워드를 선택하고, 사용자라고 구현시키기 위해서 그것을 사용하려고 노력한다. 만약에 사용자로서의 구현이 실패하면, 공격자는 사전에 패

스워드를 없애고, 다른 패스워드를 사용하면서 계속적으로 공격을 시도한다. 실행에 있어서 이러한 온라인 사전 공격을 예방하기 위한 일반적인 방법들은 사용자가 그 패스워드가 파기되어지기 전에 사용자에게 주어진 실패의 횟수를 줄이는 방법이나, 사용자의 로그인 시도 횟수의 비율을 낮추는 것이다. 이러한 이유 때문에 우리는 오프라인 사전 공격을 고려해야 한다.

- Password file compromise : 공격자들은 사용자인척 함으로써 패스워드 파일에서 비밀로 지켜지는 여러 민감한 자료들에 대해 접속을 한다.
- Server compromise : 확인자가 승인자를 의인화한다면 신분확인 도식에 대해 가능하게 한다.

2.2 표기법

표기법은 아래와 같이 나타낸다.

A, B : 시스템 관계자

P : A shared password for A and B.

X_1, Y_1, X_2, Y_2 : Integers such that$(X_1 + X_2)$ mod N≡P and$(Y_2\ Y_1)$ mod N≡P.

N, M : Positive integer suitable for symmetric key cryptosystem.

R_1, R_2 : 무작위의 수

E_K : Symmetric encryption with key K.

D_K : Symmetric decryption with key K.

H_1, H_2 : One way hash functions.

SK : session key shared between participants after completion of the protocols.

Ⅲ. EKE-E

EKE-E 프로토콜은 그림 1에서 나타낸다.

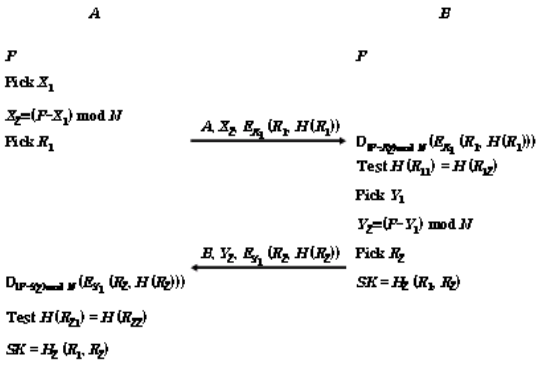

그림 1. EKE-E 프로토콜
Fig. 1 EKE-E protocol

EKE-E에서 각 참여자는 명확하게 P를 축척하고 있고, A는 무작위로 X_1과 R_1을 선택하고 $(0 \le X_1 \le N-1, 0 \le R_1 \le M-1)$, $(X_1 + X_2)$ mod N ≡P. B가 그가 단지 X_2만 받은 다고 할지라도 X_1을 학습할 수 있을 정도로 X_2를 결정할 수 있을 것이다. 유사하게 B와 함께, A는 B를 입증할 수 있다. 단지 R_1과 R_2를 회복할 수 있는 무리들은 세션 키를 공유할 수 있다.

키들과 메시지들이 닥치는 대로 선택되기 때문에 EKE-E는 재 시합 공격에 대해서 안전하다. 또한 EKE-E는 페어플레이 공격에 대해서 안전하기 때문에 실행 불가능하며 과거 통신들에 키들을 알지 않고 널리 알려진 통신을 위해 메시지를 만들기 위함이다. 각각의 키가 키에 의하여 암호화되었기 때문에 EKE-E는 들린 메시지들로부터 유용한 정보를 공격하려고 한 공격자에 대해서 안전하다. EKE-E는 man-in-the-middle 공격에 대해서 안전하기 때문에 실행 불가능하며 과거 통신들에 키들을 알지 않고 그 자신의 메시지들에 파티들 사이에 보내진 메시지들을 대체하기 위함이다.

어떠한 un-chosen 완전체가 암호문을 위해 모두 가능한 지원자들을 저장하기 위하여 선택될 수 있기 때문에 EKE-E는 분할 공격에 대해 안전하다. EKE-E는 암호 파일 타협에 상처를 입기 쉽다.

명백하게 EKE-E의 실행은 또 다른 것과 비교해서 우수하며 중요한 교환 프로토콜의 신임을 인증하였으며

표 1에서 나타낸다. 표 1에서 난수 발생기는 한 난수를 산출하며 난수의 해야 할 일은 중요하고 또 다른 부분을 위해 메시지로 사용된다.

표 1. EKE-E 평가실행
Table 1 : The performance of EKE-E

	A	B
Pass	1	1
Symmetric key crypto system	2	2
Hash function	3	3
Random number generation	1	1

Ⅳ. EKE-S

EKE-E의 변경을 무시하고 오프라인 사전공격을 하지 않으며 암호를 알기 위하여 암호파일 타협에 대해서 안전한 EKE-S을 만든다.

EKE-S에서 A는 X_1 을 선택하고 $(X_1 + X_2) \bmod N \equiv P$ 로 X_2 를 결정하고 그런 후에 $(X_1^2 + 2X_1X_2) \bmod N$ 과 X_2^2를 축척할 수 있다. 유사하게, B는 Y_1 을 선택하고 $(Y_1 + Y_2) \bmod N \equiv P$ 로 Y_2 를 결정한 후에 $(Y_1^2 + 2Y_1Y_2) \bmod N$ 과 Y_2^2.를 축척할 수 있다.

EKE-S 프로토콜은 그림 2에서 나타낸다.

3

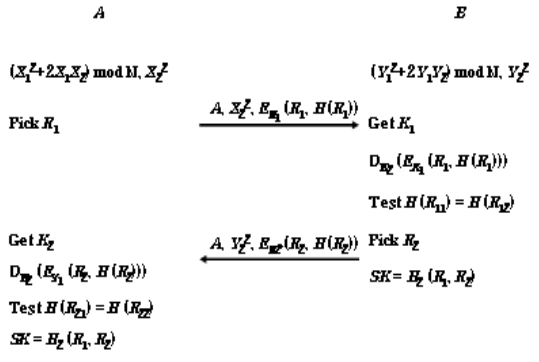

그림 2. EKE-S 프로토콜
Fig. 2 EKE-S protocol

EKE-S에서 K_1 은 $(X_1^2 + 2X_1X_2) \bmod N$ 이고 K_2 는 $(Y_1^2 + 2Y_1Y_2) \bmod N$이다. B는 $(X_1 + X_2)^2 \bmod N \equiv (Y_1 + Y_2)^2 \bmod N$ 인 사실을 이용하여 K_1 을 갖게 된 후, $H(R_{11})=H(R_{12})$이 $(R_{11}, H(R_{12}) = D_{K_1}(E_{K1}(R_1, H(R_1)))$ 인 곳을 유지되는지를 시험한다. 유사하게 B와 함께, A는 B를 입증한다.

EKE-S는 재 발송, 페어플레이, 엿보기, man-in-the-middle 공격, 분할공격 그리고 오프라인 사전공격과 같은 공격들에 대해서 안전하다. 비록 한 가지 키가 되풀이하여 사용될지라도 어떠한 un-chosen 정수가 메시지로 선출할 수 있기 때문에 EKE-S는 분할 공격에 대해서 안전하다. 제곱근 나머지 n에 대하여 주어진 복합물 정수 n과 2차 방정식 나머지를 위해 정수 모듈 n의 제곱근을 발견한다. 만약 요소 p와 q가 알려져 있으면, SQROOT 문제에 옮겨지고 n의 변화 문제는 다항식 알고리즘이 주어지지 않아 풀 수 없다.

이러한 특성은 n=p, q를 변하게 하였으며 이 두 수식 p와 q는 n이 실행 불가능 한 것을 평가하기 위해 이것을 선택한다. 그때의 모드적인 n에 x을 발견하는 문제에서 주어진 $(x+t)^2$이 다항식 알고리즘이 주어지지 않아 풀 수 없기 때문이다. 우리들은 위쪽에 소유권이 사실인 것을 쉽게 알고 있기 때문에 나머지 n에 대하여 주어진 복합물 정수 n을 위해 나머지 n의 제곱근을 발견하는 문제와 이차 방정식의 나머지는 주어진 t이며, 나머지 n에 대하여 이차 방정식의 나머지 n을 위해 $(x+t)^2$와 n에 x를 발견하는 문제의 특별한 사례이다. 공격자는 암호파일에서 비밀을 유지되도록 추측된 감지 가능 데이터에 접근을 얻을지도 모른다. 언급된 자료로부터, EKE-S는 비록 암호파일이 절충하더라도 오프라인 사전을 수행하지 않고 암호가 공격을 하는 것을 결정하기 위하여 평가 실행을 불가능 하도록 한다. 표 1은 또한 EKE-S의 실행이다.

Ⅴ. 결 론

신임도가 인증된 EKE-E와 EKE-S라 알려진 중요한 교환 프로토콜들을 주었다. 프로토콜들의 기본적인 생

각은 암호가 단위 추가 N에 의하여 나타내어질 수 있는 것이고 암호를 나타내는 가능한 단위 추가 N 수는 2^N 이다.

프로토콜들의 기본적인 생각은 암호가 단위 추가 N에 의하여 나타내어질 수 있는 것이고 암호를 나타내는 가능한 단위 추가 N 수는EKE-E이며, 오프라인 사전공격을 포함하는 공격들에 대해서 안전하고, EKE-E의 실행은 또 다른 것과 비교해 우수하며, 중요한 교환 프로토콜들의 신임도를 인증하였다.

EKE-S는 EKE-E의 약간의 변형과 그리고 EKE-S는 EKE-E의 공격을 보존하는 동안에 오프라인 사전공격을 하지 않고 암호를 알기 위하여 평가 실행이 불가능하고 공격들에 대해서 안전은 EKE-E가 보호하였다. EKE-S 실행은 EKE-E가 적당하다.

참고문헌

[1] E. Bach, Algorithmic Number Theory, Volumn 1 : Efficient Algorithms, MIT Press, Cambridge, Massachusetts, 1996.

[2] M. Bellare, D. Pointcheaval, and P. Rogaway, “Authenticated key exchange secure against dictionary attacks”, Advances in Cryptology Eurocrypt’00, LNCS Vol. 1807, Springer-Verlag, pp. 139-155, 2000.

[3] S. M. Bellovin and M. Merrit, “Encrypted key exchange : Password-based protocols secure against dictionary attack”, In Proceedings of IEEE Security and Privacy, pp. 72-84, 1992.

[4] S. M. Bellovin and M. Merrit, “Augmented encrypted key exchange : Password-based protocol secure against dictionary attack and password file compromise”, In ACM Security (CCS‘93), pp. 244. 250, 1993.

[5] V. Boyko, P. MacKenzie, and S. Prenel, “Probably secure password authenticated key exchange using Diffie-Hellman”, In B. Prenel, editor, Advances in Cryptology Eurocrypt’00, LNCS Vol. 1807, Springer -Verlag, pp. 156-171, 2000.

[6] O. Goldreich and Y. Lindell, “Session key generation using heman passwords only”, Advances in Cryptology, Crypto’01, LNCS Vol. 2137, S[romger-Verlag, pp. 408-432, 2001.

[7] D. Jablon, “Strong password-only authenticated key exchange”, ACM Computer Communication Review, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-20, October 1996.

[8] J. Katz, R. Ostrovsky, and M. Yung, “Efficient password authenticated key exchange using human memorable passwords”, Advances in Cryptology Eurocrypt’01, LNCS Vol. 2045, Springer-Verlag, pp. 475-494, 2001.

[9] S. Lucks, “Open key exchange : How to defeat dictionary attacks without encrypting public keys”, In Proceedings of the Workshop on Security Protocols, 1997.

[10] P. MacKenzie, S. Patal and S. Swaminathan, “Password authenticated key exchange based on RSA”, Advances in Cryptology Asiacrypt’00, LNCS Vol. 1976, Springer-Verlag, pp. 599-613, 2000.

[11] S. Patal, “Number theoretic attacks on secure password schemes”, In proceedings of IEEE Security and Privacy, pp. 236-247, 1997.

[12] M. Steiner, G. Tsudik, and M. Waidner, “Refinement and extension of encrypted key exchange”, ACM Operating System Review, 29, pp. 22-30, 1995.

[13] Byung-Jun Oark, Jong-Min Park, “Security in the Password-based Identification”, The Korean Institute of Maritime Information & Communication Science, Vol. 5, No. 4, pp. 346-350, 2007.

저자소개

박종민(Jong-Min Park)

1988. 조선대학교 전자계산 공학석사
2005. 조선대학교 컴퓨터공학 공학박사

2008. ~ 현재. 조선이공대학 사이버보안과 교수
※관심분야: 바이오인식, 패턴인식, 인공지능, 정보보호 및 보안

박병전(Byung-Jun Park)

1993. 서울대학교 통계학 이학석사
1998. 조선대학교 통계학 이학박사
2005. ~ 현재. 조선대학교 전산통계학과

※관심분야 : 바이오인식, 패턴인식, 통계학, 정보보안