情報保護學會論文誌
第11券 第5號, 2001. 10

복구 가능한 패스워드 기반 키 분배 프로토콜

손 기 욱*, 최 영 철**, 박 상 준**, 원 동 호***

Recoverable Password Based Key Exchange Protocol

Kiwook Sohn*, Youngcheol Choi**, Sangjoon Park**, Dongho Won***

요 약

본 논문에서는 사용자의 패스워드를 복구할 수 있는 패스워드 기반 키 분배 방식(RPKEP)을 제안하고자 한다. RPKEP는 패스워드 사용자, 사용자와 비밀 키 정보를 공유하는 서버, 사용자의 패스워드 복구를 도와주는 패스워드 복구 에이전트(PRA : Password Recovery Agency)로 구성된다. 제안하는 방식은 패스워드 기반 키 분배 방식의 안전성에서 가장 중요한 요소로 인식되고 있는 오프라인 사전 공격(off-line dictionary attack)에 대해 안전하고 서버가 저장하고 있는 사용자 비밀 정보가 노출되어도 사용자의 안전성은 유지된다는 장점이 있다. 또한, 패스워드 복구 과정에서 D. Chaum의 은닉 서명(Blind Signature) 방식을 응용하여 사용자의 패스워드 복구를 도와주는 PRA 조차 사용자 패스워드에 대한 어떤 정보도 알 수 없도록 하였다.

ABSTRACT

In this paper, we propose Recoverable Password Based Key Exchange Protocol(RPKEP). RPKEP has user who has password, server which share the secret key information with user, and password recovery agency(PRA) which help to recover the user's password. Proposed protocol has some advantages that it is secure against off-line dictionary attack which is considered most important in password based key exchange protocol and user's security is preserved even though user's secret information stored in the server is disclosed. By applying Chaum's blind signature scheme in the process of password recovery, even the PRA can't obtain any information about user's password.

keyword : *Key Recovery, Password, Key Exchange Protocol*

Ⅰ. 서 론

사용자 인증을 위하여 많은 하드웨어 토큰과 생체 인식 기술이 개발되고 있지만 이러한 기술이 실용화 되기 위해서는 특별히 고안된 인터페이스 장치가 있어야 한다. 패스워드에 기반하는 인증은 특별한 외부 인터페이스 장치를 요구하지 않기 때문에 가장 널리 사용되고 있는 방법이다. 특히, 현재의 웹 환경과 같이 어느 곳에서나 안전하게 서버와 접속하고자 하는 사용자에게는 패스워드를 이용하는 것이 가장 적절한 방법일 것이다.

그러나, 일반적으로 패스워드를 사용하는 암호 시스템은 오프라인 사전 공격(off-line dictionary attack)에 대해 취약점을 가지고 있다. 1990년대 초반부터 오프라인 사전 공격에 대한 안전성을 갖는 방식들이 연구되었으며[2] 최근에는 이러한 연구 결과를 바탕으로 패스워드 기반 키 분배 방식의 표준화를 추진하고 있다[1].

* 국가보안기술연구소(kiwook@etri.re.kr)
** (주)비씨큐어 암호기술연구소({ycchoi,sangjoon}@bcqre.com
*** 성균관대학교 전기 전자 및 컴퓨터 공학부(dhwon@dosan.skku.ac.kr)

본 논문에서는 오프라인 사전 공격에 대해 안전하고 사용자가 패스워드를 잊어버릴 경우 패스워드를 복구할 수 있는 패스워드 기반 키 분배 방식(RPKEP : Recoverable Password Key Exchange Protocol)을 제안하고자 한다. 제안하는 방식은 패스워드 복구 에이전트(PRA), 사용자와 비밀 세션키를 공유하는 서버, 패스워드를 가지고 있는 사용자로 구성된다. PRA는 사용자가 패스워드를 복구할 수 있도록 도와주기는 하지만 은닉 서명을 이용하기 때문에 사용자 패스워드에 대한 어떤 정보도 알 수 없다. 또한 제안하는 방식은 서버의 사용자에 대한 비밀 정보가 노출되어도 사용자 관점에서의 안전성이 유지되는 비대칭 신뢰 모델(asymmetric trust model)이다. 세션키 분배 과정은 기존에 Jablon등이 제안한 패스워드 기반 분배 방식과 세션키 확인을 위한 G-Q 서명 방식으로 구성된다.

패스워드 복구를 위하여 지금까지 제안된 방식들은 주로 소수 p상에서의 지수승을 이용하였으나 제안 방식은 RSA 합성수 n을 이용한다.

본 논문은 모두 7개 절로 구성된다. 2절에서는 패스워드 기반 키 분배 방식에 대한 요구 사항을 정리하였으며[1], 3절에서는 가장 널리 알려진 Jablon의 방식을 대칭 신뢰 모델(symmetric trust model)[5]과 비대칭 신뢰 모델(asymmetric trust model)[6]로 나누어 소개하고, 4절에서는 제안하는 방식에서 사용자가 세션키 확인을 위하여 사용하는 G-Q 서명 방식을 소개한다[4]. 5절에서는 본 논문에서 제안하는 패스워드 복구 가능한 패스워드 기반 키 분배 방식을 설명하고 6절에서는 제안하는 방식의 안전성과 효율성을 분석하였으며 마지막으로 7절에서 결론을 맺는다.

II. 패스워드 기반 키 분배 방식의 요구 조건

Bellare와 Rogaway는 패스워드 기반 키 분배 방식의 설계에서 고려해야할 요구 사항을 다음과 같이 정리하였다[1].

(1) 비대칭 신뢰 모델이어야 한다. 즉, 서버는 클라이언트의 패스워드를 가지고 있지 않으며 단지 클라이언트 패스워드를 인증할 수 있는 인증자(verifier)만을 갖는다.
(2) 공격자는 패스워드를 추측하여 인터랙티브하게 프로토콜에 참가하여 세션키를 계산하는 방법이외에 다른 방법을 통해 세션키를 얻을 수 없어야 한다.
(3) 여러 세션을 조작하는 능동적 공격자에 대한 안전성을 제공해야 한다.
(4) 이전에 분배된 세션키를 아는 것이 공격에 아무런 도움을 줄 수 없어야 한다.
(5) 이전에 분배된 세션키를 프로토콜에서 사용해서는 안된다.
(6) 클라이언트의 패스워드 관련 정보(pwa)와 서버의 패스워드 인증 정보(pwb)가 노출되어도 이전에 분배된 세션키를 알 수 없어야 한다(forward secrecy).
(7) 클라이언트의 패스워드 관련 정보(pwa)와 서버의 패스워드 인증 정보(pwb)가 노출되어도 단순히 서버와 클라이언트 통신 정보를 도청하는 방법으로는 현재의 세션키를 알 수 없어야 한다.
(8) 공격자가 서버의 패스워드 인증 정보(pwb)를 알게 되더라도 공격자가 정당한 클라이언트로 가장하기 위해서는 pwa에 대한 사전 공격(dictionary attack)을 수행하여야 한다.
(9) 프로토콜이 단순해야 하고 잘 알려진 암호 프리미티브로부터 만들어져야 한다.
(10) 프로토콜이 flow architecture의 다양성을 지원하여야 한다.
(11) 모듈러 곱셈, 타원곡선 연산 등과 같은 다양한 그룹에서 적용할 수 있어야 한다.
(12) 프로토콜은 기본적으로 서버가 클라이언트를 인증할 수 있어야 하며, 선택적으로 클라이언트가 서버를 인증할 수 있어야 한다.

III. Jablon의 패스워드 기반 키 분배 방식

본 절에서는 현재 가장 널리 알려진 Jablon의 패스워드 기반 키 분배 방식을 소개하고자 한다. Jablon은 1996년 클라이언트와 서버가 같은 패스워드 관련 정보를 가지고 안전하게 세션키를 공유하는 대칭 신뢰 모델(symmetric trust model)의 패스워드 기반 키 분배 프로토콜을 제안하였으며, 1997년에는 비대칭 신뢰 모델(asymmetirc trust model)로 개선하였다. 프로토콜에서 사용하는 파라미터는 다음과 같다.

- $p=2q+1$(p, q는 소수)
- w : 클라이언트 패스워드

■ Jablon 방식 1(대칭 신뢰 모델)[5]

클라이언트 (w^{2x} mod p)		서버 (w^{2y} mod p)
랜덤한 x 선택 $Q_C = w^{2x} \bmod p$ 계산	id, Q_C ---------->	
	Q_S <----------	랜덤한 y 선택 $Q_S = w^{2y} \bmod p$ 계산
세션키 K를 다음과 같이 계산한다. $K = Q_S^{2x} \bmod p$ 만일 K가 1이면 프로토콜을 중지한다		세션키 K를 다음과 같이 계산한다. $K = Q_C^{2y} \bmod p$ 만일 K가 1이면 프로토콜을 중지한다
	h(h(K)) <----------	h(h(K)) 계산
① h(h(K)) 검증 ② h(K)전송	h(K) ---------->	① h(h(K)) 검증 ② h(K)전송
		h(K) 검증

〔그림 1〕 Jablon의 대칭 신뢰 모델

■ Jablon 방식 2(비대칭 신뢰 모델)[6]

클라이언트 (w : 패스워드, g=h(w'))		서버 ($v=g^{w'} \bmod p$)
랜덤한 x 선택 $Q_C = g^{2x} \bmod p$ 계산	id, Q_C ---------->	
	Q_S <----------	랜덤한 y 선택 $Q_S = g^{2y} \bmod p$ 계산 $K_2 = v^{2y} \bmod p$ 계산
세션키 K를 다음과 같이 계산한다. $K_1 = Q_S^{2x} \bmod p$ $K_2 = Q_S^{w} \bmod p$ $K = h(K_1, K_2)$		세션키 K를 다음과 같이 계산한다. $K_1 = Q_C^{2y} \bmod p$ $K = h(K_1, K_2)$
	h(h(K)) <----------	h(h(K)) 계산
1) h(h(K)) 검증 2) h(K)전송	h(K) ---------->	
		h(K) 검증

〔그림 2〕 Jablon의 비대칭 신뢰 모델

- v : 서버의 패스워드 인증자(verifier)
- h( ) : 해쉬 함수

방식 1(〔그림 1〕 참조)은 2절에서 기술된 12가지 요구 사항 중에서 (2), (3), (4), (5), (6), (7), (9), (11), (12)를 만족하며 대칭 신뢰 모델의 기본 특성에 의해 요구사항 (1), (8)은 만족시킬 수 없다.

그리고 서버가 Q_S를 계산하기 위해서는 클라이언트를 식별해야하므로 클라이언트의 요구가 먼저 선행되어야 하기 때문에 요구사항 (10)은 만족하지 못한다.

방식 2(〔그림 2〕 참조)는 2절에서 기술된 12가지 요구 사항 중에서 (10)번을 제외한 모든 요구 사항을 만족시키며, 요구 사항 (10)번을 만족시키지 못하는 이유는 방식 1과 같다.

Ⅳ. G-Q 서명 방식

G-Q 서명 방식은 Guillou와 Quisquater가 제안한 ID 기반 서명 방식[4]으로 신뢰 기관(Trusted Center)이 각 사용자의 ID에 대응되는 서명용 비밀키를 생성하여 준다. 먼저 신뢰 센터는 시스템의 키 변수들과 사용자의 비밀키 정보를 다음과 같이 생성한다.

(1) 서로 다른 랜덤한 소수 p, q를 생성하여 $n=p \cdot q$를 구성한다.
(2) RSA[7] 공개키 e와 비밀키 d를 생성한다($e \cdot d \equiv 1 \bmod (p-1)(q-1)$).
(3) 사용자 A의 ID에 대응되는 사용자 A의 비밀키 s_A를 다음과 같이 계산한다.

$$s_A = ID_A^d \bmod n$$

(4) (e, n)은 시스템 사용자 모두에게 공개하고, s_A는 사용자 A에게 비밀리에 전달한다.

[서명 생성]
(1) 랜덤한 k를 선택하여 $r=k^e \bmod n$을 계산한다.
(2) m과 r의 해쉬값 $b=h(m \| r)$와 $c=k\, s_A^b \bmod n$을 계산한다.
(3) RSA 공개키 e와 비밀키 d를 생성한다($e \cdot d \equiv 1 \bmod (p-1)(q-1)$).
(4) m에 대한 A의 서명으로 (b, c)를 전송한다.

[서명 검증]
(1) 서명 검증 정보 (n, e, ID_A)를 얻는다.
(2) $r=s_A^e\, ID_A^b \bmod n$과 $b=h(m \| r)$을 검증한다.

V. 제안하는 RPKEP(Recoverable Password Key Exchange Protocol)

최근 패스워드 기반 암호시스템에 대한 연구가 활발해지면서 이러한 연구 결과들이 PKI Roaming, Single Sign On, 포털 사이트 보안등에 응용되고 있다. 응용 분야가 다양해짐에 따라 패스워드 관리의 중요성은 더욱 증가될 수밖에 없다. 현재 인터넷 사용자들은 인터넷 사이트의 많은 계정에서 패스워드를 사용하고 있으나 같은 패스워드를 사용할 경우 안전성 문제가 있어 일반적으로 서로 다른 패스워드를 사용할 것을 권고하고 있다. 그러나 서로 다른 패스워드 사용시 사용자가 패스워드를 잊어버릴 가능성이 높아 이러한 권고는 대부분 무시되는 경향이 있다.

본 논문에서는 패스워드 기반 키 분배 방식에서 사용자가 패스워드를 잊어버릴 경우 안전하게 패스워드를 복구할 수 있는 방식을 처음으로 제안하고자 한다. 제안하는 방식은 기존의 일반 패스워드 기반 키 분배 프로토콜과 달리 패스워드 복구 에이전트(PRA : Password Recovery Agent)가 존재하여 사용자 패스워드 복구를 도와준다. 이때, PRA는 사용자 패스워드 복구를 도와 주지만 사용자 패스워드를 알 수는 없다.

5.1 PRA의 키 파라미터 생성

먼저 PRA는 RPKEP를 위한 키 파라미터들을 다음과 같이 생성한다. PRA가 생성하는 파라미터들은 RPKEP의 안전성에서 중요한 요소가 되기 때문에 PRA는 신뢰할 수 있는 기관이어야 한다.

1) $p_1=2\,q_1+1$, $p_2=2\,q_2+1$인 소수 p_1, p_2를 선택한다. 단, q_1, q_2는 소수이다.
2) $n=p_1\,p_2$, $\nu(n)=2\,q_1\,q_2$을 계산한다.
3) (e, n)은 PRA의 공개키로 공개하고, (d, n)은 PRA의 비밀키로 안전하게 보관한다.(단, $e \cdot d \equiv 1 \bmod \nu(n)$) 공개키 e는 안전성과 효율성을 고려하여 $e=2^{128}+1$로 한다.
4) $q_1\,q_2$를 위수로 갖는 g를 선택한다.($ord(g)=q_1\,q_2$).

5.2 인증자 정보 등록

사용자의 패스워드 정보를 w라 하자. 안전성을 위하여 $w^2=1 \bmod n$이 되는 패스워드는 배제한다. 사용자는 서버가 공격되어도 공격자가 정당한 사용자로 위장할 수 없도록 하기 위하여 패스워드 w대신 PRA의 공개키 e로 암호화한 $s=w^{-e} \bmod n$와 자신의 id를 서버에 등록한다. 이때 s는 사용자와 서버가 비밀 세션키를 만들기 위하여 사용되는 정보이므로 사용자는 안전한 통로(secure channel)를 이용하여 등록하여야 하며 서버는 s가 노출되지 않도록 안전하게 보관하여야 한다. 즉, s는 사용자와 서버만의 비밀 정보이다.

5.3 사용자와 서버의 세션키 계산

[단계 1]
- 사용자 : 먼저 패스워드로 $s=w^{-e} \bmod n$를 계산한다. 랜덤한 x를 선택하여 $Q_C=s^x \bmod n$을 계산한 후 Q_C을 서버에게 전송한다.
- 서버 : 랜덤한 y를 선택하여 $Q_S=s^y \bmod n$을 계산한 후 Q_S를 사용자에게 전송한다.

패스워드 : w $s=w^e \bmod n$ 계산	id, s ---------->	id, s 저장
랜덤한 x 선택 $Q_C=s^x \bmod p$ 계산	id, Q_C ----------> Q_S <----------	랜덤한 y 선택 $Q_S=s^y \bmod p$ 계산
세션키 SK를 다음과 같이 계산한다. $SK=Q_S^{2x} \bmod n$ $SK^2=1 \bmod n$이면 프로토콜 중지 SK에 대한 G-Q 서명 (u, v) 계산 $r=k^e \bmod n$ $u=h(SK\|\|r)$ $v=w^u k \bmod n$	(u, v) ---------->	세션키 SK를 다음과 같이 계산한다. $SK=Q_C^{2y} \bmod n$ $SK^2=1 \bmod n$이면 프로토콜 중지
h(h(SK)) 값 검증	h(h(SK)) <----------	h(h(SK)) 계산 $r=v^e s^u \bmod n$ 계산 $u=h(SK\|\|r)$ 검증

〔그림 3〕 제안하는 RPKE 프로토콜

〔단계 2〕

- 사용자
  - 세션키 $SK=Q_S^{2x} \bmod n$를 계산한다. 이때, 안전성을 위하여 $SK^2=1 \bmod n$이면 프로토콜을 중지한다.
  - 세션키 SK에 대한 G-Q 서명 (u, v)를 다음과 같이 계산하여 서버에게 전송한다.(k는 랜덤수, h( )는 안전한 해쉬 함수)

$$r=k^e \bmod n$$
$$u=h(SK||r)$$
$$v=w^u k \bmod n$$

- 서버
  - 세션키 $SK=Q_C^{2y} \bmod n$를 계산한다. 이때, 안전성을 위하여 $SK^2=1 \bmod n$이면 프로토콜을 중지한다.
  - h(h(SK))를 사용자에게 전송한다.

〔단계 3〕

- 사용자 : 수신된 h(h(SK))값을 검증한다.
- 서버 : $r=v^e s^u \bmod n$를 계산하고 $u=h(SK||r)$이 되는지 검증함으로서 세션키 SK의 서명 (u, v)를 검증한다.

단계 1, 2, 3내에서 사용자와 서버는 순서에 관계없이 독립적으로 수행하여도 프로토콜의 안전성은 유지된다.

5.4 패스워드 복구 과정

제안하는 방식은 사용자가 자신의 패스워드를 잊어버린 경우에도 서버와 PRA의 도움으로 패스워드를 복구할 수 있다는 특징이 있다. 패스워드 복구는 D. Chaum의 은닉 서명을 응용하여 PRA가 패스워드 복구를 도와줄 뿐 실제 사용자 패스워드를 알 수 없도록 하였다[3]. PRA의 도움으로 사용자 패스워드를 복구하는 과정은 다음과 같다.

1) 사용자는 안전한 통신로를 통하여 서버가 저장하고 있는 비밀 정보 s를 받는다.
2) 사용자는 난수 a를 생성하여 $c=a^e s \bmod n$을 계산하여 c를 PRA에게 전송한다.
3) PRA는 자신의 비밀키 d를 사용하여 은닉 서명 $f=c^d \bmod n$을 사용자에게 전송한다.
4) 사용자는 패스워드 $w=a \cdot f^{-1} \bmod n$을 복구한다.

Ⅵ. 제안하는 방식의 특징 분석

6.1 안전성

6.1.1 패스워드 w의 안전성

D. Jablon의 SPEKE에서와 마찬가지로 일반

공격자는 사용자와 서버 사이에 교환되는 정보 Q_S, Q_C, (u, v), h(h(SK))로부터 패스워드 w에 대한 오프라인 사전 공격을 수행할 수 없다.

s를 가지고 있는 서버가 사용자 패스워드를 얻을 수 있는 방법은 합성수 n을 인수분해 하거나 $s=w^{-e} \bmod n$이 되는 패스워드 w를 추측하는 방법밖에는 없다. 따라서, 서버의 비밀 정보 s가 노출된다 하여도 w를 알 수 없다.

또한, s를 얻은 공격자가 사용자를 가장하여 서버와 비밀 세션키 SK를 공유하기 위해서는 세션키 SK에 대한 G-Q 서명을 생성하여야 하나 s만으로는 SK에 대한 G-Q 서명을 계산할 수 없다. 그러므로 제안하는 방식에서는 서버가 공격되더라도 공격자는 정당한 사용자로 위장할 수 없게된다.

그리고 PRA는 n의 인수분해를 알고 있으나 사용자와 서버 사이에 교환되는 정보로 사용자 패스워드 w에 대한 어떠한 정보도 얻을 수 없으며 패스워드 복구 과정에서도 은닉 서명을 사용하기 때문에 사용자의 패스워드를 알 수 없다.

단, PRA는 n의 소인수를 알기 때문에 서버가 제공한 비밀 정보 s로부터 w를 계산할 수 있으므로 PRA와 서버가 함께 공모하는 경우에는 패스워드 w를 구할 수 있게 된다.

6.1.2 서버의 비밀 정보 s의 안전성

서버와 사용자 사이에 교환되는 정보 Q_S, Q_C, (u, v), h(h(SK))로부터 s를 구하는 것은 SPEKE에서 패스워드 정보를 구하는 어려움과 같다. PRA는 패스워드 w에 대한 어떤 정보도 얻을 수 없듯이 마찬가지로 s에 대한 어떠한 정보도 얻을 수 없다.

6.1.3 세션키 SK의 안전성

일반 공격자가 Q_S, Q_C로부터 세션키 SK를 구하는 어려움은 SPEKE와 같다. PRA 조차도 세션키 SK를 계산하기 위해서는 패스워드를 추측하여 s를 계산하고 합성수 n상에서 이산대수 x, y를 계산하여야 하기 때문에 SK를 구할 수 없다. 또한 이전에 사용된 세션키가 노출되어도 현재 세션키의 안전성에 영향을 주지 않으며 패스워드가 공격되어도 과거에 사용된 세션키의 안전성은 보장된다.

6.2 효율성

사용자와 서버 사이의 세션키 교환 과정에서 사용자는 모두 5번의 지수승 연산을 수행하여야 하며 서버는 4번의 지수승 연산을 수행하여야 한다. 따라서, 기존 Jablon이 제안한 방식 보다 제안한 방식은 계산 복잡도가 높다. 사용자가 수행하는 지수승 연산 중 공개키 e에 대한 지수승 연산은 2번이고 서버의 공개키 e에 대한 지수승 연산은 1번이다. $e=2^{128}+1$로 하면 공개키 e에 대한 지수승 연산 시간을 줄일 수 있다. 또한, 단계 1, 2, 3에서 사용자와 서버는 병렬로 수행하는 것이 가능하기 때문에 전체 프로토콜의 처리 시간을 줄일 수 있다.

6.3 키 분배 요구사항 만족

제안된 키 분배 방식은 2절에서 기술된 패스워드 기반 키 분배 프로토콜의 12가지 요구 사항 중에서 (9), (10), (11)을 제외한 요구 사항을 만족시킨다. 제안하는 프로토콜에서는 세션키 확인을 위하여 사용자가 G-Q 서명 방법을 사용하고 있기 때문에 지금까지 알려진 방식들 보다 복잡한 면이 있으며 타원곡선 연산으로 자연스럽게 변환되지 않는다. 또한, 서버가 사용자의 식별 정보를 알아야만 하므로 프로토콜의 융통성이 부족하다.

Ⅶ. 결 론

최근 오프라인 사전 공격에 대하여 안전한 패스워드 기반 키 분배 방식 등이 연구되면서 패스워드가 여러 응용 분야에 활용되고 있다. 패스워드의 응용 분야가 넓어짐에 따라 사용자가 패스워드를 잊어버릴 경우 서버와 사용자 사이에 안전하게 패스워드를 재설정하는 부담이 커지고 있다. 이러한 문제점을 해결하기 위하여 본 논문에서는 패스워드 복구 가능한 패스워드 기반 키 분배 방식(RPKEP)을 제안하였다.

제안하는 방식에서는 PRA가 패스워드 복구를 도와주지만 사용자 패스워드를 알 수 없으며 PRA와 서버가 사용자 패스워드를 구할 수 있는 방법은 오프라인 사전 공격을 수행하거나 서로 공모하여야만 가능하다.

제안하는 방식은 패스워드 기반 키 분배 프로토콜과 패스워드 복구 기능을 결합한 것으로 서버가 인증자로부터 패스워드 복구가 가능하다는 사실을 확인할 수 있는 최초의 패스워드 기반 키 분배 방식이다. 그러나 프로토콜의 계산 복잡도가 이전의 방식들에 비하여 높기 때문에 이에 대한 연구가 좀더 필요할 것이다.

참 고 문 헌

[1] M.Bellare and P.Rogaway, "The AuthA Protocol for Password-Based Authenticated Key Exchange", Contribution to the IEEE P1363 study group, March 14, 2000. (http://www.integritysciences.com/links.html#BR)

[2] S.M.Bellovin and M.Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the IEEE Syposium on Research in Security and Privacy, Oakland, May 1992.

[3] D.Chaum, "Blind signatures for untraceable payments", Advances in Cryptology-Proceedings of Crypto'82, pp. 199~203, 1983.

[4] L.C.Guillou and J-J .Quisquater, "A 'Paradoxical' Identity-Based Signature Scheme Resulting from Zero-Knowledge", Advances in Cryptology-Proceedings of Crypto'88, pp. 216~231, 1988.

[5] D.Jablon, "Strong Password-Only Authentication Key Exchange", Computer Communication Review, Vol. 26, No. 5, pp. 5~26, October, 1996.

[6] D.Jablon, "Extended Password Key Exchange Protocols Immune to Dictionary Attacks", Proceedings of the Sixth Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET-ICE '97), IEEE Computer Society, June 18-20, 1997, Cambridge, MA, pp. 248~255.

[7] R.L.Rivest, A.Shamir and L.M.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21, (1978), pp. 120~126.

〈著者紹介〉

손 기 욱 (Kiwook Sohn) 정회원
1990년 2월 : 성균관대학교 정보공학과 졸업(학사)
1992년 2월 : 성균관대학교 대학원 정보공학과 졸업(석사)
1992년 1월~1999년 12월 : 전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 키분배 프로토콜, 공개키기반구조

최 영 철 (Youngcheol Choi) 정회원
1997년 2월 : 성균관대학교 정보공학과 졸업(학사)
1999년 2월 : 성균관대학교 대학원 정보공학과 졸업(석사)
1998년 10월~2000년 3월 : 한국정보보호센터(KISA) 연구원
2001년 2월 : 성균관대학교 대학원 전기 전자 및 컴퓨터공학부 박사 수료
2000년 5월~현재 : (주)비씨큐어 암호기술연구소 시스템개발부장
〈관심분야〉 공개키 기반구조, 디지털 컨텐츠 보호, 전자지불시스템

박 상 준 (Sangjoon Park) 정회원
1984년 2월 : 한양대학교 수학과 졸업(학사)
1986년 2월 : 한양대학교 대학원 수학과 졸업(석사)
1999년 2월 : 성균관대학교 대학원 전기 전자 및 컴퓨터공학부 졸업(박사)
1986년 2월~1999년 12월 : 전자통신연구원 책임연구원
2000년 1월~2000년 10월 : 국가보안기술연구소 책임연구원
2000년 11월~현재 : (주)비씨큐어 암호기술연구소 소장
〈관심분야〉 암호 알고리즘, 인증 및 서명, PKI, 디지털 컨텐츠 보호

원 동 호(Dongho Won) 종신회원
성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국무총리실 국가정보화 추진위원회 자문위원
1998년~1999년 : 성균관대학교 정보통신기술연구소 소장
1999년~2001년 : 성균관대학교 전기 전자 및 컴퓨터 공학부 학부장
1999년~2001년 : 성균관대학교 정보통신대학원 원장
1982년~현재 : 성균관대학교 전기 전자 및 컴퓨터공학부 교수
1999년~현재 : 한국정보보호학회 수석 부회장
2000년~현재 : 정보통신부 지정 정보보호인증기술연구센터 센터장
〈관심분야〉 암호이론, 정보이론, 공개키 기반구조