Journal of Korea Multimedia Society Vol. 11, No. 10, October 2008(pp. 1403-1408)

패스워드 기반 키 교환 및 인증 프로토콜의 안전성에 관한 분석

박 춘 식†

요 약

서버의 부담을 줄이기 위하여 스마트카드를 이용한 3자간 키 교환 프로토콜 방식과 패스워드 기반 2자간 키 교환 및 인증 프로토콜 방식들이 많이 제안되고 있다. 본 논문에서는 스마트 카드 기반 3자간 키 교환 및 인증 프로토콜 방식의 취약점에 대한 분석 및 검토를 행하였다. 또한, 심 경아 등에 의한 오프라인 패스워드 추측 공격에 취약점을 보인 곽 진 등의 방식을 분석하여 보고 이 공격에 대한 대책도 제시하고자 한다.

Analysis on Security Vulnerability of Password-based key Exchange and Authentication Protocols

Choon Sik Park†

ABSTRACT

A number of three party key exchange protocols using smart card in effort to reduce server side workload and two party password based key exchange authentication protocols has been proposed. In this paper, we introduce the survey and analysis on security vulnerability of smart card based three party authenticated key exchange protocols. Furthermore, we analyze Kwak et al's password based key exchange and authentication protocols which have shown security weakness such as Shim et al's off-line password guessing attack and propose the countermeasure to deter such attack.

Key words: key exchange(키교환), password(패스워드), password guessing attack(패스워드추측공격)

1. 서 론

Diffie - Hellman의 키 교환 프로토콜이 제안된 이래 효율이나 안전성면에서 개선된 많은 방식들이 제안되었고 또한 이들 중 많은 방식들의 취약점도 분석되었다. 비밀 키와 공개 키 인증서등에 의존한 이러한 방식 외에 패스워드의 편리성을 이용한 패스워드 기반의 키 교환 프로토콜의 제안도 많이 이루어져 왔다.

암호학적인 키와 공개 키 인증서등에 의해 이루어지는 키 교환 프로토콜은 공개키 암호, 이산대수문제의 안전성, 그리고 랜덤오라클, 해쉬 함수 등을 이용한 안전성 증명 중심으로 된 많은 방식들이 발전되어 왔다. 즉, 암호학적인 가정들을 약하게 하거나, 공격자의 공격 능력을 강화하여 프로토콜의 안전성을 높이는 등의 방법으로 제안되어 왔다[1-4].

패스워드 기반의 키 교환 프로토콜은 임의의 2자간에 패스워드를 이용한 키 교환을 이루고자 하는 것이 아니라 서버 클라이언트 환경을 전제로 서버와 클라이언트간의 비밀 통신을 위한 세션 키 공유를 목적으로 제안된 것이다. 만일 특정 사용자간의 패스워드 키 교환일 경우에는 자신이외의 키 교환 상대방

※ 교신저자(Corresponding Author) : 박춘식, 주소 : 대전시 유성우체국사서함1호(305-600), 전화 : 031)220-2589, FAX : 042)870-2369, E-mail : csp@ensec.re.kr

접수일 : 2008년 8월 14일, 완료일 : 2008년 9월 23일

† 정회원, 한국전자통신연구원부설연구소 책임연구원

모두의 패스워드 공유 정보를 사전에 갖고 있어야하는 방식이 되어 패스워드의 간편함과 같은 편리성을 이용하지 못하게 되기 때문이다. 다시 말해서, 공개키 인증서나 다른 암호학적 비밀정보를 이용하여 키 교환을 이루어야 하는 방식에 비하여 패스워드를 이용하는 이점이 없기 때문이다. 엄격한 의미에서의 패스워드 기반 키 교환 프로토콜의 정의는, 클라이언트는 자신의 패스워드만을 갖고 있으며 서버는 패스워드에 의하여 만들어진 검증자만을 갖고 세션 키 교환을 이루는 것이 일 것이다. 비록 서버 클라이언트 환경일지라도 클라이언트인 사용자가 자신의 패스워드 외에 서버의 공개키 정보 등 다른 정보를 필요로 하는 방식[5,6]은 엄격한 의미에서는 패스워드 기반 키 교환 프로토콜이라 말하기 어려운 면이 있다.

또한 스마트카드 등의 중간 매개체를 이용하여 키 교환 프로토콜을 행하는 방식[7-9]도 패스워드 외에 카드 소지를 해야 함은 물론 카드 내에 키 교환 및 인증에 필요한 비밀 정보를 두어야하기 때문에 엄격한 의미에서는 패스워드 기반이라 말하기 어려운 점도 있다.

패스워드 기반 키 교환 프로토콜은 Bellovin과 Merritt[10]에 의하여 최초로 제안된 이래 안전성과 효율성을 개선한 많은 논문들이 제안되어졌으며 이들 중 많은 방식들의 취약점이 발견되기도 하였다. Bellare 등[11,12]에 의하여 Formal Model에 의한 안전성 증명 가능한 패스워드 기반 키 교환 프로토콜 뿐만 아니라 국내에서도 효율이나 안전성면에서 성능이 개선된 많은 패스워드 기반 프로토콜이 제안되었다[13-18]. 그러나 패스워드 기반 키 교환 프로토콜 중의 많은 방식들은 대부분 오프라인 패스워드 추측 공격에 의하여 취약점이 발견되었으며 안전성 증명이 가능한 프로토콜들[11,12]만이 아직까지 오프라인 패스워드 추측 공격 등에 의한 취약점이 발견되고 있지 않는 실정이다.

최근 패스워드 기반 키 교환 프로토콜에서 서버의 부담을 줄이기 위하여 스마트카드를 이용한 방식[7-9]들이 제안되었다. 본 논문에서는 제안된 스마트카드 기반의 3자간 프로토콜[7]에 대한 취약점을 소개하고자 한다. 또한 곽 진 등[15]에 의해 제안된 패스워드 기반 키 교환 프로토콜이 심경아 등[19]에 의하여 오프라인 패스워드 추측 공격에 취약한 문제점을 분석하여 보고 그 대책을 제시하고자 한다.

2. 스마트카드 기반의 키 교환 프로토콜

본 장에서는 스마트카드 기반 키 교환 프로토콜인 KYP 프로토콜[7]에 대한 간략한 설명과 취약점을 제시하고 대책도 함께 논의하고자 한다.

2.1 KYP 프로토콜

김 용훈등[7]에 의해 제안된 KYP 프로토콜은 사용자 등록 단계와 상호 인증 및 키 교환 단계로 나누어진다. 사용자 등록 단계는 본 논문에서 제안하는 KYP 프로토콜의 취약점을 설명하는 데 별 문제가 없을 것으로 판단되어 여기서는 설명을 생략하고자 한다. KYP 프로토콜의 상호 인증 및 키 교환 단계는 그림 1과 같으며 다음과 같이 수행한다.

(1) 사용자 A는 자신의 스마트카드를 카드 리더기에 넣고 아이디 ID_A와 패스워드 PW'_A를 입력한다.

(2) 입력된 패스워드 PW'_A를 이용하여 스마트카드는 카드에 저장되어 있는 랜덤값(n_A), 해쉬키 HK_A, 서버로부터 등록 단계에서 주입받은 g^{sA}를 이용하여, $W'_A = g^{H(\hbar HKA(PW'A,\ nA)} g^{sA} \pmod P$를 계산한다. 아이디 확인과 카드에 저장되어 있는 W_A와 입력된 패스워드 PW'_A를 이용하여 계산된 W'_A를 서로 비교하여 정당한 카드의 사용자인지 검증한다.

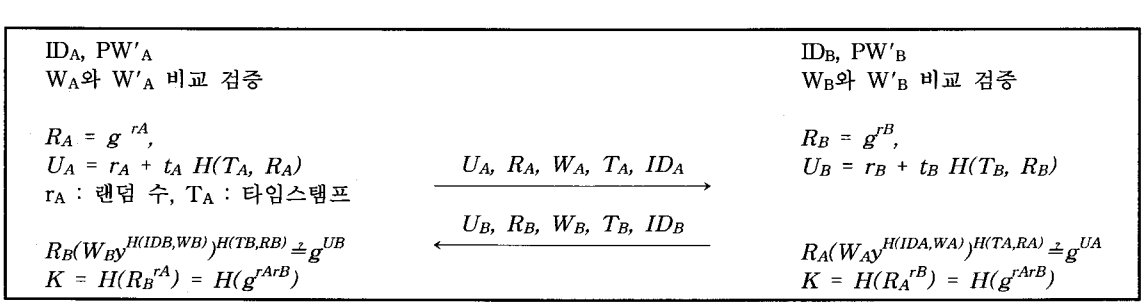

그림 1. KYP 프로토콜

(3) 정당한 카드의 검증이 완료되면, 스마트카드는 랜덤 정보 r_A와 타임스탬프 T_A 그리고 서버로부터 등록단계에서 주입된 t_A를 이용하여 R_A와 U_A를 계산하고 U_A, R_A, W_A, T_A, ID_A를 사용자 B에게 전송한다.

$$R_A = g^{rA} \pmod P,\ U_A = r_A + t_A\, H(T_A, R_A) \pmod q$$

(4) 사용자 B도 A와 같은 방법으로 U_B, R_B, W_B, T_B, ID_B를 계산하여 사용자 A에게 전송한다.

(5) 사용자 A는 사용자 B로부터 받은 정보들을 이용하여 $R_B(W_B y^{H(IDB,WB)})^{H(TB,RB)} \pmod P$와 $g^{UB} \pmod P$를 비교해서 사용자 B를 인증한 후 세션 키를 계산한다. 사용자 B도 A와 동일하게 수행하여 세션 키를 계산한다.

$$\text{세션 키} = H(R_B{}^{rA}) = H(g^{rArB}).$$

2.2 KYP 프로토콜의 취약점 분석

KYP 프로토콜은 공개된 정보를 이용하여 패스워드를 추측 공격하는 오프라인 패스워드 추측 공격에 대한 대책으로 패스워드 외에 별도의 비밀정보, n_i와 S_i를 이용하여 안전성을 유지하고 있다. 또한, Replay Attack 등 기존에 알려진 여러 공격에 대하여 안전함을 주장하고 있다. 그러나 프로토콜의 안전성은 기존의 알려진 공격에 대해서만 안전성을 검토하게 되면, 기존의 알려진 공격에 대한 충분한 검토가 없거나 새로운 공격이 제안되게 될 경우 쉽게 취약점을 드러내게 된다.

KYP 프로토콜에 대한 취약점인 Spoofing Attack에 대하여 설명하고자 한다. KYP 프로토콜에 대한 Spoofing Attack의 목적은 프로토콜의 사용자 A와 사용자 B간의 상호인증을 이루지 못하도록 하여 프로토콜의 본래의 목적을 달성하지 못하도록 방해하고자 하는 공격 방법이며 그림 2와 같다. 먼저, 사용자 A는 사용자 B와 키 교환을 하고자 하며 공격자는 정당한 사용자 E(Eve)로 한다.

(1) 정당한 사용자임을 확인한 후 사용자 A는 U_A, R_A, W_A, T_A, ID_A를 사용자 B에게 전송한다. 그러나 이를 지켜본 공격자 E는 이 정보를 가로채어 별도로 계산된 U_E, R_E, W_E, T_E, ID_E를 사용자 B에게 전송한다.

(2) 사용자 B는 사용자 E가 공격자인줄 모른 체, U_B, R_B, W_B, T_B, ID_B를 계산하여 사용자 E에게 전송한다. 사용자 E는 바로 사용자에게 사용자 B의 정보를 그대로 전송하면 된다.

(3) 사용자 A와 사용자 B는 서로 주고받은 정보를 이용하여 비교 검증한 후 세션 키를 교환하게 된다. 그러나 사용자 A는 사용자 B와의 키 교환은 이루어졌으나 사용자 B는 공격자 E와의 키 교환이 이루어지게 되어 사용자 A가 사용자 B와 상호 인증 하에 키 교환을 이루고자 하는 목적은 달성하지 못한 체 사용자 A만이 사용자 B와의 암호 통신을 시도하려고 할 것이다.

이러한 취약점이 발생하는 주요 원인으로는 스마트카드와 정당한 스마트카드 사용자임을 검증하는 프로토콜은 이용하고 있으나 상호 인증을 통한 정당한 통신상대방과의 키 교환을 이루기 위하여 통신상대방의 아이디 정보 등이 키 교환 프로토콜내의 교환 메시지 내에 매번 직접 활용되지 않기 때문이다. 또한, Replay Attack을 방지하기 위하여 사용된 타임스탬프 정보는 사용자 A가 전송하여 사용자 B로부터 받는 데 소요되는 시간 정보가 아니라 Ri와 Ui를 생성한 시점에서의 시각 정보이므로 사용자 A와 사용자 B는 공격자 Eve의 Spoofing Attack을 타임스탬프 정보로는 탐지할 수가 없다.

2.3 Spoofing Attack에 대한 대책

기본적으로 스마트카드와 정당한 사용자간의 신분확인뿐만이 아니라 키 교환하고자 하는 통신 상대방의 상호 인증을 위하여 통신 상대방의 정보를 활용하는 것이 필요하다. 즉 사용자는 신분확인에 사용된 아이디 정보를 키 교환 상대방의 정당성 확보에도 사용하는 것이다. 사용자 A는 스마트카드의 정당한

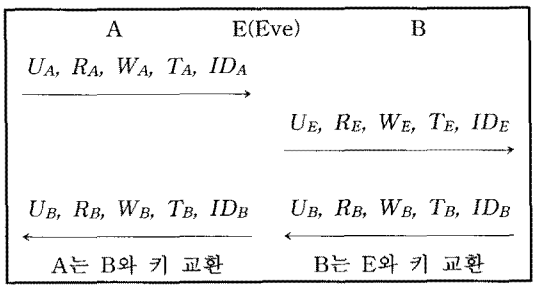

그림 2. KYP 프로토콜의 Spoofing Attack

사용자 여부를 확인한 후, 랜덤 수 r_A와 서버로부터 등록 시에 주입받은 t_A를 이용하여 키 교환을 하고자 하는 상대방 아이디 ID_B와 자신의 아이디 ID_A를 직접 해쉬 함수내의 입력으로 추가하여 U_A를 계산하도록 한다.

$$U_A = r_A + t_A\ H(T_A,\ R_A,\ \min(\boldsymbol{ID_A},\ \boldsymbol{ID_B}),\ max\ (\boldsymbol{ID_A},\ \boldsymbol{ID_B}))$$

사용자 B도 동일한 방법으로 U_B를 계산할 수 있지만 해쉬 함수의 입력으로 사용된 아이디 정보는 ID_B와 ID_E이므로 사용자 A의 비교 검증에 의하여 사용자 B와의 키 교환이 제대로 이루어지지 않았음을 알 수 있게 된다. 이는 공격자 Eve가 사용자 B로부터 보내어져오는 U_B를 사용자 A가 검증할 수 없도록 하기 위해서는 ID_B와 ID_E에 의한 해쉬 함수 값을 변경해야 하지만 사용자 B의 랜덤 수 r_B와 서버로부터 주입받은 t_B 정보를 알 수 없어 제안된 Spoofing Attack을 행할 수 없게 된다. 즉, $R_B(W_{BY}{}^{H(IDB,WB)})$ $H(T_B,R_B,\ \min(ID_A,\ ID_B),\ \max(ID_A,\ ID_B)) \neq g^{UB}$ ($\because$ $U_B = r_B + t_B\ H(T_B,\ R_B,\ \min(\boldsymbol{ID_E},\ \boldsymbol{ID_B}),\ max(\boldsymbol{ID_E},\ \boldsymbol{ID_B})$)

3. 패스워드 기반의 키 교환 프로토콜

본 장에서는 패스워드 기반의 키 교환 프로토콜인 KOYW 프로토콜[15]에 대한 심경아 등[19]에 의해 제안된 Off-line Dictionary Attack을 분석하고 그에 대한 대책을 제시하고자 한다.

3.1 패스워드 기반 키 교환 프로토콜과 Off-line Dictionary Attack 분석

KOYW 패스워드 기반 키 교환 프로토콜[15]에 대한 설명은 논문을 참조하기 바라며 여기서는 심경아 등[19]이 제안한 공격법을 간략히 살펴보도록 하며, 공격에 대한 KOYW 프로토콜의 문제점을 분석하여 보고자 한다.

(1) 공격자인 E는 사용자 A가 키를 교환하고자 하는 사용자 B에게 보내는 X_A를 가로채어 저장한다.

(2) E는 랜덤 값 b를 이용하여 $Y_B' = g^b \bmod P$를 계산하여 사용자 A에게 사용자 B인 것처럼 가장하여 Y_B'를 전송한다.

(3) A는 세션키 SK_A와 인증용 k_A을 계산하여 B에게 전송한다.

($SK_A = (g^{bQ-1})^a = g^{abQ-1} \bmod P$, $k_A = H(SK_A, Q)$)

(4) E는 다시 k_A을 가로챈 후 A에게 아무른 응답 없이 프로토콜을 중지한다. E는 임의의 패스워드 Q'을 선택하여 $k' = H((X_A)^{b(Q'-1)2}, Q')$을 계산한다. k_A과 k'비교한 후 추측 공격을 반복 시행하여 A와 B의 패스워드 Q를 찾아낸다.

(Remark) KOYW에 대한 off-line dictionary attack을 살펴보면 일단 사용자 A가 인증용 k_A를 사용자 B에게 전송하기 전에 사용자 B의 인증 여부를 행하지 않기 때문에 공격자 E가 사용자 A로부터 공격에 필요한 인증 정보 k_A를 얻게 된다. 또한 KOYW 프로토콜은 4단계의 프로토콜로 이루어져 있지만 사실은 3단계로 이루어져도 안전성에는 큰 문제가 없는 프로토콜이다. 프로토콜을 3단계로 더욱 더 효율적으로 만들면서 공격자 E가 A로부터의 인증 정보 k_A를 얻지 못하도록 보완하면 된다. 즉, 사용자 B가 인증 정보 $k_B(=H(SK_B, Q^{-1}))$를 계산하여 키 설정 정보 Y_B와 함께 사용자 A에게 동시에 전송하도록 프로토콜을 수정하면 된다. 수정된 프로토콜에 대해서는 공격자 E가 사용자 A와 B의 패스워드 정보 Q와 Q^{-1}를 알지 못하여 제대로 된 Y_B와 k_B를 사용자 A에게 전송하지 못하여 사용자 A로부터 k_A를 얻지 못하여 심경아 등[19]의 공격에 대해서는 안전할 수 가 있다.

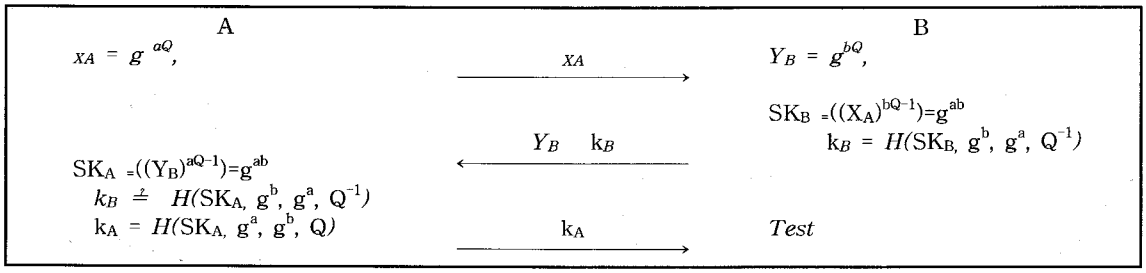

그림 3. 수정된 KOYW 프로토콜

그러나, 이러한 수정된 KOYW 프로토콜도 심 경아 등[19]의 공격에서 공격자가 사용자 A인 것처럼 위장하여 공격할 경우에는 역시 취약하게 된다.

3.2 Off-line Dictionary Attack에 대한 대책 및 분석

오프라인 패스워드 추측 공격이 가능한 프로토콜의 취약점을 분석하여 보면 대부분 상대방의 안전한 인증 절차가 없는 경우와 패스워드 추측이 용이한 형태로 패스워드가 계산식 내에 활용되고 있는 경우가 많다. KOYW 프로토콜은 이 2가지 취약점이 모두 적용되는 경우이나 3.1절의 Remark에서 설명된 바와 같이 약간의 수정으로 안전한 인증 절차는 이룰 수가 있다. 그러나 패스워드 추측 공격이 용이한 형태를 이용하여 수정된 KOYW 프로토콜을 공격하는 경우에는 대책이 될 수가 없다 .

본 절에서는 패스워드 추측이 곤란한 형태로 KOYW 프로토콜을 변경하여 오프라인 패스워드 추측 공격에 안전한 새로운 KOYW 프로토콜의 대책을 제시하고자 한다. 즉, 임의의 패스워드 정보를 이용하여 오프라인 패스워드 추측 공격을 행하더라도 패스워드와 무관한 정보인 랜덤 정보, 타임스탬프 등을 이용하여 직접적으로 패스워드가 추측되지 않도록 하는 그림 3과 같은 방식을 제안하고자 한다.

(1) 사용자 A는 $X_A=g^{aQ}$ (mod P)를 계산하여 사용자 B에게 전송한다.

(2) 사용자 B는 패스워드 정보와 X_A를 이용하여 SK_B, $Y_B=g^{bQ}$ (mod P)와 k_B를 계산하여 사용자 A에게 Y_B와 $k_B(=H(SK_B, g^b, g^a, Q^{-1}))$를 전송한다.

(3) 사용자 A는 Y_B를 이용하여 SK_A를 계산한 후 정당한 k_B인지 사용자 B를 인증한다. 만일 정당한 사용자 B라면 k_A를 계산하여 사용자 B에게 전송하며 사용자 B 역시 정당한 사용자인지 k_A를 이용하여 검증한다.

수정된 KOYW 프로토콜에서는 오프라인 패스워드 추측 공격에 대한 대책으로 공격자가 해독하거나 추측하기 어려운 Ephemeral key 정보인 랜덤 값 a, b를 이용하여 해쉬 함수내의 입력 정보로 패스워드 정보외에 Ephemeral key 정보인 g^a 또는 g^b를 이용하여 오프라인으로 패스워드를 추측하는 것이 이산대수 문제를 해결하는 계산량 만큼 소요되도록 어렵게 하여 취약점을 제거하였다. 심 경아 등에 의한 오프라인 패스워드 추측 공격은 사용자 A 또는 사용자 B 등 누가 위장 공격자가 되더라도 상대방의 Ephermeral key 정보를 알지 못하는 한, 상호 인증에 의한 키 확인 과정에서의 검증 과정 때문에 성공하지 못하게 된다.

수정된 KOYW 프로토콜의 안전성은 심 경아등에 의한 Off-Line Password Attack에 의한 공격은 g^a 또는 g^b를 이용하여 패스워드를 추측하기 때문에 이는 랜덤 값 a와 b를 알아야만 하는 이산대수문제로 귀결되며 Advanced Modification 공격, 패스워드가 노출된 경우의 안전성 등 오프라인 패스워드 이외의 공격 방법에 대한 안전성 분석은 곽진 등의 제안 프로토콜과 동일하여 나머지 공격들에 대한 안전성은 수정전의 프로토콜의 안전성과 유사하다.

또한, 수정된 KOYW 프로토콜의 효율성은 곽 진 등의 방식에 비하여 4 move에서 3 move로 라운드 수를 1회 줄이는 효과가 있는 반면 지수 연산의 계산량이 1회 증가하게 된다. 곽 진 등의 방식에서 설명된 바와 같이 나머지 부분은 KOYW 프로토콜의 계산량 및 통신량과 거의 유사하며 다른 방식과의 비교는 이미 곽 진 등의 논문에 설명되어 있어 효율면에서도 거의 유사함을 알 수 있다.

4. 결 론

본 논문에서는 최근 제안된 스마트카드 기반의 3자간 프로토콜에 대한 취약점을 소개하였으며, 최근 오프라인 패스워드 추측 공격에 취약점이 나타난 곽 진 등의 패스워드 기반 키 교환 프로토콜 방식의 문제점을 분석하여 보고 그 대책을 제시하였다. 이들 방식들 모두의 공통점은 효율성만을 고려하거나 기존의 일부 알려진 공격에 대한 검토만으로 이루어져 있어 패스워드 기반 키 교환 프로토콜의 안전성 증명의 중요성을 입증하고 있다.

참 고 문 헌

[1] B.LaMacchia, K.Lauter, and A.Mityagin, "Stronger Security of Authenticated Key Exchange," *ProvSec 2007*, LNCS 4784, pp. 1-16, 2007.

[2] K.Lauter, and A.Mityagin, "Security Analysis of KEA Authenticated Key Exchange,"

PKC2006, LNCS 3958, pp. 378-394, 2006.

[3] H.Krawczyk, "HMQV: A High Performance Secure D-H Protocol," *CRYPT 2005*, LNCS 3621, pp. 546-566, 2005.

[4] I.R. Jeong, J,Katz, and D.H. Lee, "One Round Protocols for Two Party Authenticated Key Exchange," *ACNS 2004*, LNCS 3089, 2004.

[5] 권태경,강명호,송주석, "패스워드 기반 시스템을 위한 효율적이고 안전한 인증 프로토콜의 설계 및 검증," 통신정보보호학회논문지, 제7권, 제2호, pp.27-42, 1997.

[6] L.Gong, T. Lomas, M.Needham, and J.Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks," *IEEE Journals on Selected Areas in Communications*, Vol.11, No.5, pp. 648*656, 1993.

[7] 김용훈, 윤택영, 박영호, "서버의 개입이 없는 스마트카드 기반의 3자간 키 교환 프로토콜," 정보보호학회논문지, 제18권, 제2호, pp. 11-20, 2008.

[8] 전일수, "스마트카드를 이용한 3자 참여 인증된 키 교환 프로토콜," 정보보호학회논문지, 제16권, 제6호, pp. 73-80, 2006.

[9] H.Sun, B.Chen, and T.Hwang, "Secure Key Agreement Protocols for Three-party against Guessing Attacks," *The Journal of Systems and Software*, Vol.75, pp. 63-68, 2005.

[10] S.Bellovin, and M.Meritt, "Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks," *IEEE Symposium on Research in Security and Privacy*, pp. 72-84, 1992.

[11] V.Boyko, P.MacKenzie, and S. Patel, "Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman," *EUROCRYPT 2000*, LNCS, 1807, pp. 156-171, 2000.

[12] M.Bellare, D.Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," *EUROCRYPT 2000*, LNCS, 1807, pp. 139-155, 2000.

[13] 신성철, 이성운, "동일 서버를 사용하는 두 사용자간 효율적인 패스워드 기반의 키 교환 프로토콜," 정보보호학회논문지, 제15권, 제6호, pp. 127-133, 2005.

[14] 이성운, 김현성, 유기영, "패스워드를 변경 가능한 효율적인 패스워드 기반의 인증된 키 교환 프로토콜," 전자공학회논문지(TC), 제42권, 제2호, pp. 33-38, 2005.

[15] 곽진, 오수현, 양형규, 원동호, "Advanced Modification 공격에 안전한 패스워드 기반 키 동의 프로토콜," 정보처리학회논문지(c), 제11권, 제3호, pp. 276-286, 2004.

[16] 이성운, 김현성, 유기영, "패스워드 기반의 효율적인 키 교환 프로토콜," 정보과학회논문지, 제31권, 제4호, pp. 347-352, 2004.

[17] 류종호, 염흥렬, "분할된 패스워드 기반 인증된 키 교환 프로토콜," 정보보호학회논문지, 제14권, 제5호, pp. 23-36, 2004.

[18] 박호상, 정수환, "패스워드 기반의 상호 인증 및 키 교환 프로토콜," 정보보호학회논문지, 제12권, 제5호, pp. 38-43, 2002.

[19] 심경아, 이주희, 이향숙, "두 패스워드 기반 키 교환 및 인증 프로토콜에 대한 오프라인 패스워드 추측 공격의 취약성 분석," 정보보호학회논문지, 제18권, 제1호, pp. 3-10, 2008.

박 춘 식

1981년 광운대학교 졸업
1983년 한양대학교 전자통신공학과 석사
1995년 일본동경공업대학 정보보호 전공 공학박사
1982년~1999년 한국전자통신연구원 책임연구원
2000년~현재 한국전자통신연구원 부설연구소 책임연구원
관심분야 : 암호이론, 정보이론, 네트워크보안