情報保護學會論文誌
第16卷 第2號, 2006. 4

일방향 함수를 이용한 개선된 패스워드 변경 프로토콜*

전 일 수
금오공과대학교

Improved Password Change Protocol Using One-way Function*

Il-Soo Jeon
Kumoh National Institute of Technology

요 약

최근에 Chang등[9]은 Yeh등[8]이 제안한 패스워드 기반의 인증된 키교환 프로토콜의 성능을 향상시키기 위하여 새로운 패스워드 기반의 키교환 프로토콜과 패스워드 변경 프로토콜을 제안하였다. 그러나 Wang등[10]은 Chang등의 패스워드 변경 프로토콜이 사전공격과 서비스거부 공격에 취약함을 제시하였다. 본 논문에서는 Chang등의 패스워드 변경 프로토콜에 존재하는 문제점을 해결하기 위한 개선된 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜에서는 주고받는 메시지에서 패스워드를 유추하고 유추된 패스워드를 검증하는 것이 불가능하도록 메시지의 형태를 변경한다. 제안한 프로토콜은 기존의 패스워드 기반의 프로토콜이 갖는 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결한다.

ABSTRACT

Recently, Chang et al.[9] proposed a new password-based key agreement protocol and a password change protocol to improve the efficiency in the password-based authenticated key agreement protocol proposed by Yeh et al.[8]. However, Wang et al.[10] showed that their protected password change protocol is not secure under the denial of service attack and the dictionary attack. This paper proposes an improved password change protocol to solve the problems in the Chang et al.'s protocol. In the proposed protocol, the format of communication messages is modified not to have any clue for the guessing of the password and verifying of the guessed password. The proposed protocol supports the advantages in the previous password-based protocols and solves the problems in them effectively.

Keywords : *Key exchange protocol, Password change protocol, Authentication, One-way function*

Ⅰ. 서 론

인터넷과 같은 공개된 통신망을 통하여 안전하게 통신하기 위해서는 전송하려는 정보를 암호화하여야 한다. 전송할 자료를 암호화하기 위해서는 통신 참여자들 간에 공통으로 사용하기 위한 키를 공유해야 하고, 통신하고 있는 상대가 정당한 사용자 인지를 확인할 수 있어야 한다. 따라서 참여자들이 서로를 인증하고 키를 공유할 수 있는 키 교환 프로토콜의 개발이 필요하다.

1976년에 제안된 Diffie-Hellman 키 교환 프로토콜은 안전하지 않은 통신상에서 안전하게 세션키를 공유하기 위한 가장 잘 알려진 방법이다[1]. 이 프로토콜은 유한 필드 상에서 이산대수 문제의 어려움을 이용하여 참여자들 간에 세션키를 공유한다. 하지만 이 프로토콜은 참여자들을 인증하는 방법을 제공하지

접수일: 2006년 2월 10일; 채택일: 2006년 3월 27일
* 본 연구는 금오공대 Pop-iT 인력양성사업단 연구비 지원에 의하여 연구된 논문
† 주저자 : isjeon@kumoh.ac.kr

못하기 때문에 중간 침입자 공격(man in the middle attack)에 대하여 안전하지 못하다. 이러한 문제를 해결하기 위하여 Seo와 Sweeney는 Diffie-Hellman 키 교환 프로토콜을 토대로 하여 사람이 기억할 수 있는 작은 패스워드를 이용하여 간단한 방법으로 참여자들간에 세션키를 공유하고 서로를 인증할 수 있는 SAKA (simple authenticated key agreement) 프로토콜을 제안하였다[2]. 그러나 SAKA는 여러 문제점들을 가지고 있었다. 먼저, Tseng은 SAKA 프로토콜이 중간 침입자 공격에 의해 세션키의 검증에 문제가 발생할 수 있음을 지적하고 SAKA의 키 검증 단계를 개선한 새로운 프로토콜을 제안하였다[3]. 그 후에 Ku와 Wang은 Tseng의 프로토콜이 두 종류의 중간 침입자 공격에 취약하다는 것을 보이고, SAKA의 키 검증 단계를 재 수정하였다[4]. 한편, Sun은 SAKA가 중간 침입자 공격뿐만 아니라 패스워드 추측 공격(password guessing attack)에도 안전하지 못하고 완전한 전방향 보안성(perfect forward secrecy)도 제공하지 못하는 취약점을 가지고 있음을 지적하였다[5]. Lin 등은 Sun이 지적한 이 문제들을 해결하기 위하여 SAKA의 키 검증 단계를 개선하였다[6]. 그러나 Hsieh 등은 Lin 등이 제안한 프로토콜도 여전히 패스워드 추측 공격에 안전하지 않음을 보여주었다[7]. Yeh 등은 SAKA의 패스워드 추측공격을 해결하기 위한 새로운 프로토콜을 제안하였다[8]. 최근에, Chang등은 Yeh 등의 프로토콜의 효율성을 증대시키기 위해서 새로운 패스워드 기반의 키교환 프로토콜과 패스워드 변경 프로토콜을 제안하였다[9]. 그러나 Wang등은 Chang등의 프로토콜 역시 사전공격(dictionary attack)과 서비스거부 공격(denial of service attack)에 취약함을 제시하였다[10]. Ku등은 Sun등[5]의 패스워드기반의 사용자 인증 프로토콜의 문제점을 해결하기 위한 개선된 인증 프로토콜과 패스워드 변경 프로토콜을 제안하였다[11]. Ku등의 패스워드 변경 프로토콜은 서버의 개입 없이 사용자가 본인이 원하는 시점에 패스워드를 자유롭게 변경할 수 있는 장점이 있다. 하지만 Hsu[12]는 Ku등의 패스워드 변경 프로토콜이 안전하지 않음을 보였고, Yoon등[13]은 Hsu등이 제시한 Ku등의 패스워드 변경 프로토콜에 안전성을 제시할 수 있는 개선된 프로토콜을 제안하였다. 그러나 Kumar[14]는 Yoon등의 프로토콜이 여전히 내부인 및 외부인의 공격에 취약함을 보였다.

본 논문에서는 Chang등[9]의 프로토콜에 존재하는 문제를 해결하기 위하여 암호학적으로 안전한 개선된 패스워드 변경 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜은 Chang등의 프로토콜에서 존재하는 문제점을 해결하기 위하여 주고받는 메시지에서 패스워드를 유추하고 유추된 패스워드를 검증하는 것이 불가능하게 하고 또한 서비스 거부 공격에 대항할 수 있도록 메시지의 형태를 변경한다. 본 논문에서 제안한 프로토콜은 기존의 패스워드 기반의 프로토콜이 갖는 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결할 수 있을 것이다. 제안한 프로토콜은 구성이 간단하기 때문에 하드웨어나 소프트웨어로 구현하기에 용이할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 먼저 기존의 Chang등이 제안한 보호된 패스워드 변경 프로토콜에 대해서 살펴보고 Wang등이 제시한 Chang등의 프로토콜에 존재하는 암호학적 취약성에 대해서 살펴본다. 3장에서는 개선된 패스워드 변경 프로토콜을 제안하고 4장에서는 제안된 프로토콜에 대한 암호학적 분석을 제시한다. 마지막으로 5장에서는 결론을 맺는다.

II. Chang등의 패스워드 변경 프로토콜

Chang등은 논문 [9]에서 간단한 인증된 키교환 프로토콜과 보호된 패스워드 변경 프로토콜을 제안하였다. 본 장에서는 Chang등이 제안한 보호된 패스워드 변경 프로토콜에 대해서 살펴보고, Wang등이 논문 [10]에서 제시한 이 프로토콜의 문제점을 분석한다.

1. 패스워드 변경 프로토콜

Chang등의 보호된 패스워드 변경 프로토콜에서 시스템은 q가 $(p-1)$의 약수 속성을 갖는 두개의 큰 소수 p와 q를 사용자들에게 공개하고, 유한필드 $GF(p)$상의 차수 q를 갖는 생성자 g를 공개한다. Alice는 Bob과 공유하고 있는 기존 패스워드 pw를 새로운 패스워드 pw'으로 변경하려 할 때 다음 단계를 수행한다.

Step 1. Alice는 난수 $a \in [1, q-1]$를 선택하고, $R_A = g^a \bmod p$를 계산하여 다음 메시지를 Bob에게 전송한다.

$\{ R_A \oplus pw \,||\, R_A \oplus pw' \}$

여기서 ⊕는 XOR 연산을 의미하고 ||는 접합 연산자를 의미한다.

Step 2. Bob은 Alice로부터 받은 메시지의 앞부분에 $R_A \oplus pw \oplus pw$를 연산을 수행함으로써 R_A를 찾고, 메시지의 뒷부분에 $R_A \oplus pw' \oplus R_A$을 수행함으로써 변경하고자 하는 새로운 패스워드 pw'을 찾는다. Bob은 난수 $b \in [1, q-1]$를 선택하고, $R_B = g^b \bmod p$와 $K_B = R_A{}^b = g^{ab} \bmod p$를 계산하여 다음 메시지를 Alice에게 전송한다.

$\{ R_B \,||\, h(K_B, R_A) \}$

여기서 $h()$는 공개된 일방향 해쉬 함수이다.

Step 3. Alice는 Bob으로부터 받은 메시지를 이용하여 $K_A = R_B{}^a = g^{ab} \bmod p$를 계산하고, 받은 메시지 $h(K_B, R_A)$가 $h(K_A, R_A)$와 일치하는지 검증한다. 검증이 성공하면 Alice는 다음 메시지를 계산하여 Bob에게 전송한다.

$\{ h(K_A, R_B) \oplus pw' \}$

Step 4. Bob은 Step 2에서 유도한 pw'를 이용하여 $h(K_A, R_B) \oplus pw' \oplus pw'$ 연산을 수행함으로써 $h(K_A, R_B)$를 계산하고, 그 값이 $h(K_B, R_B)$와 일치하는지를 검증한다. 검증이 성공하였다는 것은 Alice와 Bob은 성공적으로 그들이 공유한 패스워드 pw를 새로운 패스워드 pw'로 변경하였다는 것을 의미한다.

그림 1에서 이 프로토콜을 요약하였다.

2. 패스워드 변경 프로토콜의 취약점

본 절에서는 Wang등이 제시한 패스워드 변경 프로토콜에 존재하는 두 가지 취약점인 사전공격(dictionary attack)과 서비스거부공격(denial of service attack)을 제시한다[10]. 이들 공격의 상세한 내용은 다음과 같다.

[사전공격] 패스워드를 이용하는 프로토콜에서 사용자는 패스워드를 쉽게 기억하기 위해서 일반적으로 짧은 길이의 패스워드를 선택한다. 그러므로 만약 공격자가 패스워드 정보를 포함하는 연산식과 패스워드 정보가 알려지지 않은 몇몇 다른 파라메터들을 획득할 수 있다면, 공격자는 패스워드 사전에 있는 패스워드들을 반복적으로 선택하고 그 연산식을 통해서 정확성을 테스트함으로써 정확한 패스워드를 찾을 수 있을 것이다. 이러한 공격을 사전공격이라고 한다.

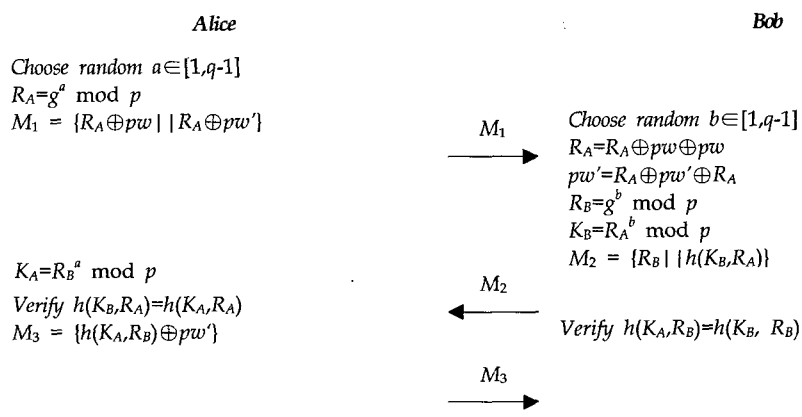

그림 1. Chang등의 패스워드 변경 프로토콜

공격자는 사전공격을 위해서 Step 1에서 { $R_A \oplus pw \,||\, R_A \oplus pw'$ }를 도청하고 $Y=pw \oplus pw'$를 계산하기 위해서 $Y=(R_A \oplus pw) \oplus (R_A \oplus pw')$ 연산을 수행한다. 여기서 공격자는 두 가지 값 pw와 pw'을 모른다. 만약 Alice가 패스워드를 선택할 때 가능한 여러 가지 (pw, pw')쌍 중에 수식 $Y=pw \oplus pw'$을 만족하는 (pw, pw')쌍을 선택했다면, 공격자는 T가 패스워드 사전의 단어의 개수라고 할 때 적어도 $O(T^2)$시간동안 사전공격을 수행함으로써 정확한 키쌍을 찾을 수 있다.

{서비스거부공격} 서비스거부공격은 정당한 사용자가 원하는 서비스를 요청하더라도 서비스가 제공되지 않도록 하는 가용성에 대한 공격이다.

공격자는 Step 1에서 { $R_A \oplus pw \,||\, R_A \oplus pw'$ }를 도청하고 이 메시지에 대해 난수 k를 이용하여 { $R_A \oplus pw \,||\, R_A \oplus pw' \oplus k$ }로 변환하여 전송한다. 그리고 Step 3에서 { $h(K_A, R_B) \oplus pw'$ }를 도청하고 이 메시지를 { $h(K_A, R_B) \oplus pw' \oplus k$ }로 변환하여 전송한다.

Bob의 관점에서는 Alice의 새로운 패스워드가 Alice에 의해서 선택된 pw'이 아니라 ($pw' \oplus k$)로 알게 된다. 그러므로 Alice와 Bob 사이에 공유된 패스워드의 불일치가 발생하게 되고 서비스거부가 발생한다.

III. 개선된 패스워드 변경 프로토콜

본 장에서는 Chang 등의 패스워드 변경 프로토콜의 문제점을 해결할 수 있는 개선된 패스워드 변경 프로토콜을 제안한다.

1. 표기

본 절에서는 제안된 패스워드 변경 프로토콜에서 사용될 용어와 표기법을 그림 2와 같이 정의한다.

Alice, Bob	각각 정당한 사용자
p, q	q가 (p-1)의 약수인 큰 소수
g	GF(p)상의 차수 q를 갖는 필드 생성자
pw	사용자 간에 공유하고 있는 패스워드
pw'	변경하고자 하는 새로운 패스워드
a, b	난수 a, b∈[1,q-1]
h()	암호학적 일방향 해쉬 함수
⊕	XOR 연산자
||	접합 연산자

그림 2. 프로토콜을 위한 표기

2. 개선된 프로토콜

본 논문에서 제안한 개선된 패스워드 변경 프로토콜에서도 두개의 큰 소수 p와 q를 사용자들에게 공개하고, 유한필드 GF(p)상의 생성자 g를 공개한다. Alice는 Bob과 공유하고 있는 기존 패스워드 pw를 새로운 패스워드 pw'으로 변경하려 할 때 다음 단계를 수행한다.

Step 1. Alice는 난수 a를 선택하고, $R_A=g^a \bmod p$와 $h(R_A)$를 계산하여 다음 메시지를 Bob에게 전송한다.

{ $R_A \oplus pw \,||\, h(R_A) \oplus pw'$ }

Step 2. Bob은 Alice로부터 받은 메시지의 앞부분에 $R_A \oplus pw \oplus pw$를 연산을 수행함으로써 R_A를 찾고 $h(R_A)$연산을 수행하여 메시지의 뒷부분에 연산 $h(R_A) \oplus pw' \oplus h(R_A)$을 수행함으로써 변경하고자 하는 새로운 패스워드 pw'을 찾는다. Bob은 난수 b를 선택하고, $R_B=g^b \bmod p$와 $K_B=R_A{}^b=g^{ab} \bmod p$, $h(K_B, R_A)$를 계산하여 다음 메시지를 Alice에게 전송한다.

{ $R_B \,||\, h(K_B, R_A)$ }

Step 3. Alice는 Bob으로부터 받은 메시지를 이용하여 $K_A=R_B{}^a \bmod p=g^{ab} \bmod p$를 계산하고 받은 메시지 $h(K_B, R_A)$가 $h(K_A, R_A)$와 일치하는지 검증한다. 검증이 성공하면 Alice는 $h(K_A, R_B)$와 $h(pw')$를 계산하여 다음 메시지를 Bob에게 전송한다.

{ $h(K_A, R_B) \oplus h(pw')$ }

Step 4. Bob은 Step 2에서 유도한 pw'를 이용하여 $h(pw')$를 계산하고, $h(K_A, R_B)\oplus h(pw')\oplus h(pw')$ 연산을 수행함으로써 $h(K_A, R_B)$를 계산하고 그 값이 $h(K_B, R_B)$와 일치하는지를 검증한다. 검증이 성공하였다는 것은 Alice와 Bob은 성공적으로 그들이 공유한 패스워드 pw가 새로운 패스워드 pw'으로 변경되었다는 것을 의미한다.

그림 3에서 제안한 프로토콜을 요약하였다.

Ⅳ. 안정성 분석

본 장에서는 본 논문에서 제안한 개선된 패스워드 변경 프로토콜의 암호학적 안정성을 분석한다. 먼저, 제안한 프로토콜은 기존의 Wang등이 제시한 Chang 등의 프로토콜에 존재하는 문제점인 패스워드 사전공격(dictionary attack)과 서비스거부공격(denial of service attack)의 측면에서 안전성을 분석하고 추가적인 요구사항에 대해서도 분석한다.

[사전공격] 공격자가 프로토콜 수행으로부터 얻을 수 있는 정보는 그림 3에서 보여준 바와 같이 주고받는 메시지인 M_1, M_2, M_3이다. 이들 메시지 가운데 패스워드와 관련된 정보를 포함하는 메시지는 M_1과 M_3이다. 공격자는 M_1과 M_3를 통하여 패스워드 pw나 pw'를 유추하려고 할 것이다. 이들 정보로부터 패스워드를 유도하기 위해서는 공격자는 R_A나 $h(R_A)$, 혹은 $h(K_A,R_B)$를 알아야 한다. 그러나 이들 정보를 주고받는 메시지를 통해서 찾는 것은 이산대수의 어려움이나 일방향 해쉬함수의 어려움에 근거한다. 또한 Wang등이 제시한 사전공격을 수행하기 위해서는 Step 1의 메시지 M_1에서 패스워드 pw나 pw'과 연계된 값을 추측할 수 있어야 하고, 추측한 값의 정당성을 확인할 수 있는 방법이 제시되어야 한다. 그러나 본 논문의 프로토콜에서 주고받는 메시지를 통해서는 이러한 사전공격은 불가능하다.

[서비스거부공격] 2.2절에서 제시한 바와 같이 서비스 공격이 가능하기 위해서 공격자는 패스워드 변경 프로토콜 수행 중 정당한 사용자가 알아채지 못하도록 주고받는 새로운 패스워드를 포함하는 메시지에 임의의 추가적인 정보를 덧붙일 수 있어야 한다. 그러나 본 논문에서 제안한 프로토콜에서는 Wang등의 공격에서 제시한 방법대로 Step 1의 메시지에 임의의 추가적인 정보를 덧붙여 보낸다면, Step 3의 검증과정에서 오류가 발생하게 되므로 이러한 공격은 불가능하다.

위의 안전성 분석에 추가하여 대부분의 보안 프로토콜에서 요구되는 메시지 재전송 공격과 위장공격에 대한 안전성을 제시한다.

[메시지 재전송 공격] 메시지 재전송 공격은 이전

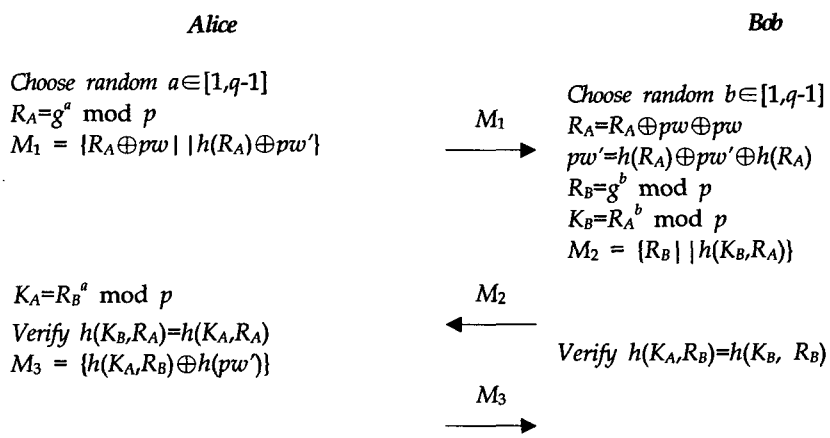

그림 3. 개선된 패스워드 변경 프로토콜

세션의 메시지를 저장하고 다음 세션들에서 재전송(replay)하는 방법으로 참여자들이 알지 못한 상태에서 불법적인 사용자가 프로토콜 참여를 시도하는 공격이다. 본 논문에서는 메시지 재전송 공격을 방지하기 위하여 세션에서 생성된 난수의 쌍을 이용하였다. 공격자가 메시지 재전송 공격을 하기 위해서는 이전 세션에서 획득한 M_1과 M_2, 그리고 M_3으로부터 현재 세션에서 사용된 난수와 연계된 메시지를 생성할 수 있어야 한다. 그러나, 그러기 위해서는 정확한 패스워드 관련 정보와 난수들을 유추할 수 있어야 하지만, 공격자가 이전 세션과 현재 세션에서 얻은 정보로부터 정확한 이들 정보를 유추할 수 있는 방법은 없다.

[위장공격] 적법한 사용자나 공격자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 패스워드를 알아야 한다. 본 논문에서 제안한 프로토콜은 현재 세션이나 이전 세션에서 주고받는 정보를 통해서 패스워드를 찾거나 사전공격을 통하여 패스워드를 찾는 것이 불가능하기 때문에 이러한 위장공격은 불가능하다.

V. 결 론

최근에 Chang등은 보호된 패스워드 변경 프로토콜을 제안하였으나 Wang등은 이 프로토콜에 사전공격과 서비스거부공격이 가능함을 보였다. 본 논문에서는 Wang등의 공격에 대한 해결책으로 개선된 패스워드 변경 프로토콜을 제안하였다.

본 논문에서 제안한 프로토콜에서는 Chang등의 프로토콜에서 존재하는 문제점을 해결하기 위하여 주고받는 메시지에서 패스워드를 유추하고 유추된 패스워드를 검증하는 것이 불가능하도록 메시지의 형태를 변경하였다. 본 논문에서 제안한 프로토콜은 기존의 패스워드 기반의 프로토콜이 갖는 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결할 수 있다. 또한, 제안한 프로토콜은 구성이 간단하기 때문에 하드웨어나 소프트웨어로 구현이 용이하므로 유용하게 사용될 수 있을 것이다.

참 고 문 헌

[1] Diffie W., and Hellman M.E., "New directions in cryptography," *IEEE Trans.*, Vol. *IT-22*, No. 6, pp. 644-654, 1976.

[2] Seo D.H., and Sweeney P., "Simple authenticated key agreement algorithm," *IEE Electronics Letter*, Vol. 35, No. 13, pp. 1073-1074, 1999.

[3] Tseng Y.M., "Weakness in simple authenticated key agreement protocol," *IEE Electronics Letter*, Vol. 36, No. 1, pp. 48-49, 2000.

[4] Ku W.C., and Wang S.D., "Cryptanalysis of modified authenticated key agreement protocol," *IEE Electronics Letter*, Vol. 36, No. 21, pp. 1770-1771, 2000.

[5] Sun H., "On the security of simple authenticated key agreement algorithm," *Proceedings of the Management Theory Workshop 2000*, 2000.

[6] Lin I.C., Chang C.C., and Hwang M.S., "Security Enhancement for the Simple Authentication Key Agreement Algorithm," *24th Ann. Int. Computer Software and Applications Conf.*, pp. 113-115, 2000

[7] Hsieh B.T., Sun H.M., and Hwang T., "Cryptanalysis of enhancement for simple authentication key agreement algorithm," *IEE Electronics Letter*, Vol. 38, No. 1, pp. 20-21, 2002.

[8] Yeh H.T. and Sun H.M., "Simple authenticated key agreement protocol resistant to password guessing attacks," *ACM SIGOPS Operating Systems Review*, Vol. 36, No. 4, pp. 14-22, 2002.

[9] Chang T.Y., Yang W.P, and Hwang M.S., "Simple authenticated key agreement and protected password change protocol," *An International Journal Computers & Mathematics with Applications*, Vol. 49, pp. 703-714, 2005.

[10] Wang C.I., Fan C.I., and Guan D.J., "Cryptanalysis on Chang-Yang-Hwang protected password change protocol," *Cryptology ePrint Archive 2005/182*,

http://eprint.iacr.org/2005/182.
[11] Ku W.C. and Chen S.M. "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electronics*, Vol. 50, No. 1, pp. 204-207, 2004.
[12] Hsu C.L. "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interface*, Vol. 26, No. 3, pp. 167-169, 2004.
[13] Yoon E.J., Ryu E.K., and Yoo K.Y., "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electronics*, Vol. 50, No. 2, pp. 612-614, 2004.
[14] Kumar M., "The password change phase is still insecure," *cs.CR/0409004* 2004.

〈著者紹介〉

전 일 수 (Il-Soo Jeon) 정회원
e-mail : isjeon@kumoh.ac.kr
1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 대학원 전자공학과(공학석사)
1995년 경북대학교 대학원 전자공학과(공학박사)
1984년~1985년 삼성전자(주)
1989년~2004년 경일대학교 컴퓨터공학과 교수
2004년~현재 금오공과대학교 전자공학부 조교수
관심분야 : 정보보호, 암호 프로토콜