스마트카드를 이용한 새로운 패스워드 기반의 원격 사용자 인증 프로토콜†

(New Password based Remote User Authentication Protocols using Smartcards)

전 일 수*
(Il-Soo Jeon)

요 약 최근에 Ku와 Chen(Ku-Chen)은 기존에 Chien등이 제안한 스마트카드를 이용한 효율적인 패스워드 기반의 원격 사용자 인증 프로토콜의 문제점을 보이고 해결책을 제시하였다. 본 논문에서는 Ku-Chen의 프로토콜 역시 재 전송 공격들에 문제점이 있음을 보이고, 이를 해결하기 위한 두 가지 프로토콜을 제안한다. 먼저, Ku-Chen의 프로토콜에서 존재하는 문제점을 해결하기 위하여 동기화된 타임스탬프(Timestamp)를 이용한 프로토콜을 제안한다. 그리고 타임스탬프에 기반 한 프로토콜이 갖는 궁극적인 문제점을 해결하기 위하여 난수에 기반 한 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜들은 기존의 패스워드 기반의 인증 프로토콜의 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결한다.

핵심주제어 : 인증 프로토콜, 스마트카드, 패스워드 기반, 타임스탬프

Abstract Recently, Ku and Chen(Ku-Chen) showed some problems in the password based remote user authentication scheme using smartcards proposed by Chien et al. and proposed an improvement from it. This paper shows some weaknesses in the Ku-Chen's scheme, especially the replay attacks, and proposes two authentication protocols to solve the problems in it. First of all, an authentication protocol using synchronized timestamps is proposed to solve the problem in the Ku-Chen's protocol. Then, a nonce-based authentication protocol is proposed to solve the inherent problems in the synchronized timestamp-based authentication protocols. The proposed authentication protocols support the advantages in the previous password-based authentication protocols and solve the problems in them effectively.

Key Words : Authentication Protocol, Smartcard, Password-based, Timestamp

1. 서 론

인터넷과 같은 안전하지 않은 공개된 통신망을 통하여 원거리에 있는 사용자의 합법성을 인증하기 위한 기법을 원거리 사용자 인증 프로토콜이라고 한다. 1981년 Lamport는 암호화 기법을 사용하지 않는 최초의 패스워드 기반의 원격 사용자 인증 프로토콜을 제안하였다[1]. 그러나 이 프로토콜은 많은 해쉬 연산으로 인한 오버헤드와 패스워드 재설정을 해야하는 문제 때문에 실질적인 응용에는 활용되지 못했다. 또한, Lamport의

† 본 연구는 금오공과대학교 학술연구비에 의하여 연구된 논문임.
* 금오공과대학교 전자공학부

프로토콜은 작은 n 공격에 취약성이 있었다[2]. 그 이후 많은 Lamport의 프로토콜과 비슷한 프로토콜들이 제안되었고, 이들 프로토콜들은 각각의 장점과 단점을 가지고 있었다[3,4]. 이러한 프로토콜들이 공유하는 가장 일반적인 특징 중 하나는 사용자 검증을 위한 테이블이 서버에 안전하게 저장되어야 한다는 것이었다. 그러나 검증을 위한 테이블이 공격자에 의해 노출된다면, 그 시스템은 부분적으로 또는 완전히 무용지물이 될 것이다.

Hwang과 Li는 2000년에 스마트카드를 이용하는 원거리 사용자 인증 프로토콜을 제안하였다[5]. 이 프로토콜에서는 ID를 암호화 시스템으로 사용하였으므로 서버에 패스워드 테이블을 저장해야 하는 기존의 문제를 해결하였다. 그러나 Chan과 Cheng은 Hwang과 Li의 프로토콜에서 적법한 사용자가 서버의 비밀키를 몰라도 서버의 인증을 통과할 수 있는 아이디와 패스워드를 생성할 수 있음을 보였다[6]. 이를 해결하기 위하여 Kim 등은 스마트카드와 지문을 이용한 ID기반의 사용자 인증 프로토콜들을 제안하였다[7]. 그러나 Scott은 이들 프로토콜들이 소극적 공격에 취약함을 보였다[8]. 이러한 문제를 해결하기 위하여 Kim 등은 효율적인 대안을 제시하였다[9]. 그러나 이들 프로토콜들은 모두 이산 대수 문제(Discrete logarithm problem)의 어려움에 근거하므로 연산의 부하가 상대적으로 큰 모듈러 지수연산을 필요로 한다.

Sun은 Hwang과 Li가 제안한 프로토콜의 효율성을 개선하기 위하여 주요 연산으로 해쉬 연산을 사용하는 스마트카드를 이용한 효율적인 원거리 사용자 인증 프로토콜을 제안하였다[10]. 그러나 Sun의 프로토콜은 양방향 인증을 제공하지 못하고 사용자가 랜덤값을 자신의 패스워드로 기억해야 하고, 패스워드를 변경하지 못하는 문제점이 있었다. Chien 등은 Sun의 프로토콜의 문제점을 해결하기 위한 해쉬함수 만을 사용하는 효율적인 패스워드 기반의 원격 사용자 인증 프로토콜을 제안하였다[11]. 하지만 최근에 Ku와 Chen은 Chien의 프로토콜이 반사공격(Reflection attack)과 내부자 공격에 취약함을 보이고 이들을 위한 해결책을 제시하였다[12].

본 논문에서는 Ku와 Chen에 의해서 제시된 프로토콜 역시 재전송 공격들과 동시 로그인 공격에 취약함을 제시하고 이러한 문제를 해결할 수 있는 스마트카드를 이용한 새로운 두 가지 인증 프로토콜을 제안한다. 먼저, Ku-Chen의 프로토콜에서 존재하는 문제점을 해결하기 위하여 동기화된 타임스탬프(Timestamp)를 이용한 프로토콜을 제안한다. 그리고 타임스탬프에 기반한 프로토콜이 갖는 궁극적인 문제점을 해결하기 위하여 난수에 기반한 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜들은 기존의 패스워드 기반의 인증 프로토콜의 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결한다.

본 논문의 구성은 다음과 같다. 2장에서는 Ku와 Chen이 제안한 스마트카드를 이용한원격 사용자 인증 프로토콜을 기술하고 이 프로토콜의 문제점을 제시한다. 3장에서는 기존의 Ku와 Chen의 프로토콜의 문제점을 해결할 수 있는 새로운 두 가지 인증 프로토콜을 제안한다. 4장에서는 제안된 프로토콜들에 대한 암호학적 안전성 분석을 제시하고 5장에서는 결론을 맺는다.

2. Ku-Chen 인증 프로토콜

본 장에서는 최근에 Ku와 Chen(Ku-Chen)이 제안한 스마트카드를 이용한 원격 사용자 인증 프로토콜[12]에 대해서 살펴보고 이 프로토콜의 문제점을 분석한다.

2.1 Ku-Chen 인증 프로토콜

Ku-Chen 프로토콜은 등록단계와 로그인단계, 그리고 검증단계의 3단계로 구성된다. Ku-Chen 인증 프로토콜의 각 단계는 다음과 같다.

[등록단계] 이 단계는 사용자 U가 서버 S에 등록하거나 재등록할 때 수행된다. 여기서 n이 U가 서버 S에게 등록을 요청한 횟수라고 가정한다.

Step R1. U는 랜덤 값 b를 선택하고 패스워드 PW를 이용하여 다음 해쉬 값을 계산한다.
$h(b \oplus PW)$

Step R2. U는 원격서버 S에게 다음을 전송한다.
$ID, h(b \oplus PW)$

Step R3. 만약 U가 처음으로 등록을 시도한다면 원격서버 S는 U를 위한 계정 데이터베이스를 생성하고 n=0으로 저장한다. 그렇지 않다면, 서버 S는 n=n+1로 U를 위해 항목을 변경한다. 그리고 S는 다음을 계산한다.
$R = h(EID \oplus x) \oplus h(b \oplus PW)$
여기서, EID=($ID||n$)이고 x는 S의 비밀키이다.

Step R4. S는 U에게 R과 $h()$가 저장된 스마트카드를 발급한다.

Step R5. U는 랜덤 값 b를 스마트카드에 저장한다.

사용자 U의 스마트카드에 R과 $h()$, 그리고 랜덤 값 b가 저장되어 있기 때문에 Step R5를 끝낸 사용자 U는 더 이상 랜덤 값 b를 기억할 필요가 없다.

[로그인단계] 이 단계는 사용자 U가 서버 S에 로그인을 요청할 때마다 수행된다.

Step L1. U는 스마트카드를 터미널에 부착된 카드리더기에 넣고 아이디 ID와 패스워드 PW를 입력한다.

Step L2. U의 스마트카드는 다음을 계산한다.

$c_1 = R \oplus h(b \oplus PW)$

$c_2 = h(c_1 \oplus T_u)$

여기서, T_u는 U의 현재 타임스탬프이다.

Step L3. U의 스마트카드는 S에게 ID, T_u, c_2를 보낸다.

[검증단계] 이 단계는 서버 S가 사용자 U의 로그인 요청을 받을 때마다 수행된다.

Step V1. 만약 ID나 T_u가 유효하지 않다면 서버 S는 사용자 U의 로그인 요청을 거절한다. 그렇지 않다면 서버 S는 $h(h(EID \oplus x) \oplus T_u)$를 계산하여 이 값이 사용자 U로부터 받은 c_2와 같다면 사용자 U의 로그인 요청을 받아들이고 서버의 타임스탬프 T_s를 이용하여 c_3=$h(h(EID \oplus x) \oplus T_s)$를 계산하고, 같지 않다면 사용자 U의 로그인 요청을 거절한다.

Step V2. S는 U에게 T_s, c_3를 보낸다.

Step V3. 만약 T_s가 유효하지 않거나 T_s=T_u라면 사용자 U는 그 세션을 종료하고, 그렇지 않다면 $h(c_1 \oplus T_s)$를 계산하여 서버 S로부터 받은 c_3와 같으면 서버를 성공적으로 인증한다.

또한 Ku-Chen 인증 프로토콜에서는 사용자가 패스워드를 변경하기 위한 부수적인 단계를 다음과 같이 제안하였다.

[패스워드변경단계] 이 단계는 사용자 U가 패스워드 PW를 새로운 패스워드 PW_{new}로 변경하고자 할 때마다 수행된다.

Step P1. U는 스마트카드를 터미널에 부착된 카드리더기에 넣고 아이디 ID와 패스워드 PW를 입력하고 패스워드 변경을 요청한다. 그리고 U는 새로운 패스워드 PW_{new}를 입력한다.

Step P2. U의 스마트카드는 다음을 계산한다.

$R_{new} = R \oplus h(b \oplus PW) \oplus h(b \oplus PW_{new})$

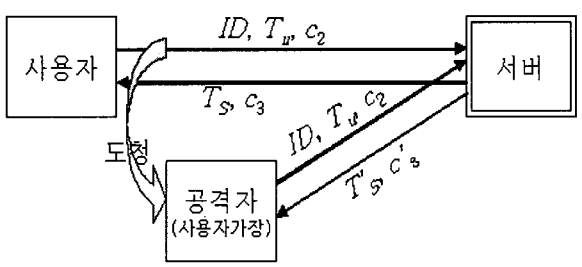
여기서, 계산된 R_{new}는 $h(EID \oplus x) \oplus h(b \oplus PW_{new})$로 저장된다. 스마트카드는 R_{new}를 R로 대체한다.

패스워드 변경은 스마트카드 안에서만 연산이 이루어지기 때문에 U는 서버 S에게 패스워드 변경에 관한 내용을 알릴 필요가 없다.

2.2 Ku-Chen 인증 프로토콜의 취약점

본 절에서는 Ku-Chen 인증 프로토콜의 취약점을 3가지 관점에서 제시한다. 먼저, Ku-Chen 인증 프로토콜은 타임스탬프를 이용하기 때문에 느슨하게 동기화된 시스템(Loosely time-synchronized system)에서는 적법한 사용자의 로그인이더라도 T_s=T_u 일 수 있으므로 이 경우 서버에 접근을 거부당할 가능성이 존재한다.

그리고 Ku-Chen 인증 프로토콜이 원격 사용자 환경을 기반으로 하기 때문에 전송지연이 고려된 적법한 시간 이내에 그림 1과 같은 재전송 공격을 이용한 동일 사용자를 가장한 동시 접속 공격이 가능하다.



<그림 1> 재전송 공격

원격 서버 접속에서 한명의 사용자가 동시에 여러개의 세션을 확립하고 작업하는 경우가 많기 때문에 Ku-Chen 프로토콜에서는 그림1과 같은 공격이 가능하다. 즉, 사용자의 로그인요청 메시지를 도청한 공격자는 그 메시지를 서버에게 재전송 함으로서 동일한 사용자가 새로운 세션을 열기위한 요구로 인식하게 할 수 있다. 또한, 서버의 인증을 위해서 서버로부터 사용자에게 전송되는 메시지를 차단하고 임의의 메시지를 삽입함으로서 사용자를 교란시킬 수 있다.

또한, 공격자는 바로 이전의 세션의 메시지를 이용하여 사용자 위장 공격을 수행 할 수 있다. 공격자가 이전 세션에서 서버의 인증을 위해서 서버가 원격 사용자에게 보낸 검증단계의 Step V3의 메시지인 T_s, c_3를 이용하여 시간지연 없이 바로 로그인단계의 Step L3를 위한 정당한 사용자의 메시지로 ID, T_s, c_3를 보내면 서버의 검증단계를 성공적으로 통과할 수 있다.

3. 새로운 원격 사용자 인증 프로토콜

본 장에서는 Ku-Chen 인증프로토콜의 문제점을 해결할 수 있는 스마트카드를 이용한 새로운 두 가지 인증 프로토콜을 제안한다. 먼저, Ku-Chen의 프로토콜에서 존재하는 문제점을 해결하기 위하여 동기화된 타임스탬프(Timestamp)를 이용한 프로토콜을 제안한다. 그리고 타임스탬프에 기반한 프로토콜이 갖는 궁극적인 문제점을 해결하기 위하여 난수에 기반한 프로토콜을 제안한다.

3.1 표기

본 절에서는 제안된 인증프로토콜에서 사용될 용어와 표기법을 그림 2와 같이 정의한다.

U, S	각각 정당한 사용자와 서버의 식별자
ID	사용자의 아이디
EID	사용자의 확장된 아이디
x	서버의 비밀키
PW	사용자의 패스워드
$f()$	암호학적 방향 해쉬 함수

<그림 2> 인증 프로토콜을 위한 표기

3.2 Timestamp-based 인증 프로토콜

본 논문에서 제안한 타임스탬프에 기반한 인증 프로토콜도 Ku-Chen의 프로토콜과 마찬가지로 등록단계와 로그인단계, 그리고 검증단계의 3단계로 구성된다. 제안한 프로토콜의 등록단계와 로그인단계는 Ku-Chen 프로토콜에서 제시한 방법을 따른다. 2.2절에서 제시한 Ku-Chen 인증 프로토콜의 문제를 해결하기 위해서 검증단계를 다음과 같이 수정한다.

[검증단계] 이 단계는 서버 S가 사용자 U의 로그인 요청을 받을 때마다 수행된다.

Step V1. 만약 ID나 T_u가 유효하지 않고, T_u가 이전 세션들에서 이용된 타임스탬프(T_u가 이전 세션들의 T_u나 T_s)라면 서버 S는 사용자 U의 로그인 요청을 거절한다. 그렇지 않다면 서버 S는 $h(h(EID \oplus x) \oplus T_u)$를 계산하여 이 값이 사용자 U로부터 받은 c_2와 같다면 사용자 U의 로그인 요청을 받아들이고 서버의 타임스탬프 T_s를 이용하여 $\underline{c_3=h(h(EID \oplus x) \oplus T_s) \oplus h(EID \oplus x)}$를 계산하고, 같지 않다면 서버 S는 사용자 U의 로그인 요청을 거절한다.

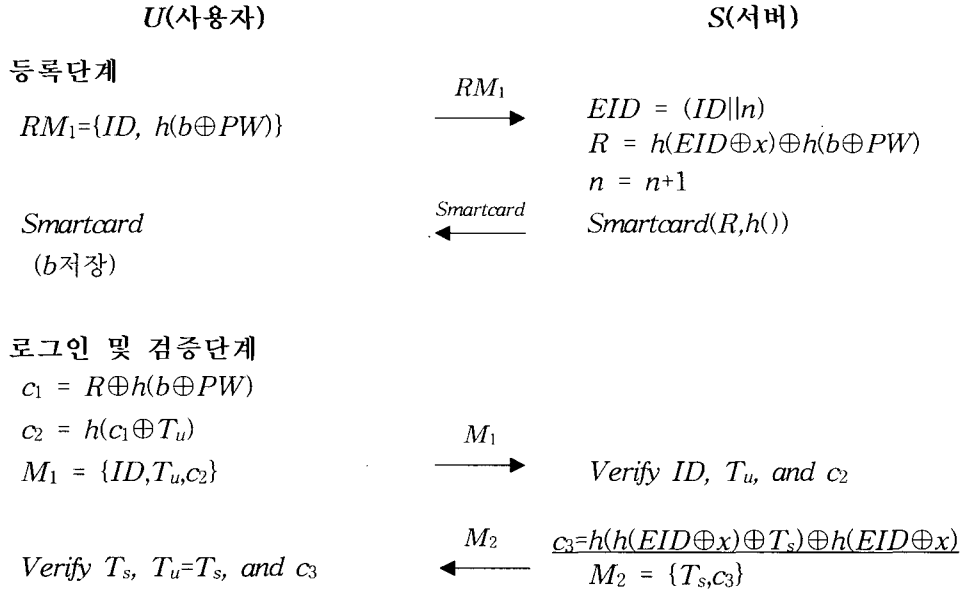
Step V2. S는 U에게 T_s, c_3를 보낸다.

Step V3. 만약 T_s가 유효하지 않거나 $T_s=T_u$라면 사용자 U는 그 세션을 종료하고, 그렇지 않다면 $h(c_1 \oplus T_s) \oplus c_1$를 계산하여 서버 S로부터 받은 c_3와 같으면 서버를 성공적으로 인증한다.

특히, 검증단계의 V1에서는 c_2와 다른 형식의 c_3를 이용함으로서 기존의 Ku-Chen 방법에서 암호학적 취약점을 해결하고 있다. 그림 3은 제안한 타임스탬프에 기반한 인증 프로토콜의 전체적인 처리 과정을 보여준다. 특히, 그림 3에서 밑줄친 부분은 Ku-Chen 방법의 문제점을 해결하기 위해서 본 논문에서 수정된 부분이다. 타임스탬프에 기반한 프로토콜들은 서버와 사용자 사이에 시간 동기화가 필요하다. 그러나 느슨한 동기화가 제공되어야 하는 네트워크 환경에서는 타임스탬프 기반의 프로토콜들은 메시지 재전송 공격에 잠재적인 취약성을 가질 수 밖에 없다. 이러한 문제를 해결하기 위해서 다음 절에서는 시간 동기화가 필요 없는 새로운 프로토콜을 제시한다.

3.3 Nonce-based 인증 프로토콜

본 절에서는 타임스탬프 대신에 랜덤값을 이용한 Nonce-based 인증 프로토콜을 제안한다. 이 프로토콜은 서버와 사용자 사이에 시간 동기화 없이도 메시지 재전송 공격을 해결할 수 있다. 제안한 프로토콜의 가정과 등록단계, 그리고 패스워드 변경 과정은 타임스탬프에 기반한 인증 프로토콜과 동일하다. 본 절에서는 로그인단계와 검증단계에 대해서만 기술한다.



<그림 3> 제안한 Timestamp-based 인증 프로토콜

[로그인단계] 이 단계는 사용자 U가 서버 S에 로그인을 요청할 때마다 수행된다.

Step L1. U는 스마트카드를 터미널에 부착된 카드리더기에 넣고 아이디 ID와 패스워드 PW를 입력한다.

Step L2. U의 스마트카드는 다음을 계산한다.

$$c_1 = R \oplus h(b \oplus PW)$$

$$c_2 = h(c_1 \oplus N_u)$$

여기서, N_u는 스마트카드에 의해 선택된 임의의 랜덤 값이다.

Step L3. U의 스마트카드는 S에게 ID, N_u, c_2를 보낸다.

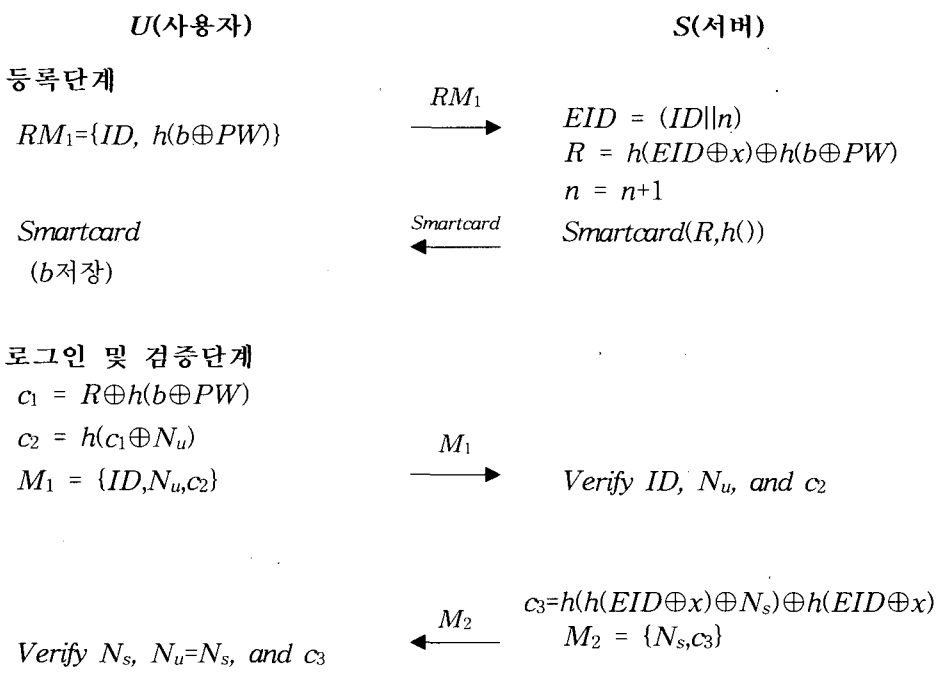
[검증단계] 이 단계는 서버 S가 사용자 U의 로그인 요청을 받을 때마다 수행된다.

Step V1. 만약 ID가 유효하지 않고 N_u가 이전 세션들에서 사용되었던 랜덤 값이라면 서버 S는 사용자 U의 로그인 요청을 거절한다. 그렇지 않다면 서버 S는 $h(h(EID \oplus x) \oplus N_u)$를 계산하여 이 값이 사용자 U로부터 받은 c_2와 같다면 사용자 U의 로그인 요청을 받아들이고 서버의 랜덤 값 N_s를 이용하여 $c_3 = h(h(EID \oplus x) \oplus N_s) \oplus h(EID \oplus x)$를 계산하고, 같지 않다면 서버 S는 사용자 U의 로그인 요청을 거절한다.

Step V2. S는 U에게 N_s, c_3를 보낸다.

Step V3. 만약 N_s가 이전 세션들에서 이용되었던 랜덤 값이거나 $N_s = N_u$라면 사용자 U는 그 세션을 종료하고, 그렇지 않다면 $h(c_1 \oplus N_s) \oplus c_1$를 계산하여 서버 S로부터 받은 c_3와 같으면 서버를 성공적으로 인증한다.

그림 4는 제안한 Nonce-based 인증 프로토콜의 전체적인 처리과정을 보여준다.



<그림 4> 제안한 Nonce-based 인증 프로토콜

4. 안전성 분석

본 장에서는 본 논문에서 제안한 새로운 두가지 인증 프로토콜의 암호학적 안정성을 분석한다. 3.2절에서 제안된 타임스탬프를 이용한 인증 프로토콜의 안정성 분석은 Ku-Chen에서와 유사하므로 생략한다[12]. 그러므로 본 장에서는 3.3절에서 제안한 Nonce-based 인증 프로토콜에 대한 다양한 공격들에 대해서 분석한다. 제안한 인증프로토콜은 패스워드 추측공격(Password guessing attack), 서버의 비밀키 추측 공격(Server's secret key guessing attack), 메시지 재전송 공격(Message replay attack), 위장공격(Impersonation attack)의 측면에서 안전성을 분석한다.

[패스워드 추측공격] 패스워드 추측공격은 온라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 패스워드 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로, 본 논문에서는 오프라인 패스워드 추측 공격에 대해서만 고려한다. 공격자는 인증을 위해서 전송되었던 메시지를 가로채어 저장해 두고, 오프라인으로 패스워드를 추측하기 위한 공격을 수행할 수 있다. 본 논문에서 제안한 인증프로토콜에서 패스워드를 획득할 수 있는 유일한 방법은 공격자가 합법적인 사용자에 대하여 도청한 메시지들 즉, $M_1 = \{ID,N_u,c_2\}$과 $M_2 = \{N_s,c_3\}$로부터 패스워드에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 패스워드를 유추하는 것은 해쉬함수의 일방향성 때문에 불가능하다.

[서버의 비밀키 추측공격] 서버의 비밀키 추측공격 또한 패스워드 추측공격에서와 마찬가지로 공격자가 합법적인 사용자에 대하여 도청한 메시지들로부터 서버의 비밀키에 관한 정보를 유추하는 것이다. 그러나 이들 정보로부터 서버의 비밀키를 유추하는 것도 해쉬함수의 일방향성 때문에 불가능하다.

[메시지 재전송 공격] 메시지 재전송 공격은 이전 세션의 메시지를 저장하고 다음 세션들에서 재전송(Replay)하는 방법으로 참여자들이 알지 못한 상태에서 불법적인 사용자가 인증을 시도하는 공격이다. 본 논문에서는 메시지 재전송 공격을 방지하기 위하여 매 세션마다 새로운 랜덤 값을 사용한다. 공격자가 메시지 재전송 공격을 하기 위해서는 이전 세션에서 획득한 $M_1 = \{ID,N_u,c_2\}$과 $M_2 = \{N_s,c_3\}$, 그리고 현재 세션에서 얻은 N_i으로부터 검증단계의 식을 만족할 수 있는 새로운 c_i로 변경할 수 있어야 한다. 그러기 위해서는 정확한 패스워드 관련 정보와 서버의 비밀키 정보를 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 아이디와 패스워드를 알아야 한다. 사용자의 아이디는 공개된 정보이기 때문에 쉽게 알 수 있지만, 본 논문에서 제안한 인증프로토콜은 사용자의 확장된 아이디인 EID를 사용하기 때문에 b값을 모르는 공격자가 확장된 아이디를 확인할 수 있는 방법은 없다. 그리고 사용자의 패스워드는 스마트카드에 저장되어 있고 $R = h(EID \oplus x) \oplus h(b \oplus PW)$을 안다고 하더라도 원격 서버의 비밀키 x를 찾는 것 역시 해쉬함수의 일방향성 때문에 불가능하다.

5. 결 론

본 논문에서는 먼저 최근에 Ku와 Chen에 의해서 제시된 패스워드 기반의 원격 사용자 인증 프로토콜(Ku-Chen) 역시 재전송 공격들과 동시 로그인 공격에 취약함을 보였다. 그리고 이러한 문제를 해결할 수 있는 스마트카드를 이용한 새로운 두 가지 인증 프로토콜들을 제안하였다. 먼저, Ku-Chen의 프로토콜에서 존재하는 문제점을 해결하기 위하여 동기화된 타임스탬프를 이용한 프로토콜을 제안하였다. 이 프로토콜에서는 상호인증을 위한 비대칭 정보를 사용함으로서 기존의 프로토콜에서 존재하는 문제를 효율적으로 해결할 수 있었다. 그리고 타임스탬프에 기반한 프로토콜이 갖는 시간동기화의 문제점을 해결하기 위하여 난수에 기반한 프로토콜을 제안하였다. 본

논문에서 제안한 프로토콜들은 기존의 패스워드 기반의 인증 프로토콜의 장점을 유지하면서 이 방식의 문제점들을 효율적으로 해결할 수 있을 것으로 기대한다.

참 고 문 헌

[1] L. Lamport, "Password authentication with secure communication," *Communication of ACM*, Vol. 24, pp. 770-772, 1981.

[2] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme," *ACM Operating Systems Review*, Vol. 30, No. 4, pp. 12-16, 1996.

[3] R. E. Lennon, S. M. Matyas, and C. H. Mayer, "Cryptographic authentication of time-invariant quantities," *IEEE Trans. Commun.*, Com-29, No. 6, pp. 773-777, 1981.

[4] S. M. Yen and K. H. Liao,, "Shared authentication token secure against replay and weak key attack," *Information Processing Letters*, pp. 78-80, 1997.

[5] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart card," *IEEE Trans. on Consumer Electron.*, Vol. 46, No. 1, pp. 28-30, 2000.

[6] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electron.*, Vol. 46, No. 4, pp. 992-993, 2000.

[7] H. S. Kim, S. W. Lee, and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM Operating Systems Review*, pp. 32-41, 2003.

[8] M. Scott, "Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *Cryptology ePrint Archive:Report 2004/017*, http://eprint.iacr.org, 2004.

[9] 김현성, 이성운, 유기영, "지문 기반의 사용자 인증 프로토콜," *한국정보과학회 정보보호 연구회지*, Vol. 4, No. 1, pp. 53-61, 2004.

[10] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electron.*, Vol. 46, No. 4, pp. 958-961, 2000.

[11] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication:smart card," *Computers & Security*, Vol. 21, No. 4, pp. 372-375, 2002.

[12] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. on Consumer Electron.*, Vol. 50, No. 1, pp. 204-207, 2004.

전 일 수 (Il-Soo Jeon)

- 1984년 경북대학교 전자공학과(학사)
- 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, 패턴인식