논문 2009-46CI-1-2

강력한 패스워드 상호인증 프로토콜

(Strong Password Mutual Authentication Protocol)

윤 은 준*, 홍 유 식**, 김 천 식***, 유 기 영****

(Eun-Jun Yoon, You-Sik Hong, Cheon-Shik Kim, and Kee-Young Yoo)

요 약

최근, 인터넷과 같이 신뢰할 수 없는 네트워크를 통한 통신환경에서, 사용자 인증은 비밀성과 무결성 보장을 위해 보안 분야에서 가장 중요한 기술로 주목받고 있다. 특히, 패스워드 기반의 사용자 인증 방법은 비용과 효율성 측면에서 갖는 장점 때문에 가장 널리 사용되는 사용자 인증 방법이다. 본 논문에서는 해쉬 함수를 사용한 강력한 패스워드 상호인증 프로토콜을 제안한다. 결론적으로, 제안한 인증 프로토콜은 기존의 관련 프로토콜들과 비교하여 보다 많은 보안성과 효율성을 제공하여 주어, 인터넷 인증 프로토콜로 실용적으로 사용되어 질 수 있다.

Abstract

Recently, user authentication is the most important part as far as security to provide confidentiality and integrity over untrusted networks like the Internet. Especially, password-based user authentication method is the most widely-used user authentication method due to various advantages, such as human-memorable simplicity, convenience, mobility, low-cost operations and efficiency. In this paper, we propose a new strong password mutual authentication protocol. As a result, the proposed authentication protocol provides more security and efficiency compare with the previously related protocols. So that, it can be used practically as the Internet authentication protocol.

Keywords : 네트워크 보안, 패스워드, 상호인증, 암호 프로토콜, 인터넷

I. 서 론

인터넷과 같은 공개된 네트워크 통신 환경 상에서 클라이언트와 서버간의 안전한 통신을 보장하기 위해서 사용자 인증(User Authentication)은 아주 중요한 보안 기술이다. 클라이언트와 서버간에 송수신하게 되는 기밀 메시지에 대한 보안성과 기밀성을 보장하기 위해 통신 상대자간의 신원증명은 반드시 안전하게 수행되어야 한다.

1981년 Lamport[1]가 제안한 원격 인증 프로토콜을 기반으로, 지금까지 많은 연구자들에 의해 사용자에게 편리하고 비용이 적게 들면서 효율성을 제공하는 패스워드 인증 프로토콜 개발에 관한 연구들이 수행되어져 오고있다[2~18].

2000년 Sandirigama 등은 SAS(Strong-password Authentication Scheme)라는 인증 프로토콜을 제안하였다[13]. 하지만 Lin 등은 SAS가 재전송 공격, 훔친 검증자(Stolen-verifier) 공격 등에 취약함을 지적하고, 이러한 공격에 안전한 OSPA(Optimal Strong-Password Authentication) 프로토콜을 제안하였다[14]. 그럼에도 불구하고, Chen 등은 OSPA 프로토콜이 SAS와 마찬가지

* 정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
** 정회원, 상지대학교 컴퓨터공학부
(School of Computer Engineering, Sangji University)
*** 정회원, 안양대학교 교양학부
(Dept. of Liberal Arts, Anyang University)
**** 정회원-교신저자, 경북대학교 컴퓨터공학과
(Dept. of Computer Engineering, Kyungpook National University)
접수일자: 2008년12월10일, 수정완료일: 2009년1월13일

로 여전히 훔친 검증자(Stolen-verifier) 공격에 취약함을 증명하였다[15]. 이후, 2003년에 Lin 등은 기존에 제안된 여러 가지 공격에 안전한 개선된 SE-OSPA (Security Enhancement for Optimal Strong-Password Authentication) 인증 프로토콜을 제안하였다[16]. 하지만 Yoon 등은 Lin 등이 제안한 SE-OSPA 프로토콜 또한 임의의 공격자에 의한 서비스 거부 공격(Denial of Service attack)을 수행하였을 때 합법적인 사용자가 올바른 패스워드를 제시하였음에도 서버가 로그인 요청을 쉽게 거부하는 서비스 거부 공격(Denial of Service attack)에 취약함을 증명하였다[17]. 가장 최근인 2006년에 Lin 등은 안전성과 효율성을 개선한 NSPA(New Strong-Password Authentication) 인증 프로토콜을 제안하였다[18].

하지만 NSPA 인증 프로토콜 또한 상호인증(Mutual authentication)을 제공하지 않는 문제점으로 인해 서버로 위장한 공격자의 위장 공격에 취약할 수 있으며, 다음 세션을 위한 패스워드 검증자가 어떻게 사용자 클라이언트 측에서 수행되는 지에 대한 과정 설명이 없어 서비스 거분 공격 등 또 다른 보안 취약점을 가질 수 있다. 이에 본 논문에서는 위 NSPA 인증 프로토콜이 가지는 보안 취약점들을 해결한 해쉬 함수를 사용한 강력한 패스워드 상호인증 프로토콜(Strong-Password Mutual Authentication)인 SPMA 인증 프로토콜을 제안한다. 결론적으로, 제안한 SPMA 인증 프로토콜은 기존의 관련 프로토콜들과 비교하여 보다 많은 보안성과 효율성을 제공하여 주어, 인터넷 인증 프로토콜로 실용적으로 사용되어 질 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 패스워드 인증 프로토콜들이 만족해야 할 보안 요구사항을 설명한다. Ⅲ장에서는 본 논문에서 제안한 해쉬 기반의 강력한 패스워드 상호인증 프로토콜인 SPMA 인증 프로토콜을 기술하고, Ⅳ장과 Ⅴ장에서 각각 안전성과 효율성을 분석한다. 최종적으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 패스워드 인증 프로토콜에서 보안 요구사항

본 장에서는 패스워드 인증 프로토콜들이 만족하여야 할 보안 요구사항들을 살펴본다. 패스워드 인증 프로토콜들이 고려해야 할 보안 특성과 요구조건은 다음과 같다[2~24].

1. 패스워드 추측 공격(Password guessing attack)에 안전해야 한다.

패스워드 추측 공격은 공격자가 사용자들이 자주 선택하여 사용하는 패스워드들에 대한 사전파일을 이용하여 사용자들의 패스워드를 추측하는 공격이다. 공격자는 임의의 세션에서 사용자와 서버간의 송수신되는 통신 메시지들을 자신의 컴퓨터 내에 저장한 후, 이들 메시지로부터 검증 값을 획득 한 후, 패스워드 사전을 이용하여 유도된 검증 값과 동일한지 여부를 비교 판단하여, 과거 통신에 사용된 패스워드와 일치하는 값을 찾아내는 공격이다.

2. 재전송 공격(Replay attack)에 안전해야 한다.

재전송 공격은 합법적인 사용자가 과거 세션에서 통신했던 메시지를 공격자가 저장했다가 이후의 통신 세션에 재전송하여 서버로부터 인증을 받게 되는 공격이다.

3. 위장 공격(Impersonation attack)에 안전해야 한다.

위장 공격은 공격자가 임의의 통신 세션에 참여하여 자신을 서버에 등록된 합법적인 사용자로 위장하여 정당한 사용자인 것처럼 행동하는 공격이다.

4. 훔친 검증자 공격(Stolen-verifier attack)에 안전해야 한다.

훔친 검증자 공격은 서버로부터 패스워드 검증자를 훔친 공격자가 임의의 인증 세션 프로토콜에서 합법적인 사용자로 가장하여 훔친 패스워드 확인자를 직접 사용하여 서버로부터 인증을 받게 되는 공격이다.

5. 서비스 거부 공격(Denial of Service attack)에 안전해야 한다.

서비스 거부 공격은 서버의 정상적인 사용을 방해하고 제지하는 공격이다. 예를 들면, 공격자가 특정한 사용자의 재등록 전까지 모든 로그인 요청을 서버가 거부하도록 하는 공격이다.

6. 상호인증(Mutual authentication)을 제공하여야 한다.

상호인증은 클라이언트와 서버 양쪽 모두 상대방의

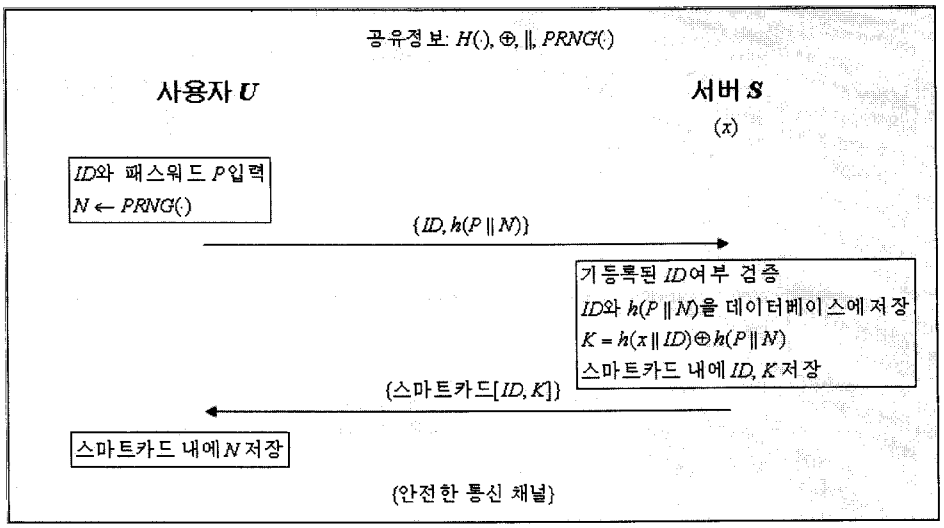


그림 1. 등록 단계
Fig. 1. Registration phase.

신원을 인증하는 것이다. 즉, 서버가 클라이언트를 인증하는 것처럼 클라이언트 또한 서버를 인증하여야 한다.

III. 강력한 패스워드 상호인증 프로토콜

본 장에서는 보안성과 효율성을 제공하는 해쉬 함수를 사용한 강력한 패스워드 상호인증 프로토콜인 SPMA 인증 프로토콜을 제안한다. 표 1은 제안한 SPMA 인증 프로토콜에서 사용되어 지는 시스템 파라미터들을 보여준다.

표 1. 시스템 파라미터
Table 1. System parameters.

기호	의미
U	원격 사용자(remote user)
S	원격 인증 서버(remote authentication server)
ID	원격 사용자의 식별자(identifier)
P	원격 사용자의 패스워드(password)
N	현재 세션을 위한 랜덤 넌스(random nonce)
N'	다음 세션을 위한 랜덤 넌스(random nonce)
x	원격 서버의 비밀키 값(server's secret key)
$h(\cdot)$	안전한 일방향 해쉬 함수(secure one-way hash function)
$PRNG(\cdot)$	의사난수생성기(Pseudo Random Number Generator)
$\oplus$	배타적 논리합 연산(Exclusive OR operation)
$\|$	연접 연산(concatenation operation)
$A \rightarrow B: X$	X가 A에서 B로 전송

제안한 SPMA 인증 프로토콜은 등록단계(Registration phase)와 인증 단계(Authentication phase)로 구성되어 진다. 등록단계에서 사용자는 서버의 도움으로 자신의 아이디와 패스워드를 담고 있는 스마트카드를 발급받게 되며, 인증단계에서 사용자는 자신의 아이디와 패스워드 그리고 스마트카드를 이용하여 서버로부터 인증을 받게 된다.

1. 등록 단계

새로운 사용자 U가 서비스 접근을 위해 서버와 함께 안전한 등록을 하기를 원한다고 가정하자. 등록 단계는 그림 1과 같이 안전한 채널(Secure channel)을 통해 수행되며, 수행 절차는 다음과 같다.

(1) $U \rightarrow S$: $ID, h(P \| N)$

사용자 U는 클라이언트 컴퓨터의 도움을 받아 $PRNG(\bullet)$로부터 랜덤 넌스 N을 생성하고, 패스워드 검증자 $h(P \| N)$을 계산한다. 안전한 채널을 통하여 자신의 식별자 ID와 패스워드 검증자 $h(P \| N)$을 서버 S에게 전송한다.

(2) $S \rightarrow U$: 스마트카드(ID, K)

서버 S는 사용자 U의 식별자 ID가 기존에 가입된 사용자의 ID 인지 여부를 검증한다. 만약 기존에 가입된 ID가 아님이 증명되면, 자신의 데이터베이스 내에 U의 식별자 ID와 패스워드 검증자 $h(P \| N)$을 저장

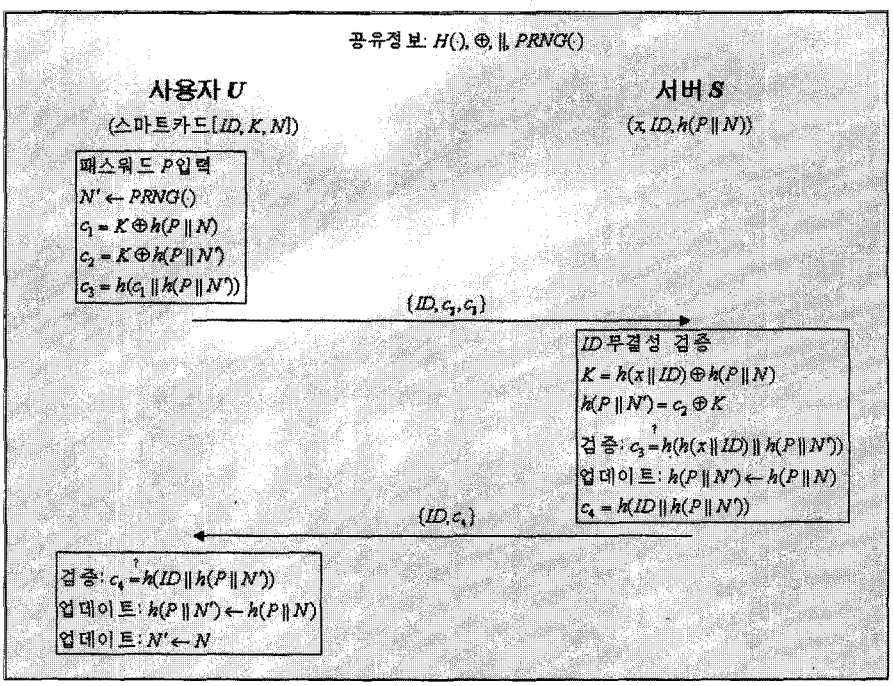


그림 2. 인증 단계
Fig. 2. Authentication phase.

한다. 이후 서버는 자신의 비밀키 값인 x를 이용하여 $K = h(x \| ID) \oplus h(P \| N)$를 계산하여, 사용자 U를 위한 스마트카드에 ID와 K값을 저장하고, 안전한 채널을 통해 사용자 U에게 스마트카드를 발급한다.

(3) 사용자 U는 발급받은 스마트카드와 자신의 클라이언트 컴퓨터 도움을 받아 랜덤 넌스 N을 스마트카드 내에 저장한다.

2. 인증 단계

그림 2는 제안한 SPMA 프로토콜의 인증 단계를 보여준다. 만일 사용자 U가 원격 서버 S에 접속하기 위하여 로그인하기를 원한다면, 자신의 클라이언트 컴퓨터에 있는 로그인 장치에 스마트카드를 입력한 후, 자신의 패스워드 P를 입력한다. 그러면 스마트카드는 클라이언트 컴퓨터와 함께 다음과 같은 연산을 수행하여 사용자 U가 서버 S에게 인증을 받을 수 있도록 도와준다.

(1) $c_1 = K \oplus h(P \| N) = h(x \| ID)$을 계산한다.

(2) 다음 세션을 위한 랜덤 넌스 N'을 $PRNG(\bullet)$로부터 생성한다.

(3) $c_2 = K \oplus h(P \| N')$을 계산한다.

(4) c_3를 다음과 같이 계산한다.

$$c_3 = h(c_1 \| h(P \| N')) = h(h(x \| ID) \| h(P \| N'))$$

(5) $U \rightarrow S$: $\{ID, c_2, c_3\}$

로그인 요청으로 서버 S에게 메시지 $\{ID, c_2, c_3\}$를 전송한다.

서버 S는 사용자 U로부터 로그인 요청 메시지 $\{ID, c_2, c_3\}$를 수신한 상태에서, 사용자 U의 신원을 확인하기 위해서 다음과 같은 인증 과정을 수행한다.

(1) 수신한 식별자 ID와 자신의 데이터베이스 내에 저장된 ID 리스트를 비교하여 유효성을 확인한다. 만약 등록된 ID가 아니면, 서버는 사용자 U와의 현재 세션 접속을 종료한다.

(2) 등록된 ID임이 확인되면, 서버 S는 등록 단계에서 자신의 데이터베이스 내에 저장한 사용자 U의 패스워드 검증자 $h(P \| N)$을 가져온다. 자신의 비밀키 값 x와 사용자 U의 ID를 이용하여 $h(x \| ID)$를 계산한 후, $K = h(x \| ID) \oplus h(P \| N)$를 구한다.

(3) 수신한 c_2와 계산된 $K=h(x \| ID) \oplus h(P \| N)$를 이용하여 다음의 연산을 수행하여 다음 세션을 위한 패스워드 검증자 $h(P \| N')$을 계산한다.

$$h(P \| N') = c_2 \oplus K = K \oplus h(P \| N') \oplus K$$

(4) 위 단계(2)에서 계산된 $h(x \| ID)$와 단계 (3)에서 계산된 다음 세션을 위한 패스워드 검증자 $h(P \| N')$을 이용하여 다음의 검증 수식을 수행하여 수신한 c_3의 무결성을 검증한다.

$$c_3 = ? h(h(x \| ID) \| h(P \| N'))$$

(5) 만약 비교 값이 동일하면 서버 S는 사용자 U를 인증하게 되며, 로그인 요청을 받아들여 서버 자원에 대한 접근 권한을 부여함과 동시에 다음번 로그인을 위해 자신의 데이터베이스에 저장된 기존의 패스워드 검증자 $h(P \| N)$을 다음번 패스워드 검증자 $h(P \| N')$로 업데이트 한다. 그렇지 않으면, 로그인 요청을 거절하고 현재 세션 접속을 종료한다.

(6) $S \rightarrow U$: $\{ID, c_4\}$

서버 S는 사용자 U와의 상호인증을 수행하기 $c_4 = h(ID \| h(P \| N'))$을 계산한 후, 사용자 U에게 메시지 $\{ID, c_4\}$를 전송한다.

사용자 U는 서버 S로부터 수신한 $\{ID, c_4\}$를 수신한 상태에서, 사용자 U의 신원을 확인하기 위해서 다음과 같은 상호인증 과정을 수행한다.

(1) 자신의 식별자 ID와 다음 세션을 위한 패스워드 검증자 $h(P \| N')$을 이용하여 다음의 검증 수식을 수행하여 수신한 c_4의 무결성을 검증한다.

$$c_4 = ? h(ID \| h(P \| N'))$$

(2) 만약 비교 값이 동일하면 사용자 U는 서버 S가 자신을 올바르게 인증하였음을 알게 되고 상호인증을 수행하게 된다. 또한 다음번 로그인을 위해 자신의 스마트카드 내에 저장된 $K=h(x \| ID) \oplus h(P \| N)$를 $K'=h(x \| ID) \oplus h(P \| N')$으로 N을 N'으로 각각 업데이트 한다. 그렇지 않으면, 상호인증 요청을 거절하고 현재 세션 접속을 종료한다.

Ⅳ. 안전성 분석

본 장에서는 제안한 SPMA 인증 프로토콜이 2장에서 언급된 보안 요구사항을 기반으로 여러 가지 공격에 대해 안전함을 증명한다. 먼저, 제안한 SPMA 인증 프로토콜의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[25~26].

정의 1. 약한 비밀 키(SPMA 인증 프로토콜에서 사용자의 패스워드 P)는 낮은 엔트로피(Low entropy)를 가지는 값으로써 다항식시간(Polynomial time) 내에 추측되어 질 수 있다.

정의 2. 강력한 비밀 키(SPMA 인증 프로토콜에서 서버의 비밀키 값 x)는 높은 엔트로피(High entropy)를 가지는 값으로써 다항식시간(Polynomial time) 내에 추측되어 질 수 없다.

정의 3. 안전한 일방향 해쉬 함수(Secure one-way hash function) $y=h(x)$에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 정의 1과 2와 3을 기반으로 제안한 SPMA 인증 프로토콜은 다음의 패스워드 추측 공격(Password guessing attack), 재전송 공격(Replay Attack), 위장 공격(Impersonation attack), 훔친 검증자 공격(Stolen-verifier attack), 서비스 거부 공격(Denial Of Service Attack), 상호인증(Mutual authentication)과 같은 6가지 보안 속성들을 만족한다.

1. 패스워드 추측 공격(Password guessing attack)

제안된 인증 단계에서 공개된 네트워크상으로 송수신되는 사용자의 로그인 요청 메시지 $U \rightarrow S$: $\{ID, c_2, c_3\}$와 서버의 답장 메시지 $S \rightarrow U$: $\{ID, c_4\}$를 공격자가 가로채기 하였다고 해도, 공격자는 가로챈 값들인 $c_2 = K \oplus h(P \| N')$와 $c_3 = h(c_1 \| h(P \| N')) = h(h(x \| ID) \| h(P \| N'))$ 그리고 $c_4 = h(ID \| h(P \| N'))$로부터 사용자의 패스워드 P를 유도할 수 없다. 즉, 공격자가 사용자의 패스워드 P를 얻기 위해서는 현재 세션을 위한 랜덤 넌스 N과

다음 세션을 위한 랜덤 넌스 N' 그리고 서버의 비밀키 x를 알아야만 패스워드 추측 공격을 수행하여 P를 얻을 수 있다. 하지만, 안전한 일방향 해쉬 함수의 성질로 인해 공격자는 $\{c_2, c_3, c_4\}$로부터 N, N', 그리고 x를 알아 낼 수 없기 때문에, 제안한 SPMA 인증 프로토콜을 패스워드 추측 공격에 안전하다.

2. 재전송 공격(Replay attack)

매 세션마다 사용자는 새로 생성되는 랜덤 넌스 N'와 패스워드 검증자 $h(P \| N')$를 사용하기 때문에, 공격자가 이전 세션에서 전송된 메시지를 가지고 있어도 다음 세션에서 그 메시지를 사용할 수 없으므로 재전송 공격을 수행할 수 없다. 즉, 서버는 사용자로부터 수신한 $c_2 = K \oplus h(P \| N')$와 $c_3 = h(c_1 \| h(P \| N')) = h(h(x \| ID) \| h(P \| N'))$를 이용하여 자신의 데이터베이스 내에 저장된 이전의 검증자와 동일한 지를 인증 한 후 새로운 검증자로 업데이트하기 때문에 공격자가 전송한 과거의 로그인 요청 메시지는 쉽게 발견될 수 있다. 서버로 위장한 공격자가 재전송한 과거의 메시지 c_4 또한 사용자가 무결성 검증을 수행하기 때문에 재전송 여부를 쉽게 발견할 수 있다. 따라서, 제안한 SPMA 인증 프로토콜은 재전송 공격에 안전하다.

3. 위장 공격(Impersonation attack)

공격자 A는 제안한 인증 단계에서 위조된 $c_{A2} = K_A \oplus h(P_A \| N_A')$와 위조된 $c_{A3} = h(h(x_A \| ID) \| h(P_A \| N_A'))$를 계산하여, 위장된 로그인 요청 메시지 $\{ID, c_{A2}, c_{A3}\}$로 위조한 후 서버에게 보내어 사용자 U인체 위장 공격을 수행할 수 있다. 위조된 $\{ID, c_{A2}, c_{A3}\}$를 수신한 서버는 로그인 요청 사용자의 신원을 검증하기 위해 인증과정을 수행할 것이다. 하지만, 위조된 $\{ID, c_{A2}, c_{A3}\}$는 서버의 인증 단계를 절대 통과할 수 없다. 즉, 서버는 자신의 데이터베이스 내에 저장한 사용자 U의 패스워드 검증자 $h(P \| N)$을 가져와서, 자신의 비밀키 값 x와 사용자 U의 ID를 이용하여 사용자를 위한 $h(x \| ID)$를 계산한 후, $K = h(x \| ID) \oplus h(P \| N)$를 계산하게 된다. 계산된 K와 수신한 $c_{A2} = K_A \oplus h(P_A \| N_A')$를 이용하여 $c_{A2} \oplus K = K_A \oplus h(P_A \| N_A') \oplus K$ 연산을 수행하여 다음 세션을 위한 패스워드 검증자를 얻게 된다. 또한, $h(x \| ID)$와 위에서 계산된 다음 세션을 위한 패스워드 검증자 $K_A \oplus h(P_A \| N_A') \oplus K$을 이용하여 다음의 검증 수식을 수행하여 수신한 c_{A3}의 무결성을 검증하게 된다.

$$c_{A3} = ?h(h(x \| ID) \| K_A \oplus h(P_A \| N_A') \oplus K)$$

공격자의 c_{A3}는 $h(h(x_A \| ID) \| h(P_A \| N_A'))$ 임으로 $h(h(x \| ID) \| K_A \oplus h(P_A \| N_A') \oplus K)$와 동일하지 않게 된다. 결론적으로 공격자 A에 의해 위조된 c_{A2}와 c_{A3}는 위 검증 수식을 만족하지 않기 때문에 무결성 검증과정을 통과할 수 없다. 따라서 공격자는 위장 공격을 행할 수 있는 어떤 기회도 가지지 못하기에 제안된 SPMA 인증 프로토콜은 위장 공격에 안전하다.

4. 훔친 검증자 공격(Stolen-verifier attack)

공격자가 서버로부터 패스워드 검증자 $h(P \| N)$을 훔치고, 공개된 통신 네트워크로부터 사용자의 $(N-1)$번째 로그인 요청 $\{ID, c_2, c_3, c_4\}$를 가로채기 하였다고 해도, 훔친 패스워드 검증자 $h(P \| N)$를 이용하여 $\{c_2, c_3, c_4\}$로부터 $h(x \| ID)$와 안전한 일방향 해쉬 함수 $h(\cdot)$로 보호되어져 있는 $h(P \| N')$을 유도할 수 없기 때문에, 제안한 SPMA 인증 프로토콜은 훔친 검증자 공격에 안전하다.

5. 서비스 거부 공격(Denial of Service attack)

제안된 SPMA 인증 프로토콜에서는 다음번 패스워드 검증자 $h(P \| N')$가 포함되어있는 $\{c_2, c_3, c_4\}$에 대한 무결성 검사를 수행하여 이 검사과정이 통과되면, 서버와 사용자는 다음번 로그인을 위해 기존 패스워드 검증자 $h(P \| N)$을 다음번 패스워드 검증자 $h(P \| N')$로 업데이트하기 때문에 서비스 거부 공격에 대하여 안전하다.

6. 상호인증(Mutual authentication)

제안된 프로토콜의 인증 단계에서 서버는 사용자로부터 수신한 로그인 요청 메시지 $c_2 = K \oplus h(P \| N')$, $c_3 = h(c_1 \| h(P \| N')) = h(h(x \| ID) \| h(P \| N'))$가 자신의 비밀키 x와 데이터베이스 내에 저장된 이전의 패스워드 검증자 $h(P \| N)$를 이용하여 메시지 무결성을 검증하여 사용자를 인증 한 후 새로운 패스워드 검증자 $h(P \| N')$로 업데이트한다. 또한 사용자는 서버로부터 수신한 메시지 $c_4 = h(ID \| h(P \| N'))$가

표 2. 연산 복잡도 비교
Table 2. Comparison of computational complexity.

단계 / 프로토콜	등록 단계	인증 단계	
		단방향인증	상호인증
SE-OSPA 프로토콜[16]	$3T(h)+2T(\oplus)$	$8T(h)+7T(\oplus)$	제공안함
NSPA 프로토콜[18]	$2T(h)+1T(\oplus)$	$7T(h)+6T(\oplus)$	제공안함
SPMA 프로토콜	$2T(h)+1T(\oplus)$	$5T(h)+4T(\oplus)$	$7T(h)+4T(\oplus)$

$T(h)$: 안전한 일방향 해쉬 함수 연산 횟수
$T(\oplus)$: 배타적 논리합 연산 횟수

정당한 서버로부터 전송된 메시지 맞는 지를 다음번 패스워드 검증자 $h(P \| N')$를 이용하여 무결성 검증을 수행하여 인증 한 후 새로운 패스워드 검증자 $h(P \| N')$로 업데이트한다. 따라서 제안한 SPMA 인증 프로토콜을 상호인증을 제공한다.

V. 효율성 분석

본 장에서는 제안한 SPMA 인증 프로토콜이 기존에 제안된 인증 프로토콜과 비교하여 보다 높은 효율성을 제공함을 증명한다. 표 2는 제안된 SPMA 인증 프로토콜이 기존에 제안된 SE-OSPA 인증 프로토콜과 NSPA 인증 프로토콜보다 더욱 효율적임을 보여준다.

제안된 SPMA 인증 프로토콜의 등록 단계에서 NSPA 인증 프로토콜과 마찬가지로 2번의 해쉬 연산과 1번의 배타적 논리합 연산을 요구한다. 이는 3번의 해쉬 연산과 2번의 배타적 논리합 연산을 요구한 SE-OSPA 인증 프로토콜과 비교하여 높은 효율성을 제공함을 알 수 있다.

또한 SE-OSPA 인증 프로토콜은 인증 단계에서 단방향 인증을 위해 8번의 해쉬 연산과 7번의 배타적 논리합 연산이 요구되며, NSPA 인증 프로토콜은 인증 단계에서 단방향 인증을 위해 7번의 해쉬 연산과 5번의 배타적 논리합 연산이 요구되고 있다. 하지만 제안된 SPMA 인증 프로토콜의 인증 단계에서 단방향 인증을 위해 5번의 해쉬 연산과 4번의 배타적 논리합 연산이 요구되고 있다. 이는 SE-OSPA 인증 프로토콜 및 NSPA 인증 프로토콜과 비교하여 높은 효율성을 제공함을 알 수 있다.

더 나아가, SE-OSPA 인증 프로토콜과 NSPA 인증 프로토콜은 상호인증을 제공하지 않지만 제안된 SPMA 인증 프로토콜은 상호인증을 제공하며, 상호인증을 제공하더라도 NSPA 인증 프로토콜과 동일한 7번의 해쉬 연산과 4번의 배타적 논리합 연산만을 요구한다. 결론적으로 제안된 SPMA 인증 프로토콜은 상호인증 등의 강화된 보안성을 제공하면서 보다 높은 효율성을 제공함을 알 수 있다.

VI. 결 론

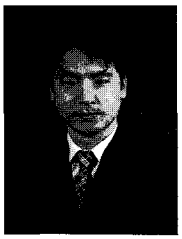
본 논문에서는 기존에 제안된 SE-OSPA 인증 프로토콜과 NSPA 인증 프로토콜이 가지는 보안 취약점들을 해결하고 보다 높은 효율성을 보장할 수 있는 해쉬 함수를 사용한 강력한 패스워드 상호인증 프로토콜(Strong-Password Mutual Authentication)인 SPMA 인증 프로토콜을 제안하였다. 또한 제안된 SPMA 인증 프로토콜이 기타 여러 가지 공격에도 안전하며 높은 효율성을 가짐을 증명하였다. 결론적으로, 제안한 SPMA 인증 프로토콜은 기존의 관련 프로토콜들과 비교하여 보다 많은 보안성과 효율성을 제공하여 주어, 사용자 인증을 요하는 인터넷 인증 프로토콜로 실용적으로 사용 및 다양한 인증 시스템에 유용하게 적용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] L. Lamport, "Password authentication with insecure communication," Communication of ACM, Vol. 24, pp. 770-772, 1981.
[2] M. S. Hwang, "Cryptanalysis of remote login

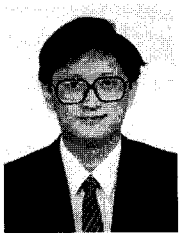
authentication scheme," Computer Communications, Vol. 22, no. 8, pp. 42-744, 1999.
[3] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, Vol. 70, pp. 657-666, 1999.
[4] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," Computers & Security, Vol. 18, no. 8, pp. 727-733, 1999.
[5] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, no. 1, pp. 28-30, 2000.
[6] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," Journal of Systems and Software, Vol. 55, pp. 287-290, 2001.
[7] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," International Journal of Informatica, Vol. 12, no. 2, pp. 297-302, 2001.
[8] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," IEEE Transactions on Neural Networks, Vol. 12, no. 6, pp. 1498-1504, 2001.
[9] C. K. Chan and L. M. Cheng, "Cryptanlysis of timestamp-based password authentication scheme," Computers & Security, Vol. 21, no. 1, pp. 74-76, 2002.
[10] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," ACM Operating Systems Review, Vol. 36, no. 3, pp. 46-52, 2002.
[11] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," ACM Operating Systems Review, Vol. 36, no. 4, pp. 23-29, 2002.
[12] Y. L. Tang, M. S. Hwang, and C. C. Lee, "A simple remote user authentication scheme. Mathematical and Computer Modelling," Vol. 36, pp. 103-107, 2002.
[13] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (sas). IEICE Transactions on Communications," Vol. E83-B, no. 6, pp. 1363-1365, June 2000.
[14] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," IEICE Transactions on Communications, Vol. E84-B, no. 9, pp. 2622-2627, September 2001.
[15] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," IEICE Transactions on Communications, Vol. E85-B, no. 11, pp. 2519-2521, November 2002.
[16] C. W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong- password authentication protocol," ACM Operating Systems Review, Vol. 37, no. 2, April 2003
[17] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Secure SE-OSPA protocol against DoS attack," Proceeding of LSRC Summer Conference in Korean Institute of Information Scientists and Engineers, Vol. 2, no. 1, pp. 27-31, 2003
[18] C. W. Lin, C. S. Tasi, and M. S. Hwang, "A new strong-password authentication scheme using one-way hash function," Journal of Computer and Systems Sciences International, Vol. 45, no. 4, pp. 623-626, 2006.
[19] 김천식, 윤은준, 홍유식, 문남미, "이러닝 시스템에서 사용자 인증을 위한 키스트로크의 응용 기술," 전자공학회논문지, 제45권, 제CI-5호, pp. 25-31, 2008.
[20] 권정호, 박종태, "IEEE 802.11 무선랜에서 고속 이동성 지원을 위한 사용자 사전 인증 기법," 전자공학회논문지, 제44권, 제TC-10호, pp. 191-200, 2007.
[21] 이규환, 이주화, 김재현, "무선 메쉬 네트워크의 패스워드 기반 인증 프로토콜," 전자공학회논문지, 제44권, 제TC-5호, pp. 54-62, 2007.
[22] 이성운, 김현성, 유기영, "패스워드를 변경 가능한 효율적인 패스워드 기반의 인증된 키 교환 프로토콜," 전자공학회논문지, 제42권, 제TC-2호, pp. 33-38, 2005.
[23] 강명희, 유황빈, "유비쿼터스 컴퓨팅 환경을 위한 익명성을 보장하는 사용자 인증 및 접근제어 모델," 전자공학회논문지, 제42권, 제CI-4호, pp. 25-32, 2005.
[24] 송영상, 신인철, "서명을 이용한 스마트카드 사용자 인증을 위한 COS 설계," 전자공학회논문지, 제41권, 제CI-4호, pp. 421-430, 2004.
[25] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "*Handbook of applied cryptography*," CRC Press, New York, 1997.
[26] B. Schneier, "*Applied cryptography protocols*," Algorithms and Source Code in C, 2nd edn. John Wiley, Chichester, 1995.

저 자 소 개



윤 은 준(정회원)

1995년 경일대학교 졸업 (공학사)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년~현재 경북대학교 전자전기컴퓨터학부 연구교수
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>



홍 유 식(정회원)

1984년 경희대학교 전자공학과 (공학사)
1989년 뉴욕공과대학교 전산학과 (공학석사)
1997년 경희대학교 전자공학과 (공학박사)
1985년~1987년 대한항공(N.Y.지점 근무)
1989년~1990년 삼성전자 종합기술원 연구원
1991년~현재 상지대학교 컴퓨터공학부 교수
2000년~현재 한국 퍼지 및 지능시스템학회 이사
2004년~현재 대한전자공학회 ITS 분과위원장
2001년~2003년 한국정보과학회 편집위원
2001년~2003년 한국컴퓨터교육산업학회 이사, 편집위원
2004년~현재 건설교통부 ITS 전문심사위원
2004년~현재 원주 시 인공지능신호등 심사위원
2005년~현재 정보처리학회 이사
2005년~현재 인터넷 정보학회 이사
2005년~현재 정보처리학회 강원지부 부회장
2006년~현재 인터넷 방송통신 TV학회 상임이사
<주관심분야: 퍼지 시스템, 전문가시스템, 신경망, 교통제어, TIS 보안>

김 천 식(정회원)

1997년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
2003년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
2000년~2003년 경동대학교 정보통신공학부 교수
2004년~현재 안양대학교 교수
2007년~현재 대한전자공학회 컴퓨터소사이어티 분과위원장
2008년~현재 인터넷 방송통신 TV학회 상임이사
2006년~현재 인터넷 정보학회 학회편집위원
2006년~현재 대한교통학회 정회원
2005년~현재 한국데이터베이스학회 정회원
<주관심분야: 데이터베이스, 데이터마이닝, 유비쿼터스, 텔리매틱스, TPEG, DMB, 홈네트워크 보안, e-Learning 보안>

유 기 영(정회원)

1976년 경북대학교 수학과 (이학사)
1978년 한국 과학 기술원 컴퓨터 공학과 (공학석사)
1992년 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터 과학과 (이학박사)
1978년~현재 경북대학교 컴퓨터공학과 교수
1997년~1998년 한국정보과학회 영남지부장
1999년~현재 한국정보과학회 이사
2006년~현재 제12대 한국정보보호학회 부회장
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>