情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

재전송 공격에 안전한 개선된 강력한 패스워드 인증 프로토콜 설계

김 준 섭† , 곽 진‡
순천향대학교 정보보호학과 정보보호응용및보증연구실

Design of Improved Strong Password Authentication Scheme to Secure on Replay Attack

Jun-Sub Kim† , Jin Kwak‡
Information Security Application & Assurance Lab,
Department of Information Security Engineering, Soonchunhyang University

요 약

패스워드 기반 인증은 2개의 개체가 사전에 패스워드를 공유하고 인증의 기초로 패스워드를 사용하는 프로토콜이다. 패스워드 인증 방식은 약한 패스워드 인증 방식과 강력한 패스워드 인증 방식이 있다. 강력한 패스워드 인증 방식 중, SPAS는 서비스 거부 공격에 안전한 프로토콜로 제안되었으나 재전송 공격에 대한 취약성을 가지고 있다. 따라서 본 논문에서는 SPAS에 대한 재전송 공격 취약성을 분석하고, 재전송 공격에 안전한 개선된 강력한 패스워드 인증 프로토콜을 제안한다.

ABSTRACT

Password-based authentication is the protocol that two entities share a password in advance and use the password as the basic of authentication. Password authentication schemes are divided into weak-password and strong-password authentication scheme. SPAS protocol, one of the strong-password authentication scheme, was proposed for secure against DoS attack. However it has vulnerability of the replay attack. In this paper, we analyze the vulnerability to the replay attack in SPAS protocol. Then we also propose an Improved-Strong Password Authentication Scheme (I-SPAS) with secure against the replay attack.

Keywords: Password Authentication, Replay Attack, Hash Function, Security

I. 서 론

사용자 인증은 네트워크를 통하여 컴퓨터에 접속하는 사용자의 정당성 여부를 검증하는 과정이다. 사용자를 인증하기 위한 방법으로는 패스워드를 기반으로 하는 인증 기술이 널리 사용되고 있으나, 많은 사용자들은 상대적으로 낮은 엔트로피의 패스워드를 선택하여 사용하기 때문에 공격자에 의해 쉽게 추측될 수 있다. 이러한 프로토콜의 안전성을 강화하기 위해서 약한 패스워드 인증 프로토콜은 약한 패스워드를 암호화하기 위해 공개키 기술을 사용하여 여러 가지 공격에 저항할 수 있다. 반면 강한 패스워드 인증 프로토콜은 암호용 해시 함수와 XOR 연산 이후 높은 엔트로피를 가지는 강한 패스워드를 얻게 되기 때문에 패스워드를

접수일(2011년 5월 25일), 수정일(2011년 8월 25일), 게재확정일(2011년 11월 6일)
† 주저자, jskim0911@sch.ac.kr
‡ 교신저자, jkwak@sch.ac.kr

암호화하기 위한 공개키 기술이 필요 없다. 따라서 강한 패스워드 인증 프로토콜은 낮은 계산 오버헤드, 단순한 설계 및 낮은 네트워크 대역폭의 유용성 때문에 모바일 장치와 같이 한정된 환경에 적합하다.

1981년 Lamport는 강력한 패스워드 기반 사용자 인증 프로토콜을 제안하였다[1]. 이 방식은 높은 오버헤드와 패스워드 재설정에 대한 문제로 인하여 실제 구현에 대한 어려움이 있다. 이 후 SAS[2], OSPA[3], SE-OSPA[5] 프로토콜 등이 제안되었지만, 각각의 프로토콜들 또한 여러 보안 취약점이 존재한다[3, 4, 6]. 2010년 Jiang은 SE-OSPA 프로토콜을 개선하여 서비스 거부 공격에 안전한 SPAS(Strong Password Authentication Scheme)를 제안하였다[7]. 그러나 SPAS는 이전의 인증 메시지를 도청하여 전송하는 재전송 공격에 대한 취약성이 존재한다.

따라서 본 논문에서는 SPAS의 보안 취약성을 분석하고, 재전송 공격에 안전한 개선된 SPAS(I-SPAS : Improved SPAS)를 제안한다.

II. 보안 요구사항

본 장에서는 패스워드 인증 프로토콜들이 만족해야 할 보안 요구사항들은 다음과 같다.

2.1 패스워드 추측 공격 (password guessing attack)

패스워드 추측 공격은 수동적인 오프라인 공격으로 공격자가 사용자들이 통신했던 메시지를 도청하여 자신의 컴퓨터 내에 저장한 후, 이들 메시지로부터 검증 값을 획득한 후, 패스워드 사전을 이용하여 유도된 검증 값과 동일한지 여부를 비교 판단하여 패스워드와 일치하는 값을 찾아내는 공격이다.

2.2 재전송 공격(replay attack)

재전송 공격은 사용자가 과거 세션에서 서버와 통신했던 메시지를 공격자가 저장했다가 이후의 세션에서 이 메시지를 재전송하여 서버로부터 인증 받게 되는 공격이다.

2.3 위장 공격(impersonation attack)

위장 공격은 공격자가 임의의 통신 세션에 참여하여 자신을 시스템의 합법적 사용자인 것처럼 위장하여 정당한 사용자인 것처럼 행동하는 공격이다.

2.4 훔친 검증자 공격(stolen-verifier attack)

훔친 검증자 공격은 공격자가 서버로부터 패스워드 검증자를 훔쳐 임의의 인증 세션에서 시스템의 합법적 사용자로 가장하여 훔친 패스워드 검증자를 직접 사용하여 서버로부터 인증을 받게 되는 공격이다.

2.5 서비스 거부 공격(denial of service attack)

서비스 거부 공격은 공격자가 임의의 통신 세션에 참여하여 특정한 사용자의 재등록 전까지 모든 로그인 요청을 서버가 거부하도록 하는 공격이다.

III. 강력한 패스워드 인증 프로토콜 분석

3.1 SPAS

SPAS는 등록 단계와 인증 단계로 구성되어 있으며, [그림 1]은 SPAS의 등록 및 인증 단계를 나타낸다. 등록 단계는 새로운 사용자 U가 서비스 접근을 위해 서버에 안전한 등록을 요청하며, 인증 단계는 사용자 U가 서버 S에 접속하기 위해 스마트카드와 패스워드를 입력하여 로그인을 요청한다. 등록 및 인증 단계의 수행 절차는 다음과 같다.

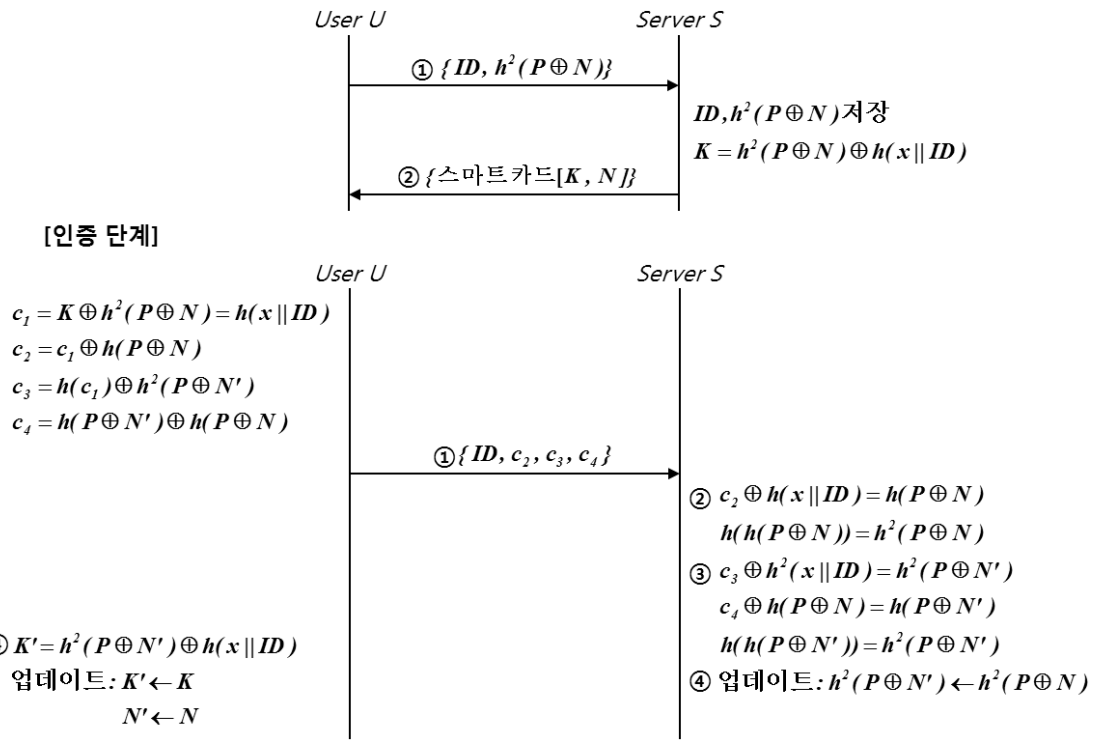
[등록 단계]

① 사용자 U는 랜덤 넌스 N을 생성하고, 패스워드 P를 이용하여 패스워드 검증자 $h^2(P \oplus N)$를 계산한다. 안전한 채널을 통하여 자신의 식별자 ID와 패스워드 검증자 $h^2(P \oplus N)$를 서버 S에게 전송한다.

② 서버 S는 사용자 U의 식별자 ID와 패스워드 검증자 $h^2(P \oplus N)$를 데이터베이스 내에 저장한다. 이후 서버 S는 자신의 비밀키 x를 이용하여 $K = h^2(P \oplus N) \oplus h(x||ID)$를 계산하고, 스마트카드 내에 K와 N 값을 저장하여 안전한 채널을 통하여 사용자 U에게 스마트카드를 발급한다.

[인증 단계]

① 사용자 U는 다음 세션을 위한 랜덤 넌스 N'을 생성하여 $c_1 = K \oplus h^2(P \oplus N) = h(x||ID)$, $c_2 = c_1 \oplus h(P \oplus N)$, $c_3 = h(c_1) \oplus h^2(P \oplus N')$, $c_4 = h(P \oplus N')$



〔그림 1〕 SPAS의 등록 및 인증 단계

$\oplus h(P\oplus N)$를 계산한 후 서버 S에게 로그인 요청을 위해 메시지 $\{ID,\ c_2,\ c_3,\ c_4\}$를 전송한다.

② 서버 S는 $c_2\oplus h(x||ID)$를 연산하여 $h(P\oplus N)$를 계산한 후 현재 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N))=h^2(P\oplus N)$)한다.

③ 서버 S는 $c_3\oplus h^2(x||ID)$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$를 계산한다. 이후 $c_4\oplus h(P\oplus N)$를 연산하여 $h(P\oplus N')$을 계산한 후 다음 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N'))=h^2(P\oplus N')$)한다.

④ 서버 S는 $h(h(P\oplus N'))$와 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$가 동일하다면 사용자 U를 인증한 후 다음의 로그인을 위해 자신의 데이터베이스 내에 저장된 현재 세션을 위한 패스워드 검증자 $h^2(P\oplus N)$를 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$으로 업데이트한다. 또한 사용자 U는 다음의 로그인을 위해 $h^2(P\oplus N')\oplus h(x||ID)$를 연산하여 K'를 계산한 후 자신의 스마트카드 내에 저장된 $K=h^2(P\oplus N)\oplus h(x||ID)$를 $K'=h^2(P\oplus N')\oplus h(x||ID)$로 현재 세션을 위한 랜덤 넌스 N을 다음 세션을 위한 랜덤 넌스 N'으로 각각 업데이트한다.

3.2 SPAS에 대한 취약성 분석

사용자 U가 서버 S로부터 n번째 로그인을 하기 전에 공격자 A는 두 가지의 인증 메시지 $\{ID,\ c_2^{(n-1)},\ c_3^{(n-1)},\ c_4^{(n-1)}\}$과 $\{ID,\ c_2^{(n-2)},\ c_3^{(n-2)},\ c_4^{(n-2)}\}$를 도청한다. 이 후 공격자 A는 사용자 U가 n번째 로그인을 할 때 메시지 $\{ID,\ c_2^{(n)},\ c_3^{(n)},\ c_4^{(n)}\}$을 $\{ID,\ c_2^{(n)}=h(x||ID)\oplus h(P\oplus N^{(n)}),\ c_3^{(n-2)}=h(c_1)\oplus h^2(P\oplus N^{(n-1)}),\ c_4^{(n-1)}=h(P\oplus N^{(n)})\oplus h(P\oplus N^{(n-1)})\}$로 교환하여 전송한다.

서버 S는 $c_2^{(n)}\oplus h(x||ID)$를 연산하여 $h(P\oplus N^{(n)})$를 계산한 후 현재 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N^{(n)}))=h^2(P\oplus N^{(n)})$)한다. 서버 S는 $c_3^{(n-2)}\oplus h^2(x||ID)$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$를 계산한다. 이 후 $c_4^{(n-1)}\oplus h(P\oplus N^{(n)})$를 연산하여 $h(P\oplus N^{(n-1)})$를 계산한 후 다음 세션을 위한 패스워드 검증

자와 동일한지 확인($h(h(P\oplus N^{(n-1)}))=h^2(P\oplus N^{(n-1)})$)한다. 서버 S는 $h(h(P\oplus N^{(n-1)}))$와 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$가 동일하기 때문에 사용자 U를 인증하고, 다음의 로그인을 위해 자신의 데이터베이스 내에 저장된 현재 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n)})$를 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$로 업데이트한다.

이 후 사용자 U가 다음의 로그인을 하기 전에 공격자 A는 사용자 U로 위장하기 위해 $\{ID, c_2^{(n-1)}, c_3^{(n-1)}, c_4^{(n-1)}\}$을 전송하여 서버 S로부터 인증을 받을 수 있다. 즉, 서버 S는 $h(c_2^{(n-1)}\oplus h(x||ID))$와 현재 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$가 동일하기 때문에 $c_3^{(n-1)}\oplus h^2(x||ID)$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n)})$를 계산한다. 이 후 $h(c_4^{(n-1)}\oplus h(P\oplus N^{(n-1)}))$와 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n)})$가 동일하기 때문에 공격자 A를 인증하고, 다음의 로그인을 위해 데이터베이스 내에 저장된 현재 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$를 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n)})$로 업데이트한다. 따라서 공격자 A가 이전 메시지를 재전송하는 재전송 공격에 성공할 수 있으므로 SPAS는 재전송 공격에 취약하다.

IV. 개선된 강력한 패스워드 인증 프로토콜

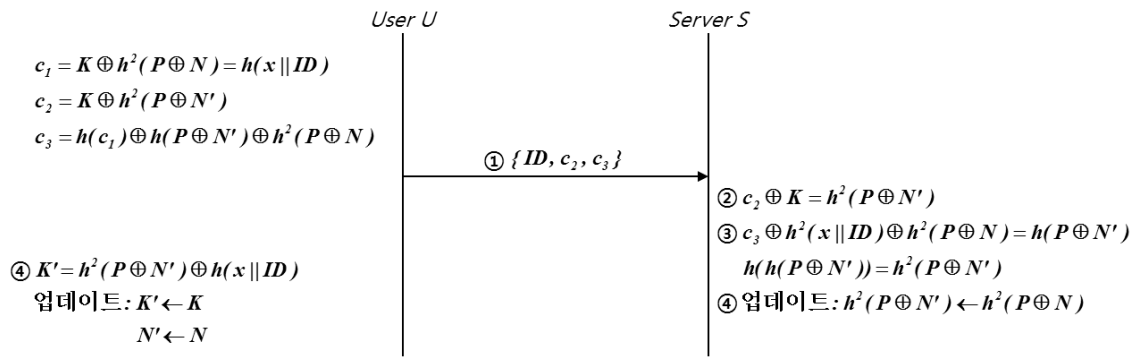
본 장에서는 SPAS의 재전송 공격에 안전한 개선된 강력한 패스워드 인증 프로토콜인 I-SPAS를 제안한다. SPAS는 $h(P\oplus N)$를 이용하여 현재 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N))=h^2(P\oplus N)$)한 후 $h(P\oplus N')$을 이용하여 다음 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N'))=h^2(P\oplus N')$)하기 때문에 재전송 공격이 발생한다. 제안한 I-SPAS에서는 재전송 공격을 방지하기 위해 서버 S에 저장되어 있는 현재 세션을 위한 패스워드 검증자 $h^2(P\oplus N)$를 사용자 U가 전송한 패스워드 검증자 $h^2(P\oplus N)$와 동일한지 비교하지 않고, $c_3\oplus h^2(P\oplus N)\oplus h(c_1)$를 연산하여 $h(P\oplus N')$을 계산한 후 c_2에서 획득한 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$와 동일한지 확인($h(h(P\oplus N'))=h^2(P\oplus N')$)함으로써 현재 세션을 위한 패스워드 검증자와 다음 세션을 위한 패스워드 검증자의 무결성을 확인한다.

I-SPAS에서 사용하는 시스템 파라미터는 각각 U는 사용자, S는 서버, ID는 사용자의 식별자, P는 사용자의 패스워드, x는 서버의 비밀키이다. 또한 N과 N'은 각 세션마다 생성되는 서로 다른 랜덤 넌스이다. 제안한 I-SPAS는 등록 단계와 인증 단계로 구성되며, 등록 단계는 SPAS와 동일하다. 〔그림 2〕는 I-SPAS의 인증 단계를 나타내며, 인증 단계에서는 사용자가 서버에 접속하기 위해 스마트카드를 입력한 후 자신의 아이디, 패스워드를 입력하여 서버로부터 인증을 받는다. 인증 단계의 수행 절차는 다음과 같다.

〔인증 단계〕

① 사용자 U는 다음 세션을 위한 랜덤 넌스 N'을 이용하여 $c_1=K\oplus h^2(P\oplus N)=h(x||ID)$, $c_2=K\oplus h^2(P\oplus N')$, $c_3=h(c_1)\oplus h(P\oplus N')\oplus h^2(P\oplus N)$를 계산한 후 서버 S에게 로그인 요청을 위해 메시지 $\{ID, c_2, c_3\}$을 전송한다.

② 서버 S는 자신의 비밀키 x와 사용자 U의 식별자 ID를 이용하여 $h(x||ID)$를 계산한 후 데이터베이



〔그림 2〕 I-SPAS의 인증 단계

〔표 1〕 안전성 비교·분석

구분	패스워드 추측 공격	재전송 공격	위장 공격	훔친 검증자 공격	서비스 거부 공격
SE-OSPA	○	×	○	○	×
SPAS	○	×	○	○	○
I-SPAS	○	○	○	○	○

스에 저장된 사용자 U의 패스워드 검증자 $h^2(P\oplus N)\oplus h(x||ID)$를 연산하여 $K=h^2(P\oplus N)\oplus h(x||ID)$를 계산한다. 이 후 서버 S는 $c_2\oplus K$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$를 계산한다.

③ 서버 S는 $c_3\oplus h^2(x||ID)\oplus h^2(P\oplus N)$를 연산하여 $h(P\oplus N')$을 계산한 후 다음 세션을 위한 패스워드 검증자와 동일한지 확인($h(h(P\oplus N'))=h^2(P\oplus N')$)한다.

④ 서버 S는 $h(h(P\oplus N'))$와 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$가 동일하다면 사용자 U를 인증한 후 다음의 로그인을 위해 자신의 데이터베이스 내에 저장된 기존의 패스워드 검증자 $h^2(P\oplus N)$를 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')$으로 업데이트한다. 또한 사용자 U는 다음의 로그인을 위해 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N')\oplus h(x||ID)$를 연산하여 K'를 계산한 후 자신의 스마트 카드 내에 저장된 $K=h^2(P\oplus N)\oplus h(x||ID)$를 $K'=h^2(P\oplus N')\oplus h(x||ID)$로 현재 세션을 위한 랜덤 넌스 N을 다음 세션을 위한 랜덤 넌스 N'으로 각각 업데이트한다.

V. 안전성 분석

본 장에서는 2장에서 언급된 보안 요구사항을 기반으로 제안한 I-SPAS에 대한 안전성을 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격, 서비스 거부 공격으로 구분하여 분석한다. 〔표 1〕은 제안된 I-SPAS가 기존에 제안된 SE-OSPA 프로토콜과 SPAS 보다 여러 공격에 안전함을 나타낸다.

5.1 패스워드 추측 공격 (password guessing attack)

공격자 A가 사용자 U의 패스워드를 추측하기 위해 $\{ID, c_2, c_3\}$을 가로챘다고 가정한다. 공격자 A가 패스워드 추측 공격을 수행하여 P를 획득하기 위해서는 현재 세션을 위한 랜덤 넌스 N, 다음 세션을 위한 랜덤 넌스 N', 서버의 비밀키 x를 알아야 한다. 하지만 일방향 해시 함수의 복구불가능성으로 인해 공격자 A는 메시지 $\{c_2, c_3\}$로부터 N, N', x를 알아낼 수 없기 때문에 제안한 I-SPAS는 패스워드 추측 공격에 안전하다.

5.2 재전송 공격(replay attack)

공격자 A가 공개된 네트워크에서 이전 로그인 단계에서 전송된 메시지 $\{c_2, c_3\}$을 도청한 것으로 가정한다. 사용자는 로그인을 할 때마다 새로 생성되는 랜덤 넌스 N'과 패스워드 검증자 $h^2(P\oplus N')$을 사용하기 때문에 공격자는 이전 로그인에서 전송된 메시지를 획득하여 다음 로그인에 그 메시지를 사용하더라도 서버로부터 인증을 받을 수 없다.

즉, 사용자 U가 서버 S로부터 n번째 로그인을 하기 전에 공격자 A는 두 가지의 인증 메시지 $\{ID, c_2^{(n-1)}, c_3^{(n-1)}\}$과 $\{ID, c_2^{(n-2)}, c_3^{(n-2)}\}$를 도청하는데 이는 공격자가 n번째 로그인을 하기 위해서 랜덤 넌스 N과 패스워드 검증자 $h^2(P\oplus N)$를 알아야 하지만, 공격자는 알 수 없기 때문에 이전의 메시지를 도청하는 것으로 가정한다. 그 후 공격자 A는 사용자 U가 n번째 로그인을 하기 전에 사용자 U로 위장하기 위해 메시지 $\{ID, c_2^{(n)}, c_3^{(n)}\}$을 메시지 $\{ID, c_2^{(n-1)}, c_3^{(n-2)}\}$로 교환하여 전송하는데 이는 공격자가 $c_2^{(n-1)}$를 전송하게 되면 서버는 $c_2^{(n-1)}$에서 계산된 $n-1$번째 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$를 c_3에서 계산된 $h(P\oplus N^{(n-1)})$와 동일한지 확인($h(h(P\oplus N^{(n-1)}))=h^2(P\oplus N^{(n-1)})$)하기 때문에 공격자는 $c_3^{(n-2)}$을 전송한다.

$$c_2^{(n-1)}=K^{(n-1)}\oplus h^2(P\oplus N^{(n)}) \quad (1)$$

$$c_3^{(n-2)}=h(c_1)\oplus h(P\oplus N^{(n-1)})\oplus h^2(P\oplus N^{(n-2)}) \quad (2)$$

서버 S는 $c_2^{(n-1)}\oplus K^{(n)}$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$를 계산한다.

$$\begin{aligned} & c_2^{(n-1)}\oplus K^{(n)} \\ &= K^{(n-1)}\oplus h^2(P\oplus N^{(n)})\oplus K^{(n)} \\ &= h(x||ID)\oplus h^2(P\oplus N^{(n-1)})\oplus h^2(P\oplus N^{(n)})\oplus \end{aligned}$$

$h(x||ID)\oplus h^2(P\oplus N^{(n)})$
$= h^2(P\oplus N^{(n-1)})$ (3)

이 후 서버 S는 $c_3^{(n-2)}\oplus h^2(x||ID)\oplus h^2(P\oplus N^{(n)})$를 연산하여 $c_2^{(n-1)}$에서 계산된 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$와 동일한지 확인한다.

$$v_1 = c_3^{(n-2)}\oplus h^2(x||ID)\oplus h^2(P\oplus N^{(n)}) = h(P\oplus N^{(n-1)})\oplus h^2(P\oplus N^{(n-2)})\oplus h^2(P\oplus N^{(n)}) \quad (4)$$

$$h(v_1)\neq h^2(P\oplus N^{(n-1)}) \quad (5)$$

서버 S는 $h(v_1)$와 다음 세션을 위한 패스워드 검증자 $h^2(P\oplus N^{(n-1)})$가 동일하지 않기 때문에 현재 세션을 종료한다. 따라서 공격자 A는 재전송 공격에 실패하기 때문에 제안한 I-SPAS는 재전송 공격에 안전하다.

5.3 위장 공격(impersonation attack)

공격자 A가 사용자 U로 위장하기 위해 $c_{A2}=K_A\oplus h^2(P_A\oplus N_A)$, $c_{A3}=h(h(x_A||ID))\oplus h(P_A\oplus N_A')\oplus h^2(P_A\oplus N_A)$를 계산하여 위조된 로그인 요청 메시지 $\{ID, c_{A2}, c_{A3}\}$을 서버 S에게 전송한 것으로 가정한다. 서버 S는 $c_{A2}\oplus K$를 연산하여 다음 세션을 위한 패스워드 검증자 $K_A\oplus h^2(P_A\oplus N_A)\oplus K$를 계산한다. 이 후 $c_{A3}\oplus h^2(x||ID)\oplus h^2(P\oplus N)$를 연산하여 $v_2=h^2(x_A||ID)\oplus h(P_A\oplus N_A')\oplus h^2(P_A\oplus N_A)\oplus h^2(x||ID)\oplus h^2(P\oplus N)$를 계산한 후 다음 세션을 위한 패스워드 검증자와 동일한지 확인한다. 다음 세션을 위한 패스워드 검증자 $K_A\oplus h^2(P_A\oplus N_A)\oplus K$와 $h(v_2)$는 동일하지 않기 때문에 공격자 A는 사용자 U로 위장할 수 없다. 따라서 제안한 I-SPAS는 위장 공격에 안전하다.

5.4 훔친 검증자 공격(stolen-verifier attack)

공격자 A는 사용자 U의 $n-1$번째 로그인 후에 패스워드 검증자 $h^2(P\oplus N^{(n)})$를 훔쳤다고 가정한다. 사용자 U가 서버 S로부터 n번째 로그인을 하는 동안 공격자 A는 로그인 요청 메시지 $\{ID, c_2^{(n)}, c_3^{(n)}\}$을 차단하고 복사한다. 공격자 A는 P_A, $N_A^{(n+1)}$, x_A을 선택하고 $c_{A2}^{(n)}=h^2(P\oplus N^{(n)})\oplus h(x_A||ID)\oplus h^2(P_A\oplus N_A^{(n+1)})$, $c_{A3}^{(n)}=h^2(x_A||ID)\oplus h(P_A\oplus N_A^{(n+1)})\oplus h^2(P\oplus N^{(n)})$를 계산한 후 로그인 요청 메시지 $\{ID, c_2^{(n)}, c_3^{(n)}\}$을 $\{ID, c_{A2}^{(n)}, c_{A3}^{(n)}\}$로 교환하여 전송한다. 서버 S는 $c_{A2}^{(n)}\oplus K^{(n)}$를 연산하여 다음 세션을 위한 패스워드 검증자 $v_3=h(x_A||ID)\oplus h^2(P_A\oplus N_A^{(n+1)})\oplus h(x||ID)$를 계산한다. 이 후 $c_{A3}^{(n)}\oplus h^2(x||ID)\oplus h^2(P\oplus N^{(n)})$를 연산하여 $v_4=h^2(x_A||ID)\oplus h(P_A\oplus N_A^{(n+1)})\oplus h^2(x||ID)$를 계산한 후 다음 세션을 위한 패스워드 검증자와 동일한지 확인한다. 다음 세션을 위한 패스워드 검증자 v_3과 $h(v_4)$는 동일하지 않기 때문에 공격자 A는 훔친 검증자 공격에 실패한다. 따라서 제안한 I-SPAS는 훔친 검증자 공격에 안전하다.

5.5 서비스 거부 공격(denial of service attack)

사용자 U가 서버 S로부터 로그인을 할 때 공격자 A는 메시지 $\{ID, c_2, c_3\}$을 차단하고 복사한다. 공격자 A는 c_2와 동일한 크기 랜덤 수인 $R(=c_2')$을 선택하고 메시지 $\{ID, c_2, c_3\}$을 $\{ID, c_2', c_3\}$으로 교환하여 전송한다. 서버 S는 $c_2'\oplus K$를 연산하여 다음 세션을 위한 패스워드 검증자 $R\oplus K$를 계산한 후 $c_3\oplus h^2(x||ID)\oplus h^2(P\oplus N)$를 연산하여 $h(P\oplus N')$를 계산한 후 다음 세션을 위한 패스워드 검증자와 동일한지 확인한다. 다음 세션을 위한 패스워드 검증자 $R\oplus K$와 $h(h(P\oplus N'))$는 동일하지 않기 때문에 공격자 A는 서비스 거부 공격에 실패한다. 따라서 제안한 I-SPAS는 서비스 거부 공격에 안전하다.

VI. 결론

본 논문에서는 Jiang이 제안한 SPAS에 대한 재전송 공격 취약성을 분석하였으며, 재전송 공격에 안전한 개선된 강력한 패스워드 인증 프로토콜을 제안하였다. 또한 제안하는 프로토콜이 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격, 서비스 거부 공격에 안전하다는 것을 증명하였다.

참고문헌

〔1〕 L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, Vol. 24, no. 11, pp. 770-772, Nov. 1981.

〔2〕 M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol," *IEICE Transactions on Communications*, Vol. E83-B, no. 6, pp. 1363-1365, Jun. 2000.

〔3〕 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, Sep. 2001.

〔4〕 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, Nov. 2002.

〔5〕 C.W. Lin, J.J. Shen, and M.S. Hwang, "Security enhancement for optimal strong-password authentication protocol," *ACM SIGOPS Operating Systems Review*, Vol. 37, no. 2, pp. 7-12, Apr. 2003.

〔6〕 W.C. Ku, H.C. Tsai, and S.M. Chen, "Two simple attack on Lin-Shen-Hwang's strong-password authentication protocol," *ACM SIGOPS Operating Systems Review*, Vol. 37, no. 4, pp. 26-31, Oct. 2003.

〔7〕 H. Jiang, "Strong password authentication protocols," *2010 4th International Conference on Distance Learning and Education*, pp. 50-52, Oct. 2010.

〈著者紹介〉

김 준 섭 (Jun-Sub Kim) 학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 암호프로토콜 등

곽 진 (Jin Kwak) 종신회원
성균관대학교 (공학사, 공학석사, 공학박사)
2006~2006년: 일본 큐슈대학교 방문연구원
2006~2006년: 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007년: 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009년: 정보통신연구진흥원 집필위원
2007~현재: 순천향대학교 정보보호학과 교수
2009~2009년: 순천향대학교 공과대학 교학부장
2009~2010년: 순천향대학교 정보보호학과 학과장
2010~2010년: 교육과학기술부 국가기술수준평가 전문위원
현재: 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
〈관심분야〉 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안 등