한국항행학회 논문지 제17권 제1호 2013년 2월 (JKONI 17(1): 24-32, Feb. 2013)

비동기 공격에 안전한 패스워드기반 상호 인증 프로토콜

Enhancement of Password-based Mutual Authentication Protocol against De-synchronization Attacks

육형준*, 임강빈*0

Hyeong-Jun Yuk*, Kang-Bin Yim*0

요 약

네트워크 환경에서 사용자에 대한 인증은 반드시 필요한 요소이며, 그 중 SPMA(Strong Pass Mutual Authentication), I-SPMA(Improved Strong Password Mutual Authentication) 프로토콜은 과거 프로토콜이 갖는 상호인증, 재전송 공격 등에 대한 취약점에 취약하다는 것을 증명하고, 이를 보안한 안전한 사용자 인증 프로토콜을 제안하였다. 하지만 이 프로토콜은 서버와 사용자가 공유한 정보가 동기화되지 않을 경우 심각한 문제를 발생하며, 이를 복구할 수 있는 대안이 없어 더욱 심각하다. 따라서 본 논문에서는 비동기 되었을 때 스스로 복구할 수 있는 프로토콜을 제안하고, 보안 요구조건에 따른 안전성을 검증하였다. 제안한 프로토콜은 상기 SPMA, I-SPMA가 갖는 취약점을 보안하였을 뿐만 아니라 비동기 시 발생하는 취약점도 보완하여 더욱 안전한 사용자 인증 프로토콜임을 확인하였으며, 이를 사용자 인증을 활용하는 시스템에 도입할 경우 매우 효과적일 것으로 사료된다.

Abstract

Authentication is one of the necessary elements in the network environment. Many researches have detected security vulnerabilities to the existing authentication mechanisms and suggested secure mutual authentication protocols by resolving these vulnerabilities. The representative ones of them are SPMA(Strong Pass Mutual Authentication) and I-SPMA(Improved Strong Password Mutual Authentication). However, these protocols cause a critical problem when the shared secret information is de-synchronized between the server and the client. This paper proposes a revised protocol to resolve the de-synchronization problem. Based on a security assessment on the proposed protocol, we consider the proposed protocol is safer than the previous ones and possible to effectively make a user authentication system mre secure.

Key words : user authentication protocol, de-synchronization Attack, mutual authentication

I. 서 론

네트워크의 발전과 더불어 온라인에서 올바른 사용자를 인증하고 인가하기 위한 기술이 필요하게 되

* 순천향대학교 정보보호학과(Department of Information Security engineering, Soonchunhyang University)
· 제1저자 (First Author) : 육형준(Hyeong-jun Yuk)
0 교신저자(Corresponding Author) : 임강빈(Kangbin Yim, tel : +82-041-530-1741 email : yim@sch.ac.kr)
· 접수일자 : 2013년 1월 23일 · 심사(수정)일자 : 2013년 1월 25일 (수정일자 : 2013년 2월 24일) · 게재일자 : 2013년 2월 28일
http://dx.doi.org/10.12673/jkoni.2013.17.01.024

었으며, 가장 일반적인 사용자 인증 기술은 패스워드 기반 인증 기술이다. 패스워드기반 사용자 인증 기술이란 사용자가 온라인을 통해 서비스를 이용할 경우 아이디와 패스워드를 설정하여 이를 등록하고, 등록 시 입력한 아이디, 패스워드와 로그인 시 입력한 아이디와 패스워드를 비교하여 올바른 사용자인지를 판단한 후 올바른 사용자일 경우 서비스를 인가하는 기술이다. 과거 일회용 패스워드 방식[1]을 기준으로, 사용자 편의를 고려하고 저비용으로 효율을 극대화 할 수 있는 연구들이 진행되어 왔으며, 대표적인 인증 프로토콜은 표 1과 같다.

SPMA 이전의 프로토콜들은 단방향으로 사용자 인증을 하였지만, SPMA, I-SPMA 프로토콜은 상호 인증을 제공한다. 이는 양방향으로 인증하는 것을 의미하고 있으며, 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격 등에 강인하도록 설계되었다. 하지만 양방향 인증 시 발생하는 문제는 공격자가 서비스를 거부할 목적으로 응답을 가로채어 사용자에게 전송하지 않을 경우 내부에서 공유하는 비밀정보가 달라져 이후의 모든 인증요청은 정상적인 인증정보임에도 불구하고 항상 인증에 실패한다. 즉, 공격자에 의해 전송되는 정보가 차단되면 이를 복구할 방법도 없을 뿐 아니라 이후의 사용자 인증 프로토콜 자체가 성립되지 않는다. 따라서 본 논문에서는 SPMA, I-SPMA가 가진 서비스 거부 공격, 비동기 공격을 개선하기 위한 프로토콜을 제안한다. 제안하는 프로토콜은 기존의 프로토콜이 갖는 안전성을 모두 가질 뿐 아니라 서비스 거부 공격, 비동기 공격에 대한 안전성을 제공한다.

본 논문의 구성은 다음과 같다. 제2장에서는 I-SPMA 프로토콜에 대해 설명하고, 비동기 공격 시 발생가능한 문제점에 대해 분석한다. 제3장에서는 제안하는 비동기 공격에 안전한 개선된 강력한 패스워드 상호 인증 프로토콜에 대해 설명하고, 제4장에서 제안한 프로토콜에 대해 안전성을 분석한 후 제5장에서 결론을 도출한다.

표 1 인증 프로토콜 현황 및 취약점[11]
Table. 1. Authentication protocols and vulnerabilities

제안 프로토콜	제안자	아이디어	취약점
CINON (Chanied one-way data verification method)[2][3] (1990, 1991)	A. Shimizu	난수를 메모리 장치 등 별도의 장치에 저장	휴대성 결여, 고비용
PERM (Privacy enhanced information reading and writing management method)[4] (1994)	A. Shimizu, T. Horioka, H. Inagaki	난수 문제 해결	중간자 공격에 취약
SAS(Simple and secure)[5] (2000)	M. Sandirigama, A. Shimizu, M. T. Noda	중간자 공격 취약점 보완	훔친 검증자 공격, 재전송 공격, 서비스 거부 공격에 취약
OSPA (Optimal strong-password authentication)[6] (2001)	C. L. Lin, H. M. Sun, T. Hwang	재전송 공격, 서비스 거부 공격 보완	훔친 검증자 공격에 취약
SE-OSPA (Security enhancement for optimal strong-password authentication)[7] (2003)	C.W. Lin, J. J. Shen, M. S. Hwang	OSPA 프로토콜 안전성 강화	서비스 거부 공격에 취약
NSPA (New strong-password authentication)[8] (2006)	C. W. Lin, C. S. Tsai, M. S. Hwang	SE-OPSA 프로토콜 안전성, 효율성 강화	상호 인증을 제공하지 않음, 위장 공격, 서비스 거부 공격에 취약
SPMA (Strong password mutual authentication)[9] (2009)	윤은준, 홍유식, 김천식, 유기영	상호 인증 제공	재전송 공격에 취약
I-SPMA (Improved Strong Password Mutual Authentication)[10] (2010)	김준섭, 곽진	재전송 공격 보완	비동기 공격, 서비스 거부 공격에 취약

Ⅱ. I-SPMA 프로토콜의 비동기 공격에 대한 취약점 분석

2-1. I-SPMA 프로토콜

I-SPMA 프로토콜은 등록 과정과 인증 과정을 통해 사용자를 인증하며, 등록 과정에서 사용자는 아이디와 패스워드가 저장된 스마트카드를 발급받고, 인증 과정에서 아이디, 패스워드, 스마트카드를 통해 상호 인증을 한다. 또한 SPMA 프로토콜은 비밀키와 아이디를 해쉬한 정보를 통해 인증 메시지에 대한 무결성을 검증함으로써 재전송 공격에 대한 취약점을 현재 세션 패스워드 검증자, 다음 세션 패스워드 검증자 등의 정보를 이용하여 보완하였다. 표 2는 I-SPMA에서 사용하는 용어이다.

표 2. I-SPMA 용어
Table. 2. Terminology of I-SPMA protocol

용어	설명
U	사용자(User)
S	서버(Server)
ID	사용자 아이디(Identifier)
PW	사용자 패스워드(Password)
N	현재 세션에서 사용하는 랜덤 수(Random Number)
N'	다음 세션에서 사용하기 위한 랜덤 수
x	서버에 저장된 비밀키(Private Key)
h()	일방향 해시 함수(One way hash function)
PRNG()	의사 난수 생성기(Pseudo random number generator)
⊕	배타적 논리합
‖	연접 연산

2-1-1. 등록 과정

등록 과정에서 사용자가 아이디와 패스워드를 입력하면 난수를 생성하여 패스워드와 해쉬 연산을 한 후 그 결과를 서버에 전송하고, 서버는 이 정보를 저장하며 인증 과정에서 필요한 정보를 생성한 후 스마트카드에 저장한다. 이에 대한 절차를 그림 1에 나타내었다.

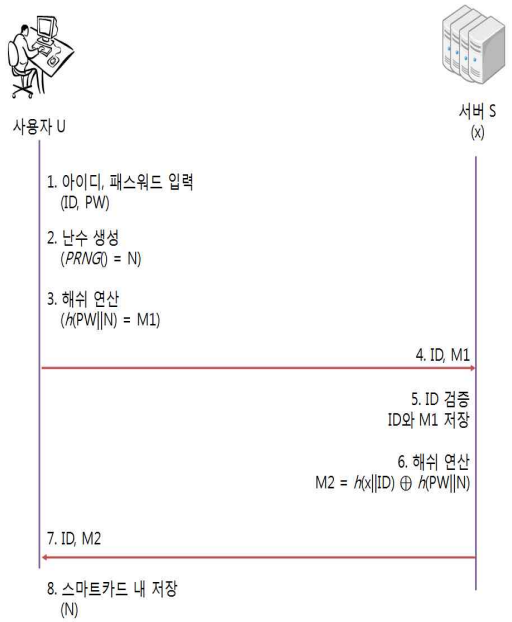

그림 1. I-SPMA 프로토콜 등록 과정
Fig. 1. Registration process of I-SPMA protocol

Step 1. 사용자는 아이디(ID)와 패스워드(PW)를 입력한다.

Step 2. *PRNG*()를 통해 난수(N)를 생성한다.

Step 3. 패스워드(PW)와 생성한 난수(N)를 연접하여 해쉬 연산을 수행하여 패스워드 검증자(M1)를 생성한다.

Step 4. 아이디(ID)와 생성한 패스워드 검증자(M1)를 서버로 전송한다.

Step 5. 서버는 수신한 아이디(ID)가 이미 존재하는지 확인한 후, 존재하지 않는다면 사용자 등록을 수락하고, 사용자 인증 과정에서 사용할 아이디(ID)와 M1을 데이터베이스에 저장한다.

Step 6. 추가적으로 비밀키(x)와 아이디(ID)를 연접하여 해쉬 연산을 수행하고, 패스워드(PW)와 난수(N)를 연접하여 해쉬 연산을 수행한 결과의 배타적 논리합을 구한다. 연산 결과(M2)는 이후 사용자 인증 과정에서 검증을 위해 사용된다.

Step 7. 아이디(ID)와 M2를 스마트카드로 전송하

고, 스마트카드 내에 아이디와 M2를 저장한 후 사용자에게 스마트카드를 발급한다.

Step 8. 사용자는 발급받은 스마트카드 내에 난수(N)를 저장한다.

2-1-2. 인증 과정

인증 과정에서는 사용자가 인증을 위해 스마트카드를 삽입한 후 패스워드를 입력한다. 패스워드 입력 후 인증 과정은 그림2와 같다.

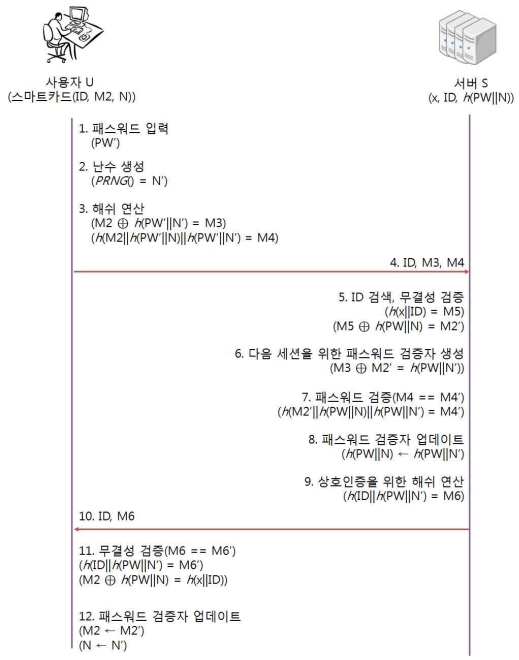

그림 2. I-SPMA 프로토콜 인증 과정
Fig. 2. Authentication process of I-SPMA protocol

Step 1. 사용자는 패스워드(PW')를 입력한다.

Step 2. *PRNG*()를 통해 난수(N')를 생성한다.

Step 3. 인증을 위해 스마트카드에 저장된 M2와 입력한 패스워드(PW'), 난수(N')를 연접하여 해쉬 연산을 수행한 결과의 배타적 논리합(M3)을 구한다. 추가적으로 패스워드(PW')와 난수(N)를 연접하여 해쉬 연산을 수행한 결과, 패스워드(PW')와 난수(N')를 연접하여 해쉬 연산을 수행한 결과, M2를 전부 연접하여 해쉬 연산을 수행(M4)한다.

Step 4. 사용자 인증을 위해 아이디(ID), M3, M4를 서버로 전송한다.

Step 5. 서버는 수신한 아이디(ID)가 존재하는 아이디(ID)인지 검색한 후, 존재한다면 무결성을 검증한다. 무결성 검증을 위해 비밀키(x)와 ID를 연접하여 해쉬 연산을 수행(M5)하고, 저장된 패스워드(PW)와 난수(N)를 연접하여 해쉬 연산 수행 결과의 배타적 논리합을 계산(M2')한다.

Step 6. 서버는 수신한 M3와 계산된 M2'를 이용하여 다음 세션을 위한 패스워드 검증자를 생성한다.

$(h(x \| ID) \oplus h(PW \| N)) \oplus h(PW \| N') = M3$ 이므로 $h(PW \| N') = M3 \oplus (h(x \| ID) \oplus h(PW \| N))$ 가 성립하기 때문에 생성된 N'의 패스워드 검증자를 계산할 수 있다.

Step 7. 서버는 수신한 패스워드 검증자를 검증한다. 계산한 M2', 저장된 $h(PW \| N)$, 다음 세션의 패스워드 검증자($h(PW \| N')$)을 모두 연접하여 해쉬 연산을 수행(M4')한 후 수신한 M4를 비교하여 일치하는지 확인하여 사용자를 인증한다.

Step 8. 서버는 다음 세션을 위해 계산한 패스워드 검증자($h(PW \| N')$)를 $h(PW \| N)$로 업데이트한다.

Step 9. 상호 인증을 위한 정보를 계산한다. 패스워드(PW)와 난수(N')를 연접하여 해쉬 연산을 수행한 를 ID와 연접하여 해쉬 연산을 수행(M6)한다.

*Step 1*결과*0.* 서버는 계산한 M6를 ID와 함께 사용자에게 전송한다.

Step 11. 사용자는 M6'을 생성하고 이를 비교함으로써 서버를 인증한다.

Step 12. 서버가 인증되면 저장된 M2와 N을 M2'과 N'으로 업데이트한다.

2-2. 비동기 공격 취약점 분석[11]

본 논문에서 제안하는 비동기 공격은 사용자 인증 시 발생한다. 서버와 사용자는 1번의 송/수신을 하는데, 서버에서 사용자로 전송되는 정보를 차단할 경우 심각한 문제를 야기하며, 이를 그림 3에 나타내었다.

공격자에 의해 10번째 과정, 즉, 서버가 ID와 M6를 사용자에게 전송할 때 이를 차단한다면 서버는 사용자를 올바르다고 인증하였지만 사용자는 서버를 인증하지 못하므로 상호 인증이 성립하지 않는다. 또

한 무결성 검증과 패스워드 검증자를 업데이트 하는 과정을 수행하지 않기 때문에 서버와 사용자(스마트카드)가 공유하는 정보의 비동기가 발생한다. 서버는 사용자를 인증하였으므로 h(PW||N)을 h(PW||N')로 업데이트하지만, 사용자는 N과 M2(h(x||ID)⊕h(PW||N)의 값을 업데이트 하지 못한다. 공격자에 의해 차단된 이후 스마트카드에 저장된 N의 값과 서버에 저장된 N의 값은 일치하지 않으므로 사용자가 아이디(ID), 패스워드(PW)를 올바르게 입력한다 할지라도 인증은 성립되지 않는다. 그리고 I-SPMA 프로토콜은 이를 복구할 수 있는 방안이 제시되어 있기 않기 때문에 스마트카드를 다시 발급받지 않는 한 항상 사용자 인증이 되지 않는다. 이는 치명적인 문제점이라 할 수 있으며, 비동기 공격에 의해 서버와 스마트카드의 정보가 일치되지 않더라도 스스로 복구할 수 있는 프로토콜이 제안되어야 한다.

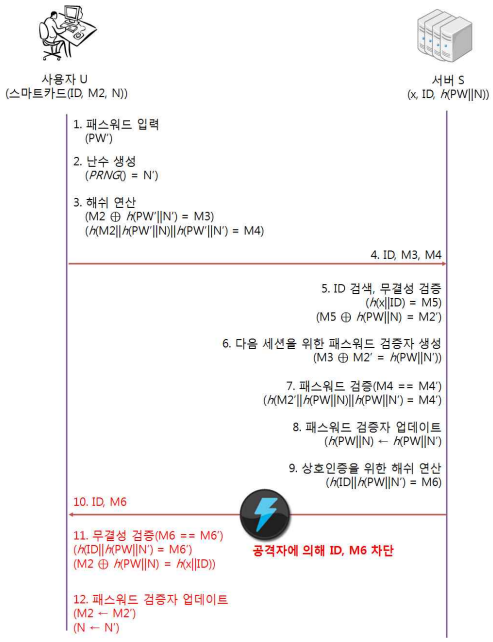

그림 3. I-SPMA 프로토콜의 비동기 공격 취약점
Fig. 3. De-synchronization attack to I-SPMA protocol

Ⅲ. 제안 프로토콜

본 논문은 상기했듯이 I-SPMA 프로토콜이 갖는 비동기 공격에 대한 취약점을 보완하기 위해 개선된 패스워드기반 상호 인증 프로토콜을 제안한다. I-SPMA 프로토콜은 사용자 검증을 위한 검증자를 하나(h(M2||(h(PW||N)||h(PW||N'))만 가지고 있기 때문에 비동기 공격의 취약점이 발생하며, 이를 복구하기 위한 방안도 제시되어 있지 않다. 따라서 현재 세션에 대한 검증자와 다음 세션을 위한 검증자 모두를 저장하여 비동기 공격이 발생했을 경우 이전 세션에 대한 검증자와 비교하여 비동기된 정보를 복구한다면 서비스 거부가 발생하지 않는다.

제안하는 프로토콜은 등록 과정과 인증 과정으로 구성되며, 등록 과정은 스마트카드를 발급받으며, 인증 과정은 발급받은 스마트카드와 아이디, 패스워드로 수행된다. 시스템 파라미터는 표 2와 같다.

3-1. 등록과정

제안하는 프로토콜의 등록 과정은 그림 4와 같다.

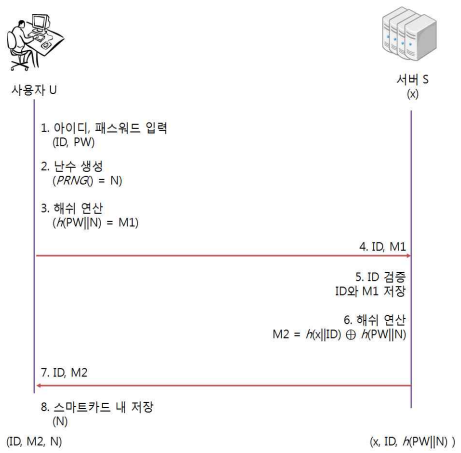

그림 4. 제안하는 프로토콜의 등록 과정
Fig. 4. Registration process of the proposed protocol

Step 1. 사용자는 아이디(ID)와 패스워드(PW)를 입력한다.

Step 2. *PRNG*()를 통해 난수(N)를 생성한다.

Step 3. 패스워드(PW)와 생성한 난수(N)를 연접한 후, 해쉬 연산을 수행하여 패스워드 검증자(M1)를 생성한다.

Step 4. 아이디(ID)와 생성한 패스워드 검증자(M1)

를 서버로 전송한다.

Step 5. 서버는 수신한 아이디(ID)가 이미 존재하는지 확인한 후, 존재하지 않는다면 사용자 등록을 수락하고, 사용자 인증 과정에서 사용될 아이디(ID)와 M1을 데이터베이스에 저장한다.

Step 6. 추가적으로 비밀키(x)와 아이디(ID)를 연접하여 해쉬 연산을 수행하고, 패스워드(PW)와 난수(N)를 연접하여 해쉬 연산을 수행한 결과의 배타적 논리합을 구한다. 연산 결과(M2)는 이후 사용자 인증 과정에서 검증을 위해 사용된다.

Step 7. 아이디(ID)와 M2를 스마트카드로 전송하고, 스마트카드 내에 아이디와 M2를 저장한 후 사용자에게 스마트카드를 발급한다.

Step 8. 사용자는 발급받은 스마트카드 내에 난수(N)를 저장한다.

스마트카드에 저장된 정보는 ID, M2, N이고, 서버에 저장된 정보는 x, ID, h(PW||N)이며, 등록 과정 후 현재 세션 검증자와 다음 세션 검증자의 정보를 업데이트하기 위해 한 번의 인증 과정이 추가로 수행된다.

3-2. 인증 과정

제안하는 프로토콜의 등록 과정은 그림 5와 같다.

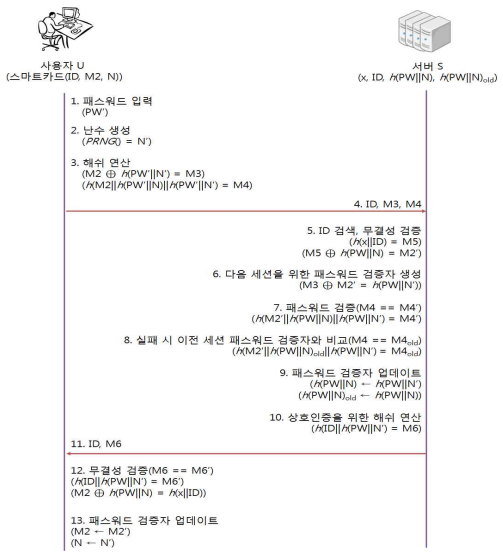

그림 5. 제안하는 프로토콜의 인증과정
Fig. 5. Authentication process of the proposed protocol

Step 1. 사용자는 패스워드(PW')를 입력한다.

Step 2. *PRNG*()를 통해 난수(N')를 생성한다.

Step 3. 인증을 위해 스마트카드에 저장된 M2와 입력한 패스워드(PW'), 난수(N')를 연접하여 해쉬 연산을 수행한 결과의 배타적 논리합(M3)을 구한다. 추가적으로 패스워드(PW')와 난수(N)를 연접하여 해쉬 연산을 수행한 결과, 패스워드(PW')와 난수(N')를 연접하여 해쉬 연산을 수행한 결과, M2를 전부 연접하여 해쉬 연산을 수행(M4)한다.

Step 4. 사용자 인증을 위해 아이디(ID), M3, M4를 서버로 전송한다.

Step 5. 서버는 수신한 아이디(ID)가 존재하는 아이디(ID)인지 검색한 후, 존재한다면 무결성을 검증한다. 무결성 검증을 위해 비밀키(x)와 ID를 연접하여 해쉬 연산을 수행(M5)하고, 저장된 패스워드(PW)와 난수(N)을 연접하여 해쉬 연산 수행 결과의 배타적 논리합을 계산(M2')한다.

Step 6. 서버는 수신한 M3와 계산된 M2'를 이용하여 다음 세션을 위한 패스워드 검증자를 생성한다.

$(h(x \| ID) \oplus h(PW \| N)) \oplus h(PW \| N') = M3$ 이므로 $h(PW \| N') = M3 \oplus (h(x \| ID) \oplus h(PW \| N))$ 가 성립하기 때문에 생성된 N'의 패스워드 검증자를 계산할 수 있다.

Step 7. 서버는 수신한 패스워드 검증자를 검증한다. 계산한 M2', 저장된 $h(PW \| N)$, 다음 세션의 패스워드 검증자($h(PW \| N')$)을 모두 연접하여 해쉬 연산을 수행(M4')한 후 수신한 M4를 비교하여 일치하는지 확인하여 사용자를 인증한다.

Step 8. 만약 검증에 실패한다면 비동기 공격과 같은 위협이 발생하였을 수도 있기 때문에 이전 세션 패스워드 검증자를 통해 검증한다. 검증 과정은 Step 7과 같으며, $h(PW \| N)$, $h(PW \| N')$ 대신 이전 세션 정보인 $h(PW \| N)_{old}$, $h(PW \| N')$을 이용한다.

Step 9. 서버는 패스워드 검증자($h(PW \| N)_{old}$)를 $h(PW \| N)$, $h(PW \| N))$를 $h(PW \| N')$로 업데이트한다.

Step 10. 상호 인증을 위한 정보를 계산한다. 패스워드(PW)와 난수(N')를 연접하여 해쉬 연산을 수행한 결과를 ID와 연접하여 해쉬 연산을 수행(M6)한다.

Step 11. 서버는 계산한 M6를 ID와 함께 사용자에게 전송한다.

Step 12. 사용자는 M6'을 생성하고 이를 비교함으로써 서버를 인증한다.

Step 13. 서버가 인증되면 저장된 M2와 N을 M2'과 N'으로 업데이트한다.

Ⅳ. 제안 프로토콜 안전성 분석

본 장은 제안한 프로토콜의 안전성을 분석하며, 보안 요구 조건인 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격, 서비스 거부 공격, 상호 인증, 비동기 공격에 대한 안전성 분석을 통해 제안한 프로토콜을 검증한다.

4-1. 패스워드 추측 공격

공격자가 탈취할 수 있는 정보는 ID, M3(h(X ‖ ID) ⊕h(PW ‖ N)⊕h(PW ‖ N')), M4(h(x ‖ ID)⊕h(PW ‖ N) ‖ h(PW ‖ N) ‖ h(PW ‖ N')), M6(h(ID ‖ h(PW ‖ N')))이다. M3, M4, M6는 난수(N, N'), 비밀키(x)에 의해 생성되었기 때문에 이에 대한 정보를 구해낼 수 없다면 패스워드(PW)를 계산할 수 없다. M3, M4, M6는 난수(N, N'), 비밀키(x)를 이용하여 해쉬 연산을 수행한 결과이기 때문에 해쉬 연산의 일방향 특성 상 역 연산은 불가능하므로 패스워드(PW)를 추출할 수 없다. 따라서 제안한 프로토콜은 패스워드 추측 공격에 안전하다.

4-2. 재전송 공격

재전송 공격은 서버에 전송되는 ID, M3, M4를 공격자에 의해 탈취당한 후 다음 인증 과정에 이를 이용하여 정상적으로 인증하는 것을 의미한다. 하지만 M3, M4는 난수(N, N')을 기반으로 생성되었기 때문에 매 세션마다 M3, M4가 바뀐다. 따라서 탈취된 M3와 M4를 이용하여도 서버에 의해 인증이 되지 않으므로 제안하는 프로토콜은 재전송 공격에 안전하다.

4-3. 위장 공격

M3, M4는 난수(N, N'), 비밀키(x)에 의해 생성되었기 때문에 이를 알지 못하면 인증에 성공할 수 없다. 임의로 M3, M4를 생성한다고 하더라도 일방향 해쉬 함수의 특성 상 확률적으로 매우 낮기 때문에 제안하는 프로토콜은 위장 공격에 안전하다.

4-4. 훔친 검증자 공격

공격자가 패스워드 검증자(h(PW ‖ N))를 탈취하고, M3, M4, M6를 탈취하였다고 하더라도 공격자는 h(x ‖ ID)를 구할 수 없다. h(x ‖ ID)는 일방향 해쉬 함수로 보호되어 있기 때문에 공격자는 이를 계산할 수 없으므로 제안하는 프로토콜은 훔친 검증자 공격에 안전하다.

4-5. 서비스 거부 공격

제안하는 프로토콜은 다음 세션을 위한 패스워드 검증자(h(PW ‖ N'))가 포함된 M3, M4, M6의 무결성 검사를 통해 인증 유무를 판단하며, 인증이 올바르다면 현재 세션 패스워드 검증자(h(PW ‖ N))를 다음 세션 패스워드 검증자(h(PW ‖ N'))로 업데이트 하므로 서비스 거부 공격에 안전하다.

4-6. 상호 인증

서버는 사용자가 생성한 M3, M4를 이용하여 인증하며, 사용자는 서버가 생성한 M6를 이용하여 인증한다. 또한 매 세션마다 현재 세션 패스워드 검증자(h(PW ‖ N))를 다음 세션 패스워드 검증자(h(PW ‖ N')), M2를 M2', N을 N'으로 업데이트하므로 제안하는 프로토콜은 상호 인증을 제공한다.

4-7. 비동기 공격

공격자에 의해 M6가 차단되었을 경우 비동기로 인한 서비스 거부가 발생한다. 제안하는 프로토콜의 경우 M6를 차단하더라도 이후에 올바른 사용자에 의해 인증되었다면 비동기를 복구하기 위한 검증자(h(PW ‖ N)old)를 통해 사용자를 인증할 수 있으며, 인증 후 패스워드 검증자(h(PW ‖ N)old)를 h(PW ‖ N),

h(PW ‖ N))를 h(PW ‖ N')로 업데이트하기 때문에 스스로 복구 가능하다. 따라서 제안하는 프로토콜은 비동기 공격에 강인하다.

표 3. 안전성 비교/분석
Table 3. Security comparison/analysis

구분	SE-OSPA 프로토콜	NSPA 프로토콜	SPMA 프로토콜	I-SPMA 프로토콜	제안 프로토콜
패스워드 추측 공격	O	O	O	O	O
재전송 공격	X	O	X	O	O
위장 공격	O	O	O	O	O
훔친 검증자 공격	O	O	O	O	O
서비스 거부 공격	X	O	X	X	O
상호 인증	X	X	O	O	O
비동기 공격	O	O	X	X	O

Ⅴ. 결 론

본 논문에서는 패스워드기반 상호 인증 프로토콜인 I-SPMA 프로토콜의 보안성을 분석하였으며, 분석결과 I-SPMA 프로토콜은 비동기 공격에 취약하며, 이로 인해 서비스 거부가 발생한다. 따라서 이를 보완할 수 있는 프로토콜을 제안하였으며, 제안한 프로토콜은 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격, 서비스 거부 공격, 상호 인증, 비동기화 공격에 대한 안전성을 분석하였다. 또한 이미 제안된 SPMA, I-SPMA 프로토콜에 비해 한 번의 추가적인 연산만으로 비동기 공격에 대한 취약점을 보완하였으므로 높은 효율성을 제공한다. 본 논문에서 제안한 프로토콜은 네트워크를 이용하는 패스워드기반 인증 방식에 보다 효과적으로 활용될 수 있을 것으로 판단되며, 보다 경량화하기 위한 방안을 향후 연구되어야 할 것이다.

Reference

[1] L.Lamport, "Password authentication with insecure communication", Communication of ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[2] A. Shimizu, "A dynamic password authentication method by one-way function", IEICE Transactions on Communications, vol. J73-D-1, no. 7, pp. 630-636, Jul. 1990.

[3] A. Shimizu, "A dynamic password authentication method by one-way function", System and Computers in Japan, vol. 22, no. 7, pp. 32-40, Jul. 1991.

[4] A. Simizu, T. Horioka, and H. Inagaki, "A password authentication method for contents communication on the internet", IEICE Transactions on Communications, vol. E81-B, no. 8, pp. 1666-1673, Aug. 1998.

[5] M. Sandirigame, 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.

[6] 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.

[7] C. W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong-password authentication protocol", ACM SIGOPS Operating System Review, vol. 37, no. 2, pp. 7-12, Apr. 2003.

[8] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", Journal of Computer and System Sciences International, vol. 45, no. 4, pp. 623-626, Jan. 2006.

[9] Eun-Jun Yoon, You-Sik Hong, Cheon-Shik Kim, Kee-Young Yoo, "Strong Password Mutual Authentication Protocol", The Institute of Electronics Engineers of Korea, 46-CI(1), pp. 11-19, Jan. 2009.

[10] Jun-sub kim, Jin Kwak, "Improved Strong Password Mutual Athentication Protocol to Secure on Replay

Attack", The Korea Navigation Institute, 14(3), pp. 415-425, Jun. 2010.

[11] Kyung-Roul Lee, Kang-Bin Yim, "Vulnerability Analysis on the Strong-Password Mutual Authentication Protocols", The Korea Navigation Institute, 15(5), pp.722-728, Oct. 2011.

육 형 준 (Hyeong-Jun Yuk)

2010년 2월 : 동양대학교 전자유도기술학과(공학사)

2012년 8월 : 순천향대학교 정보보호학과(공학석사)

2013년 3월~현재 : 순천향대학교 정보보호학과 박사과정

관심분야 : vulnerability analysis, virtualized obfuscation, system security, insider threats

임 강 빈 (Kang-Bin Yim)

1992년 2월 : 아주대학교 전자공학과(공학사)

1994년 2월 : 아주대학교 전자공학과(공학석사)

2001년 2월 : 아주대학교 전자공학과(공학박사)

1999년 3월~2000년 2월 : (미)아리조나주립대학교 연구원

2003년 3월~ 현재 : 순천향대학교 정보보호학과 교수

2005년 3월~ 2010년 현재 : 한국정보보호학회 이사

2009년 3월~ 2010년 현재 : 한국인터넷정보학회 이사

2010년 12월~2012년 2월: (미)퍼듀대학교 객원교수

관심분야 : vulnerability analysis, insider threats, secure hardware architecture, authentication protocol, homeland security