한국항행학회 논문지 제15권 제5호 2011년 10월

강력한 패스워드 상호인증 프로토콜 취약점 분석

Vulnerability Analysis on the Strong-Password Mutual Authentication Protocols

이경률*, 임강빈*

Kyung-Roul Lee*, Kang-Bin Yim*

요 약

네트워크 환경에서 사용자에 대한 인증은 반드시 필요한 요소이며, 이를 위하여 많은 사용자 인증기술이 연구되고 발전되어 왔다. 그 중 SPMA, I-SPMA 프로토콜은 과거 프로토콜이 가지는 상호인증 결여, 재전송 공격 등 취약점에 대하여 지적하고, 이를 보완한 안전한 사용자 인증 프로토콜을 제안하였다. 하지만 이들 프로토콜은 서버와 사용자가 공유한 비밀정보가 동기화되지 않을 경우 심각한 문제를 발생하며, 이를 복구할 수 있는 대안이 없어 그 실효성을 입증하지 못한다. 따라서 본 논문은 상기 프로토콜이 비동기 문제로 인한 서비스 거부 공격에 대하여 고려하고 있지 않음을 증명함으로써 제안된 프로토콜의 안전성을 분석하였다.

Abstract

Most services need to have authentication protocols to verify users' eligibility in the network environment. For this, a lot of user authentication protocols have been researched and developed. Two of them, SPMA and I-SPMA protocols, introduced the lack of mutual authentication and vulnerability to the reply attack of the prior protocols and suggested revised protocols. Nevertheless, these protocols did not mention about the critical problem caused when the server and the client lose synchronization on the secret information between them. Therefore, in this paper, we analyze the security characteristics of the existing protocols and prove the vulnerability to the synchronization of the protocols.

Key words : Password-based authentication, Authentication protocol, Mutual authentication, Desynchronization attack, Denial of service attack

Ⅰ. 서 론

네트워크의 발전과 더불어 온라인에서 올바른 사용자를 인증하고 인가하기 위한 기술이 필요하게 되었다. 가장 일반적인 사용자 인증기술은 패스워드기반 인증기술로서 이는 사용자가 온라인을 통해 서비스를 이용할 경우 아이디와 패스워드를 설정하여 이를 등록하고, 등록 시 입력한 아이디, 패스워드와 로그인 시 입력한 아이디, 패스워드를 비교하여 두 정보가 올바른지 판단한 후 올바른 사용자일 경우 서비스를 인가하는 기술이다. 과거 일회용 패스워드 방식[1]을 기준으로, 사용자 편의를 고려하고 저비용으로

* 순천향대학교(Soonchunhyang University)
· 제1저자 (First Author) : 이경률
· 교신저자 (Corresponding Author) : 임강빈
· 투고일자 : 2011년 8월 3일
· 심사(수정)일자 : 2011년 8월 4일 (수정일자 : 2011년 9월 19일)
· 게재일자 : 2011년 10월 30일

표 1. 인증 프로토콜 현황 및 취약점
Table 1. Authentication protocols and their vulnerabilities

제안 프로토콜	제안자	아이디어	취약점
CINON(Chanied one-way data verification method)[2][3] (1990, 1991)	A. Shimizu	난수를 메모리 장치 등의 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	상호인증을 제공하지 않음, 위장 공격, 서비스 거부 공격에 취약
SPMA(Strong password mutual authentication)[9] (2009)	윤은준, 홍유식, 김천식, 유기영	상호인증 제공	재전송 공격에 취약
I-SPMA(Improved Strong Password Mutual Authentication)[10] (2010)	김준섭, 곽진	재전송 공격 보완	비동기 공격, 서비스 거부 공격에 취약

효율을 극대화할 수 있는 연구들이 진행되어 왔으며, 대표적인 인증 프로토콜은 표 1과 같다.

SPMA 이전의 프로토콜들은 단방향 인증 프로토콜이지만, SPMA, I-SPMA 프로토콜은 상호인증을 제공하기 위하여 양방향으로 인증하고 있으며, 패스워드 추측 공격, 재전송 공격, 위장 공격, 훔친 검증자 공격 등에 강인하도록 설계되었다. 하지만 양방향 인증 시 공격자가 서비스를 거부할 목적으로 응답을 가로채어 사용자에게 전송하지 않을 경우 내부에서 공유하는 비밀정보가 달라지기 때문에 이후의 모든 인증요청은 정상적인 인증정보임에도 불구하고 항상 일치하지 않는다. 즉, 공격자에 의해 전송되는 정보가 차단되면 이를 복구할 방법도 없을 뿐 아니라 이후의 모든 사용자 인증 프로토콜 자체가 성립되지 않는다. 최근 사용자 인증, RFID 등을 포함한 기존 프로토콜 및 시스템의 문제점 및 취약점을 증명하고, 이에 대응하기 위한 연구가 활발히 진행되고 있으므로[11][12][13][14][15], 본 논문에서는 SPMA, I-SPMA가 가진 서비스 거부 공격, 비동기 공격 가능성에 대하여 분석함으로써 안전성을 평가하고자 한다.

Ⅱ. 관련연구

2-1 인증 프로토콜의 발전과정

표 1에서 나타난 바와 같이 제안된 인증 프로토콜은 최초 1990년, 1991년 A. Shimizu에 의해 처음 제안되었으며, 난수를 메모리 장치 등 별도의 장치에 저장하여 인증하는 CINON 프로토콜을 제안하였다. 이에 A.Shimizu, T. Horioka, H. Inagaki는 CINON 프로토콜의 휴대성 결여와 고비용에 대한 문제를 제기함으로써 PERM 프로토콜을 제안하였지만 중간자 공격에 취약한 문제를 가지고 있었다. M. Sandirigama, A. Shimizu, M. T. Noda는 중간자 공격 취약점을 보완한 SAS 프로토콜을 제안하였지만 이 역시 훔친 검증자 공격, 재전송 공격, 서비스 거부 공격에 대한 취약점을 가지고 있었다. C. L. Lin, H. M. Sun, T. Hwang은 재전송 공격, 서비스 거부 공격을 보완한 OSPA 프로토콜을 제안하였으나 훔친 검증자 공격에 대해서는 보완하지 못하였으며 이에 C. W. Lin, J. J. Shen, M. S. Hwang이 훔친 검증자 공격을 보완하고 OSPA 프

로토콜의 안전성을 강화한 SE-OSPA 프로토콜을 제안하였다. 하지만 SE-OSPA 프로토콜은 서비스 거부 공격에 취약점을 가지고 있어 C.W. Lin, C.S. Tsai, M. S. Hwang이 안전성과 효율성을 강화한 NSPA 프로토콜을 제안하였으나 제안한 프로토콜은 상호인증을 제공하지 않으며, 위장 공격, 서비스 거부 공격에 대하여 취약함이 드러났다. 따라서 NSPA 프로토콜에 대하여 상호인증을 제공하기 위해 윤은준, 홍유식, 김천식, 유기영은 SPMA 프로토콜을 제안하였으나 재전송공격에 대한 취약점이 존재하였으며, 이에 김준섭, 곽진은 재전송 공격을 보완한 I-SPMA 프로토콜을 제안하였다. 하지만 상호인증을 제공하기 위해 제안된 SPMA, I-SPMA 프로토콜은 프로토콜의 구조 상 비동기 공격, 서비스 거부 공격 등에 대한 취약점을 가지게 되므로 본 논문에서는 이를 분석하고자 한다.

2-2 개선된 강력한 패스워드 상호인증 프로토콜(I-SPMA 프로토콜)

본 논문은 SPMA, I-SPMA을 분석대상으로 하고 있으나 제시하는 취약점에 대하여는 동일하므로 본 절에서는 가장 최근에 개선된 I-SPMA 프로토콜의 특성을 소개하고자 한다. I-SPMA 프로토콜은 등록과정과 인증과정으로 이루어져 있으며, 등록과정에서 사용자는 아이디와 패스워드가 저장된 스마트카드를 발급받고, 인증과정에서 사용자가 입력한 아이디, 패스워드 그리고 스마트카드를 통해 상호인증을 수행한다. 또한 I-SPMA 프로토콜은 무결성을 검증하기 위해 해쉬된 비밀키와 아이디 정보를 이용함으로써 발생 가능한 재전송 공격에 대한 취약점을 현재 세션 패스워드 검증자, 다음 세션 패스워드 검증자 등의 정보를 이용하여 보완하였다. 표 2는 I-SPMA 프로토콜에서 사용하는 용어이다.

2-2-1 등록과정

등록과정은 사용자가 아이디와 패스워드를 입력하고, 난수를 생성하여 사용자가 입력한 패스워드와 해쉬 연산을 한 후 그 결과를 서버에 전송하며, 서버는 수신한 정보를 저장하고 인증과정에서 필요한 비밀 정보를 생성한 후 스마트카드에 저장하는 단계로 이루어져 있다. 이에 대한 절차는 그림 1과 같다.

표 2. I-SPMA 프로토콜의 용어
Table 2. Definitions in the 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

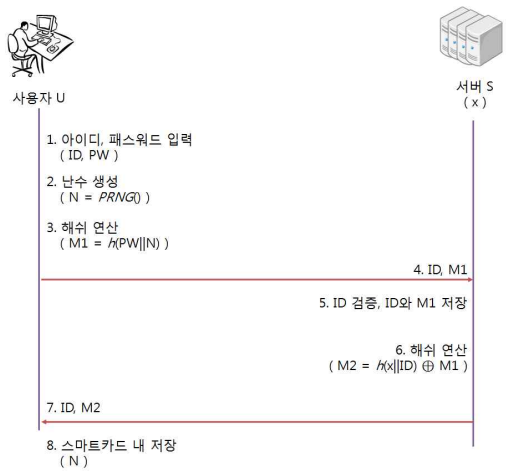


그림 1. I-SPMA 프로토콜 등록과정
Fig. 1. Registration process of I-SPMA

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 인증과정에서 사용될 아이디(ID)와 M1을 데이터베이스에 저장한다.

Step 6. 비밀키(x)와 아이디(ID)를 연접하여 해쉬 연산을 수행하고, 그 결과를 패스워드 검증자(M1)와 배타적 논리합을 구한다. 연산 결과(M2)는 이후 사용자 인증과정에서 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.

2-2-2 인증과정

인증과정은 사용자가 스마트카드를 삽입한 후 등록 시 설정한 패스워드를 입력하고 공유된 비밀정보를 토대로 검증자를 생성하여 서버로 전송하며, 서버는 이를 수신한 후 자신의 검증자와 비교하여 일치하는지 확인하는 단계로 이루어져 있다. 패스워드 입력 후 사용자 인증과정을 그림 2에 나타내었다.

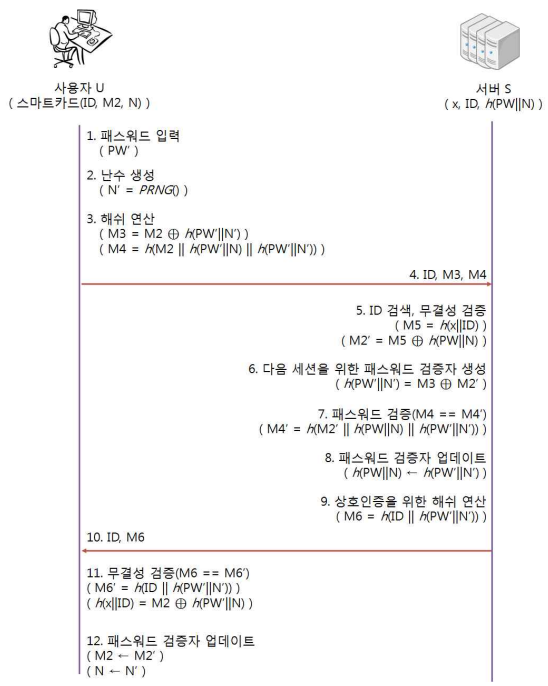


그림 2. I-SPMA 프로토콜 인증과정
Fig. 2. Authentication process of I-SPMA protocol

Step 1. 사용자는 패스워드(PW')를 입력한다.

Step 2. PRNG()를 통해 난수(N')를 생성한다.

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

Step 4. 아이디(ID), M3, M4를 서버로 전송한다.

Step 5. 서버는 이미 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($h(PW' \| N')$)를 모두 연접하여 해쉬 연산을 수행(M4')한 후 수신한 M4와 비교하여 일치하는지 확인하여 사용자를 인증한다.

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

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

Step 10. 서버는 계산한 M6를 ID와 함께 사용자에게 전송한다.

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

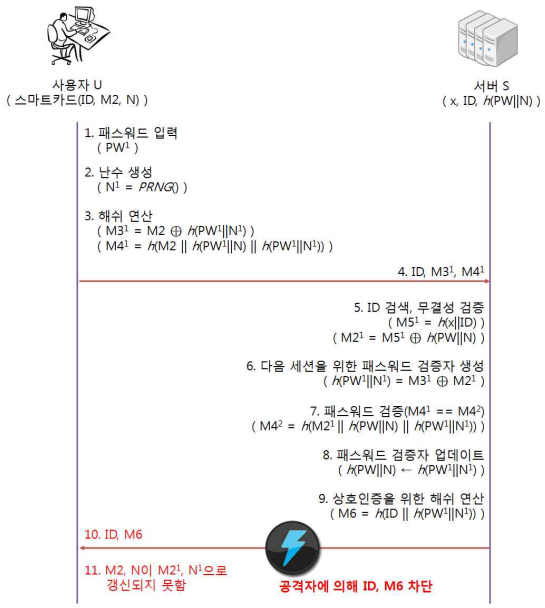
Step 12. 서버가 인증되면 저장된 M2와 N을 M2'과 N'으로 업데이트한다.

Ⅲ. 비동기 공격 취약점 분석

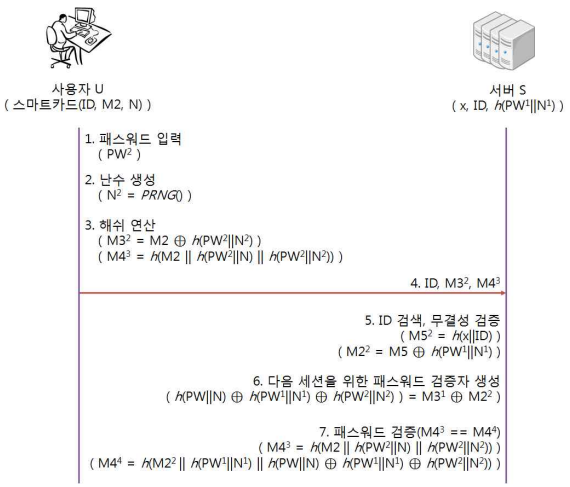
비동기 공격이란 비밀정보를 공유하는 개체들 간 송/수신 시 발생하는 오류 또는 송/수신하는 정보를 공격자가 악의적으로 차단하여 각 개체들 간 비밀정보의 불일치를 유도하는 공격을 말하며, 서비스 거부 공격(Denial of Service attack)의 일종이다. I-SPMA 프로토콜은 두 개체 간의 상호인증을 수행하고 상호인증 시 두 개체의 공유정보 검증을 위한 단계를 제공한다. 상호 송/수신하는 이 공유정보는 재전송 공격 등과 같이 인증 과정에서의 노출된 정보를 활용하는 공격에 대응하기 위해 매 세션마다 그 값이 바뀌어야 하므로 이를 위하여 매 세션마다 새로운 난수를 생성하고 생성한 난수를 기반으로 해쉬연산을 수행하되 이 값은 다음 세션에서의 공유정보 검증을 위하여 유지되어야 하므로 세션마다 해당 값을 갱신한다. 하지만 이 과정에서 한 개체가 검증 값을 갱신하였다 하더라도 다른 개체가 이를 갱신하지 못하였을 경우 즉, 서버의 정보는 갱신되었지만 클라이언트의 정보가 갱신되지 못하였을 경우, 이후 인증과정에서 클라이언트는 이전 세션에서 생성한 난수를 사용하기 때문에 서버에서 올바른 사용자로 인증되지 못한다. 프로토콜 수행과정에서의 비동기 공격 발생 상황을 그림 3에 나타내었다.

공격자에 의해 10번째 과정, 즉, 서버가 ID와 M6를 사용자에게 전송하는 절차에서 이를 차단한다면 서버는 사용자를 올바른 사용자로 인증하였지만 사용자는 서버를 인증하지 못하므로 상호인증이 성립하지 않는다. 또한 무결성 검증과 패스워드 검증자를 업데이트하는 과정(11번째, 12번째)이 수행되지 않았기 때문에 서버와 사용자(스마트카드)가 공유하는 비밀정보의 비동기가 발생한다. 서버는 사용자를 인증하였으므로 h(PW||N)을 h(PW1||N1)로 업데이트하지만, 사용자는 N과 M2(h(x||ID)⊕h(PW||N))를 갱신하지 못하므로 비동기 공격 후 스마트카드에 저장된 N과 서버에 저장된 N1가 일치하지 않아 사용자가 아이디(ID), 패스워드(PW)를 올바르게 입력한다 할지라도 인증은 항상 실패한다.

이와 같이 비동기 공격은 공격자가 쉽게 접근할 수 있는 형태의 공격이며 단 한 번의 공격으로 인해



a) 공격자에 의한 정보 차단
a) Corrupted transactions by attacker



b) 비동기 공격 후의 사용자 인증 결과
b) User authentication result after desynchronization attack

그림 3. I-SPMA 프로토콜에 대한 비동기 공격
Fig. 3. Desynchronization attack to I-SPMA

사용자는 해당 서비스를 이용할 수 없게 된다. 이는 서비스의 지속을 위해서 사용자가 스마트카드를

다시 발급받아야 하는 심각한 상황을 유발하므로 I-SPMA 프로토콜은 비동기 공격이 발생할 경우 공유 정보를 스스로 복구할 수 있도록 별도의 조치를 프로토콜 내에 구성하여 사용자 인증 프로토콜의 안전성을 확보할 필요가 있다. 참고로 기존의 인증 프로토콜에 대한 비동기 공격 분석 결과를 표 3에 나타낸다.

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

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

Ⅳ. 결 론

본 논문은 패스워드 기반 상호인증 프로토콜인 SPMA 및 I-SPMA 프로토콜의 보안성을 분석하였으며, 분석 결과 이들 프로토콜이 비동기 공격에 취약함을 증명하였다. SPMA, I-SPMA 프로토콜은 상호인증은 제공하지만 비동기 공격으로 인한 서비스 거부 공격에 대하여 고려하고 있지 않기 때문에 취약점이 존재하며, 난수를 통해 검증문제를 해결하고 있으므로 비동기된 난수를 복원하기 위한 방안을 고려하여야 한다. 해결방안으로 이전 세션에서 활용되었던 검증자를 저장하고 현재 세션에서 이전 세션의 검증자인지 현재 세션의 검증자인지를 비교함으로써 비동기 공격을 탐지하는 방법이 가능할 것으로 사료된다.

참 고 문 헌

[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 Systems Sciences International, vol. 45, no. 4*, pp. 623-626, Jan. 2006

[9] 윤은준, 홍유식, 김천식, 유기영, “강력한 패스워드 상호인증 프로토콜,” *전자공학회 논문지, 46-CI(1)*, pp. 11-19, 2009년 1월

[10] 김준섭, 곽진, “재전송 공격에 안전한 개선된 강력한 패스워드 상호인증 프로토콜,” *항행학회 논문지, 14(3)*, pp. 415-425, 2010년 6월

[11] 윤택영, 김창한, “위임기반 인증 프로토콜의 프라이버시 취약성 분석,” *정보보호학회 논문지, 20(6)*, pp. 53-57, 2010년 12월

[12] 김정태, “RFID 태그 보안과 프로토콜의 취약점 분석 및 보안성 향상을 위한 기법,” *한국해양정보*

통신학회논문지, 15(6), pp. 1307-1312, 2011년
[13] 김정윤, 강성용, 장학범, “Pay-TV 방송 시스템을 위한 Sun 등이 제안한 접근제어 시스템의 취약점 분석에 관한 연구,” 한*국정보처리학회 춘계학술발표대회*, pp. 808-811, 2011년 4월
[14] 장학범, 강성용, 최형기, “Return Routability 프로토콜의 취약점 및 개선 방안,” *한국정보처리학회 춘계학술발표대회*, pp. 945-948, 2011년 4월
[15] 김준섭, 곽진, “Yang의 강력한 패스워드 인증 스킴에 대한 보안 취약점 분석,” 한*국정보처리학회 춘계학술발표대회*, pp. 797-799, 2011년 4월

이 경 률 (李庚栗)

2008년 8월 : 순천향대학교 정보보호학과(공학사)
2010년 8월 : 순천향대학교 정보보호학과(공학석사)
2010년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2011년 5월~현재 : (미)퍼듀대학교 정보보호교육연구센터 연구원
관심분야 : vulnerability analysis, virtualized obfuscation, system security, insider threats

임 강 빈 (任綱彬)

1992년 2월: 아주대학교 전자공학과 (공학사)
1994년 2월: 아주대학교 전자공학과 (공학석사)
2001년 2월: 아주대학교 전자공학과 (공학박사)
1999년 3월~2000년 2월: (미)애리조나 주립대학교 연구원
2003년 3월~현재: 순천향대학교 정보보호학과 교수
2005년 3월~현재: 한국정보보호학회 이사
2009년 3월~현재: 한국인터넷정보학회 이사
2010년 12월~현재: (미)퍼듀대학교 정보보호교육연구센터 객원교수
관심분야 : vulnerability analysis, insider threats, secure hardware architecture, homeland security