http://dx.doi.org/10.7236/JIWIT.2012.12.6.91
JIWIT 2012-6-11

스마트카드 기반 상호인증 스킴의 보안성 개선

Security Improvements on Smart-Card Based Mutual Authentication Scheme

주영도*

Young-Do Joo

요 약 허가받지 않은 접근을 통해 위험에 노출될 수 있는 자원을 보호하기 위해 패스워드 기반의 인증 스킴들이 최근에 폭넓게 채택되어 사용되고 있다. 2008년에 Liu 등은 위조공격에 견딜 수 있는 패스워드 기반의 스마트카드를 사용하는 새로운 상호인증 스킴을 제안하였다. 본 논문은 안전성 분석을 통해 Liu 등의 스킴이 여전히 다양한 보안 공격에 취약함을 증명한다. 아울러, 공격자가 스마트카드에 저장된 비밀 정보를 불법으로 취득한 경우에도 이러한 보안상의 약점을 극복하면서 동시에 사용자와 원격 인증서버 간 상호인증을 제공하는 개선된 스킴을 제안한다. 저자는 본 연구에서 안전성 분석과 결과 비교를 통해, 제안하는 스킴이 Liu 등의 스킴에 비하여 다양한 공격들로부터 보다 안전하고 효율적인 스킴임을 보여준다.

Abstract Password-based authentication schemes have been widely adopted in order to protect resources from unauthorized access. In 2008, Liu et al. proposed a new mutual authentication scheme using smart cards which can withstand the forged attack. In this paper, author has proven that Liu et al.'s scheme is still vulnerable to the various attacks by analyzing the security of their scheme. This paper introduces an enhanced scheme to overcome these security weakness and to provide mutual authentication between the user and the server, even if the secrete information stored in the smart card is revealed by an attacker. The comparative result from the security analysis demonstrates that the proposed scheme is more secure against the possible attacks than Liu et al.'s scheme.

Key Words : Mutual Authentication, Smart Card, User Impersonation Attack, Password Guessing Attack

I. 서 론

컴퓨터 네트워크 기술의 급속한 발달과 함께 스마트카드를 이용하는 사용자 인증 스킴은 주요한 보안 이슈가 되고 있다. 부주의한 패스워드 관리와 고도화된 공격 방법으로 인하여, 원격 사용자 인증 스킴은 심각할 정도의 공격 위험에 노출되어 있다. 따라서 스마트카드를 이용하는 인증과 관련된 보안 안전성을 개선한 다양한 스킴들이 지속적으로 제시되고 있다[1-12].

1991년에 Yang[1] 등이 제안한 스마트카드를 사용하는 time-stamp 기반의 패스워드 스킴은 사용자 인증을 위한 패스워드와 검증 테이블이 필요 없는 방안을 소개하

*정회원, 강남대학교 컴퓨터미디어정보공학부
접수일자 2012년 9월 18일, 수정일자 2012년 11월 8일
게재확정일자 : 2012년 12월 14일

Received: 27 September 2012 / Revised: 24 November 2012 / Accepted: 14 December 2012
*Corresponding Author: ydjoo@kangnam.ac.kr
Dept. of Computer and Media Information, Kangnam University, Korea

였다. 2003년에 Shen[2] 등은 Yang 등의 스킴이 위조공격을 막아낼 수 없다고 지적하면서 상호인증이 가능한 새로운 개선안을 제안 게재하였다. 그러나 2005년에 Yoon[6] 등은 Shen 등이 제안한 스킴 역시 위조공격에 취약할 수 있음을 보여주었다. 2008년에 Liu[10] 등도 Shen 등의 스킴에 대하여 공격자에 의한 위조공격이 가능함을 조사하였고, 위조공격을 견디어낼 수 있는 새로운 nonce 기반의 상호인증 스킴을 제안하였다. Liu 등은 자신들의 스킴이 시스템의 정보 유출과 도용 시에도 사용자와 인증서버 간 안전한 상호인증을 제공한다고 주장하였다.

본 논문은 Liu 등이 제시한 스킴의 안전성을 분석하여, Liu 등의 스킴이 여전히 위조 공격, 패스워드 추측공격, 내부자 공격에 취약함을 갖고 있으며, 따라서 안전한 상호인증을 제공하지 못함을 밝혀낸다. 본 논문에서는 Liu 등의 인증 스킴에 대한 안전성을 평가하기 위해 공격자가 다음의 능력을 갖고 있다고 가정한다. 즉 Kocher[13] 등과 Messerges[14] 등이 지적한 바와 같이, 공격자는 스마트카드의 전력소비를 모니터링함으로 스마트카드 안에 저장된 비밀정보를 추출 할 수 있고 사용자와 인증서버 간에 통신하는 메시지를 가로챌 수 있게 된다. 본 논문에서 저자는 스마트카드의 저장된 정보가 누출되는 경우에도 보안상의 결함을 극복할 수 있는 개선된 스킴을 새로이 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 Liu 등이 제안한 스킴을 고찰하고, 보안상의 취약점을 분석함으로 침투 가능한 공격을 기술한다. 3장에서는 본 연구에서 제안하는 개선된 상호인증 스킴을 제시하고, 아울러 제안 스킴의 안전성 분석에 기초하여 Liu 등의 스킴과 비교함으로써 보안 특성상 우위를 입증한다. 마지막으로 4장에서 간략히 결론을 맺는다.

II. Liu 등의 인증 스킴 고찰 및 안전성 분석

1. Liu 등의 인증 스킴 고찰

2008년에 Liu 등에 의해 제안된 인증 스킴은 스마트카드를 이용한 nonce 기반의 상호인증을 보여준다[10]. Liu 등의 스킴은 초기화 단계 (initialization phase), 등록 단계 (registration phase), 로그인 단계 (login phase) 그리고 인증 단계 (authentication phase)에 걸친 4개의 단계로 구성된다. 각 단계별 과정은 아래에서 간략히 기술한다. 표 1은 본 논문에서 사용된 약어 표기 및 정의를 요약 정리한 것이다.

표 1. 약어 표기 및 정의
Table 1. Abbreviation Notation and Definition

표기	정의
KIC	주요정보센터(Key Information Center)
Ui	사용자 (User i)
S	원격 인증 서버 (Remote Server)
PWi	사용자 i 의 패스워드
IDi	사용자 i 의 아이디
CIDi	사용자 i 의 스마트카드 아이디
h()	단방향 해쉬(hash) 함수
x⊕y	x 와 y에 대한 Exclusive-OR 연산

• 초기화 단계

패러미터 값을 생성하여 새로운 사용자에게 스마트카드를 제공하는 역할을 하는 KIC는 다음의 초기화 과정을 수행한다.

(1) KIC는 2개의 큰 소수 p와 q를 생성한다. 그리고 $n = p \cdot q$ 를 계산한다.

(2) KIC는 식 (1)을 만족하는 소수 e 와 정수 d를 구한다.

$$e \cdot d = 1 \bmod (p-1)(q-1) \quad (1)$$

여기서, e는 시스템의 공개키이고 d는 시스템의 비밀키이다. 이러한 암호 패러미터들은 안전한 경로를 통해 인증서버에 전달된다.

(3) KIC는 GF(p)와 GF(q) 양쪽에 존재하는 원시원소이며 시스템의 공개 정보인 정수 값 g를 구한다.

• 등록 단계

새로운 사용자 U_i가 자신의 아이디 ID_i와 패스워드 PW_i를 안전한 경로를 통해 KIC에게 제출하는 등록단계에서 KIC는 다음 과정을 수행한다.

(1) KIC는 식 (2)로부터 사용자의 비밀정보 S_i를 계산한다.

$$S_i = ID_i^d \bmod n \quad (2)$$

(2) KIC는 식 (3)과 (4)에 의해 스마트카드 아이디 CID_i와 h_i를 계산한다.

$$CID_i = h(ID_i \oplus d) \quad (3)$$
$$h_i = g^{PWi \cdot d} \bmod n \quad (4)$$

(3) KIC는 안전한 경로를 통해 해당 사용자에게 스마트카드를 발급한다. 이때 스마트카드 내에 n, e, g, ID_i, CID_i, S_i, h_i 와 같은 비밀정보들이 저장되어 진다.

• 로그인 단계

사용자가 인증 서버 S에 로그인 하여 인증을 받으려 할 때 수행되는 로그인 단계에서, 사용자 U_i는 자신의 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 나서 스마트카드는 다음 과정을 수행한다.

(1) 스마트카드는 식 (5)와 같이 SID_i를 계산하고 인증서버에게 메시지 $M_1 = \{ID_i, SID_i\}$를 전송한다.

$$SID_i = h(CID_i) \quad (5)$$

(2) 메시지 M_1을 수신한 인증서버는 식 (6)으로부터 CID_i를 계산하고 나서, 수신한 SID_i와 구한 값 $h(CID_i)$를 비교한다. 만약 두 값이 같으면 인증서버는 로그인 요청을 받아들인다.

$$CID_i = h(ID_i \oplus d) \quad (6)$$

(3) 인증서버는 랜덤 세션 nonce N_s를 생성하고, 식 (7)에 의해 S_n을 계산하여 스마트카드에 전송한다..

$$S_n = N_s \oplus CID_i \quad (7)$$

(4) S_n을 수신한 스마트카드는 식 (8)로부터 N_s를 구하게 되고 랜덤 수 r_c를 생성한다.

$$N_s = S_n \oplus CID_i \quad (8)$$

(5) 스마트카드는 랜덤 수 r_c를 사용하는 식 (9)와 (10)에 의해 메시지 $M_2 = \{X_i, Y_i\}$를 계산하여 인증서버 S에게 전송한다.

$$X_i = g^{rc \cdot PWi} \bmod n \quad (9)$$
$$Y_i = S_i \cdot h_i^{rc \cdot Ns} \bmod n \quad (10)$$

• 인증 단계

인증요청 메시지 M_2를 수신한 인증서버와 스마트카드는 사용자와 인증서버 간 상호인증을 위해 다음 과정을 수행한다.

(1) 인증 서버 S는 $Y_i^e = ID_i \cdot X_i^{Ns} \bmod n$ 이 성립하는지 확인한다. 만약 값이 같으면 인증서버는 성공적으로 스마트카드를 인증한다.

(2) 상호인증을 수행하기 위해 인증서버는 식 (11)로부터 메시지 M_3를 계산하여 스마트카드에 전송한다.

$$M_3 = (h(CID_i, X_i))^d \bmod n \quad (11)$$

(3) 인증서버로부터 메시지 M_3를 수신한 스마트카드는 $M_3^e = h(CID_i, X_i) \bmod n$ 이 유효한지 검증한다. 만약 등식이 성립한다면 사용자의 스마트카드는 성공적으로 인증서버를 인증한다.

2. Liu 등의 인증 스킴에 대한 안전성 분석

Liu 등의 인증 스킴에 대한 안전성을 분석하기 위해, 저자는 스마트카드에 저장된 정보들이 전력소비를 모니터링함으로 불법적으로 추출될 수 있고, 이에 따라 사용자와 인증서버가 상호 통신하는 메시지들도 가로채기를 당할 수 있음을 가정한다[13,14]. Liu 등의 인증 스킴은 다음에 기술할 다양한 공격 가능성에 노출되어 있고, 보안상 취약점을 내재하고 있다.

• 사용자 위장 공격

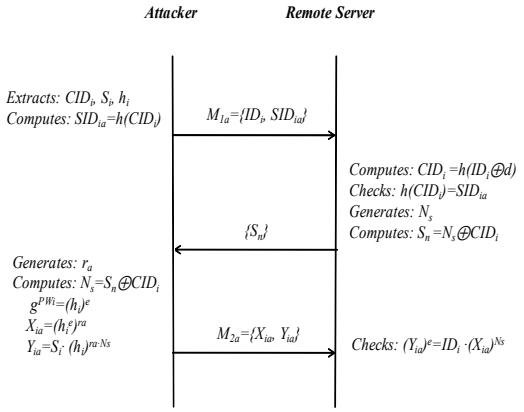

그림 1. 사용자 위장 공격
Fig 1. User Impersonation Attack

공격자가 적법한 사용자의 스마트카드로부터 비밀정보 값 CID_i, S_i, h_i를 추출한 경우, 그는 다음의 과정을 통해 사용자 위장 공격을 시도할 수 있다. 그림 1은 사용자 위장 공격을 수행하는 단계적 절차를 보여준다.

(1) 공격자는 식 (12)를 계산하여 인증서버에게 위조된 메시지 $M_{1a} = \{ID_i, SID_{ia}\}$를 전송한다.

$$SID_{ia} = h(CID_i) \quad (12)$$

(2) 메시지 M_{1a}를 수신한 인증서버는 식 (13)으로부터 CID_i를 계산하고 나서, 수신한 SID_{ia}와 계산 값 $h(CID_i)$를 비교하여 같으면 로그인 요청을 받아들인다. 따라서 인증서버는 식 (14)로부터 S_n을 계산하여 공격자에게 넘겨주게 된다.

$$CID_i = h(ID_i \oplus d) \quad (13)$$
$$S_n = N_s \oplus CID_i \quad (14)$$

(3) 자연스럽게 S_n을 받은 공격자는 적법한 사용자의 패스워드 없이 아래의 4개의 식 (15), (16), (17), (18)에 의해 위조된 로그인 요청 메시지 $M_{2a} = \{X_{ia}, Y_{ia}\}$를 계산하여 인증서버 S에게로 전송할 수 있게 된다.

$$N_s = S_n \oplus CID_i \quad (15)$$
$$g^{PW_i} = (h_i)^e \bmod n \quad (16)$$
$$X_{ia} = (h_i^e)^{r_a} \bmod n \quad (17)$$
$$Y_{ia} = S_i \cdot h_i^{r_a \cdot N_s} \bmod n \quad (18)$$

여기서 r_a는 공격자에 의해 생성된 랜덤 수이다.

(4) 메시지 M_{2a}를 수신한 인증서버 S는 $Y_i^e = ID_i \cdot X_i^{Ns} \bmod n$ 이 성립하는지 확인한다. 만약 값이 같으면 공격자는 인증서버에 의해 합법적인 사용자로 인증을 받게 된다.

• 패스워드 추측 공격

일반적으로 대부분의 사용자들은 편리성 때문에 쉽게 기억되는 패스워드를 선택하는 경향이 짙다. 그러므로 스마트카드를 이용하는 다수의 인증 스킴들이 잠재적으로 패스워드 추측 공격을 언제든지 받을 수 있다. 패스워드 추측 공격자는 적법한 사용자의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 비밀정보 h_i를 빼낼 수 있다고 가정한다. 일단 공격자가 h_i를 획득하게 되면 해당 사용자의 패스워드 PW_i를 어렵지 않게 찾아낼 수 있다. 이러한 off-line 패스워드 추측 공격은 다음 과정을 통해 시도 된다.

(1) 공격자는 등록 단계에서 추측한 패스워드 PW_i^* 를 적용하여 식 (19)를 계산한다.

$$(h_i)^e = g^{PWi^*} \bmod n \quad (19)$$

(2) 공격자는 계산의 결과를 통해 PW_i^*가 사용자의 패스워드와 일치하는 지를 확인한다.

(3) 공격자는 사용자의 정확한 패스워드를 찾기 위해 자신이 추측한 패스워드 PW_i^*를 계속 바꾸면서 위의 과정 (1)과 (2)를 반복하여 수행한다. 궁극적으로 공격자는 사용자의 올바른 패스워드 PW_i를 유도해낼 수 있다.

• 내부자 공격

인증서버로부터 인증을 받고자 하는 사용자는 등록 단계에서 자신의 패스워드를 KIC에 제출해야 한다. 만일 사용자의 패스워드 PW_i가 서버 시스템에 노출되어 있다면, 서버 담당 내부자가 곧바로 패스워드 PW_i를 얻게 된다. 그러므로 내부자가 보안 공격을 시도할 가능성이 열려있으며, 같은 패스워드를 사용하는 다른 서버의 사용자 계정들에 접근하여 적법한 사용자로 손쉽게 위장하는 것이 가능하다.

III. 개선된 상호인증 스킴 및 안정성 분석

1. 보안성 개선의 상호인증 스킴

본 장에서는 연구의 핵심 내용이 되는 사용자와 인증서버와의 상호인증을 보장하며, 다양한 공격 가능성을 차단 할 수 있도록 보안이 개선된 인증 스킴을 기술한다. 제안하는 인증 스킴은 초기화 단계, 등록 단계, 로그인 단계, 인증 단계로 구성된다. 초기화 단계는 전 장에서 이미 다룬 내용과 특이한 차이가 없어 생략하고 나머지 3 단계에 대하여 절차와 과정을 제시한다. 그림 2는 본 논문이 제안하는 인증 스킴의 로그인 단계와 인증단계를 보여준다.

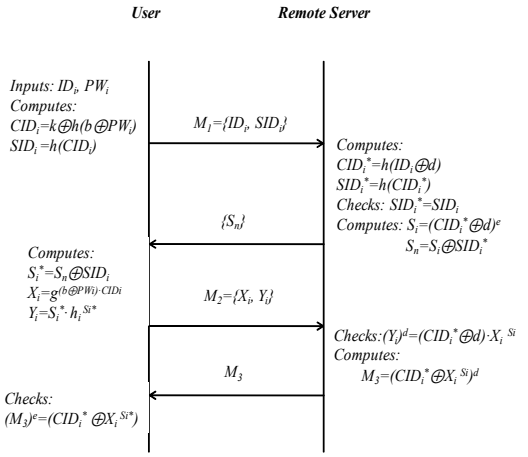

그림 2. 제안하는 스킴의 로그인 단계와 인증 단계
Fig 2. Login Phase and Authentication Phase of the Proposed Scheme

• 등록 단계

이 단계는 사용자 U_i가 KIC에 처음으로 등록하고자 할 때 수행된다. 사용자는 자신의 아이디 ID_i와 패스워드 정보 $h(ID_i\oplus PW_i)$를 안전한 경로를 통해 KIC에게 제출한다. 여기서 b는 사용자에 의해 선택된 랜덤 수이다. 등록단계에서 KIC는 다음 과정을 수행한다.

(1) KIC는 식 (20), (21), (22)로부터 스마트카드 아이디 CID_i와 사용자 비밀정보 k와 h_i를 계산한다.

$$CID_i = h(ID_i\oplus d) \quad (20)$$
$$k = CID_i\oplus h(b\oplus PW_i) \quad (21)$$
$$h_i = g^{h(b\oplus PWi)\cdot CIDi\cdot e} \bmod n \quad (22)$$

(2) KIC는 비밀정보에 해당하는 n, e, g, k, h_i를 저장한 스마트카드를 사용자에게 발급한다.

(3) 사용자 U_i는 새로운 스마트카드에 b를 저장하여 그 값을 별도로 기억할 필요가 없게 된다.

• 로그인 단계

이 단계는 사용자 U_i가 인증서버 S에 로그인 하려고 할 때 수행된다. 사용자 U_i는 자신의 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 로그인 단계에서 스마트카드는 다음 과정을 수행한다.

(1) 스마트카드는 식 (23)과 (24)로부터 SID_i를 계산하고 인증서버에게 메시지 $M_1 = \{ID_i, SID_i\}$를 전송한다.

$$CID_i = k\oplus h(b\oplus PW_i) \quad (23)$$
$$SID_i = h(CID_i) \quad (24)$$

(2) 메시지 M_1을 수신한 인증서버는 식 (25)와 (26)을 계산한다. 결과 값인 SID_i^*와 수신한 SID_i를 비교하여 값이 같으면 인증서버는 로그인 요청을 받아들인다.

$$CID_i^* = h(ID_i\oplus d) \quad (25)$$
$$SID_i^* = h(CID_i^*) \quad (26)$$

(3) 인증서버는 식 (27)과 (28)로부터 S_n을 계산하여 스마트카드에게 전송한다.

$$S_i = h(CID_i^*\oplus d)^e \quad (27)$$
$$S_n = S_i\oplus SID_i^* \quad (28)$$

(4) S_n을 수신한 스마트카드는 식 (29), (30), (31)에서 X_i와 Y_i를 계산하여, 메시지 $M_2 = \{X_i, Y_i\}$를 인증 서버로 전송한다.

$$S_i^* = S_n\oplus SID_i \quad (29)$$
$$X_i = g^{h(b\oplus PWi)\cdot CIDi} \bmod n \quad (30)$$
$$Y_i = S_i^*\cdot h_i^{Si*} \bmod n \quad (31)$$

• 인증 단계

이 단계는 인증서버 S가 사용자 U_i의 로그인 요청을 수신하여 인증을 하고자 할 때 수행된다. 인증요청 메시지 M_2를 수신한 인증 서버와 스마트카드는 사용자와 인증서버 간 상호인증을 위해 다음 과정을 수행한다.

(1) 인증서버는 $(Y_i)^d = (CID_i^*\oplus d)\cdot X_i^{Si} \bmod n$ 이 성립하는지 확인한다. 만약 양쪽의 값이 같으면 인증서버는 성공적으로 스마트카드를 인증한다.

(2) 상호인증을 수행하기 위해 인증서버는 식 (32)와 같이 메시지 M_3를 계산하여 스마트카드에 전송한다.

$$M_3 = (CID_i^*\oplus X_i^{Si})^d \bmod n \quad (32)$$

(3) 인증서버로부터 메시지 M_3를 수신한 스마트카드는 $(M_3)^e = (CID_i^*\oplus X_i^{Si}) \bmod n$ 이 유효한지 검증한다.

만약 등식이 성립한다면 사용자의 스마트카드는 성공적으로 인증서버를 인증한다.

2. 안전성 분석 및 결과 비교

여기서는 본 논문이 제안하는 인증 스킴의 안전성을 분석하고 Liu 등의 스킴과 보안 특성을 비교한다. 그리하여 제안하는 스킴이 앞 장에서 기술한 바 있는 몇 가지 공격과 상호인증의 관점에서 드러난 Liu 등의 인증 스킴 보안 문제를 개선한 효율적인 인증 스킴임을 입증한다. 저자가 제시하는 개선된 상호인증 스킴의 안전성 분석은 기본적으로 단방향 해쉬 함수와 공개키 암호시스템에 기초한다.

• 사용자 위장 공격

공격자는 적법한 사용자로 위장하기 위하여 인증 서버에 의해 인증을 획득할 수 있는 위조된 로그인 요청 메시지를 고안하려고 시도한다. 제안하는 스킴에서는 공격자는 사용자의 스마트카드로부터 저장된 비밀 정보 (k, h_i)를 추출하고 사용자와 인증서버 간 전송되는 메시지 (M_1, M_2, M_3, S_n)을 도청한다고 할지라도 위조된 로그인 요청 메시지를 만드는 것이 불가능하다. 인증서버 쪽에 숨겨있는 비밀키 d 를 알지 못하고서는 인증서버로 보내지는 메시지 (M_{1a}, M_{2a})를 성공적으로 계산하여 위조할 수 없기 때문이다. 그러므로 개선된 인증 스킴에서 사용자 위장 공격을 통한 공격자의 로그인 시도는 그 목적을 달성할 수 없게 된다.

• 패스워드 추측 공격

사용자의 스마트카드에서 불법적으로 획득한 비밀정보 (k, h_i)를 사용하여 공격자는 등록단계에서 반복적으로 $k = CID_i \oplus h(b \oplus PW_i)$ 를 계산하는 방법으로 사용자의 패스워드 PW_i를 추측하여 찾아내려고 시도할 것이다. 그러나 공격자는 서버에 저장된 비밀키 d를 여전히 모르기 때문에 사용자 패스워드 PW_i를 추측할 방법이 없게 된다. 따라서 개선된 인증 스킴은 오프라인 패스워드 추측 공격을 견디어 낼 수 있다.

• 내부자 공격

사용자의 패스워드 PW_i가 등록단계에서 인증서버에 노출되어 지면, 서버 측 내부자는 손쉽게 사용자 패스워드 PW_i를 획득하여 같은 패스워드를 이용하는 다른 서버의 사용자 계정에 접근하는 것이 가능해진다. 그러나 개선된 스킴은 이러한 내부자 공격의 취약점을 해결 할 수 있다. 사용자가 서버에 패스워드 PW_i를 대신하여 사용자 패스워드 정보인 $h(b \oplus PW_i)$를 제출하기 때문에 서버 측의 내부 공격자가 곧바로 사용자 패스워드 PW_i를 취득할 수 없기 때문이다.

• 상호인증

앞에서 나타난 공격에 노출될 수 있는 보안 취약점을 해결하는 과정에서 살펴본 것처럼, 제안하는 인증 스킴은 사용자와 인증 서버가 서로를 인증해야만 하는 상호인증을 제공하고 있다. 인증 서버는 적법한 사용자를 검증할 수 있고, 사용자 또한 적법한 인증 서버를 확인할 수 있다. 공격자의 입장에서 적법한 사용자로 인증받기 위해 서버로 전송하는 로그인 요청 메시지 (M_{1a}, M_{2a})를 성공적으로 위조할 수 없을 뿐 아니라, 적법한 서버로 인증 받고자 사용자에게 보내는 응답 메시지 역시 위조하는 것이 불가능하다. 공격자가 사용자의 스마트카드의 비밀정보 (k, h_i)를 갖고 있다고 하더라도 서버의 비밀키 d의 값을 알아내지 않고는 상호 인증을 위한 해킹 목적을 달성할 수 없기 때문이다. 따라서 제안하는 스킴은 사용자와 인증 서버 간 상호인증이 보안상 위험없이 구현된 개선된 인증 스킴임을 확인할 수 있다.

표 2는 Liu 등의 스킴의 안전성 분석과 본 연구의 제안 스킴의 안전성 분석의 결과를 비교하여 요약한 내용이다. 표에서 나타난 바대로 제안하는 스킴이 상대적으로 Liu 등의 스킴보다 다양한 공격을 견디어 낼 수 있는 보다 안전한 보안 특성을 갖고 있음을 볼 수 있다. 한편, 사용자와 인증서버 상호간의 인증에 있어서도 제안하는 스킴은 상호인증을 투명하게 지원하는 개선된 인증 스킴으로 입증된다.

표 2. 안전성 분석 비교
Table 2. Comparison of Security Analysis

보안 특성	Liu 등의 스킴	제안 스킴
사용자 위장 공격	가능	불가능
패스워드 추측 공격	가능	불가능
내부자 공격	가능	불가능
상호인증	미제공	제공

IV. 결 론

본 논문은 Liu 등이 제시한 인증 스킴을 분석하고, 그들의 스킴에서 노출될 수 있는 보안 취약점을 해결하기 위한 개선된 인증 스킴을 제안하였다. Liu 등의 스킴은 Shen 등이 제기하였던 스킴보다 상대적으로 안전함에도 불구하고, 여전히 사용자 위조 공격, 패스워드 추측 공격, 그리고 내부자 공격에 따른 보안성 보장을 할 수 없다는 것을 본 연구는 밝혀내었다. 아울러, 본 논문에서 제안한 인증 스킴은 Liu 등의 스킴의 장점을 유지하면서, 이러한 보안상의 문제점을 극복하고 동시에 사용자와 인증서버 간의 상호인증을 제공하는 효율적인 스킴임을 입증하였다. 스마트카드의 비밀정보가 노출되는 경우에도, Liu 등의 스킴보다 보안 특성상 보다 안전하다는 사실을 안전성 분석을 통해 제시함으로, 본 논문은 기존의 스마트카드 기반 상호인증 스킴의 보안 연구에 기여할 것으로 기대한다.

참고 문헌

[1] W. H. Yang, and S. P. Shieh, “Password Authentication with Smart Card”, Computers and Security, Vol. 18, No. 8, pp. 727-733, 1999.

[2] J. J. Shen, C. W. Lin, and M. S. Hwang, “Security Enhancement for Timestamp-based Password Authentication Scheme Using Smart Cards”, Computers and Security, Vol. 22, No. 7, pp. 591-595, 2003.

[3] S. T. Wu, and B. C. Chieu, “A User Friendly Remote Authentication Scheme with Smart Cards”, Computers and Security, Vol. 22, No. 6, pp. 629-631, 2003.

[4] M. L. Das, A. Sxena, and V. P. Gulathi, “A Dynamic ID-based Remote User Authentication Scheme”, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 629-631, 2004.

[5] H. Y. Chien, and C. H. Chen, “A Remote Password Authentication Preserving User Anonymity”, Proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA '05), 2005.

[6] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, “Attack on the Shen et al.'s Timestamp-based Password Authentication Scheme Using Smart Cards”, IEICE Transactions on Fundamentals E88-A (1), pp. 319-321, 2005.

[7] 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, 2006.

[8] C. S. Bindu, P. C. Reddy, and B. Satyanarayana, “Improved Remote User Authentication Scheme Preserving User Anonymity”, International Journal of Computer Science and Network Security, Vol. 8, No. 3, pp. 62-66, 2008.

[9] C. C. Chang, and C. Y. Lee, “A Friendly Password Mutual Authentication Scheme for Remote Login Network System”, International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 1, pp. 59-63, 2008.

[10] J. Y. Liu, A. M. Zhou, and M. X. Gao, “A New Authentication Scheme based on Nonce and Smart Cards”, Computer Communication, Vol. 31, pp. 2205-2209, 2008.

[11] M. Choi, T. Kim, S. Yeo, and E. Cho, “A Study on the Network Security Level Management”, Journal of Korean Institute of Information Technology, Vol. 7, No. 1, pp. 214-219, 2009.

[12] H Lee, and Y. Park, “A Design and Implementation of User Authentication System using Biometric Information”, Journal of Korea Academia-Industrial cooperation Society, Vol. 11, No. 9, pp. 3548-3557, 2010.

[13] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, Proceedings of Advances in Cryptology, pp. 388-397, 1999.

[14] T. S. Messerges, E. A. Dabbish, and R.H. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks”, IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, 2002.

저자 소개

주 영 도(정회원)

- 1983년 : 한양대학교 전자통신공학과 학사
- 1988년 : 미국 University of South Florida 컴퓨터공학과 석사
- 1995년 : 미국 Florida State University 전산학과 박사
- 1996년 ~ 2000년 : KT 통신망 연구소 선임 연구원
- 2000년 ~ 2005년 : 시스코 시스템즈 코리아 상무
- 2005년 ~ 2006년 : 화웨이 기술 코리아 부사장
- 2007년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수

<관심분야 : 정보보안, 네트워크 보안, 정보검색, 데이터베이스>