韓國컴퓨터情報學會 論文誌
第15卷 第2號, 2010. 2.

2010-15-2-3-4

스마트카드를 이용한 Hsiang-Shih의 원격 사용자 인증 스킴의 개선에 관한 연구

안 영 화*

Improvements of the Hsiang-Shih's remote user authentication scheme using the smart cards

An Young Hwa*

요 약

최근 Hsiang-Shih는 Yoon 등의 스킴[7]을 개선한 사용자 인증 스킴을 제안하였다[10]. 그러나 제안된 스킴은 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못한다. 본 논문에서는, Hsiang-Shih가 제안한 스킴은 off-line 패스워드 추측공격에 취약함을 보였다. 즉, 공격자가 사용자의 스마트카드를 훔치거나 일시적으로 접근하여 그 안에 저장된 정보를 추출하여 사용자의 패스워드를 알아낼 수 있음을 보였다. 또한 이와 같은 문제점들을 해결한 해쉬함수와 난수에 기반한 개선된 사용자 인증스킴을 제안하였다. 제안한 인증 스킴은 패스워드 추측공격, 위조 및 위장공격이 불가능함을 알 수 있었다. 그리고 사용자와 서버가 상대방을 인증할 수 있는 효율적인 상호 인증방식을 제시하였다.

Abstract

Recently Hsiang-Shih proposed the user authentication scheme to improve Yoon et al's scheme. But the proposed scheme has not been satisfied security requirements considering in the user authentication scheme using the password based smart card. In this paper, we proved that Hsiang-Shih's scheme is vulnerable to the off-line password guessing attack. In other words, the attacker can get the user's password using the off-line password guessing attack on the scheme when the attacker steals the user's smart card and extracts the information in the smart card. Also, the improved scheme based on the hash function and random number was introduced, thus preventing the attacks, such as password guessing attack, forgery attack and impersonation attack etc. And we suggested the effective mutual authentication scheme that can authenticate each other at the same time between the user and server.

▸ Keyword : 사용자 인증(User Authentication), 스마트카드(Smart Card), 패스워드 추측공격(Password Guessing Attack), 위조공격(Forgery Attack)

• 제1저자 : 안영화
• 투고일 : 2010. 02. 02, 심사일 : 2010. 02. 11, 게재확정일 : 2010. 02. 22.
* 강남대학교 컴퓨터미디어정보공학부 교수
※ 본 연구는 2008학년도 강남대학교 교내연구비 지원에 의해 이루어짐.

Ⅰ. 서 론

최근 네트워크 기술의 발달과 함께 컴퓨터 및 휴대폰 등을 이용하여 언제 어디서나 다양한 인터넷 서비스를 제공받고자 하는 사용자가 증가하고 있다. 인터넷 서비스 제공자는 아무에게나 정보를 제공하는 것이 아니라 합법적인 사용자에게 정보를 제공하려고 할 것이다.

사용자 인증 프로토콜이란 서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 사용자와 서버라는 검증을 수행하는 프로토콜이다[1-12]. 이와 같은 프로토콜에 의하여 사용자는 사전에 서비스를 제공하는 서버에 미리 자신의 신원을 확인받을 수 있는 정보를 등록하고, 정당한 사용자임을 검증받고 서비스를 제공 받고 싶을 때 언제 어디서나 서버가 제공하는 서비스를 이용할 수 있다.

1981년에 Lamport는 암호화 기법을 사용하지 않은 패스워드 기반의 원격 사용자 인증 스킴을 처음으로 제안하였다[1]. 그 이후 다수의 스킴이 안전성, 또는 효율을 개선하기 위해 제안되었다[2-3]. 그러나 이들 스킴들의 공통된 특징은 검증 테이블이 서버에 안전하게 저장되어 있어야 한다. 만약 검증 테이블이 공격자에 의해 노출된다면, 이 시스템은 부분적으로 또는 전부 파괴될 것이다. 이 후로 이와 같은 문제점들을 해결한 스마트카드에 기반한 인증 스킴들이 제안되었다[4-10,13-14]. 2002년에 Chien 등은 효율적인 패스워드 기반 원격 사용자 인증 스킴을 제안하였다[4]. 이 스킴은 상호 인증을 제공하고 검증 테이블이 불필요하고 자유로이 패스워드를 변경할 수 있으며, 그리고 오직 소수의 해쉬 연산을 수행하였다. 그러나 2004년에 Ku-Chen은 Chien 등이 제안한 스킴은 반사공격(reflection attack), 내부자 공격(insider attack)에 취약함을 지적하고 이들을 개선한 스킴을 제안하였다[6]. 또한, Yoon 등은 개선된 스킴이 여전히 병렬 세션 공격(parallel session attack)이 의심되며, 패스워드 변경 단계에서 사용자 패스워드 변경이 안전하지 못한 것을 지적하고 개선된 스킴을 제시하였다[7]. 그 후에 2008년에 Hsiang-Shih는 Yoon 등의 스킴이 Duan 등이 기술한 병렬 세션 공격에 취약하고[8]. 위장 공격(masquerading attack), 그리고 패스워드 추측 공격(password guessing attack)에도 취약함을 보였으며, 이들 문제점들을 개선한 효율적인 스킴을 제안하였다[10].

본 논문에서는 Hsiang-Shih이 제안한 개선된 스킴도 여전히 패스워드 추측 공격 및 위조 공격(forgery attack)에 취약함을 제시하였다. 즉, 공격자가 사용자의 스마트카드에 불법적으로 접근할 수 있다면 스마트카드에 저장된 정보를 추출함으로서 패스워드 추측과 함께 합법적인 시스템 사용자로 가장할 수 있다. 그러므로 Hsiang-Shih의 스킴은 스마트카드 기반 인증 시스템이 갖춰야 하는 안전성 요구사항을 만족하지 못 한다. 또한 본 논문에서 제안된 스킴은 Hsiang-Shih이 제안한 스킴의 특성을 그대로 유지하면서, 이와 같은 문제점들을 개선한 스마트카드 기반 인증 시스템을 제안하였다.

본 논문의 구성은 다음과 같다. 제Ⅱ장과 Ⅲ장에서는 Hsiang-Shih이 제안한 스마트카드를 이용한 원격 사용자 인증 스킴을 기술하고, 안전성을 분석하였다. 제Ⅳ장과 Ⅴ장에서는 개선된 Hsiang-Shih의 인증 스킴을 제안하고, 안전성을 분석하였다. 그리고 Ⅵ장에서 결론을 맺는다.

Ⅱ. Hsiang-Shih의 인증 스킴

본 장에서는 Hsiang-Shih이 제안한 스마트카드를 이용한 원격 사용자 인증 스킴[10]을 간략히 기술한다. 이 스킴은 등록 단계, 로그인 단계, 그리고 인증 단계로 구성된다.

2.1 등록 단계

이 단계는 사용자 U가 서버 S에 등록하거나 재등록할 때 수행된다. 여기서 n은 U가 S에 재등록한 횟수를 나타낸다.

(1) U는 랜덤 값 b를 선택하고, 패스워드 PW를 이용하여 해쉬값 $h(b \oplus PW)$를 계산한다.
(2) U는 S에게 ID, $h(PW)$, $h(b \oplus PW)$를 전송한다.
(3) 만약 U가 초기 등록이라면, S는 U를 위한 계정 데이터베이스를 생성하고 n=0을 저장한다. 그렇지 않다면, S는 n=n+1로 U를 위해 항목을 변경한다. 그리고 S는 다음 계산을 수행한다.

$$P=h(EID \oplus x),$$
$$R=P \oplus h(b \oplus PW),$$
$$V=h(P \oplus h(PW)) \quad \cdots\cdots (2.1)$$

여기서, $EID=(ID \| n)$이다.

(4) S는 U에게 V, R, 그리고 h()이 저장된 스마트카드를 발급한다.
(5) U는 b를 스마트카드에 저장한다.

2.2 로그인 단계

이 단계는 U가 S에게 로그인을 요청할 때마다 수행된다.

(1) U는 스마트카드를 스마트카드 리더에 넣고 ID와 PW를 입력한다.
(2) U의 스마트카드는 다음 계산을 수행한다.

$C1=R \oplus h(b \oplus PW)$,

$C2=h(C1 \oplus Tu)$ ····· (2.2)

여기서, Tu는 U의 현재 타임스탬프이다.
(3) U는 S에게 C={ID, Tu, C2}를 송신한다.

2.3 검증 단계

인증요청 메시지 {ID, Tu, C2}을 수신한 후에 원격 시스템 및 스마트카드는 다음을 수행한다.

(1) 만약 ID 또는 Tu가 유효하지 않거나, 또는 $Ts-Tu \leq 0$ 이면, S는 U의 로그인 요청을 거절한다. 그렇지 않다면 S는 C2′을 계산한다.

$C2'=h(h(EID \oplus x) \oplus Tu)$ ····· (2.3)

만약 C2′=C2 이면 S는 U의 로그인 요청을 받아들이고, S의 타임스탬프 Ts를 이용하여 C3를 계산한다.

$C3=h(h(EID \oplus x) \oplus Ts$ ····· (2.4)

(2) S는 U에게 Ts, C3를 전송한다.
(3) 만약 Ts가 유효하지 않거나 Ts=Tu이면 U는 이 세션을 종료한다. 그렇지 않다면 U는 C3′를 계산한다.

$C3'=h(C1 \oplus h(Ts))$ ····· (2.5)

수신된 C3과 C3′를 비교하여 같으면 U는 성공적으로 S를 인증한다.

III. Hsiang-Shih 인증 스킴의 안전성 분석

본 장에서는 스마트카드 기반 사용자 인증 스킴의 안전성을 분석하기 위하여 공격자는 다음과 같은 공격능력을 갖고 있다고 가정한다.

(1) 공격자는 서버와 사용자간에 통신하는 과정(로그인 단계 및 인증 단계)을 모두 통제할 수 있다. 다시 말하면 공격자는 서버와 사용자간에 전달되는 메시지의 내용을 도청, 삭제, 수정, 또는 첨가 할 수 있다.
(2) 공격자는 사용자의 스마트카드 안에 저장되어 있는 내용을 추출하거나 또는 사용자의 패스워드를 획득할 수 있다.

따라서 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴의 안전성은 다음 두 가지 상황 중 한 가지만 발생할 때 그 안전성을 보장해야 한다. 만일 두 가지 상황이 모두 발생했을 때는 패스워드를 기반으로 하는 스마트카드를 이용한 어떤 사용자 인증 스킴도 그 안전성을 보장 받을 수 없다.

- 사용자의 스마트카드가 분실된다.
- 사용자의 패스워드가 노출된다.

본 장에서는 Hsiang-Shih 인증 스킴에 대해서 패스워드 추측공격(*password guessing attack*) 측면에서 안전성을 분석한다.

Kocher와 Messerges가 제안한 논문[11-12]에서 그들은 스마트카드 안에 저장된 정보를 전력소비 공격 등을 이용해서 추출할 수 있다고 주장하였다. 이런 사실에 근거하여 사용자의 스마트카드를 획득하여 그 안에 저장된 정보를 추출한 공격자는 이를 이용하여 사용자의 패스워드를 알아낼 수 있는 패스워드 추측공격을 수행할 수 있다.

본 장에서는 Hsiang-Shih이 제안한 인증 스킴이 공격자가 사용자의 패스워드를 알아낼 수 있는 패스워드 추측공격에 취약함을 보인다. 이 공격을 수행하기 위해 공격자 Ua는 사용자 U의 스마트카드에 일시적으로 접근하여 그 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다. 사용자 U의 스마트카드로부터 V, R과 b를 추출한 공격자 Ua는 사용자 U의 패

스워드를 알아낼 수 있다. 그 수행과정은 다음과 같다.

단계 1. 평상시와 다름없이 인증서버에 로그인하기 위한 사용자 U는 C1, C2를 계산하고 로그인 요청 메시지 {ID, Tu, C2}를 인증서버에 전송한다.

단계 2. 이때를 기다리고 있던 공격자 Ua는 사용자 U의 로그인 메시지를 가로채서 Tu,와 C2를 획득한다.

단계 3. 마침내 공격자 Ua는 오프라인(off-line) 패스워드추측 공격을 사용해서 U의 패스워드를 알아낼 수 있다.

(1) 공격자 Ua는 사용자 U의 패스워드를 PW′로 추측한다.

(2) $C1' = R \oplus h(b \oplus PW')$, $C2' = h(C1' \oplus Tu,)$를 계산한다.

(3) C2′와 C2가 동일한 값을 갖는 지를 확인한다.

(4) 공격자는 자신이 추측한 PW′가 (3)의 조건을 만족할 때까지 (1), (2), 그리고 (3) 세 개의 과정을 차례로 반복 수행한다. 만족하면 반복 수행을 멈춘다.

결국 (3)의 조건을 만족하는 PW′가 발견되면, 이 패스워드가 사용자 U의 올바른 패스워드가 된다. 이와 같이 Hsiang-Shih이 제안한 스마트카드를 이용한 사용자 인증 스킴은 오프라인 패스워드 추측 공격 방식을 이용하면 사용자의 패스워드를 알아 낼 수 있기 때문에 안전성에 취약하다는 것을 알 수가 있다.

IV. 개선된 Hsiang-Shih의 인증 스킴

본 장에서는 랜덤값을 이용하여 Hsiang-Shih의 인증 스킴을 개선하였다. 제안된 스마트카드를 이용한 원격사용자 인증 스킴은 Hsiang-Shih의 인증 스킴의 특성을 유지하면서 III장에서 기술된 안전성 문제점을 해결할 수 있다. 제안된 스킴은 그림 1과 같이 등록 단계, 로그인 단계, 그리고 인증 단계로 구성된다.

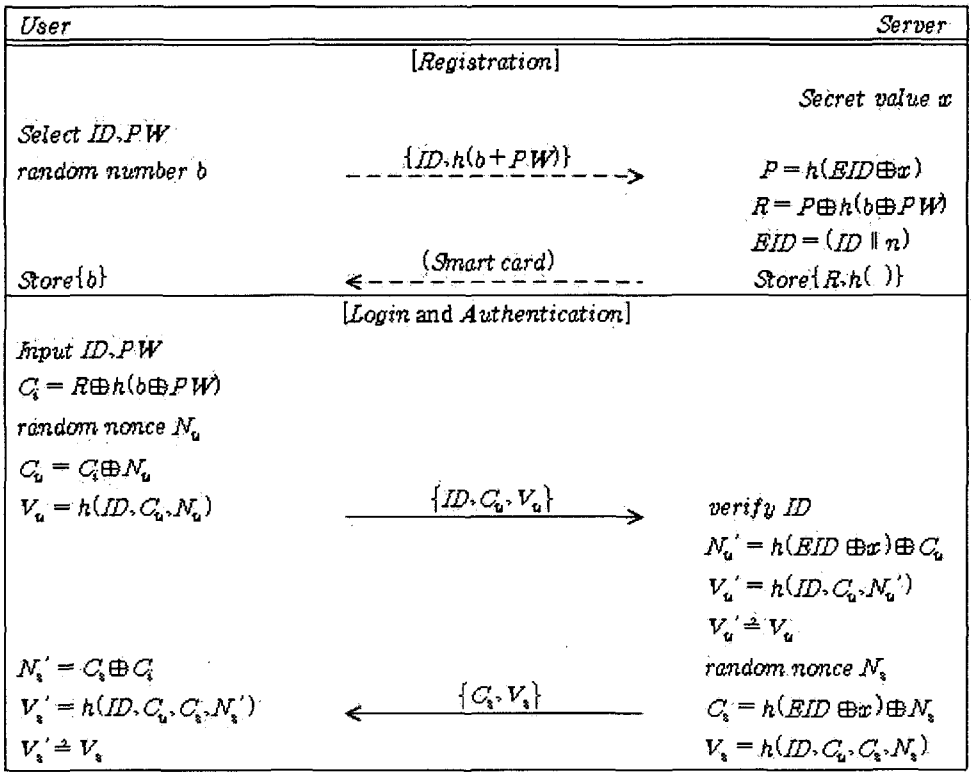

그림 1. 제안한 인증 스킴
Fig 1. The proposed authentication scheme

4.1 등록 단계

이 단계는 사용자 U가 서버 S에 등록하거나 재등록할 때 수행된다. 여기서 n은 U가 S에 재등록한 횟수를 나타낸다.

(1) U는 랜덤 값 b를 선택하고, 패스워드 PW를 이용하여 해쉬값 h(b⊕PW)를 계산한다.
(2) U는 S에게 ID, h(b⊕PW)를 전송한다.
(3) 만약 U가 초기 등록이라면, S는 U를 위한 계정 데이터베이스를 생성하고 n=0을 저장한다. 그렇지 않다면, S는 n=n+1로 U를 위해 항목을 변경한다. 그리고 S는 다음 계산을 수행한다.

$$P=h(EID \oplus x),$$

$$R=P \oplus h(b \oplus PW) \quad \cdots\cdots (4.1)$$

여기서, EID=(ID ‖ n)이다.
(4) S는 U에게 R 그리고 h()이 저장된 스마트카드를 발급한다.
(5) U는 b를 스마트카드에 저장한다.

4.2 로그인 단계

이 단계는 U가 S에게 로그인을 요청할 때마다 수행된다.

(1) U는 스마트카드를 스마트카드 리더에 넣고 ID와 PW를 입력한다.
(2) U의 스마트카드는 다음 계산을 수행한다.

$$Ci=R \oplus h(b \oplus PW),$$

$$Cu=Ci \oplus Nu,$$

$$Vu=h(ID, Cu, Nu) \quad \cdots\cdots (4.2)$$

여기서, Nu는 스마트카드에 의해 선택된 랜덤수이다.
(3) U는 S에게 메시지 Mu={ID, Cu, Vu}를 송신한다.

4.3 검증 단계

원격 시스템 S 및 스마트카드는 인증요청 메시지 {ID, Cu, Vu}을 수신한 후에 다음을 수행한다.

(1) 만약 ID가 유효하지 않다면 S는 U의 로그인 요청을 거절한다. 그렇지 않다면 S는 Nu', Vu'를 계산한다.

$$Nu'=h(EID \oplus x) \oplus Cu$$

$$Vu'=h(ID, Cu, Nu') \quad \cdots\cdots (4.3)$$

만약 Vu'=Vu이라면 S는 U를 인증하고 로그인 요청을 받아들인다.
(2) 그런 다음 S는 생성된 랜덤 값 Ns를 생성하여 Cs와 Vs를 계산한다.

$$Cs=h(EID \oplus x) \oplus Ns$$

$$Vs=h(ID, Cu, Cs, Ns) \quad \cdots\cdots (4.4)$$

(3) S는 U에게 메시지 Ms={Vs, Cs}를 전송한다.
(4) 서버 인증요청 메시지 {Vs, Cs}를 수신한 사용자 스마트카드는 Ns'과 Vs'를 계산한다.

$$Ns'=Cs \oplus Ci$$

$$Vs'= h(ID, Cu, Cs, Ns') \quad \cdots\cdots (4.5)$$

만약 Vs'=Vs이면 U는 성공적으로 S를 인증한다.

V. 제안한 스킴의 안전성 분석

본 장에서는 본 논문에서 제안한 원격 사용자 인증 스킴에 대해서 패스워드 추측공격(password guessing attack)과 위조공격(forgery attack)/위장공격(masquerading attack) 측면에서 안전성을 분석한다.

5.1 패스워드 추측공격

본 논문에서 제안된 인증 스킴에서 패스워드를 획득할 수 있는 방법은 공격자가 사용자의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 정보를 추출하고 합법적인 사용자의 메시지를 도청함으로써 오프라인 패스워드 추측공격을 수행하는 것이다. 즉, 메시지 Mu={ID, Cu, Vu}와 Ms={Vs, Cs}, 그리고 스마트카드 저장 정보 R, h(), b로부터 패스워드를 추측하는 것이다. 그러나 이들 정보로부터 패스워드를 추

측하는 것은 해쉬함수의 일방향성, 그리고 random nonce의 일회성 값 때문에 불가능하다.

5.2 위조공격/위장공격

본 논문에서 제안된 인증 스킴에서 공격자가 합법적인 사용자로 위장하기 위해서는 아이디와 패스워드를 알아야 한다. 사용자의 아이디는 공개된 정보이기 때문에 쉽게 알 수 있지만 사용자의 패스워드는 앞 절에서 기술한 바와 같이 패스워드 추측공격이 불가능하다. 즉, 공격자는 획득가능한 모든 정보를 사용하더라도 Cu, Vu, 그리고 Vs, Cs를 생성할 수 없으므로 위조정보에 의한 위장공격이 불가능하다.

5.3 기타 공격

메시지 재전송 공격(replay attack)은 이전 세션의 메시지를 다음 세션에서 재전송하는 방법으로서 불법적인 사용자가 인증을 시도하는 공격이다. 본 논문에서 제안된 인증 스킴에서는 매 세션마다 새로운 랜덤 값을 사용하기 때문에 공격자는 이전 세션의 정보와 현재 세션의 정보들로부터 인증 및 검증 정보를 유추할 수 있는 방법이 없다.

또한, 서버의 비밀키 추측공격도 불가능하다. 이것은 공격자가 획득한 정보로부터 서버의 비밀키에 관한 정보를 유추하는 것으로서 해쉬함수의 일방향성 때문에 불가능하다.

5.4 안전성 비교분석

본 절에서는 사용자 인증 스킴의 안전성을 검토하기 위하여, 본 논문에서 제안한 인증 스킴과 Hsiang-Shih이 제안한 인증 스킴을 비교분석하였다.

표 1. 안전성 분석
Table 1. Analysis of security

스킴	패스워드 추측 공격	위조/위장 공격	재전송 공격	비밀키 추측 공격	상호 인증
Hsiang-Shih 스킴	가능	가능	불가능	불가능	가능
제안한 스킴	불가능	불가능	불가능	불가능	가능

표 1에서 제시된 바와 같이, Hsiang-Shih의 인증스킴은 일부 공격에 취약함을 알 수 있고, 본 논문에서 제안한 인증스킴은 이와 같은 문제점들을 해결한 개선된 인증스킴임을 알 수 있었다.

VI. 결론

스마트카드를 이용한 사용자 인증 스킴은 공격자가 사용자의 스마트카드 내부에 저장된 정보를 추출하여도 그 정보를 이용하여 사용자의 패스워드를 추출하는데 이용하거나 사용자 또는 서버로 위장 할 수 없도록 설계되어야 한다.

본 논문에서는 Hsiang-Shih에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴이 off-line 패스워드 추측공격에 취약함을 지적하였다. 즉, 공격자가 사용자의 스마트카드에 저장된 정보를 추출한 후 그것을 이용하여 사용자의 패스워드를 알아낼 수 있음을 보였다. 또한 본 논문에서는 이와 같은 문제점들을 해결한 해쉬함수와 난수에 기반한 개선된 사용자 인증 스킴을 제안하였다. 제안한 사용자 인증 스킴은 패스워드 추측공격이 불가능하고, 위조 및 위장공격 등도 불가능함을 알 수 있었다. 그리고 사용자와 서버가 상대방을 인증할 수 있는 효율적인 상호 인증방식을 제시하였다.

따라서 본 논문에서 제안한 스킴은 기존의 스마트카드 기반 사용자 인증 스킴의 장점을 유지하면서 이 방식들의 문제점들을 효율적으로 해결할 수 있을 것으로 기대한다.

참고문헌

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, 24(11), pp. 770-772, 1981.

[2] R.E. Lennon, S.M. Matyas, C.H. Mayer, "Cryptographic authentication of time-invariant quantities," IEEE Trans. Communication, COM-29, Vol. 6, pp. 773-777, 1981,

[3] S.M. Yen, K.H. Liao, "Shared authentication token secure against replay and weak key attack," Information Proceeding Letters,pp. 78-80, 1997.

[4] H.Y. Chien, J.K. Jan, Y.M. Tseng, "An efficient and practical solution to remote authentication using smart card," Computers & Security, 21 (4), pp. 372 - 375. 2002.

[5] C.W. Lin, J.J. Shen, and M.S. Hwang, "Security Enhancement for Optimal Strong-Password Authentication Protocol," ACM Operating Systems Review, 37 (2), 2003.

[6] S.M. Chen, W.C. Ku, "Weakness and improvements of an efficient password based remote user authentication

scheme using smart cards," IEEE Transactions on Consumer Electronics, 50(1), pp. 204-207, 2004.

[7] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Further improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, 50(2), pp. 612-614, 2004.

[8] X. Duan, J.W. Liu, Q. Zhang, "Security improvements on Chien et al.'s remote user authentication scheme using smart cards," IEEE International conference on Computational Intelligence and Security (CIS 2006), 2, pp. 1133-1135, 2006.

[9] 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,

[10] H.C Hsiang, W.K. Shih, "Weakness and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications, 32, pp. 649-652, 2009.

[11] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388 - 397, 1999.

[12] T.S. Messerges, E.A. Dabbish, R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, 51 (5), pp. 541 - 552, 2002.

[13] 신광철, "서비스거부공격에 안전한 OTP 스마트카드 인증 프로토콜," 한국컴퓨터정보학회논문지, 제12권, 제6호, 201-206쪽, 2007년 12월.

[14] 안영화, 이강호, "스마트카드를 이용한 사용자 인증 스킴의 안전성 분석," 한국컴퓨터정보학회논문지, 제14권, 제3호, 133-138쪽, 2009년 3월.

저 자 소 개

안 영 화

1990년 2월 : 성균관대학교 전자공학과 공학박사

1990년 ~ 현재 : 강남대학교 컴퓨터미디어 정보공학부 교수

관심분야 : 정보보호, 네트워크 보안