韓國컴퓨터情報學會 論文誌
第14卷 第3號, 2009. 3.

2009-14-3-3-3

스마트 카드를 이용한 사용자 인증 스킴의 안전성 분석

안 영 화*, 이 강 호**

Analysis to a Remote User Authentication Scheme Using Smart Cards

An Young Hwa *, Lee Kang Ho **

요 약

최근 Lin[7] 등은 자신이 선택한 패스워드와 스마트카드를 이용하여 원격지에 있는 사용자를 인증할 수 있는 스킴을 제안하였다. 그러나 제안된 스킴은 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못한다. 본 논문에서는, Lin 등이 제안한 스킴에서 공격자가 사용자의 스마트 카드를 훔치거나 일시적으로 접근하여 그 안에 저장된 정보를 추출하여 사용자의 패스워드를 알아낼 수 있음을 off-line 패스워드 추측 공격 방식을 이용하여 증명하였다. 또한 스마트 카드를 이용한 인증 스킴을 분석하기 위해 보안 요구사항을 제안하였고, 분석 결과 Lin 등에 의해 제안된 인증 스킴은 다수의 보안 요구사항들을 만족하지 못함을 알 수 있었다. 이를 개선한 방식으로서 사용자의 패스워드 검증자를 서버에 저장하지 않고 사용자와 서버가 동시에 상대방을 인증할 수 있는 상호 인증방식을 제시하였다.

Abstract

Recently Lin et al. proposed the remote user authentication scheme using smart cards. 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 showed that he can get the user's password using the off-line password guessing attack on the scheme when the adversary steals the user's smart card and extracts the information in the smart card. Also, we proposed the seven security requirements for evaluating remote user authentication schemes using smart card. As a result of analysis, in Lin et al.'s scheme we have found the deficiencies of security requirements. So we suggest the improved scheme, the mutual authentication scheme that does not store the user's password verifier in server and can authenticate each other at the same time between the user and server.

▸ Keyword : 사용자 인증(User Authentication), 스마트카드(Smart Card), 오프라인 패스워드 추측 공격(Off-line password pre-computation attack)

• 제1저자 : 안영화
• 투고일 : 2009. 1. 30, 심사일 : 2009. 2. 11, 게재확정일 : 2009. 3. 20.
* 강남대학교 컴퓨터미디어정보공학부 교수 ** 국립한국재활복지대학 정보보안과 교수

Ⅰ. 서 론

최근 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.

서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 사용자와 서버라는 검증을 수행하는 것이 바로 사용자 인증 프로토콜이다. 이런 프로토콜에 근거하여 사용자는 사전에 서비스를 제공하는 서버에 미리 자신의 신원을 확인받을 수 있는 정보를 등록하고 정당한 사용자임을 검증받고 서비스를 제공 받고 싶을 때 마다 언제든지 어디서나 서버가 제공하는 서비스를 이용할 수 있다.

패스워드 기반의 스마트카드를 이용한 사용자 인증 스킴[1-4,6,9,10,12]의 특징은 원격지에 있는 사용자들이 자신이 기억하고 있는 패스워드와 스마트카드를 이용하여 인증서버로부터 정당한 사용자임을 인증 받을 수 있다. 스마트카드는 마이크로프로세서와 메모리를 내장하고 있어서 카드 내에서 정보의 저장과 처리가 가능한 플라스틱 카드로서 사용자로부터 입력받은 정보를 이용하여 사용자의 로긴 요청 메시지를 생성하여 사용자를 인증하는 인증서버로 전송한다. 인증서버와 사용자의 스마트카드는 서로 상대방의 신원 확인과정을 마친 후 상대방이 정당한 통신 상대자임을 검증받고 비로소 안전한 통신을 수행한다. 이러한 스킴을 이용하면 원격지에 있는 사용자는 보다 간편하고 안전하게 서버에 접근할 수 있다.

최근 Lin과 그의 동료들은 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴[7]을 제안하였다. 만일 공격자가 사용자의 스마트카드에 접근하여 그 내부에 저장된 정보를 추출할 수 있고 그 정보를 이용하여 사용자의 패스워드를 알아낼 수 있다면 그것은 패스워드 보안상 대단한 취약점이 될 것이다. 그러므로 스마트카드를 이용하여 사용자를 인증하는 스킴을 제안할 때 고려사항으로 스마트카드 내부에 저장되어 있는 정보가 노출된다고 할지라도 그것을 이용하여 공격자가 사용자인척 하거나 또는 서버인척 할 수 없도록 설계하여야 한다[11].

본 논문에서는 Lin 등이 제안한 스마트 카드를 이용한 사용자 인증 스킴 방식이 우리가 제안한 공격 방식에 취약하다는 것을 보여준다. 즉, 공격자가 사용자의 스마트카드 내부에 저장되어 있는 정보를 추출한 후 그 정보를 이용하여 사용자의 패스워드를 알아낼 수 있다는 것을 본 논문에서 제안한 방식인 off-line 패스워드 추측공격을 이용하여 증명하였다. 또한, 이와 같은 공격 방식에 대응할 수 있는 개선 방안을 제시하였다.

본 논문의 구성은 다음과 같다. 2장에서는 Lin 등에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴에 대하여 기술하고, 3장에서는 이 스킴에 대한 공격방식을 기술하고 안전성을 분석한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. Lin의 스마트 카드를 이용한 사용자 인증 스킴

Lin 등에 의해 제안된 인증 스킴[7]은 그림 1과 같이 사용자 등록과정, 그리고 인증 과정으로 이루어졌다.

2.1 사용자 등록과정

사용자 등록과정은 인증서버에 사용자가 등록하고자 할 때 오직 한번 수행된다. 등록과정이 수행되기 전에 인증서버는 시스템 파라미터로서 해쉬함수 h()와 암호학적 키 x를 선정한다. 서버의 비밀키인 x는 인증 서버가 비밀리 보관한다.

Step 1. 인증서버 S 에 등록하고자 하는 사용자 U_i 는 자신의 패스워드 PW_i와 임의의 nonce N_1을 선택하고 $Z_i = h(PW_i \| N_1)$를 계산하다. 사용자 U_i는 안전한 방법을 이용하여 인증서버로 (ID_i, Z_i, N_1)를 전송한다.

Step 2. 사용자의 로긴 요청 메시지가 도착하자마자 인증서버 S 는 $K_i = h(x \| ID_i) \oplus Z_i$를 계산하고 자신의 데이터베이스에 Z_i를 저장한다. 인증서버 S는 사용자 U_i 에게 $(N_1, K_i, h(\cdot))$이 저장되어 있는 스마트카드를 제작하여 발급한다.

2.2 인증 과정

인증과정은 원격지에 있는 사용자가 인증서버에 로그인할 때마다 동작한다. 사용자 U_i 는 인증 서버로부터 발급받은 스마트카드와 자신의 아이디 ID_i와 패스워드 PW_i를 카드 리더기에 입력한다. 스마트카드는 사용자로부터 입력받은 값을 이용하여 다음 과정을 수행한다.

Step 1. 스마트카드는 사용자 U_i 의 패스워드 PW_i 를 이용하여 임의의 nonce N_2를 생성하고, $C_1 = K_i \oplus h(PW_i \| N_1)$, $C_2 = h(K_i) \oplus h(PW_i \|$

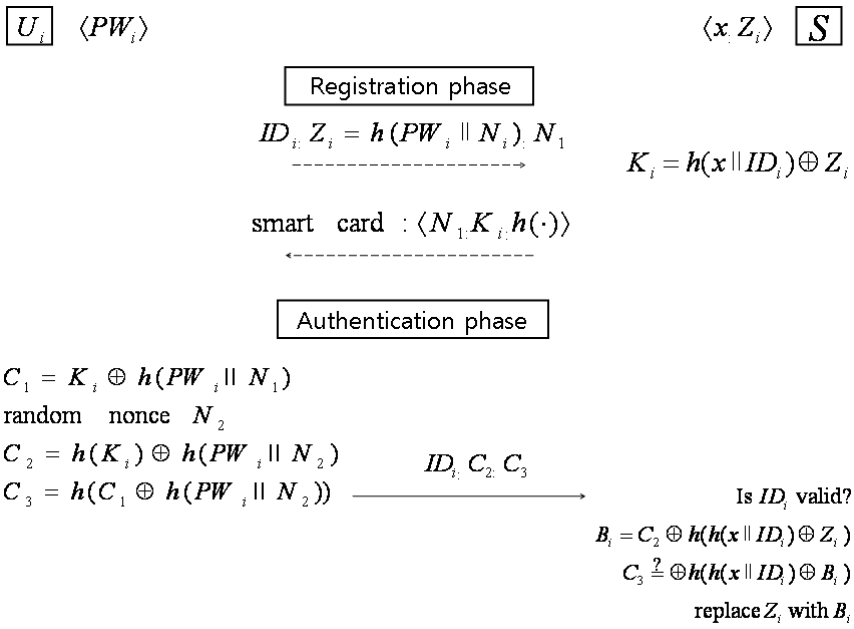

그림 1. Lin등이 제안한 사용자 인증 스킴
Fig. 1. User authentication scheme that Lin proposed

N_2), 그리고 $C_3 = h(C_1 \oplus h(PW_i \| N_2))$를 계산한다.

그런 다음 스마트카드는 사용자 U_i의 로긴 요청 메시지 (ID_i, C_2, C_3)를 인증서버 S 에게 전송한다.

Step 2. 사용자의 로긴 요청 메시지를 수신한 인증서버 S는 우선, $B_i = C_2 \oplus h(h(x \| ID_i) \oplus Z_i)$를 계산한다. 그 후에 사용자 U_i 의 정당성을 검증하기 위해 다음 과정을 수행한다.

- 사용자 U_i 의 아이디 ID_i가 정당한가?
- C_3가 $h(h(x \| ID_i) \oplus B_i)$와 일치하는가?

만일 위의 두 개의 조건을 모두 만족하면 인증서버 S 는 자신의 데이터베이스에 Z_i 대신 B_i를 저장하고 사용자 U_i의 시스템 접근을 허락한다. 반면 두 가지 중 하나의 조건이라도 만족하지 않으면 사용자 U_i의 로긴 요청을 거절한다.

III. 제안된 Lin의 사용자 인증 스킴에 대한 공격 방식 및 안전성 분석

Lin 등이 제안한 스마트카드를 이용한 인증 스킴을 이용하는 시스템에서 공격자가 수행 가능한 공격방식을 가정하면 다음과 같다[11].

- 공격자는 서버와 사용자간에 통신하는 과정(등록과정과 인증과정)을 모두 통제할 수 있다. 다시 말하면 공격자는 서버와 사용자간에 전달되는 메시지의 내용을 도청, 삭제, 또는 첨가 할 수 있다.
- 공격자는 사용자의 스마트카드 안에 저장되어 있는 내용을 추출할 수 있거나 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.

Kocher[5]와 Messerges[8]가 제안한 논문에서 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 수행하려 할 것이다. 이런 공격을 방지하기 위해서는 스킴을 설계할 때 사용자의 스마트카드 안에 저장된 정보가 노출되더라도 그것을 사용하여 사용자의 패스워드가 노출되지 않도록 설계하는 것이다.

Lin이 제안한 스마트카드를 이용한 사용자 인증 스킴은 본 논문에서 제안한 다음과 같은 공격 방법으로 사용자의 패스워드를 알아 낼 수 있음을 보여준다. 즉, 스마트카드를 분실하여 그 안의 정보를 획득할 수 있으면 스마트카드 사용자의 패스워드를 알아 낼 수 있다.

3.1 패스워드 추측공격

Lin과 그의 동료들이 제안한 사용자 인증 스킴은 공격자가 사용자의 패스워드를 알아낼 수 있는 패스워드 추측공격에 취약하다. 이 공격을 수행하기 위해 공격자 U_a는 사용자 U_i의 스마트카드에 일시적으로 접근하여 그 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다[5, 8]. 사용자 U_i의 스마트카드로부터 N_1과 K_i를 추출한 공격자 U_a는 사용자 U_i의 패스워드를 알아낼 수 있다. 그 과정은 다음과 같다.

Step 1. 평상시와 다름없이 인증서버에 로긴하기 위한 사용자 U_i는 C_1, C_2, 그리고 C_3를 계산하고 로긴 요청 메시지 (ID_i, C_2, C_3)를 인증서버에 전송한다.

Step 2. 그러나 이때를 기다리고 있던 공격자 U_a는 사용자 U_i의 로긴 메시지를 가로채서 C_2와 C_3를 획득한다.

Step 3. 마침내 공격자 U_a는 off-line 패스워드추측 공격을 사용해서 U_i의 패스워드를 알아낼 수 있는데 그 과정은 다음과 같다. 공격자는

(1) 사용자 U_i의 패스워드 PW_i로 PW_i'를 추측한다.

(2) $C_1' = K_i \oplus h(PW_i' \oplus N_1)$, $B_i' = C_2 \oplus h(K_i)$ 그리고 $C_3' = h(C_1' \oplus B_i')$를 계산한다.

(3) C_3'와 C_3가 동일한 값을 가지는지를 확인한다.

(4) 공격자는 자신이 추측한 PW_i'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_i'가 발견되면, 이 패스워드가 사용자 U_i의 올바른 패스워드이다.

이와 같이 Lin 등이 제안한 스마트카드를 이용한 사용자 인증 방식은 본 논문에서 제안한 방식인 off-line 패스워드 추측 공격 방식을 이용하면 사용자의 패스워드를 알아 낼 수 있기 때문에 안전성에 취약하다는 것을 알 수가 있다.

3.2 안전성 분석

스마트카드를 이용하여 사용자 인증을 수행하는 스킴은 사용자의 스마트카드가 분실 되더라도 그 스마트카드를 습득한 공격자는 사용자의 패스워드를 알 수 없기 때문에 그 안전성을 보장 받는다. 반대로 사용자의 패스워드를 입수한 공격자일지라도 사용자의 스마트카드를 획득하지 못하고서는 사용자 인척 할 수 없다. 그러므로 스마트카드를 이용한 패스워드 기반의 사용자 인증 메커니즘은 공격자가 사용자의 스마트카드와 패스워드를 모두 입수한 경우 어떠한 안전성도 보장 할 수 없다.

스마트 카드를 이용한 사용자 인증 스킴의 안전성을 분석하기 위해 다음과 같이 7가지 보안 요구사항을 제안한다.

Req.1 패스워드 또는 검증 테이블이 컴퓨터 내부에 저장되어 있지 않다.

Req.2 패스워드가 사용자에 의해 임의로 선택되고 바뀔 수 있다.

Req.3 프로토콜은 재생공격에 대해 보안대책을 제공해야야 한다.

Req.4 누구나 서버에 로그인하기 위해 합법적 사용자로 가장할 수 없다.

Req.5 누구나 인증 서버로 가장할 수 없다.

Req.6 프로토콜은 인증 서버와 사용자 사이에 상호 인증이 가능하다.

Req.7 패스워드는 스마트 카드를 분실한 경우라도 패스워드 추측공격에 깨어지지 않는다.

표 1. 사용자 인증 스킴들의 보안 요구사항 분석
Table 1. Comparison of security requirements between the previously published protocols

Requir e-ment	Chien et al.[13]	Das et al.[14]	Liao et al.[15]	Lin et al.[7]	Impro-v ed Protocol
Req.1	Yes	Yes	Yes	No	Yes
Req.2	Yes	Yes	Yes	Yes	Yes
Req.3	No	Yes	No	Yes	Yes

Req.4	Yes	No	No	No	Yes
Req.5	No	No	No	No	Yes
Req.6	No	No	No	No	Yes
Req.7	No	No	No	No	Yes

표 1은 기존에 제안된 사용자 인증 스킴들의 보안 요구사항들을 비교 분석한 것이다. 본 논문에서 기술한 Lin 등의 사용자 인증 스킴은 사용자의 스마트 카드를 가로챈 공격자가 스마트 카드 안에 저장되어 있는 정보를 이용해서 사용자의 패스워드를 알아낼 수 있으므로 표 1에서와 같이 다수 보안 요구사항을 만족하지 못한다. 그러므로 보안 요구사항들을 모두 만족시킬 수 있는 개선된 스킴을 향후 과제로서 검토할 수 있다.

3.3 개선 방식

Lin 등의 스킴은 기술된 문제점들을 해결하는 것 이외에 다음과 같이 개선하는 것이 바람직하다.

- 그들이 제안한 방식은 사용자의 패스워드가 올바른가를 검증할 수 있는 패스워드 검증자(Z_i)를 서버에 저장한다. 서버 입장에서 보면 이것을 안전하게 관리하는데 추가적인 비용 및 노력이 필요하다. 이러한 이유로 Lin 등의 스킴은 사용자의 패스워드 검증자를 서버에 저장시키지 않는 방법으로 개선하여 효율성을 증진시키는 것이 바람직하다.
- Lin 등이 제안한 스킴은 서버만이 사용자를 인증하는 일방향 인증(one-way authentication) 방식이다. 그러므로 Lin의 스킴을 사용자와 서버가 동시에 상대방을 인증할 수 있는 상호 인증(mutual authentication)방식으로 개선하여 안정성을 향상시키는 것이다.

이와 같이 개선된 방식을 분석하면, 효율성에서 통신 횟수를 동일하게 설계할 수 있으며, 또한 보안성에서 키 확인과정을 프로토콜에 구현하도록 설계할 수 있다. 표 2는 통신 횟수와 키확인 과정의 유무를 개선방식을 비교 분석한 것이다.

표 2. 개선방식의 통신량 및 키확인 과정의 비교
Table 2. Comparison of communication rounds and key confirmation between the schemes

Protocol	Round	Key Confirmation
Lin et al.[7]	3	No
Improved Protocol	3	Yes

Ⅳ. 결 론

스마트카드를 이용한 사용자 인증 스킴은 공격자가 사용자의 스마트카드 내부에 저장된 정보를 추출하여도 그 정보를 이용하여 사용자의 패스워드를 알아내는데 이용하거나 사용자인척 하거나 또는 서버인척 할 수 없도록 설계되어야 한다[11].

그러나 Lin 등이 제안한 스킴은 공격자가 사용자의 스마트카드 내부에 저장된 정보를 추출한 후 그것을 이용하여 사용자의 패스워드를 알아낼 수 있다. 본 논문에서 이러한 안전성 취약점을 off-line 패스워드 추측공격을 이용해서 밝혀냈다. 또한 보안 요구사항들을 제안하고 스마트카드를 이용한 사용자 인증 스킴들의 안전성을 분석하였다. 분석 결과, Lin 등이 제안한 스킴은 다수의 보안 요구사항들을 만족하지 못함을 알 수 있다. 따라서 본 논문에서는 이와 같은 문제점들을 해결할 수 있는 개선된 두 가지 방안을 제시하였다. 첫째, Lin 등의 스킴은 사용자의 패스워드 검증자를 서버에 저장시키지 않는 방법으로 개선하여 효율성을 증진시키는 방법이다. 둘째, Lin 등의 스킴을 사용자와 서버가 동시에 상대방을 인증할 수 있는 상호 인증방식으로 개선하여 안정성을 향상시키는 방법이다. 이와 같이 개선된 서버와 사용자가 서로 상호 인증할 수 있는 보다 안전하고 효율성이 향상된 스킴은 향후 과제로서 검토할 수 있다.

참고문헌

[1] 정경숙, 정태충, "효율적 사용자 인증을 위한 SRP 기반의 독립적 인증 프로토콜 설계," 한국컴퓨터정보학회논문지,제 8권 제3호, 130-137쪽, 2003년 9월.

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

[3] C.-C. Chang and T.-C. Wu, "Remote Password Authentication with Smart Cards," IEEE Proceedings E-Computers and Digital Techniques, Vol. 138, No. 3, pp. 165-168, 1991.

[4] M.-S. Hwang and L.-H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Trans. on Consumer Electronics,

Vol. 46, No. 1, pp. 28-30, 2000.
〔5〕 P.Kocher,J.Jaffe, and B.Jun, "Differential Power Analysis," Proceedings of Advances in Cryptology (CRYPTO 1999),pp.388-397, 1999.
〔6〕 C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and Solutions on Strong-Password Authentication," IEICE Trans. Communications, Vol. E84-B, No. (9), pp. 2622-2627, 2001.
〔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〕 T.-S. Messerges, E.-A. Dabbish, and R.-H. Sloan, "Examining Smart Card Security Under The Threat of Power Analysis Attacks," IEEE Trans. on Computers, Vol. 51, No. 5, pp. 541-552, 2002.
〔9〕 M.Sandirigama, A. Shimizu, and M. T. Noda, "Simple and Secure Password Authentication Protocol (Sas)," IEICE Transactions on Communications, Vol. E83-B, pp. 1363-1365, 2000.
〔10〕 H.-M. Sun, "An efficient remote user authen -tication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp. 958. 961, 2000.
〔11〕 X. Tian, R. W. Zhu, and D. S. Wong, "Improved Efficient Remote User Authentication Schemes," International Journal of Network Security, Vol. 4, No. 2, pp. 149-154, June 2007.
〔12〕 W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart card", Computers & Security, Vol. 18, No. 8, pp. 727-733, 1999.
〔13〕 H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card", Computer & Security, Vol. 21, No. 4, pp. 372-375, 2002.
〔14〕 M.-L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transaction on Computer Electronics, Vol. 50, No. 2, pp. 629-631, 2004.
〔15〕 I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "Security Enhancement for A Dynamic ID-Based Remote User Authentication Scheme," IEEE Proceeding of The International Conference on Next Generation Web Services Practices (NWeSp'05), pp. 437-440, 2005.

저 자 소 개

안 영 화

1990년 2월 성균관대학교 전자공학과 공학박사
1990년 ~ 현재 강남대학교 컴퓨터미디어 정보공학부 교수
관심분야 : 정보보호, 네트워크 보안

이 강 호

1991년 중앙대학교 전자공학과 공학박사
1990년 ~ 2000년 대덕대학 사무자동화과 교수
2000년 ~ 2003년 송호대학 정보산업계열 교수
2003년 ~ 현재 국립한국재활복지대학 정보보안과 교수
관심분야 : 정보보안, 디지털 영상처리