韓國 컴퓨터情報學會 論文誌
第12卷 第6號, 2007. 12.

2007-12-6-2-4

서비스거부공격에 안전한 OTP 스마트카드 인증 프로토콜

신 광 철*

Secure OTP Smart Card Authentication Protocol for Denial of Service

Shin Kwang Cheul*

요 약

정보통신기술의 발전은 인터넷뱅킹과 e-business의 활성화를 가져왔고 그 매체로써의 스마트카드는 전자서명 인증관리센터의 사용자인증용으로 전자화폐, 교통카드, 출입카드 등으로 널리 보급되어 보편화 되고 있다. 정보통신 공중망을 이용하는 분야에서는 스마트카드에 대한 보안과 카드 소지자의 프라이버시 보호가 매우 중요하다. 스마트카드 보안의 핵심은 사용자 인증으로 스마트카드에 대한 안전한 사용이다. 프라이버시 보호를 위한 익명성 보장과 가용성을 위한 서비스거부공격에 대한 대책이 필요하다. 본 논문에서는 Hwang-Li's, Sun's, L-H-Y scheme을 분석한 다음 일회용 해시함수를 사용하여 세션마다 안전하게 패스워드 확인자를 변경하고 익명성과 서비스거부공격에 안전한 보다 효율적인 새로운 스마트카드 인증 프로토콜을 제안한다.

Abstract

Development of Information and Communication technology coming to activity of internet banking and electronic business, and smart card of medium is generalized prevailing for user authentication of electronic signature certificate management center with cyber cash, traffic card, exit and entrance card. In field that using public network, security of smart cart and privacy of card possessor's is very important. Point of smart card security is use safety for smart card by user authentication. Anonymous establishment for privacy protection and denial of service attack for availability is need to provision. In this paper, after analyze for Hwang-Li, Sun's, L-H-Y scheme, password identify element is a change of safety using one time password hash function. We proposed an efficient new smart card authentication protocol against anonymity and denial of service.

▸ Keyword : Authentication(인증), Smart Card(스마트카드), Mutual Authentication(상호인증), DoS (서비스 거부공격), Anonymity(익명성), OTP(일회용 패스워드)

• 제1저자 : 신광철
• 접수일 : 2007.10.22, 심사일 : 2007.10.31, 심사완료일 : 2007.12.20.
* 성결대학교 e-비즈니스 IT학부 교수

Ⅰ. 서 론

메모리와 CPU를 마이크로 칩으로 내장하여 정보를 저장 및 처리할 수 있는 플라스틱 형태의 스마트카드는 사용과 휴대 편리성, 인증의 용이성으로 전자상거래와 인터넷 뱅킹 등에서 다양하게 사용되고 있다.

스마트카드는 다양한 응용분야에 사용되므로 사용방법에 따라 서로 다른 스마트 인증체제의 도입으로 인하여 보안의 문제가 복잡하고 어려워지고 있다.

특히 스마트카드 수요가 급격하게 증가함에 따라 각종 보안과 해킹사고에 대한 대비책이 필요하다.

공중망에서 사용자 인증은 보안의 중요문제로써 그동안 다양한 패스워드 기반의 인증 프로토콜이 제안되었다[1-8]. 원격지의 서버자원에 대한 접근과 정당성 확보를 위해 일반적으로 패스워드와 ID를 통하여 인증이 이루어지는데 이들은 어떤 보안이 보장되지 않은 상태에서는 제3자의 가로채기에 취약하다.

스마트카드는 패스워드 기반의 인증서 프로토콜을 사용하여 가장 안전한 방법 같지만 다음과 같은 대비가 없이는 제3자의 공격에 취약할 수밖에 없다.

즉, 사용자의 패스워드에 대한 추측공격에 안전해야 하며 과거의 메시지를 재사용하는 공격에 대비하여야 한다. 또 제3자가 합법적인 사용자로 위장하여 훔친 패스워드로 직접 사용될 수도 있다. 정상적인 사용자가 서버로부터 인증을 받기 위한 로그인 과정을 거부해서는 안 된다.

스마트카드 보안의 핵심은 사용자 인증으로 프라이버시 보호를 위한 익명성 보장이며 무결성과 가용성을 보장받기 위해서는 서비스거부공격에 대한 대책이 필요하다. 본 논문에서는 보안위협요소와 대응 방안으로 Hwang-Li's, Sun's, Lee-Hwang-Yang scheme(이하 L-H-Y scheme)을 분석[2, 3, 7, 8]한 다음 일회용 해시함수를 사용하여 세션마다 안전한 패스워드 확인자 변경으로 익명성과 서비스거부공격에 안전하고 보다 효율적인 새로운 OTP(One Time Password) 스마트카드 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장의 관련연구와 3장에서 Lee and Li 프로토콜을 분석한 다음 새로운 프로토콜을 제시하고 4장에서 제안된 프로토콜의 안전성과 효율성을 분석한다. 5장에서 결론을 맺는다.

Ⅱ. 관련연구

스마트카드를 활용하는데 여러 요인 중 가장 큰 문제점은 스마트카드 해킹에 대한 위험이다. 스마트카드의 ROM이나 ERPROM등 메모리 데이터의 해독 뿐 아니라 외부로부터의 고의적인 훼손도 문제이지만 스마트카드 비밀키나 운용프로그램이 외부로 유출되었을 경우 가장 취약함을 알 수 있다. 스마트카드 해킹에 대한 위험 대응으로 보안블록과 개인 식별번호 부여, 카드 소지자의 정당성을 인증하는 것이다.

최근 패스워드에 의한 스마트카드 인증 scheme의 여러 기법들이 제안되었다.[1,2,3,4,5] 이 scheme들은 서버접근을 위한 원격사용자의 합법적임을 증명하기 위한 것이다. 그러나 이들 스킴들은 대부분 패스워드의 설정과 변경을 쉽게 할 수 없다는 문제를 가진다.

2.1 The Hwang-Li's Scheme

각 사용자는 서버가 사용자의 ID로 생성한 패스워드를 스마트카드에 탑재하여 수신하고 이를 이용하여 서버에 접근을 허용 받는 스킴으로 연산비용이 많이 드는 비효율성을 가지고 있다. 이러한 비효율성을 해결하기 위해 Sun's 스킴이 발표되었다.

2.2 Sun's scheme

Sun's scheme은 Hwang-Li's Scheme과 두 가지의 차이를 보인다. 하나는 h()로 64비트의 출력을 위한 단방향함수의 사용이고 또 서버가 Client의 패스워드를 생성하는데 이산대수를 대신해서 해시함수를 사용한 점이다.

Sun's scheme은 단방향 해시만으로 계산과정을 줄임으로써 효율성을 강조하고 있다. 그러나 Sun's scheme과 Hwang-Li's Scheme 모두 임의 패스워드 선정과 변경에 취약성을 갖는다. 이것을 L-H-Y scheme이 해결하고 있다.

2.3 L-H-Y scheme

앞에서의 인증에 비해 자유로운 패스워드 변경과 Sun's의 스킴과 같은 해시함수를 기반으로 한다.

L-H-Y scheme은 타임스탬프와 단방향 해시함수를 사용함으로써 재전송 공격과 위조와 같은 보안성과 연산비용의 증가가 없어도 패스워드의 임의 선택과 변경을 자유롭게 할 수 있는 효율성을 강조한다.

Hwang-Li's Scheme의 등록, 로그인, 인증단계에서의 이산대수 연산을 단방향 해시함수를 적용하여 연산비용을 줄였다.

III. 해시함수를 이용한 OTP 인증 스킴

최근에 여러 방법에 의한 스마트카드에 대한 인증으로 많은 패스워드 인증 스킴이 연구되고 있다. 이러한 스킴들은 합법적인 사용자가 원격에서 로그인을 할 경우 허용하고 서버 접근을 승인한다. Chang과 Liao는 ElGamal's에 기초한 원격 패스워드 인증 스킴을 제안했으며 Chang과 Wu는 Chinese Remainder Theorem(CRT)에 기초를 둔 원격 패스워드 인증 스킴을 제안했고 Wu는 geometric euclidean plane에 기초를 둔 원격 로그인 인증 스킴을 제안했다. 그러나 이들 스킴들은 패스워드의 변경과 선택에 제한적인 취약함을 갖는다. 본 논문에서는 Lee and Li의 프로토콜에 대해 분석하고 이를 통해 패스워드의 자유로운 선택과 변경과정에서 계산처리를 증가시키지 않으면서 1-way 통신으로 overhead를 단축하고 익명성을 보장하며 서비스 거부공격에 안전한 프로토콜을 설계한다.

3.1 Lee and Li 프로토콜

이번 장에서는 Lee and Li의 프로토콜에 대한 단계별 구성과 특성을 알아보고 취약점을 분석한다.[2]

Lee and Li 프로토콜에서 guessing attack에 의한 패스워드의 취약성과 서비스 거부공격에 취약함을 중점적으로 살펴본다. 이 프로토콜은 Peyravian and Zunic's scheme(이하 P&Z)을 해시함수에 기반을 두고 향상시켰다. P&Z scheme은 통신망에서 해시함수에 기반의 패스워드를 전송하여 검증테이블에 해시 값을 변경하는 절차를 보호하기 위한 것이며 프로토콜이 단순하고 효율적이나 제3자의 추측공격에 취약하다.

Lee and Li의 프로토콜은 등록단계, 로그인단계, 인증 및 패스워드 변경단계로 구성되어 있으며 등록단계는 P&Z scheme과 동일하다.

3.1.1 등록단계

〈그림 1〉과 같이 단말기의 사용자 i는 랜덤한 식별자 IDi와 패스워드PWi를 선택하여 식별자와 패스워드를 해시하여 다음을 계산한다.

HPWi = H(IDi, PWi)

사용자 i는 서버로 IDi와 HPWi를 전송한다.

그림 1. 사용자 등록단계
Fig 1. User Registration Phase

서버는 사용자 i의 전송정보를 수신하여 IDi를 확인하고 검증테이블에 IDi와 HPWi를 저장한다.

3.1.2 로그인 및 인증, 패스워드변경 단계

사용자 i의 서버접속을 위한 로그인과 인증과정은 〈그림 2〉와 같다.

Step 1. 사용자 i는 Client인 단말기에서 IDi와 PWi를 입력하게 되면 Client는 랜덤한 Rc를 선택하여 다음을 계산한다.

HPWi = H(IDi, PWi)

Rc ⊕ HPWi

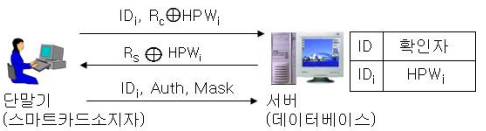

그림 2. 로긴 및 인증을 위한 3-way 통신
Fig 2. 3-way communication for Login and Authentication

사용자 i는 IDi와 Rc ⊕ HPWi를 서버로 전송한다.

Step 2. IDi와 Rc ⊕ HPWi를 수신한 서버는 IDi의 확인자 HPWi를 검증테이블에서 검색하여 다음과 같이 Rc를 구한다.

Rc ⊕ HPWi ⊕ HPWi = Rc

서버는 랜덤한 Rs를 선택하고 다음연산을 수행하여 Rs ⊕ HPWi를 Client로 전송한다.

Step 3. Rs ⊕ HPWi를 수신한 Client는 다음을 수행하여 Rs를 얻고 IDi, AUTH, Mask를 생성하여 서버로 전송한다.

(Rs ⊕ HPWi) ⊕ HPWi = Rs

Auth = H(HPWi, Rc, Rs)

NewHPWi = H(IDi, NewPWi)

Mask = NewHPWi ⊕ H(HPWi, Rc+1, Rs)

Step 4. IDi, AUTH, Mask를 수신한 서버는 사용자 i의 검증테이블에서 HPWi를 검색해서 사용자 i를 인증한다.

AUTH′ =? AUTH

서버가 생성한 AUTH′와 Client의 AUTH 값이 동일하면 서버의 접속을 허용하고 검증테이블의 Client의 확인자를 변경한다.

NewHPWi = Mask ⊕ H(HPWi, Rc+1, Rs)

서버는 검증테이블의 HPWi를 NewHPWi로 대치한다.

3.1.3 Lee and Li의 프로토콜 분석

Lee and Li 프로토콜은 P&Z scheme의 패스워드 취약성(weak key or short string or easy memory)을 해결하기 위해 패스워드를 해시 값으로 변경하여 제안하였다.

그러나 Lee and Li 프로토콜을 분석해 볼 때 P&Z scheme과 마찬가지로 패스워드에 대한 취약성을 배제할 수 없다.

제3자는 HPWi를 가로채서 공개되어 있는 사용자의 IDi와 사회공학공격방법으로 획득한 추측된 패스워드를 가지고 해시값으로 변환하여 HPWi와 값이 동일할 때까지 반복할 것이다.

HPWi =? H(IDi, 추측된 PWi)

이와 같이 추측공격이 가능한 것은 사용자 i에 대한 스마트카드 정보가 없기 때문이다.

HPWi를 확보한 제3자는 Rc와 Rs를 쉽게 얻을 수 있고

NewHPW3 = H(IDi, NewPW3)

Mask = NewHPW3 ⊕ H(HPWi, Rc+1, Rs)로 변경하여 서버로 전송함으로써 서버는 검증테이블의 사용자 i의 확인자를 NewHPW3로 변경하게 된다.

다음번의 인증절차에서 사용자 i는 로그인 요청을 위해 Step 3.의 메시지를 전송하면 Step 4.의 과정에서 제3자가 NewHPWi를 NewHPW3로 변경되었기 때문에 확인자가 일치하지 않아 로그인 서비스를 거부당하게 된다.

Auth = H(NewHPWi, Rc, Rs) ≠ H(NewHPW3, Rc, Rs)

3.2 제안 프로토콜

본 논문에서는 3절에서의 Lee and Li 프로토콜이 서비스공격에 취약한 점을 보완하고 스마트카드에 사용자정보를 탑재함으로써 1-way 통신으로 제3자의 서비스공격에 강한 사용자와 서버간의 일회용 인증 프로토콜을 제안한다.

제3자에 의한 익명성보장과 재 전송공격 방지, 서비스공격, 가장공격을 효율적으로 차단할 수 있는 프로토콜이다.

본 프로토콜은 등록단계, 로그인단계, 인증 및 패스워드 변경의 3단계로 구성되어 있다.

3.2.1 시스템 계수

본 논문에서 프로토콜에 사용될 용어에 대한 정의이다.

- h() : Hash Function
- TS : Time of System
- Xs : secret key of Server
- IDi : ID of User
- As : Authenticator of Server
- pw : password
- rc : random number of client

3.2.2 등록단계

등록단계는 각 사용자가 안전한 채널을 통해 서버에 ID와 확인자(h(pw, rc))를 등록하고 서버에서 사용자 인증정보를 생성하여 스마트카드를 통해 배달받는 단계이다.

① 사용자가 서버에 등록하기를 원할 때 자신의 ID와 패스워드(pw)와 임의 난수(rc)를 해시하여 서버로 전송한다〈그림 3〉.

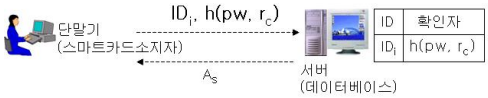

그림 3. 제안한 scheme의 등록단계
Fig 3. Proposed Registration Phase

② 서버는 사용자를 인증하기 위한 인증정보(AS : Authenticator of Server)로 다음을 계산한다.

AS = h(IDi ⊕ Xs) ⊕ h(pw, rc)

Xs는 서버의 비밀키이며 등록센터(DB)는 ID, 확인자를 저장하고 AS를 스마트카드에 담아 사용자에게 배달한다.

3.2.3 로그인 단계

시스템과 자원접근의 로그인을 위해 사용자는 스마트카드를 단말기의 리더기를 통해 IDi, pw를 입력하면 다음을 수행한다.

① Ac1 = As ⊕ h(pw, rc) = h(IDi ⊕ Xs)

② Ac2 = IDi ⊕ TS

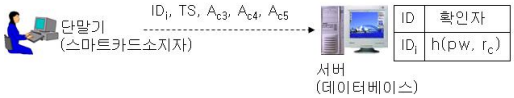

그림 4. 제안한 scheme의 인증단계
Fig 4. Proposed Authentication Phase

③ Ac3 = h(Ac1 ⊕ Ac2)

④ Ac4 = h(Ac1) ⊕ h(pw, rc′) /* rc′는 서버에 등록된 사용자의 확인자를 변경하기 위한 임의의 난수로 사용자 인증용 값 */

⑤ Ac5 = h(pw, rc) ⊕ h(pw, rc′)

인증을 위해 〈그림 4〉와 같이 서버로 메시지{ IDi, TS, Ac3, Ac4, Ac5 }를 전송 한다.

3.2.4 인증 단계

서버는 메시지 { IDi, TS, Ac3, Ac4, Ac5 }를 TS′ 시간에 수신한다.
사용자로부터 메시지를 수신한 서버는 사용자 로그인을 검증하기 위해 다음을 수행한다.

① IDi의 유효성 체크한다. 틀리다면 사용자의 로그인을 거절한다.
② Ac3체크
h(h(IDi ⊕ Xs) ⊕ IDi ⊕ TS)
IDi의 유효성을 다시 한번 체크한다.
서버는 h(IDi ⊕ Xs)를 이용하여 Ac3‘ = h(h(IDi ⊕ Xs) ⊕ IDi ⊕ TS) =?Ac3 의 유효성을 확인한다.
TS와 TS′간의 시간간격을 체크한다. / * TS′ 는 사용자로부터 메시지를 수신한 순간의 시간 * /
(TS′ - TS) ≥ ΔTS이면 거절된다. ΔT는 전송지연에 대한 예상되는 합법적인 시간간격이다.
Ac3와 TS와 TS′간의 시간간격을 비교하여 값이 같으면 서버는 사용자의 로그인 요청을 받아들여 접근권한을 허용하고 그렇지 않으면 로그인 요청을 거절한다.

3.2.5 확인자 변경

③ Ac4, Ac5 인증
서버는 Ac4를 통해 Ac4‘ = Ac4 ⊕ h(IDi ⊕ Xs)를 연산하여 h(pw, rc′)을 도출하고 다시 Ac5를 통해 Ac5‘ = Ac5 ⊕ h(pw, rc)를 연산하여 h(pw, rc′)을 도출한다.
다음과 같이 확인자를 인증하기 위한 연산을 수행한다.
Ac4‘ =? Ac5’
위에서 비교한 값이 같으면 서버는 다음번의 로그인을 위해 사용자의 확인자 h(pw, rc)를 새로운 확인자 h(pw, rc‘)로 수정 기록한다.

Ⅳ. 제안 프로토콜 안전성 분석

본 논문에서 제안한 프로토콜의 여러 가지 공격에 대한 안전성과 기능성을 분석하면 〈표 1〉과 같다.

4.1 일회용 해시함수에 의한 인증

P&Z scheme이나 Lee and Li 프로토콜에서는 임의 난수를 생성하여 상호 교환함으로써 3-way 핸드쉐이크로 인증절차를 갖는다.
본 논문에서는 해시함수를 사용한 1-way 통신으로 통신부담이 줄었다.

4.2 추측공격 안전

통신망에서 제3자가 로그인 요청메시지인 IDi, Ac3, Ac4, Ac5를 가로채기 하였다 해도 TS와 User의 확인자, 서버의 비밀키 Xs를 구할 수 없기 때문에 스마트카드의 As정보를 알아내지 못한다.

표 1. 기능분석
Table 1. Function analyze

프로토콜	통신량	상호 인증	익명성	replay 공격	DoS 공격
L-H-Y	3	o	x	x	x
P&Z	3	o	x	x	x
Lee and Li	3	o	o	o	x
제안 프로토콜	1	o	o	o	o

4.3 위장공격

제3자는 메시지 { IDi, TS, Ac3, Ac4, Ac5 }를 위조하여 정당한 사용자처럼 합법적인 역할을 하기 위해서는 서버의 비밀키와 사용자의 확인자를 알아야 한다.

4.4 재전송 공격

제안된 프로토콜에서는 인증단계에서 타임스탬프(time stamp) TS를 사용하여 생성시간과 전송시간을 확인한다. 제3자는 통신망으로 전송되는 Ac3 에서 서버의 비밀키와 User i의 확인자를 알지 못하고는 TS를 확인할 수 없다. 따라서 제안된 프로토콜에서는 재전송공격에 안전하다.

4.5 DOS공격

서버는 Ac4를 통하여 서비스거부 공격을 방지할 수 있다. Ac4가 없다면 다음과 같은 상황이 발생한다. 제3자는 메시지 { IDi, TS, Ac3, Ac5 }를 가로채서 Ac5를 다른 임의의 값 A5로 변경했을 때 서버는 Ac3를 통하여
Ac3 = h(Ac1 ⊕ Ac2)
Ac3‘ = h(h(IDi ⊕ Xs) ⊕ IDi ⊕ TS) 와 같이
Ac3 = Ac3‘가 같은지를 확인하고
Ac5 = h(pw, rc) ⊕ h(pw, rc′) = Ac5 ⊕ A5 = NewA5를 다음번의 패스워드 확인자로 업데이트 된다.

다음번의 인증절차에서 사용자는 로그인 요청을 위해 서버에게 메시지{ IDi, TS, Ac3, Ac5 }를 전송하면 서버는 위 과

정을 수행하여 Ac3 = Ac3'가 같은지를 확인하는 과정에서 패스워드 확인자가 일치하지 않아 서버로부터의 로그인요청이 거절된다.

Ⅵ. 결론

본 논문에서는 Cheng-Chi Lee와 Li-Hua Li, Min-Shiang Hwang가 제안한 프로토콜의 단계별 통신과 서비스거부공격에 취약함을 보았다.

제안한 프로토콜은 일회성 단방향 통신으로 로그인, 인증, 패스워드(확인자) 변경을 모두 마칠 수 있으며 사용자의 로그인 요청 때마다 확인자를 변화시킴으로써 제3자에 대한 익명성을 제공하고 있다.

일회용 해시함수에 의한 인증으로 3-way handshake 인증절차를 해시함수를 사용한 1-way 통신으로 통신부담이 줄었다.

통신망에서 제3자가 로그인 메시지를 가로채기 하였다 해도 TS와 User의 확인자, 서버의 비밀키 Xs를 구할 수 없기 때문에 스마트카드에 대한 추측공격과 위장공격에 안전함을 보였다.

인증단계에서의 타임스탬프(time stamp) TS를 사용하여 재 전송공격에 안전하며 정당한 사용자자는 세션마다 자신의 확인자를 변경함으로써 제3자에 대한 익명성을 제공해 준다. 특히 서버는 Ac3를 통하여 무결성 검사를 수행하고 검증이 되면 패스워드 확인자를 갱신하기 때문에 서비스 공격에 안전하다.

본 논문에서 제안한 프로토콜은 스마트카드를 사용하는 사용자인증에 효율적인 메커니즘으로 기대된다.

참고문헌

〔1〕 Chih-Wei Lin. Jau-Ji Shen. Min-Shiang Hwang. "Security Enhancement for Optimal Strong-Password Authentication Protocol" . ACM Operating Systems Review, Volume 37 Issue 2, April 2003

〔2〕 Cheng-Chi Lee. Li_Hua. Min-Shiang Hwang. "A Remote User Authentication Scheme Using Hash Functions". ACM Operating Systems Review, 36(4):23-29, 2002.

〔3〕 Cheng-Chi Lee. Min-Shiang Hwang. Wei-Peng Yang. "A Flexible Remote User Authentication Scheme Using Smarts Cards". ACM Operating Systems Review, 36(3): 46-52, 2002

〔4〕 Chi-Kwong Chan and L. M. Cheng. "Cryptanlysis of time stamp-based password authentication scheme". Computers & Security, 21(1):74-76, 2002

〔5〕 Chien-Ming Chen and Wei-Chi Ku. "Stolen-verifier attack on two new storing-password authentication protocols". IEICE Transactions on Communications, E85-B(11):2519-2521, November 2002.

〔6〕 Li-Hua Li, Iuon-Chung Lin, and Min-Shiang Hwang. "A Remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Networks, 12(6):1498-1504, 2001.

〔7〕 Min-Shiang Hwang and L. H. Li, "A New Remote User Authentication Scheme Using Smarts Cards". IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp.28-30, 2000.

〔8〕 Hung-Min Sun, "An Efficient Remote Use Authentication Scheme Using Smarts Cards". IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp.958-961, 2000.

〔9〕 I-En Liao , Cheng-Chi Lee, Min-Shiang Hwang : Identity-based deniable authentication protocol from pairings. IMSA 2006 : 112-114

저 자 소 개

신 광 철

2003년 8월 : 성균관대학교 정보공학과 공학박사

2004년 ~ 현재 : 성결대학교교수

관심분야 : 전자지불시스템, 전자상거래보안기술, 라우터보안, RFID 보안응용