안전한 인터넷 뱅킹을 위한 트랜잭션 서명기법에 관한 연구

Enhanced Transaction Signing-based Authentication Scheme for Secure Internet Banking

임 형 진* 이 정 근** 김 문 성***
Lim Hyung-Jin Jeong-Gun Lee Moonseong Kim

요 약

현재 전세계에서는 다양한 인증기법을 통해 인터넷 뱅킹을 하고 있다. 특히 강한 사용자 인증 기법으로 OTP(One Time Password)기반의 멀티팩터 인증기법을 사용하고 있으나 정교한 공격에 여전히 취약하다. 본 논문은 인터넷 뱅킹 트랜잭션에 부인방지 및 MITB(Man in the Browser Attack)에 대응할 수 있는 서명 기반 프로토콜을 제안하고 있다. 본 프로토콜은 PKI 기반 인증서 및 OTP의 장점을 결합함으로서 정교한 공격에 대응할 수 있는 주요 기능을 제시하고 있으며, 이는 다양한 형태로 현실에 응용될 수 있을 것이다.

Abstract

Nowadays, all over the world's banks use internet banking through various authentication methods. Although there are strong authentication methods using OTP (One Time Password), there still has vulnerability from sophisticated attacks such as MITM (Man In The Middle). This letter proposes signing-based authentication protocol that copes with attacks, such as MITB (Man In The Browser), and provides non-repudiation function. The protocol shows generic method to prevent the sophisticated attacks through connecting advantages from OTP and PKI (Public Key Infrastructure) certificate, and that can be deployed to various extended form in internet banking.

☞ keyword : Secure Internet banking, One time passwrod, Transaction verification

1. 서 론

세계의 각 국가에서는 인터넷 뱅킹을 위해 강한 사용자 인증 기법을 도입하여 사용하고 있다. 이와 관련하여 미국의 FFIEC 가이드라인의 경우 멀티팩터 인증을 포함에 프런트엔드(Front-end) 및 백엔드(Back-end) 인증 기법을 2007년까지 도입하여 사용할 것을 권고 하고 있다[1]. 백엔드 방식은 사용자 인증을 위한 정보와 트랜잭션 정보에 대한 위험 분석을 통해 공격자의 악의적인 시도를 감지해 낼 수 있다. 프런트 엔드 방식은 종단 컴퓨터와 사용자에게 다양한 인증 방식을 적용함으로서 좀더 강한 사용자 인증기법을 적용하려하는 기법들이다. 프런트 엔드 방식에서 사용되는 대표적인 인증방식은 암호에 기반한 방식과 멀티팩터 방식에 근거해서 권고되고 있다. 한 예로서 프런트 엔드 방식들은 공개키 기반의 인증서를 사용하는 방식이나 대칭키 기반의 OTP를 채택하고 있다. 이 방식들은 전통적인 아이디/패스워드 방식에 부가적으로 트랜잭션 요청을 인증하기 위해 사용된다.

OTP의 경우 전통적인 아이디/패스워드 방식의 고정된 패스워드를 매번 바꾸어 인증정보의 가로챔

* 정 회 원 : 금융보안연구원 인증관리팀 선임연구원
dream.hjlim@gmail.com
** 정 회 원 : 한림대학교 컴퓨터 공학과 조교수
jeonggun.lee@hallym.ac.kr(교신저자)
*** 정 회 원 : 미시간주립대학교 박사후연구원
mkim@msu.edu
[2008/06/30 투고 - 2008/07/04 심사 - 2008/08/08 심사완료]

및 재사용 공격을 방지하고 있다. 그러나 OTP는 논리적으로 MITM 공격에 취약함이 알려져 있었다. 올해 1월 시만텍 연구소에서 보고한 BankSlient 와 같은 멀웨어의 출현은 이러한 논리적 취약성에 우려를 나타낼 수 있는 공격 시나리오를 가지고 있다 [2]. MITM(Man-In-The-Middle) 공격의 경우 공격자와 뱅킹 사용자가 서로 다른 컴퓨터에 위치하고 있지만, 이 멀웨어는 MITB 에 기반하고 있다. 즉, 공격자는 원격에서 사용자 정보를 가로채거나 변경하지 않고, 뱅킹 이용자의 컴퓨터에 설치된 프로그램에 의해 악의적 행위를 가능할 수 있도록 시도하고 있다. 아직 까지 이러한 공격으로 나타난 피해사례를 없지만, 보안 연구자들은 공격 기술의 정교화가 향후 이러한 공격을 현실화 할 것이라는 것을 예견하고 있다.

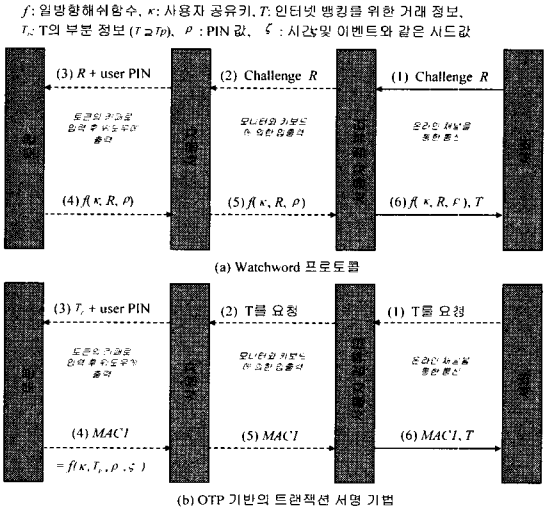
반면에 공인인증서 기반의 사용자 인증 기법을 채택하여 사용하는 국가들이 존재한다. 최근 한국에서는 소프트웨어 기반의 공인인증서가 악의적인 해커에 의해 탈취되는 금융사고가 일어났었다. 더 정확하게 이야기하면 소프트웨어 기반의 공인인증서의 이러한 취약성으로 인해 현재 한국에서는 OTP와 병행하여 사용하고 있다 [3]. 그러나 메모리 해킹과 같은 공격이 시도되고 있고 이는 소프트웨어 기반의 PKI 인증서가 아무리 별도의 소프트웨어 및 하드웨어 기반의 부가 암호 기법을 채용하더라도 트랜잭션의 위변조 및 공인인증서 탈취에 대한 문제에는 완전하게 대응하기 어렵게 만든다. 이러한 문제에 대해서 Transaction Signing기법이 제안되었었다[3].

본 논문은 2절에서 트랜잭션 서명 기법을 소개한다. 3절에서는 제안 기법에 대해서 소개하며, 4절에서는 BAN 로직을 사용하여 제안 프로토콜의 보안성을 분석한다. 5절에서는 본 제안 방식의 실제 적용에 대해 결론을 제시한다.

2. 관련 연구

트랜잭션 서명 기법은 와치월드(watchworld) 프로토콜로부터 개념이 출발한다[3, 4]. 그림1(a)에서 보여주는 바와 같이 이 방식은 사용자가 핸드핸드 디바이스를 가지고 있어야 한다. 현재 이러한 장치들은 일반화되어 가고 있다. 리더기를 가진 스마트카드나, PIN 패드와 디스플레이 장치를 가진 OTP가 사용되고 있다. 사용자가 소지한 장치와 뱅킹 서버는 공유키를 사전 분배하여 저장한 상태이다. 와치월드 프로토콜은 서버로부터 챌린지 값을 사용자가 소지한 별도의 장치에 입력하여 해쉬된 출력 결과 값을 얻게 되며, 웹브라우저로 그 결과 값을 입력한다. 이 방식의 취약점은 R의 값을 공격자가 수정하는 것이 가능하다는 것이다.

와치월드의 문제를 해결하기 위해 R 대신에 사용자가 소지한 장치에 거래정보(T)를 시드(seed)로 하여 입력하고 해쉬된 결과를 얻는 OTP기반의 사이닝 방식이 제안되었다. 사용자의 거래 트랜잭션 정보는 거래 시간, 전송 계좌, 송금 금액 등 다양한 정보가 포함될 수 있으며, 이들 중 사용자 입력 편의성을 위해 거래 계좌 일부와 송금 금액 일부를 조합한 조합 정보(Tp)를 구성할 수 있다. 이를 확장한 OTP 기반의 사이닝 기법의 경우 (그림 1-b)와 같이 매 트랜잭션 요청시 현재의 거래 트랜잭션 정보(계좌번호, 송금값)을 넣기 때문에 재전송 공격을



f: 일방향해쉬함수, K: 사용자 공유키, T: 인터넷 뱅킹을 위한 거래 정보,
T_p: T의 부분 정보 ($T \supseteq Tp$), P : PIN 값, ζ : 시간및 이벤트와 같은 시드값

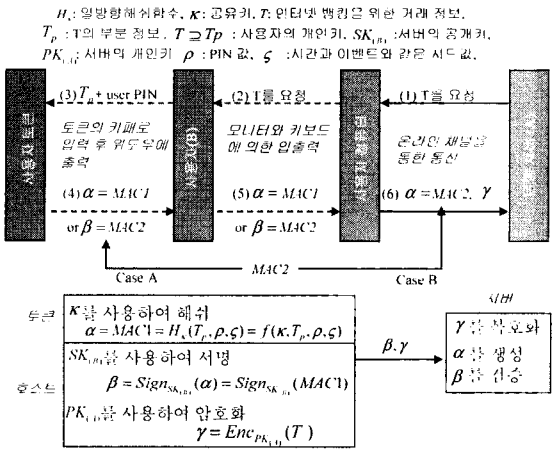
〔그림 1〕 서명 기반의 인증프로토콜

방지할 수 있다. 그러나 이 두 방식은 여전히 사전에 공유된 대칭키를 사용하고 있기 때문에 부인방지가 필요한 트랜잭션환경에서 이를 검증할 수 없다 [6-10].

3. 트랜잭션 서명 기반 인증 프로토콜

앞서 지적한 문제를 해결하기 위해 공인인증서와 사이닝 기반의 OTP의 장점을 결합하는 개선된 프로토콜을 제안하며 (그림 2)에서 나타내고 있다.

본 논문에서는 단일 서비스 프로바이더 혹은 다중의 프로바이더들에 서비스되는 글로벌하게 신뢰된 인증 기관(Certificate Authority)이 존재한다고 가정한다. 각 사용자는 이를 통해 개인키와 공개키 등을 포함하는 자신의 인증서를 소지하고 있다. 이때 사용자는 인증서를 OTP 기능을 포함한 별도의 장치에 함께 저장하거나(Case A), OTP 토큰과는 별도로 자신의 컴퓨터에 이를 저장(적용방안 2)하고 사용한다. 또한 OTP 토큰은 PIN 패드와 디스플레이기능을 갖는 사용자 장치를 소지한 상태이다. 사용자는 원하는 은행 거래를 위해 별도의 인증 방식을 사용하여 로그인하고 거래를 위한 트랜잭션 입력을 서버로부터 요청받은 상태를 그림 2의 (2)의 플로우에서 나타내고 있다. 이때 제안 프로토콜은



〔그림 2〕 개선된 트랜잭션 서명 기반 인증 프로토콜

아래 두 경우에 대해서 다음과 같이 동작할 수 있다.

- 적용방안 1

스마트 토큰 기반의 공인인증서는 현재 유럽에서 주로 사용되고 있다[3]. 그림 2의 플로우 3은 OTP 기반의 서명 기법과 동일한 절차를 갖는다. 사용자의 장치는 OTP 지원 모듈과 공인인증서를 저장하고 있기 때문에 OTP 생성을 위한 키(κ)를 가지고 생성한 MAC1(α)에 대해서 인증서에 포함된 개인키($SK_{(B)}$)를 추출하여 MAC2(β)를 생성한다. 그때 이것을 브라우저로 입력하고, 완전한 트랜잭션 정보를 B의 개인키로 암호화하여 서버로 전송한다.

- 적용방안 2

사용자의 공인인증서가 소프트웨어 형태로 사용자의 PC에 저장된 경우에는 그림 2의 플로의 (5)까지는 OTP기반의 트랜잭션서명 방식과 동일하다. 그러나 사용자가 완전한 거래정보와 MAC1(α)을 웹브라우저에 입력할 때, 인증서에 포함된 개인키를 통해 MAC1(α)을 서명하여 MAC2(β)를 생성하게 된다. 그리고 서버로 이것을 전송한다.

위 두 cases를 통해 MAC2(β)와 서버의 개인키를 사용하여 트랜잭션 정보(T)를 암호화한 γ를 수신한 서버는 고객에게 OTP 배포시 등록된 PIN(ρ), 공유키(κ) 그리고 동기정보 (ζ)를 사용하여 f(κ, T_p, ρ, ζ)을 생성하여 검증하고, β를 복호화 한다. 서버는 B의 공개키로 서명된 MAC2를 검증하여 MAC1와 동일하면 트랜잭션 요청을 승인한다. 본 제안 프로토콜에서는 거래 정보 이외에 전송 채널의 암호화 과정은 언급하지 않았다. 이는 SSL(Secure Socket Layer)과 같은 전송 보안 프로토콜과 연동할 수 있으며, 사용자 측에 별도의 보안 모듈을 설치하여 기밀성을 제공할 수 있다[3].

4. 제안 프로토콜의 보안 분석

본 절에서는 해당 제안 기법이 MITB 및 부인방지 기능을 제공함을 보여주기 위하여 BAN 로직을 사용하여 제안 프로토콜을 검증한다.

4.1 BAN 로직

본 절에서는 BAN 로직을 소개하고자 하며, 세부적인 내용은 M. Burrows[5]의 논문에서 언급되고 있다. BAN 로직의 핵심 요소는 통신 주체들 간에 전송되는 메시지가 최근의 것이고 적절한 키를 사용하여 암호화가 되었다면 인증될 수 있다는 정의에서부터 시작된다. 이 정의는 암호화에 사용되는 알고리즘이 안전하다는 것을 가정하고 있으며, 많은 보안 프로토콜에 대한 분석과 암호 분석을 위한 도구로서 사용되고 있다.

BAN 로직의 주요 구조 및 본 논문에서 사용하는 기호는 다음의 표기를 사용하여 기술된다.

A: 은행의 인증 서버, B: 은행 거래 이용자, ρ: PIN 값,

ς: 동기정보 혹은 시드 값으로 사용되는 시간이나 카운터 값

A|≡X: A는 X를 신뢰해도 된다.

A|~ X : A는 X에게 메시지를 전송한다.

A◁X : A는 X를 확인한다.

#X : X메시지는 최근의 것이다. ,

$\xrightarrow{K}A$: K는 A의 공개키이다. (개인키 K^{-1}은 A만이 가지고 있다.)

$A \xleftrightarrow{K} B$: A와 B는 안전한 통신을 위해 공유키 K를 사용할 수 있다.

$A \xleftrightarrow{K} B$: A와 B사이에 공유하는 비밀값 K가 존재한다.

$\{X\}_K$: 메시지 X는 키 K를 사용하여 암호화 되었다.

$\langle X \rangle_Y$: X는 비밀값 Y와 결합되었다.

이상에서 언급된 정의들을 사용하여 다음의 공리들을 기술할 수 있다.

• 공개키 암호 방식에 대한 메시지 규칙

K가 B의 공개키일 때, A는 B가 K-1을 사용하여 암호화한 메시지 X를 확인이 가능하다면, A는 메시지X가 B로부터 전송된 메시지라는 것을 믿을 수 있다.

$$\frac{A \mid\equiv \overset{K}{\mapsto} B, A \lhd \{X\}_{K^{-1}}}{A \mid\equiv B \mid\sim X} \quad (1)$$

• 대칭키 암호 방식에 대한 메시지 규칙

A가 B와 대칭키 K를 공유하고 있을 때, A는 B가 K을 사용하여 암호화한 메시지 X를 확인이 가능하다면, A는 메시지 X가 B로부터 전송되었다는 것을 믿을 수 있다.

$$\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B, A \lhd \{X\}_K}{A \mid\equiv B \mid\sim X} \quad (2)$$

• 비밀키 암호 방식에 대한 메시지 규칙

A가 B와 비밀키 Y를 공유하고 있을 때, A는 B가 Y을 사용하여 암호화한 메시지 $\langle X \rangle_Y$를 확인이 가능하다면, A는 메시지 X가 B로부터 전송되었다는 것을 믿을 수 있다.

$$\frac{A \mid\equiv A \overset{Y}{\Leftrightarrow} B, A \lhd \langle X \rangle_Y}{A \mid\equiv B \mid\sim X} \quad (3)$$

• 비표(Nonce) 검증 규칙

특정 통신 주체가 메시지를 전송하였고, 그 메시지가 최근의 것이라면 비표를 신뢰할 수 있다.

$$\frac{A \mid\equiv \#(X), A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X} \quad (4)$$

이상의 가정들은 분자부분에서 조건을 나타내고 있으며, 분모에는 이 조건이 만족할 경우 결과를 기술하고 있으며, M. Burrows[5]의 논문에서는 더 많은 공리들을 기술하고 있지만 본 논문에서 필요한 4가지 가정만을 기술하였다.

4.2 제안 프로토콜의 검증

제안프로토콜을 BAN 로직에 따라 정규화한다면 식 (5)와 같이 기술할 수 있으며, 식(6)부터 식 (12)까지는 가정을 나타내고 있다.

$$\beta = \alpha = \{\langle X, \zeta \rangle_{\rho}, \rho\}_{K_\kappa},\ \{A \xleftrightarrow{K_\kappa} B\},\ \{A \xleftrightarrow{\rho} B\},$$

$$\{A \xleftrightarrow{\zeta} B\},\ \{\xrightarrow{K_{(B)}} B\}_{K_{(B)}^{-1}},\ \gamma = \{M, \{\xrightarrow{K_{(A)}} A\}\}_{K_{(A)}}. \quad (5)$$

$$A \mid\equiv A \xleftrightarrow{K_\kappa} B \ (6),\quad A \mid\equiv A \xleftrightarrow{\rho} B \ (7),$$

$$A \mid\equiv A \xleftrightarrow{\zeta} B \ (8),\quad A \mid\equiv \xrightarrow{K_{(A)}} A \ (9),$$

$$A \mid\equiv \xrightarrow{K_{(B)}} B \ (10),\quad B \mid\equiv \#(\zeta) \ (11),$$

$$A \mid\equiv A \xleftrightarrow{K_\kappa} B (12)$$

우리는 정규화된 프로토콜을 가정과 공리를 사용하여 로직을 다음과 같이 검증한다.

- 단계 1: A 는 가정 (6), (7), (8), (11)가정에 의해 K_κ와 ρ를 가지고 있으며, OTP특성에 따라 시드(seed) 정보로서 ζ을 가지고 있다.
- 단계 2: 가정 (9)와 공리 (1)로부터 서버 A는 B가 전송한 γ를 읽을수 있고, 트랜잭션 X를 확인할 수 있다.
- 단계 3: (11) 가정과 (4)의 공리로부터 A는 최근의 ζ을 생성하고, (8), (12)의 가정에 의해 동일한 α를 생성할 수 있다. 이 때 A는 (2)와 (3) 공리에 의해 B로부터 생성된 트랜잭션이라는 것을 믿을 수 있다.
- 단계 4: A는 (1)의 가정과 (4)의 공리에 의해 B의 개인키(K^{-1})로 서명된 β를 B의 공개키(K)를 사용하여 검증하고, B가 최근에 거래 요청한 트랜잭션서명이란 것을 믿을 수 있다. 이상의 논리적인 검증을 통해 A는 B가 전송한 트랜잭션 요청 정보를 검증할 수 있다.

4.3 정교한 공격에 대한 대응 분석

사용자의 컴퓨터에는 사용자의 거래입력정보를 탈취, 위변조를 수행하는 멀웨어가 설치되어 있는 상태이라고 가정한다. 따라서 공격자는 인증서 정보에 대한 제어 권한을 탈취한 상태이며, 사용자 입력 정보를 변경할 수 있는 권한을 획득한 상태이다.

- 공격자는 고객이 전송한 M을 자신의 계좌정보와 송금액으로 M'으로 변경하여 거래를 시도한다.

  공격자는 $\gamma' = \{\{M', \{\xrightarrow{K_{(A)}} A\}\}_{K_{(A)}}$를 생성하여 MITB 공격을 시도한다. A는 단계 2에서 M'를 추출하고 단계3를 수행한다. 그러나 A가 생성한 α'는 $\{\langle M', N\rangle, \rho\}_{K_\kappa}$이고 실제로 B가 시도한 α는 $\{\langle M, N\rangle, \rho\}_{K_\kappa}$이기 때문에 해당 트랜잭션은 거절된다.
- 은행 고객은 거래 성공이후 자신의 거래 요청을 부인한다.

  B는 현재 생성된 γ를 자신의 것이 아니라고 부인하더라도 가정 (9), (10)에 기반하여 (1)의 공리는 B가 서명한 트랜잭션이란 것을 나타내고 있다.

  B는 개인키가 공격자에게 탈취되어 악의적으로 서명된 트랜잭션이라고 주장하더라도, 사용자 B만이 소유한 토큰으로부터 생성된 일부 정보가

있어야만 트랜잭션검증이 성공할 수 있다. 따라서 α의 내용이 정상적으로 검증된다면 (2), (3)으로부터 B의 트랜잭션이라는 것을 다시 증명하게 된다.

제안 프로토콜은 MITM 공격을 OTP의 서명기법으로 막고, OTP에 부인방지 기능을 인증서의 개인키로 서명하여 제공해 줄 수 있다. 정교한 공격들이 시도된다고 하더라도 A만이 요청한 정보에 대해 거래가 수행되는 것을 가능하게 해준다.

5. 결론

현재 인증서 및 OTP방식은 기술적으로 상당히 안정화된 강한 사용자 인증 기술이지만 두 방식 모두 정교한 공격에 취약성을 가지고 있다. 그러나 두 방식을 단순히 혼용하는 방식은 개별 취약성을 그대로 가질 수 있다. 본 제안은 두 방식의 장점을 혼합한 제안에 해당한다. 본 논문의 제안은 현재 시도되고 있는 공격들에 대한 논리적인 대응방안으로 제시될 수 있으며, 다양한 변형들이 확장 적용될 수 있다. 여기서 우리가 고려해야 할 것은 사용자의 편의성을 고려해야한다는 것이다. 그러나 최근 또한 이동통신 단말의 지능화와 토큰 기능의 융합은 사용자 편의성 저해를 최소화 하면서 제안 내용을 적용할 수 있도록 하는데 기여할 수 있다고 확신한다.

결론적으로 본 논문의 제안 내용은 두 방식의 근원적인 원리를 간단히 조합하여 금융트랜잭션의 요구사항과 정교한 공격 논리에 대응할 수 있는 핵심 인증 방식을 제시하고 있다.

참 고 문 헌

[1] Federal Financial Institutions Examination Council (FFICE), "Authentication in an Internet Banking Environment", www.ffiec.gov/pdf/authentication_guidance.pdf

[2] NetworkWorld, "New Trojan intercepts online banking information", Jan. 14, 2008.

[3] A. Hiltgen, T. Kramp, and T. Weigold, "Secure Internet Banking Authentication", IEEE Security and Privacy, Mar. 2006.

[4] E. Gallery, "Identity Verification", www.isg.rhul.ac.uk/~eimear /03.ppt.

[5] M. Burrows, M. Abadi, R. Needham: A logic of authentication. ACM Transactions on Computer Systems, 8(1):18 - 36, February 1990.

[6] G. Tubin, The Sky is Falling: The Need for Stronger Consumer Online Banking Authentication, Apr 2005.

[7] G. Tubin, Emergence of Risk-Based Authentication in Online Financial Services; You Can't Hide Your Lyin' IPs, May 2005.

[8] J. Brainard, Ari Juels, and Ronald L. Rivest, "Fourth-Factor Authentication: Somebody You Know", 2006.

[9] FDIC, "Putting and End to Account-Hijacking Identity Theft-Study Supplement", 2005.

[10] B. Pinheiro, "Comments on FDIC Report - reference of No 23", 2005

◐ 저 자 소 개 ◑

임 형 진(Lim Hyung-Jin)

1998년 2월 한림대학교 컴퓨터공학과 졸업(학사)
2001년 8월 성균관대학교 정보통신대학원 정보통신공학과 졸업(석사)
2006년 8월 성균관대학교 대학원 컴퓨터공학과 졸업(박사)
2007년 8월 성균관대학교 BK21 Post-Doctor
2007년 10월~현재 금융보안연구원 인증관리팀 선임연구원
관심분야 : IP 이동성 관리 기술 (Netlmn, Network Mobility, Ad-hoc Mobility 등), VPN 기술 (MPLS, IPSec, SSL 등), AAA(Authentication, Authorization and Accounting) 및 접근 제어, 키 관리 및 인증 프로토콜, 멀티팩터 인증기술
E-mail : dream.hjlim@gmail.com

이 정 근(Jeong-Gun Lee)

1996년 2월 한림대학교 전자계산학과 졸업 (학사)
1998년 2월 광주과학기술원 정보통신공학과 졸업 (석사)
2005년 2월 광주과학기술원 정보통신공학과 졸업 (박사)
2005년 5월 ~ 2007년 6월 University of Cambridge, Computer Lab. 박사후연구원
2006년 3월 ~ 2006년 4월 University of California Los Angeles, 컴퓨터공학과, 방문연구원
2007년 8월 ~ 2008년 2월 광주과학기술원 정보통신공학과 연구교수
2008년 3월 ~ 현재 한림대학교 컴퓨터 공학과 조교수
관심분야 : 컴퓨터 구조, 비동기 회로 설계, 병행시스템 이론, 센서 네트워크, 시스템 보안 및 정형 검증
E-mail : jeonggun.lee@hallym.ac.kr

김 문 성(Moonseong Kim)

2002년 8월 성균관대학교 수학과 졸업(석사)
2007년 2월 성균관대학교 전기전자 및 컴퓨터공학과 졸업(박사)
2005년 7월 ~ 2006년 2월 한국전자통신연구원(ETRI) 위촉연구원
2007년 3월 ~ 2008년 2월 성균관대학교 정보통신공학부 연구교수
2007년 12월 ~ 현재 미국 미시간주립대학교 박사후연구원
관심분야 : 라우팅 프로토콜, 모바일컴퓨팅, 센서네트워크, 네트워크 보안
E-mail : mkim@msu.edu