情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

무선 네트워크 환경에서 모바일 디바이스 기반 효율적인 사용자 인증 기법*

신 수 복,[1†] 예 홍 진,[1] 김 강 석[2‡]
[1]아주대학교 정보통신전문대학원, [2]아주대학교 대학원 지식정보공학과

An Efficient User Authentication Scheme with Mobile Device in Wireless Network Environment*

Soobok Shin,[1†] Hongjin Yeh,[1] Kangseok Kim[2‡]
[1]Graduate School of Information and Communications, Ajou University,
[2]Department of Knowledge Information Engineering, Graduate School of Ajou University

요 약

최근 스마트 폰, 스마트 패드와 같은 모바일 디바이스의 발전과 무선 네트워크 및 이동통신 네트워크의 발전으로 모바일 디바이스를 이용하는 서비스는 증가하고 있다. 그러나 무선 네트워크는 유선 네트워크에 비해 보안에 취약하므로 보다 강한 보안의 적용이 필요한 반면 배터리 기반의 모바일 디바이스는 낮은 계산 능력과 메모리 공간의 제약 및 무선통신에 사용되는 비용이 높기 때문에 보안의 적용은 효율적이어야 한다. 따라서 본 논문에서는 모바일 디바이스를 이용한 서비스에서 요구되는 보안 요구사항을 충족시키고 모바일 환경에 적합한 티켓 기반의 인증 기법을 제안한다.

ABSTRACT

Recently, with rapid advances of mobile devices such as smart phone and wireless networking, a number of services using mobile device based wireless network have been explosively increasing. From the viewpoint of security, because wireless network is more vulnerable than wired network, strong security is required in wireless network. On the contrary, the security for mobile devices has to be efficient due to the restrictions of battery powered mobile device such as low computation, low memory space and high communication cost. Therefore, in this paper, we propose an efficient authentication scheme with mobile devices in wireless network environment. The proposed scheme satisfies security requirements for the service using mobile device and it is suitable in wireless network environment.

Keywords: Authentication, Ticket, Mobile Device, Wireless Network

I. 서 론

최근 무선 네트워크와 이동통신 네트워크를 통해 모바일 디바이스를 이용한 많은 서비스가 생겨나고 있다. 따라서 안전한 서비스를 제공하기 위해 무선 및 이동통신 네트워크 환경에서의 보안은 매우 중요한 이슈이다. 그러나 무선 네트워크 환경에서의 서비스는

접수일(2012년 9월 28일), 수정일(2012년 12월 7일), 게재확정일(2013년 1월 22일)
* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원 사업"의 연구결과로 수행되었음.
† 주저자, watermel@ajou.ac.kr
‡ 교신저자, kangskim@ajou.ac.kr

유선 네트워크 환경에서의 서비스보다 무선 네트워크 환경의 특성 때문에 강한 보안이 요구되는 반면 모바일 디바이스 자원의 제약과 무선 네트워크의 환경적 제약을 갖고 있다. 따라서 강한 보안을 위해 연산 오버헤드가 높은 공개키 알고리즘을 적용하거나 서버와 사용자 간에 많은 통신을 통해 보안을 강화할 수 없는 실정이다. 특히 서비스 제공자는 원활한 서비스 제공과 서버에서 제공하는 서비스와 자원의 안전성을 제공하기 위해 정상적인 사용자만 서비스를 이용할 수 있도록 사용자의 인증 메커니즘을 제공해야 한다. 즉 이러한 환경에 실제 적용 가능한 인증 메커니즘은 발생 가능한 공격으로부터 안전해야하며 효율적으로 설계되어야 한다.

본 논문에서는 모바일 디바이스 기반 무선 네트워크 환경에서 실제 적용 가능하도록 티켓을 이용한 사용자 인증 기법을 제안한다. 제안하는 기법은 배터리 기반의 모바일 디바이스에서 사용되는 연산 오버헤드와 인증을 위한 통신을 최소화하였다. 또한 무선 네트워크 환경에서 발생 가능한 공격으로부터 안전하고 사용자와 CA (Certificate Authority), 사용자와 서버 간에 상호인증을 제공하고 인증 완료 후에 사용자와 서버는 안전한 통신을 위한 세션 키를 공유하게 된다.

본 논문의 2장에서 무선 네트워크 환경에서의 사용자인증에 대한 관련 연구를 살펴보고 3장에서 이러한 환경에서 사용자 인증의 보안 요구사항을 살펴본다. 4장에서 보안 요구사항을 만족하는 효율적인 사용자 인증 기법을 제안하고 5장에서는 제안하는 기법의 안전성과 효율성을 분석한다. 마지막으로 6장에서 결론과 향후 연구에 대해 기술한다.

II. 관련연구

사용자 인증은 네트워크를 통해 서버에 접속하는 사용자의 정당성을 검증하는 메커니즘으로 안전한 서비스를 제공하기 위해 필수적인 보안 요구사항이다. 따라서 현재까지 다양한 환경을 고려한 많은 사용자 인증기법이 제안되었다. 특히 패스워드 기반의 인증기법은 보편적으로 사용되는 기법이다.

기존의 아이디 / 패스워드 기반의 사용자 인증은 등록 단계에서 사용자의 아이디와 패스워드를 입력받아 서버에 저장한 후 사용자가 서버로부터 서비스를 받고자 할 때 사용자는 아이디와 패스워드를 입력하여 서버에 전송하고 서버는 전송된 아이디와 패스워드를 저장된 값과 비교함으로 사용자를 인증하는 기법이다. Lamport의 연구 [1] 에서 처음으로 패스워드 기반의 인증 기법을 제안하였으나 많은 해쉬 연산의 오버헤드를 갖고 있으며 또한 패스워드의 재설정이 요구되는 단점이 존재한다. 또한 많은 아이디 / 패스워드 기반의 사용자 인증 기법은 등록 단계에서 악의적인 내부자의 공격에 취약하고 사용자의 인증을 위한 아이디와 패스워드 테이블을 서버에 저장하고 있기 때문에 공격자의 서버 해킹, 관리자의 관리 소홀 등으로 인증 테이블이 노출되면 전체 인증 메커니즘의 붕괴를 가져올 수 있다. 게다가 사용자는 편의를 위해 동일한 아이디와 패스워드를 여러 서비스의 인증을 위해 사용하는 경향이 있으므로 한 곳에서 노출된 인증 정보는 사용자가 가입한 많은 서비스에 영향을 미칠 수 있다.

다른 많은 연구 [2-7] 에서는 스마트카드를 이용한 인증 기법을 제안하였다. 스마트카드를 이용한 인증 기법은 스마트카드에서의 낮은 계산능력과 적은 저장 공간 등의 제약 사항을 고려하여 XOR (eXclusive OR), 해쉬 연산과 같은 적은 연산을 이용하여 인증을 수행하는 기법이 제안되었다. 더욱이 이들 연구에서는 훔친 검증자 공격 (stolen-verifier attack)의 안전을 위해 사용자의 아이디와 패스워드 테이블을 유지하지 않고 사용자를 인증하는 기법을 제안하였다.

다른 연구 [8-13] 에서는 모바일 환경에서의 사용자 인증 기법이 제안되었다. 모바일 환경에서 사용자는 언제 어디서든 서비스를 제공하는 서버에 접속하여 서비스를 받을 수 있다. 따라서 모바일 환경에서 로밍 사용자는 홈 에이전트(Home Agent)에 등록하고 외부 네트워크(Foreign Network)를 통해 서비스를 받고자 할 때 모바일 사용자는 외부 에이전트(Foreign Agent)에게 인증을 위한 정보를 전송한다. 외부 에이전트는 사용자의 인증 정보를 사용자의 홈 에이전트에게 전송하여 홈 에이전트로부터 사용자를 인증한다. 이러한 기법의 장점은 사용자는 홈 에이전트에 한 번만 등록하고 여러 외부 네트워크에 접속하여 서비스를 제공받을 수 있다. 모바일 환경에서의 많은 인증 기법에서 서비스를 받는 주체는 모바일 디바이스이므로 모바일 디바이스가 갖는 자원의 제약을 고려한 효율적인 사용자 인증기법에 초점을 맞추었다.

다른 연구 [12-14] 에서는 모바일 환경 및 이종 네트워크 환경에서 티켓 (ticket) 기반의 인증 기법을 제안하였다. Shin et al의 연구 [14] 에서는 유비쿼터스 환경(이종의 디바이스와 네트워크가 공존하

는 환경)에서 그룹 통신을 위한 티켓 기반의 인증 기법을 제안하였다. 이 기법은 가상 컨퍼런스 환경에서 사용자는 참가하고자 하는 컨퍼런스의 세션에 참가하기 위한 티켓을 발급받고 각 세션에 티켓을 제시함으로써 사용자 인증을 받고 세션에 참여하게 된다. 이 기법은 모바일 디바이스에서 연산을 최소화하여 효율적으로 인증을 수행하는 반면 이종의 디바이스로 이루어진 그룹 통신을 위한 인증 기법으로 그룹의 관리자가 모바일 디바이스이고 관리하는 그룹의 멤버가 많을 경우 모바일 디바이스에서의 연산이 보다 많아질 수 있다. 또한 이 기법은 내부자 공격에 취약하고 상호인증과 사용자의 익명성을 제공하지 않는다.

Moon et al의 연구 [12] 에서는 모바일 통신환경에서 홈 에이전트로부터 외부 에이전트로의 사용자 로밍을 지원하는 아이디 기반의 티켓을 이용한 사용자 인증 기법을 제안하였다. 이 기법에서 모바일 사용자는 등록한 네트워크 내의 서비스 제공자로부터 서비스를 제공받기 위해 등록을 수행한 네트워크의 인증 서버로부터 발급받은 티켓을 전송하여 서비스를 제공받을 수 있지만 외부 네트워크의 서비스 제공자로부터 서비스를 제공받기 위해서는 외부 에이전트로부터 인증을 받거나 티켓을 갱신해야 하는 단점이 존재한다. 또한 인증 서버는 사용자의 아이디와 패스워드를 저장하고 있다. 따라서 내부자 공격과 훔친 검증자 공격에 취약하고 사용자가 서버를 인증하는 메커니즘이 없다. 즉 상호인증을 제공하지 않는다.

Park et al의 연구 [13] 에서는 유비쿼터스 환경에서 모바일 디바이스에서의 티켓 기반 인증 기법을 제안하였다. 이 기법에서 사용자는 티켓발급을 위해 인증 서버에 등록과 티켓발급 과정을 거쳐 티켓을 발급받는다. 발급받은 하나의 티켓을 여러 서비스 서버에 제출함으로 서비스를 제공받을 수 있다. 그러나 이 기법에서 사용자 인증 메시지와 티켓을 안전하게 전송하기 위해 공개키 알고리즘을 사용한다. 공개키 알고리즘은 모바일 디바이스에서 많은 연산 오버헤드를 초래한다.

III. 보안 요구사항

이번 절에서 모바일 디바이스 기반의 무선 네트워크 환경의 사용자 인증에서 발생할 수 있는 공격과 안전한 인증을 위한 보안 요구사항을 살펴본다. 사용자의 인증에는 다음과 같은 공격이 존재한다. 따라서 인증 기법은 그러한 공격으로부터 안전하게 설계되어야 하며 보안의 강화를 위해 상호인증과 인증 이후 안전한 통신을 위한 키를 공유할 수 있어야 한다.

1) 내부자 공격(Insider attack)

패스워드 기반의 인증 기법에서 내부자 공격은 사용자의 등록 메시지로부터 악의적인 내부자가 사용자의 아이디와 패스워드를 수집하여 악의적으로 사용하는 공격이다. 대부분의 사용자는 가입한 여러 서비스의 아이디와 패스워드를 다르게 설정하였을 경우 아이디와 패스워드의 유지 및 관리가 어렵기 때문에 사용의 편의를 위해 동일한 값을 사용하는 경향이 있다. 따라서 한번 노출된 아이디와 패스워드는 사용자가 가입한 여러 사이트에 영향을 미칠 수 있다.

2) 재생 공격(Replay attack)

인증 기법에서 재생 공격은 이전에 정상적인 사용자가 인증을 위해 전송한 인증 요청 메시지를 공격자가 수집하여 저장하고 있다가 이후의 세션에 수집한 인증 요청 메시지를 전송하여 정상적인 사용자로 인증받는 공격이다. 무선 네트워크 환경에서 공격자는 인증 요청 메시지를 쉽게 수집할 수 있다. 따라서 공격자가 정상적인 사용자로 인증되지 않기 위해 인증 기법은 재생 공격으로부터 안전하게 설계되어야 한다.

3) 추측 공격(Guessing attack)

추측 공격은 공격자가 인증을 위한 통신 과정의 메시지를 저장한 후 그 메시지에서 아이디와 패스워드를 이용하는 값으로부터 사용자의 아이디와 패스워드를 알아내는 공격이다. 아이디 / 패스워드 기반의 인증 기법에서 정상적인 사용자의 아이디와 패스워드는 인증을 위한 중요한 요소이기 때문에 인증을 위한 통신 과정에서의 메시지로부터 아이디와 패스워드를 얻을 수 있는 것은 보안상 큰 위협이 될 수 있다. 또한 내부자 공격에서 설명하였듯이 사용자는 여러 사이트에 동일한 아이디와 패스워드를 사용하기 때문에 그 파장은 더 크다고 볼 수 있다. 따라서 안전한 인증 기법은 추측 공격으로부터 안전해야 한다. 게다가 사용자는 아이디와 패스워드를 기억하기 쉽게 하기위해 본인 혹은 관련자의 생일, 차량번호, 폰 번호와 같이 본인과 관련이 깊은 값을 주로 사용하기 때문에 공격자가 직접 추론할 수도 있다. 따라서 아이디와 패스워드가 노출

되었더라도 공격자는 인증 받을 수 없는 메커니즘이 제공되어야 한다.

4) 중간자 공격(Man in the middle attack)

중간자 공격은 사용자와 인증 서버의 중간에서 사용자와 서버 사이의 모든 메시지를 가로채 사용자 또는 인증 서버로 가장하는 공격이다. 중간자 공격은 데이터를 불법 수정하여 거짓 데이터를 생성하고 그 데이터를 전송하므로 서버 혹은 사용자에게 심각한 타격을 줄 수 있는 적극적인 공격이다. 또한 사용자와 서버 간에 통신하는 모든 데이터를 볼 수 있으므로 사용자의 프라이버시를 위협할 수 있으며 중요한 데이터가 공격자에게 노출될 수 있다. 중간자 공격을 막기 위해 인증 기법은 공격자가 통신상의 메시지 수집을 통해 사용자 또는 인증 서버로 가장할 수 없도록 설계하여야 한다.

5) 훔친 검증자 공격(Stolen-verifier attack)

훔친 검증자 공격은 서버 혹은 CA(Certificate Authority)에서 사용자의 인증을 위해 저장한 사용자의 아이디 패스워드 테이블과 같이 인증을 위한 중요한 정보가 악의적인 내부자에 의해 유출되거나 공격자의 인증서버 해킹으로 정보가 노출되어 전반적인 인증 메커니즘의 붕괴를 일으키는 공격이다. 특히 아이디 패스워드 기반의 인증 메커니즘은 훔친 검증자 공격으로부터 안전하게 설계되어야 한다.

〔표 1〕 제안하는 기법에서 사용되는 표기법

표기	내용
CA	인증 서버
AI	사용자의 인증 및 권한 정보
life-time	인증을 위한 티켓의 만기시간
ID_u	사용자의 아이디
PW_u	사용자의 패스워드
N_*	*에서 생성한 난수
$h(\bullet)$	일방향 해쉬함수
$\oplus$	배타적 논리합
$\|$	연결 연산자
$E_{K_X}(M)$	대칭키 K_X로 메시지 M의 암호화
$D_{K_X}(M)$	대칭키 K_X로 메시지 M의 복호화
$E_{K_{pub-Y}}(M)$	Y의 공개키로 메시지 M의 암호화
$D_{K_{pri-Y}}(M)$	Y의 비밀키로 메시지 M의 복호화
$Sign_Z(M)$	메시지 M에 대한 Z의 서명

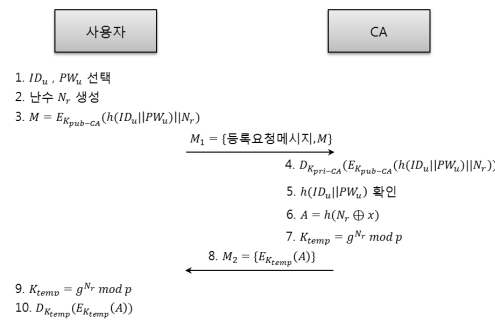
IV. 제안하는 기법

제안하는 기법은 등록, 티켓발급요청 그리고 티켓을 이용한 사용자 인증의 세 단계로 구분된다. 등록 단계에서 모바일 단말기 사용자는 사전에 인증 서버(CA)에 등록하고 서비스를 제공받고자 할 경우 CA로부터 티켓을 발급 받고 서버에 티켓을 제출하여 인증 받는다. 제안하는 기법의 등록단계에서 사용자는 CA의 공개키를 이용해 등록을 수행한다. 따라서 등록 단계에서 안전한 채널을 이용해 등록하거나 사전에 키를 공유하고 있다는 가정을 수반하지 않는다. 그리고 공개키 알고리즘의 이용은 단지 등록단계에서만 수행된다. 서비스를 제공받기 위해 모바일 단말기 사용자는 발급받은 티켓을 서버에 제출하여 인증을 받는다. 〔표 1〕은 제안하는 기법에서 사용되는 표기와 그에 대한 설명이다.

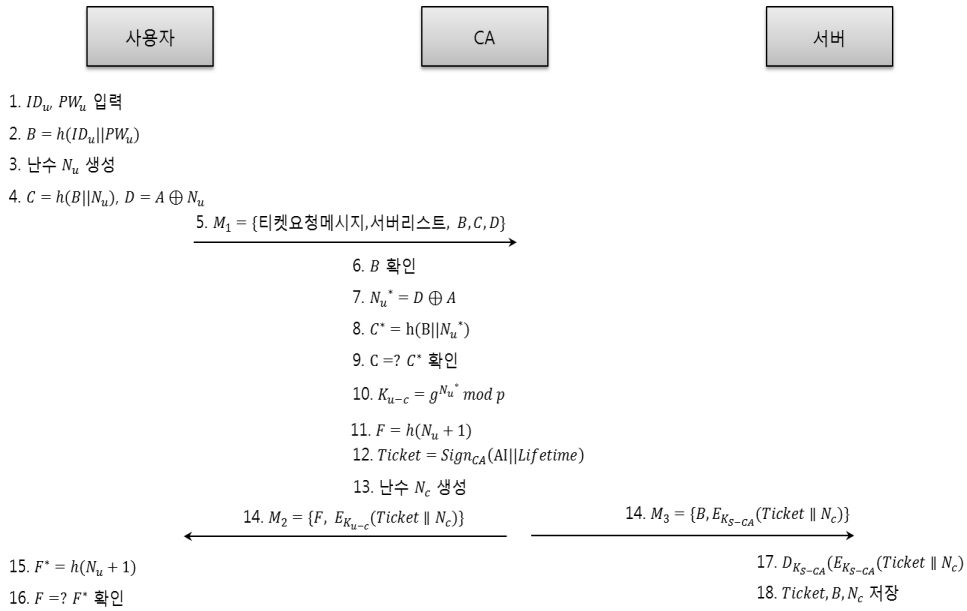
4.1 등록 단계

모바일 단말기 사용자가 서버로부터 서비스를 받기 위해서는 사전에 CA에 등록을 하여야 한다. 사용자는 아이디와 패스워드를 자유롭게 선택하고 CA에게 전송한다. CA는 사용자로부터 전송받은 데이터를 이용하여 향후 인증에 사용될 값들을 생성하여 사용자에게 전송한다. 등록단계에서 사용자는 전송되는 데이터를 안전하게 전송하기 위하여 CA의 공개키를 이용한다. 모바일 단말기에서 공개키를 이용한 암호화는 등록 단계에서만 수행한다. 등록은 최초 한번만 수행한다. 〔그림 1〕은 등록 단계의 절차를 나타내고 자세한 등록 과정은 다음과 같다.

1. 사용자는 인증에 사용될 아이디(ID_u)와 패스워드(PW_u)를 선택한다.
2. 난수(N_r)를 생성한다.



〔그림 1〕 등록 절차



〔그림 2〕 티켓 발급 절차

3. $E_{K_{pub-CA}}(h(ID_u \| PW_u) \| N_r)$을 계산하고 CA에게 등록 요청 메시지와 함께 전송한다.
4. CA는 사용자로부터 받은 메시지를 비밀키를 이용해 복호화 $D_{K_{pri-CA}}(E_{K_{pub-CA}}(h(ID_u \| PW_u) \| N_r))$한다.
5. 기존에 등록한 사용자인지 확인을 위해$h(ID_u \| PW_u)$ 값을 확인한다. CA는 사용자의 아이디와 패스워드를 저장하지 않는다. 위의 값은 등록된 사용자를 구분하기 위한 값으로 사용한다.
6. 등록되어있지 않은 사용자라면 향후 인증을 위해 $A = h(N_r \oplus x)$을 생성한다. 여기서 x는 CA만 알고 있는 비밀 값이다.
7. 사용자에게 인증정보를 안전하게 전달하기 위한 임시키 $K_{temp} = g^{N_r} \bmod p$을 생성한다. 여기서 g는 그룹 $< Z_p^*, \times >$의 생성원이고 p는 300자리 십진수(1024비트)에 해당하는 큰 소수이다.
8. CA는 임시키를 이용해 값을 암호화 $E_{K_{temp}}(A)$하여 사용자에게 전송한다.
9. 사용자는 자신이 생성한 난수(N_r)를 이용하여 임시키를 생성한다.
10. CA로부터 받은 메시지를 복호화하여 인증에 사용될 A값을 얻는다.

4.2 티켓발급 단계

티켓발급 단계에서 사용자는 서비스를 받고자 하는 서버로부터의 인증을 위한 티켓을 CA에게 요청한다. CA는 사용자로부터 받은 메시지를 이용해 사용자를 인증하고 사용자에게 티켓을 발급한다. 이 단계에서 사용자는 인증을 위해 필요한 값과 서비스를 제공받기 원하는 서버의 리스트를 전송한다. CA는 사용자에게 티켓을 전송하고 사용자는 전송받은 티켓을 이용하여 여러 서버로부터 인증 받을 수 있다. 모바일 디바이스는 서버와 같은 디바이스에 비해 계산 능력, 메모리, 배터리 전원 등과 같은 자원의 제약이 있으므로 제안하는 기법에서는 모바일 디바이스에서 수행되는 계산을 최소화하기 위해 비교적 연산량이 적은 해쉬 함수와 배타적 논리합과 같은 연산을 사용한다. 이 단계에서 우리는 CA와 서버 간에는 각각 안전한 전송을 위한 대칭키를 공유하고 있다고 가정한다. 〔그림 2〕는 티켓 발급 단계의 절차를 나타내고 자세한 티켓 발급 과정은 다음과 같다.

1. 사용자는 등록 단계에서의 아이디(ID_u)와 패스워드(PW_u)를 입력한다.
2. $B = h(ID_u \| PW_u)$를 계산한다.
3. 난수(N_u)를 생성한다. 난수는 티켓을 요청할 때마다 새로운 수를 생성한다.

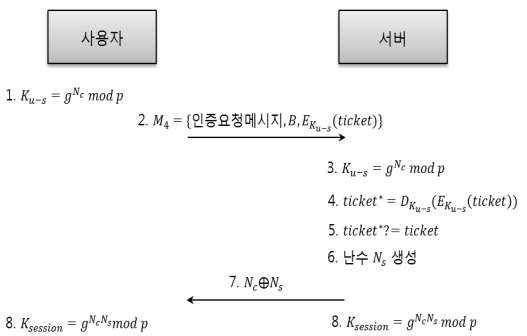
4. $C=h(B\|N_u)$과 $D=A\oplus N_u$를 계산한다.
5. 서비스를 받고자 하는 서버의 리스트와 함께 티켓 요청 메시지를 CA에게 전송한다.
6. CA는 사용자로부터 받은 B값을 확인하여 등록된 사용자인지 확인한다.
7. B값에 대응되는 A값을 이용해 $N_u^*=D\oplus A$를 얻는다.
8. $C^*=h(B\|N_u^*)$를 계산한다.
9. 사용자로부터 전송받은 C와 CA에서 생성한 C^*의 값이 같은지 확인한다. 만약 두 값이 일치하지 않으면 더 이상 이후의 과정을 수행하지 않고, 일치하면 티켓 발급을 위한 다음 과정을 계속 진행한다.
10. 티켓을 안전하게 전송하기 위한 키 $(K_{u-c}=g^{N_u}\bmod p)$를 생성한다.
11. 사용자가 CA를 인증하기 위한 $F=h(N_u+1)$를 계산한다.
12. 티켓 $Ticket=Sign_{CA}(AI,lifetime)$을 생성한다. 티켓은 인증정보와 티켓의 만료기간, CA의 서명을 포함한다.
13. CA는 난수(N_c)를 생성한다.
14. CA는 F 값, 난수(N_c)와 티켓을 키 K_{u-c}로 암호화하여 사용자에게 전송하고 난수(N_c), B와 티켓을 CA와 각 서버 간에 공유하는 대칭키로 암호화 하여 사용자의 서비스를 받고자 하는 서버 리스트의 각 서버에 전송한다.
15. CA로부터 메시지를 받은 사용자는 메시지를 복호화하고 $F^*=h(N_u+1)$를 계산한다.
16. 사용자는 $F^*=F$ 인지 확인하고 같으면 CA를 인증한다.
17. CA로부터 메시지를 받은 각 서버는 메시지를 복호화하고 티켓과 그에 해당하는 B 값과 난수 N_c을 저장한다.

4.3 티켓인증 단계

사용자는 CA로부터 받은 티켓을 이용하여 서비스를 받고자 하는 서버에 티켓을 제출하여 인증을 받음으로써 서버로부터 제공되는 서비스에 접근할 수 있다. 사용자는 한번 발급받은 티켓을 이용하여 티켓 발급 요청 메시지에 포함된 서버리스트에 있는 모든 서버로부터 하나의 티켓을 이용하여 인증을 받을 수 있으며 서비스 도중 세션이 끊기거나 접속을 해지한 후에도 이전에 접속하였던 서버에 기존의 티켓을 사용하여 인증 받을 수 있다. 즉 티켓에 명시되어 있는 티켓 만료기간(lifetime)이 유효하다면 다시 티켓을 발급받지 않고 인증 받을 수 있다.

〔그림 3〕은 티켓인증 단계의 절차를 나타내고 자세한 티켓 인증 과정은 다음과 같다.

1. 사용자는 CA로부터 받은 난수 N_c를 이용하여 티켓을 안전하게 전송하기위한 키를 생성한다. $K_{u-s}=g^{N_c}\bmod p$
2. 생성한 키를 이용하여 티켓을 암호화하고 서비스를 받고자 하는 서버의 식별자와 B 값과 암호화된 티켓을 포함한 인증 요청 메시지를 전송한다. $M_4=\{\text{인증요청메시지},B,E_{K_{u-s}}(ticket)\}$
3. 서버는 사용자로부터 인증 요청 메시지의 B에 해당하는 난수 N_c을 이용하여 티켓의 복호화를 위한키 $K_{u-s}=g^{N_c}\bmod p$을 생성한다.
4. 서버는 생성한 키를 이용 복호화하여 티켓 $Ticket^*=D_{K_{u-s}}(E_{K_{u-s}}(Ticket))$을 얻는다.
5. 티켓의 만료기간을 확인하고 CA로부터 받은 티켓과 사용자로부터 받은 티켓이 동일한지 확인한다.
6. 난수 N_s를 생성한다. 이 난수는 사용자와 서버 간의 안전한 통신을 위한 세션 키를 만드는데 사용한다.
7. 사용자에게 인증완료 메시지와 함께 $N_c\oplus N_s$ 값을 전송한다.
8. $N_s=(N_c\oplus N_s)\oplus N_c$을 얻고 사용자와 서버는 각자 세션 키를 생성한다. $K_{session}=g^{N_cN_s}\bmod p$



〔그림 3〕 티켓인증 절차

〔표 2〕 보안 비교

기법	S1	S2	S3	S4	S5	S6	S7	S8
제안기법	○	○	○	○	○	○	○	✖
〔12〕	✖	○	○	○	✖	✖	○	△
〔13〕	○	○	○	○	○	○	✖	○
〔14〕	✖	○	○	○	○	✖	○	✖

S1 : 내부자 공격 (Insider attack)
S2 : 재생 공격 (Replay attack)
S3 : 추측 공격 (Guessing attack)
S4 : 중간자 공격 (Man in the middle attack)
S5 : 훔친 검증자 공격 (Stolen verifier attack)
S6 : 상호인증 (Mutual authentication)
S7 : 세션 키 동의 (Session key agreement)
S8 : 사용자 익명성 (User anonymity)
○ : 보안 제공, △ : 일부 제공, ✖ : 보안 제공 안됨

V. 분석

이 절에서 제안하는 인증기법의 보안 분석과 성능 평가를 한다. 무선 통신환경 기반의 서비스는 유선 통신환경 기반의 서비스보다 보안에 취약하므로 보다 강력한 보안이 요구된다. 그러나 무선 환경에서 서비스를 제공받기위한 디바이스는 배터리 전원 기반의 모바일 디바이스로 계산능력과 메모리 공간 등의 제약사항을 갖고 있다. 따라서 제한된 자원으로 무선 통신 환경에서 발생할 수 있는 다양한 공격을 막을 수 있어야 하며 효율적이어야 한다.

5.1 보안 분석

3절에서 모바일 디바이스 기번의 무선네트워크 환경에서 안전한 사용자 인증을 위한 보안 요구사항을 살펴보았다. 여기서 제안하는 기법이 이들 보안 요구사항을 충족시킴을 보이고 추가적으로 상호인증과 세션 키 동의 기능을 제공함을 보인다. 〔표 2〕는 제안하는 기법과 Moon et al의 기법〔12〕, Park et al의 기법〔13〕, Shin et al의 기법〔14〕의 보안성에 대한 비교를 보여준다.

1) 내부자 공격(Insider attack)

등록 단계에서 사용자는 자신의 아이디와 패스워드를 직접 보내지 않고 아이디와 패스워드를 해쉬한 값 ($h(ID_u \| PW_u)$)을 보낸다. 일방향 해쉬함수로부터 원래의 값을 알아낼 수 없기 때문에 악의적인 내부자는 등록 요청 메시지에 포함된 값으로부터 사용자의 아이디와 패스워드를 수집할 수 없다. 따라서 제안하는 기법은 내부자 공격으로부터 안전하다.

2) 재생 공격(Replay attack)

제안하는 기법에 대한 재생 공격의 안전성은 티켓 발급 단계에서와 티켓인증 단계에서 살펴보아야 한다. 티켓발급 단계에서 공격자가 $n-1$번째의 티켓 요청을 위한 메시지($M_1^{(n-1)}$)를 수집하고 n번째의 티켓 요청 메시지를 가장하여 CA에게 보냈다고 가정하자. 이때 CA는 메시지에 대한 검증을 수행하고 티켓을 안전하게 전송하기 위해 사용자로부터 받은 N_u을 이용하여 키($K_{u-c} = g^{N_u} \bmod p$)를 생성하고 생성한 키를 이용하여 티켓과 CA의 난수를 암호화($E_{K_{u-c}}(Ticket \| N_c)$)하여 전송한다. 그러나 공격자는 난수 N_u을 알지 못하기 때문에 CA로부터 받은 메시지로부터 티켓을 얻을 수 없다. 또한 공격자는 A를 알지 못하기 때문에 티켓 요청 메지시의 $D(=A \oplus N_u)$로부터 난수 N_u를 구할 수 없다.

티켓인증 단계에서 $n-1$번째의 티켓 인증을 위한 메시지($M_4^{(n-1)}$)를 수집하고 n번째의 티켓 인증 메시지를 가장하여 서버에게 보냈다고 가정하자. 이때 서버는 전송받은 티켓에 대한 인증절차를 마치고 세션 키 생성을 위한 $N_c \oplus N_s$로부터 N_c와 N_s를 계산할 수 없기 때문에 세션 키를 생성할 수 없다.

따라서 제안하는 기법에서 공격자는 재생 공격을 성공할 수 없다.

3) 추측 공격(Guessing attack)

공격자가 통신 과정상의 모든 메시지를 도청하였다고 가정하자. 공격자는 티켓요청 단계에서의 $B(=h(ID_u \| PW_u))$로부터 사용자의 아이디와 패스워드를 얻고자 할 것이다. 그러나 사용자의 아이디와 패스워드는 일방향 해쉬함수에 의해 계산된 값이기 때문에 B

로부터 사용자의 아이디와 패스워드를 구한다는 것은 불가능하다.

추가적으로 공격자는 추측 혹은 다른 방식으로 정상적인 사용자의 아이디(ID_u*)와 패스워드(PW_u*)를 알아냈다고 가정하자. 공격자는 알아낸 ID_u*와 PW_u*를 이용하여 $B^* = h(ID_u^* \| PW_u^*)$를 계산하고 이전에 저장한 B의 값과 계산한 B^*와 비교하여 같다는 것으로 사용된 등록에 사용된 아이디와 패스워드를 확인할 수 있다. 그러나 제안하는 기법에서 공격자가 정상적인 사용자의 아이디와 패스워드를 알아냈을 지라도 A 값을 알지 못하기 때문에 정상적인 사용자가 생성할 수 있는 티켓 요청 메시지의 값 $D(=A \oplus N_u)$를 계산할 수 없다. 즉 정상적인 사용자의 아이디와 패스워드를 알아낸 공격자 일지라도 사용자의 A값을 알 수 없는 한 정상적인 사용자의 티켓 요청 메시지를 생성할 수 없다.

따라서 제안하는 기법은 추측 공격으로부터 안전하다. 게다가 공격자가 정상적인 사용자의 아이디와 패스워드를 알아냈을지라도 공격자는 정상적인 사용자로 인증 받을 수 없다.

4) 중간자 공격(Man in the middle attack)

티켓발급 단계에서 공격자는 사용자가 CA에게 전송하는 메시지 M_1을 가로채고 사용자로 가장하기 위해 B값과 공격자가 생성한 난수 N_A를 이용해 $C' = h(B \| N_A)$를 생성하고 C'를 포함하는 메시지 $M_1' = \{$티켓요청메시지, 서버리스트, $B, C', D\}$를 보냈다고 가정하자. 여기서 공격자는 사용자가 생성한 N_u는 모르기 때문에 D값을 수정할 수 없다. 공격자로부터 M_1'메시지를 받은 CA는 메시지를 인증하기 위해 $N_u^* = D \oplus A$를 계산하고 $C^* = h(B \| N_u^*)$를 계산한다. 그러나 CA가 생성한 C^*와 공격자가 보낸 C'는 일치하지 않기 때문에 인증에 실패한다. 따라서 공격자는 사용자로 가장할 수 없으며 공격자는 사용자의 난수 N_u를 모르기 때문에 메시지 M_2에서 티켓과 CA의 난수 N_c 역시 알아낼 수 없다. 따라서 공격자는 사용자와 CA간의 모든 메시지를 수집했을 지라도 사용자와 CA로 위장할 수 없으며 중요한 정보를 보거나 얻을 수 없다.

티켓인증 단계에서 공격자는 사용자와 서버 간에 주고받는 메시지를 모두 수집하였더라도 CA의 난수 N_c와 서버의 난수 N_s를 알지 못하기 때문에 사용자와 서버 사이의 안전한 메시지 전송을 위한 세션 키를 계산할 수 없다. 따라서 제안하는 기법은 중간자 공격으로부터 안전하다.

5) 훔친 검증자 공격(Stolen-verifier attack)

등록 단계에서 사용자는 자신의 아이디와 패스워드를 직접 전송하지 않고 이를 해쉬한 값 $h(ID_u \| PW_u)$을 전송한다. 따라서 CA 조차도 사용자의 아이디와 패스워드를 알 수 없으며 그 값으로부터 계산하여 그 값을 구해낼 수 없다. 또한 CA는 인증을 위해 사용자의 아이디와 패스워드 테이블을 저장하지 않고 사용자가 등록 당시 전송한 $B = h(ID_u \| PW_u)$와 대응되는 등록 당시 사용자의 난수 N_r로 이루어진 테이블만 저장하고 있다. 공격자에게 이 테이블이 노출 되었더라도 공격자는 CA의 비밀 값 x를 알지 못하기 때문에 인증을 위한 $A = h(N_u \| x)$를 계산할 수 없다. 따라서 공격자는 인증 요청 메지지의 $D = A \oplus N_u$를 생성할 수 없으므로 정상적인 티켓 요청 메시지를 생성할 수 없다. 따라서 제안하는 기법에서 비록 사용자 인증에 사용되는 테이블이 노출 되었을 지라도 전체적인 인증 메커니즘에 영향을 주지 못한다.

6) 상호인증(Mutual authentication)

상호인증은 사용자와 CA, 사용자와 서버 간에 이루어져야 한다. 티켓요청 단계에서 CA는 등록단계에서 CA에 등록한 정보(사용자의 B값과 난수 N_r)와 모바일 디바이스에 저장한 정보(A)를 바탕으로 사용자를 인증한다. 정상적인 사용자만이 정확한 아이디와 패스워드를 입력할 수 있으므로 $B = h(ID_u \| PW_u)$를 생성할 수 있고 A와 함께 전송할 수 있으므로 CA는 제안된 인증절차를 거쳐 정상적인 사용자를 인증할 수 있다. 또한 사용자는 CA로부터 인증이 완료된 이후 $F = h(N_u + 1)$를 CA의 인증을 위해 받는다. F값은 CA의 비밀 값 x를 알고 있는 정상적인 CA만이 인증절차를 거쳐 N_u를 알아낼 수 있으므로 사용자는 자신이 생성한 난수를 이용해 F^*를 생성하고 CA로부터 전송받은 F와 비교함으로써 CA를 인증할 수 있다.

또한 티켓인증 단계에서 사용자는 CA의 난수 N_c를 이용해 키를 생성하고 티켓을 암호화해 서버에 전송한다. 서버 역시 CA의 난수 N_c를 이용해 키를 생성하고 사용자로부터 받은 티켓과 CA로부터 받은 티켓을 비

〔표 3〕 모바일 디바이스에서의 인증을 위한 연산비용 비교

기법	티켓발급 단계	티켓인증 단계
제안기법	3H+1X+1SD	2E+1M+1SE
〔12〕	1H+5E+2X+1M+1SE+1SD	3X+1SE
〔13〕	1H+3E+1M+1AE+1AD	1AE+1AD
〔14〕	1SD	1SE

H : 해쉬연산 X : XOR 연산 SE : 대칭키 암호화 연산 AE : 비대칭키 암호화 연산
E : 지수연산 M : 곱 연산 SD : 대칭키 복호화 연산 AD : 비대칭키 복호화 연산

교함으로 사용자를 인증한다. 여기서 서버는 암호화된 키와 티켓의 일치를 통해 정상적인 사용자임을 인증할 수 있다. 이후 서버는 사용자에게 세션 키 생성을 위해 서버의 난수 N_s와 CA의 난수 N_c의 XOR 값을 전송한다. 사용자는 이 값에서 서버의 난수 N_s를 구하고 세션 키 $K_{session} = g^{N_c N_s} \bmod p$를 생성하여 서버로부터 암호화된 메시지를 생성한 세션 키로 복호화함으로 서버를 인증할 수 있다. 이는 정상적인 서버라면 동일한 세션 키를 생성할 수 있기 때문이다. 따라서 제안하는 기법은 사용자와 CA, 사용자와 서버 간에 상호인증을 제공한다.

7) 세션 키 동의(Session key agreement)

사용자와 서버는 세션 키 $K_{session} = g^{N_c N_s} \bmod p$를 공유한다. 여기서 세션 키를 생성할 때 필요한 CA의 난수 N_c는 티켓요청 단계에서 K_{u-c}와 K_{S-CA}로 암호화하여 각각 사용자와 서버에서 전송되므로 네트워크 상에서 직접 노출되지 않는다. 서버는 서버의 난수 N_s 역시 CA의 난수 N_c와 XOR 연산 값을 사용자에게 전송하므로 CA의 난수 N_c를 알지 못하는 공격자는 N_s를 알아낼 수 없다. 따라서 제안하는 기법은 인증 단계에서 사용자와 서버의 안전한 세션 키 동의 메커니즘을 제공한다.

5.2 효율성 분석

무선 네트워크 환경에서 모바일 디바이스를 이용한 서비스는 모바일 디바이스에서 수행되는 연산비용과 통신비용이 서비스의 효율성 및 안정성에서 중요한 요소이다. 따라서 실제 서비스에 적용하기 위해 사용자의 인증 메커니즘은 모바일 디바이스에서 연산과 통신의 오버헤드를 최소화한 효율적인 메커니즘으로 설계되어야 한다. 본 논문에서는 티켓을 이용해 사용자를 인증하는 기법을 제안하였다. 티켓을 이용한 사용자 인증 기법은 인증 서버로부터 하나의 티켓을 발급받고 여러 서비스 제공자에게 티켓을 제출하여 인증 받을 수 있기 때문에 다른 서버에 접속할 때마다 인증을 수행하는 기법보다는 효율적이다. 따라서 본 논문에서 효율성 분석을 위해 제안하는 기법과 티켓을 이용해 사용자를 인증하는 최근의 연구 Moon et al의 기법〔12〕과 Park et al의 기법〔13〕, Shin et al의 기법〔14〕의 인증 기법과 효율성을 비교 / 분석한다.

〔표 3〕은 제안하는 기법과 Moon et al의 기법〔12〕, Park et al의 기법〔13〕, Shin et al의 기법〔14〕의 모바일 디바이스에서의 연산 비용을 티켓발급 단계와 티켓인증 단계에서 비교하였다. 또한 모바일 디바이스(안드로이드 기반의 스마트 폰)에서의 주요 연산(해쉬, 대칭키, 비대칭키 연산)에 대한 비용을 측정하기 위한 실험을 수행하였다. 실험결과 해쉬 연산 0.13, 대칭키 연산 1.7/0.5(암호화/복호화), 비대칭키 연산 4.51.7/52.8(암호화/복호화)의 연산 비용을 보였다. 실험에서의 비용은 시간비용으로 단위는 밀리세컨드(milliseconds)이고 각 값은 실험의 평균값이다. Shin et al의 기법〔14〕의 기법은 티켓 발급 단계와 티켓 인증 단계에서 대칭키 암호화를 한번만 이용하다. 따라서 가장 효율적이나 그 기법에서 제안하는 환경은 이종 디바이스와 네트워크에서 티켓을 이용한 효율적인 인증 기법에 초점을 맞추었기 때문에 앞에서 설명한 몇 가지의 보안과 기능에 대한 문제가 존재한다. Moon et al의 기법〔12〕의 기법은 사용자가 외부 네트워크의 서비스 제공자로부터 서비스를 받을 경우 외부 네트워크의 인증 서버로부터 인증을 받고 서비스 제공자에 접근해야하거나 티켓 갱신이 필요하다. 따라서 외부 네트워크에 접속하여 서비스를 제공받을 때마다 추가적인 인증 절차가 필요하다. Park et al의 기법〔13〕은 인증을 위한 메시지의 전송의 안전을 위해 공개키를 이용해 암호화와 복호화를 한다. 이는 자원이 제약이 있는 모바일 디바이스에서 인증 지연을 발생시킨다. 공개키 기반의 알고리즘 사용은 보안성 측면에서 많은 이점을 제공하지만 많은 연산 오버헤드를 초래하므로 모바일 디바이스를 이용하는 실제 서비스

에 적용에 부적합하다. 제안하는 기법은 티켓발급 단계와 티켓인증 단계에서 안전한 메시지 전송을 위해 각각 한 번의 대칭키 연산을 수행한다. 티켓발급 단계에서 한 번의 메시지 복호화 연산과 티켓인증 단계에서 한 번의 메시지 암호화 연산만 수행한다. 따라서 Moon et al의 기법[12], Park et al의 기법[13]의 인증기법보다 제안하는 인증 기법은 모바일 디바이스에서 적은 연산 오버헤드를 갖는다.

VI. 결 론

본 논문에서 모바일 디바이스 기반의 무선 네트워크 환경에서 티켓을 이용한 효율적인 인증 기법을 제안하였다. 제안하는 기법은 보안성 측면에서 사용자의 인증에서 발생할 수 있는 내부자 공격, 재생 공격, 추측 공격, 중간자 공격, 훔친 검증자 공격으로부터 안전하다. 또한 사용자와 CA, 사용자와 서버 간에 상호 인증할 수 있으며 인증완료 후에 사용자와 서버는 안전하게 세션 키를 공유할 수 있다. 효율성 측면에서 모바일 디바이스의 계산 능력의 한계와 배터리 전원 소모의 최소화를 위해 모바일 디바이스에서의 적은 연산을 수행하는 기법을 제안하였다. 제한기법에서 사용자는 CA로부터 티켓을 발급받고 서비스를 받고자 하는 서버에 티켓을 제출하여 인증을 받을 수 있으며 다른 서버로부터 서비스를 받고자 할 때 다시 티켓을 발급받지 않고 동일한 티켓을 제출하여 다른 서버로부터도 인증 받을 수 있다.

그러나 제안하는 기법에서는 사용자의 익명성과 패스워드 변경 메커니즘을 제공하지 않는다. 이동이 자유로운 모바일 환경에서 사용자의 익명성은 사용자의 프라이버시를 위해 매우 중요한 보안 요구사항이며 패스워드 기반의 인증 기법에서 안전한 패스워드 업데이트의 제공은 강화된 보안의 제공을 위해 중요한 요구사항이므로 향후 연구로 현재 제안하는 기법의 보안을 보다 강화하기 위해 사용자의 익명성과 패스워드 변경 기법에 대한 추가 연구를 할 것이다.

참고문헌

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[2] C.H. Liao, H.C. Chen, C.T. Wang, "An Exquisite Mutual Authentication Schemes with Key Agreement Using Smart Card," Informatica, vol. 33, no. 2, pp. 125-132, May. 2009.

[3] W.S. Juang, "Efficient password authenticated key agreement using smart cards," Computer & Security, vol. 23, no. 2, pp. 167-173, Mar. 2004.

[4] S.W. Lee, H.S. Kim, K.Y. Yoo, "Comment on 'A Remote User Authentication Scheme using Smart Cards with Forward Secrecy'," In IEEE Transaction on Consumer Electronics, vol. 50, no. 2, pp. 576-577, May. 2004.

[5] Y.P. Liao, S.S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interface, vol. 31, no. 1, pp. 24-29, Jan. 2009.

[6] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," International Journal of Communication Systems, vol. 24, no. 3, pp. 347-362, Mar. 2011.

[7] S.B. Shin, H.J. Yeh, K.H. Kim, K.S. Kim, "A Remote User Authentication Scheme with Anonymity for Mobile Devices," International Journal of Advanced Robotic Systems, vol. 9, pp. 1-7, Apr. 2012.

[8] D. He, S, Chan, C. Chen, J. Bu, R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Communications, vol. 61, no. 2, pp. 465-476, Nov. 2011.

[9] J. Xu, W.T. Zhu, D.G, Feng, "An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks," Computer Communications, vol. 34, no. 3, pp. 319-325,

Mar. 2011.
〔10〕 Z.J. Tzeng, W.G. Tzeng, "Authentication of mobile users in third generation mobile systems," Wireless Personal Communications, vol. 16, no. 1, pp. 35-50, Jan. 2011.
〔11〕 J. Zhu, J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 231 - 235, Feb. 2004.
〔12〕 J.S. Moon, I.Y. Lee, "An AAA scheme using ID-based ticket with anonymity in future mobile communication," Computer Communications, vol 34, no 3, pp. 295-304, Mar. 2011.
〔13〕 J.H. Park, "An authentication protocol offering service anonymity of mobile device in ubiquitous environment," The Journal of Supercomputing, vol 62, no 1, pp. 105-117, Oct. 2012.
〔14〕 S.B. Shin, H.J. Yeh, K.S. Kim, "A Ticket based Authentication Scheme for Group Communication," In Proceedings of The 2012 International Conference on Information Security and Assurance, pp. 152-155, Apr. 2012.

〈著者紹介〉

신 수 복 (Soobok Shin) 학생회원
2003년 8월: 아주대학교 수학, 정보컴퓨터공학 학사
2006년 8월: 아주대학교 정보통신공학 석사
2013년 2월: 아주대학교 정보통신공학 박사
〈관심분야〉 네트워크, 사용자/디바이스 인증, 네트워크 보안

예 홍 진 (Hongjin Yeh) 종신회원
1986년 2월: 서울대학교 수학교육 학사
1988년 2월: 아주대학교 전자계산 석사
1993년 6월: 리용1대학교 전자계산 박사
1993년 8월~현재: 아주대학교 정보컴퓨터공학부 부교수
〈관심분야〉 정보보호, 모바일 보안, 애플리케이션 보안

김 강 석 (Kangseok Kim) 정회원
2007년 11월: 인디애나대학교 컴퓨터공학 박사
2010년 9월~현재: 아주대학교 지식정보공학과 연구교수
〈관심분야〉 모바일 컴퓨팅, 유비쿼터스 컴퓨팅, 스마트폰 애플리케이션, 모바일 보안, 데이터 마이닝, 바이오인포메틱스