Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 3 pp. 1428-1438, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.3.1428

스마트 보안패드를 이용한 안전한 인터넷 서비스 제공 모델에 관한 연구

이재식[1], 김형주[1*], 전문석[1]
[1]숭실대학교 컴퓨터학과

A Study on a Secure Internet Service Provider Model Using Smart Secure-Pad

Jae-Sik Lee[1], Hyung-Joo Kim[1*] and Moon-Seog Jun[1]
[1]**Department of Computer Science, Soongsil University**

요 약 인터넷 환경에서 이루어지는 서비스는 사용자와 서비스 제공자 사이에 신뢰관계를 형성하고 서비스를 제공한다. 이를 위하여 아이디/비밀번호와 같은 간단한 사용자 인증에서부터, 공개키 기반구조의 공인인증서를 이용한 인증까지 다양한 인증방안이 제안되고 있다. 또한, 전자금융거래의 경우 거래내역의 무결성 및 부인방지 기능도 제공하고 있다. 이처럼 인터넷 환경에서 제공되는 서비스들은 서비스의 안전성을 보장하기 위한 다양한 방법들을 활용하고 있다. 하지만 웹브라우저의 메모리영역을 조작하는 MITB 공격과 같은 기존의 보안기술을 이용하여 예방하기 어려운 공격들이 등장하고, 피싱/파밍과 같은 사회공학적 공격들이 등장하면서 새로운 보안기술의 적용이 필요하게 되었다. 본 논문에서는 스마트 보안패드라는 개념을 제안하고, 이를 활용하여 사용자와 서비스 제공자 사이에 신뢰관계를 안전하게 형성하고, 전송되는 데이터의 안전성을 보장하는 모델을 제안한다. 제안하는 모델은 보안성 평가 결과 기존의 보안기술이 예방하기 어려운 MITB 및 피싱/파밍과 같은 공격에 안전함을 보인다. 또한, 제안하는 모델을 적용한 대표적인 서비스 예시를 통하여 서비스를 제공하는 사업자가 쉽게 해당 모델을 적용하여 안전한 환경에서 인터넷 서비스를 제공할 수 있다.

Abstract Services take place in Internet environment, a formation of the trust relationship between user and service provider for services. Different authentication schemes such as using Certificate of Public Key Infrastructure authentication and using ID/PW for a simple user authentication have been proposed for trust relationship. In addition, in the case of electronic financial transactions, transaction integrity and non-repudiation features are provided. These services are provided in Internet environment, use various measures to ensure service safety. However, it was difficult to prevent attacks using existing security technology because of emergence of MITB attack that manipulate the memory area of the Web browser and social engineering attacks such as phishing/pharming, requires application of new security technologies became. In this paper, we propose a concept of smart secure-pad, and utilize it safely formed a trust relationship between user and service provider, a model has been proposed to ensure safety of data transmission. Proposed model's security evaluation results show security against to MITB attack and phishing/pharming that can't be prevent attack using existing security technology. In addition, service provider can easily apply the model in safe environment can provide Internet service using provided representative services applying the proposed model.

Key Words : Authentication, End-to-End Encryption, Internet Banking, MITB, Smart Secure-Pad

*Corresponding Author : Hyung-Joo Kim(Soongsil Univ.)
Tel: +82-2-826-6526 email: j30231@ssu.ac.kr
Received February 13, 2013 Revised February 27, 2013 Accepted March 7, 2013

1. 서론

정보통신기술의 발달로 사용자는 인터넷 환경에서 다양한 서비스를 제공받고 있다. 인터넷 환경은 기존의 오프라인 환경에서 제공하던 서비스를 온라인 환경에서 제공할 수 있도록 도와준다. 과거 오프라인 상에서 상품을 거래하던 쇼핑이, 현재는 온라인 쇼핑몰을 통하여 이루어지고 있으며, 오프라인 창구에서 이루어지던 금융거래도 전자금융거래로 확정되어 서비스가 제공되고 있다. 이처럼 온라인상에서 서비스가 이루어지기 위해서는 사용자와 서비스를 제공하는 서비스 제공자(SP:Service Provider) 사이에 신뢰적인 관계가 형성되어야 한다. 이를 위하여 아이디/비밀번호 등과 같은 간단한 사용자 인증에서부터 공개키 기반구조(PKI:Public Key Infrastructure)의 공인인증서를 통한 인증까지 다양한 인증 방안이 제공되고 있다[1]. 제공되는 서비스에 따라서 인증의 보안강도는 달리 적용될 수 있다. 이는 보안강도를 높이 적용하는 경우 안전한 서비스를 제공할 수 있으나, 그에 따른 추가적 비용이 발생할 수 있고, 사용자의 편의성을 떨어뜨릴 수 있는 단점이 발생하기 때문이다. 보안강도가 높게 적용되는 서비스의 예로 인터넷 뱅킹과 같은 전자금융거래 서비스를 들 수 있다.

보안성 향상을 위한 방법으로 다양한 인증 요소를 이용한 인증 기술이 제안되었다[1,2]. 국내의 경우 인터넷 뱅킹 서비스 제공을 위하여, 보안카드, OTP, 공인인증서 등 다양한 인증 수단을 제공하고 있다. 또한, 중간자 공격(MITM:Man-In-The-Middle), 브라우저 조작 공격(MITB:Man-In-The-Browser)과 같은 공격에 대비하여, ARS전화인증 서비스 등 투 채널(Two-Channel) 인증 서비스도 제공하고 있다. 국외의 경우도 CAPTCHA를 활용한 인증[3], 안전한 사용자 토큰을 이용한 인증[1,2] 등 다양한 인증기법이 소개되고 있으나, 실제 사용함에 있어 사용자의 불편함 또는 비용적인 이슈가 존재한다. 특히, 하나의 채널을 통하여 인증을 제공하는 경우, 메모리 공격과 같은 MITB 형태의 공격에 취약하므로, 두 개 이상의 채널을 통한 인증서비스의 제공을 통하여 안전성을 확보해야 한다. 하지만, 현재 국내에서 제공되는 투 채널 인증서비스는 ARS전화인증 서비스만 유일하게 제공되어 있어, 다양한 투 채널 인증서비스의 개발이 필요한 실정이다.

본 논문에서는 안전한 인터넷서비스를 제공하기 위하여 현재 널리 사용 중인 스마트폰, 스마트패드와 같은 스마트 기기를 이용하여 안전성을 제공하는 모델을 제안한다. 제안하는 모델은 인터넷서비스 이용 시 중요한 데이터를 “스마트 보안패드”를 이용하여 입력함으로 공격자로부터 입력되는 데이터의 안전성을 보장한다. “스마트 보안패드”는 서비스 제공자와 사용자가 안전하게 데이터를 전송할 수 있는 기기를 의미하며, 본 논문에서는 이러한 기능을 제공하는 스마트 보안패드 프로그램이 설치된 스마트 기기를 “스마트 보안패드”라 한다.

제안하는 논문의 구성은 다음과 같다. 2장에서는 기존에 제안된 인증 기술에 관하여 살펴보고 문제점을 도출한다. 3장에서는 스마트 보안패드를 이용한 제안 모델을 살펴본다. 4장에서는 제안하는 모델을 이용하여 서비스를 제공하는 경우 보안성에 관하여 평가를 하고, 5장에서 본 논문을 정리하고 결론을 맺는다.

2. 관련연구

인터넷 환경에서 인증 기술은 아이디/비밀번호의 간단한 인증 기술부터 공개키 기반구조의 공인인증서를 활용한 전자금융거래 인증 기술까지 다양한 형태로 발전되어 왔다[1,2,4,5]. 이번 장에서는 이러한 인증 기술의 발전 형태를 살펴본다. 2.1절에서는 보안성이 가장 강화된 형태인 전자금융거래 보안기술을 살펴본다. 그리고 2.2절에서는 웹브라우저의 메모리를 조작하는 형태의 공격인 MITB 공격을 살펴보고, 2.3절에서는 MITB 공격을 예방하고자 등장한 종단 대 종단 간 전자금융거래 인증 기술에 관하여 알아보고, 그 한계점을 살펴본다.

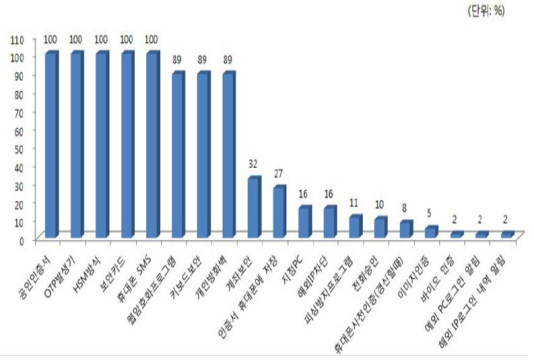
2.1 전자금융거래 인증 기술

전자금융거래 인증 기술은, 과거 오프라인 금융거래에서부터 정보통신기술의 발달로 온라인 전자금융거래까지 인증 기술이 발전한 형태이다. 과거 금융거래에서의 인증 기술은, 오프라인 창구서비스에서 법적 기관으로부터 획득된 신원확인정보를 이용해 대면확인을 통한 인증으로 시작하였다[2]. 하지만, 금융거래가 수행되는 환경이 온라인으로 변함에 따라, 전자금융거래상에서 요구되어지는 새로운 인증 기술이 필요하게 되었고, 전자금융거래 서비스를 제공하는 서비스 제공자(SP:Service Provider)는 온라인에서 사용될 수 있는 새로운 인증 기술을 필요로 하게 되었다.

국내 전자금융거래 인증 기술의 주요 목표는 클라이언트와 서버 간 통신 채널의 안전성 보장이며[4], 전자금융거래 인증 기술로 PKI를 적용해 클라이언트 및 서버 인증, 통신 패킷에 대한 기밀성 및 무결성, 그리고 부인방지와 같은 전자금융거래에 필요한 보안 요구사항을 만족시켰다.

전자금융거래 인증 기술이 발달함에 따라, 통신 채널의 보안은 강화되었고, 안전성이 매우 높아졌다. 하지만, 공격자는 보안이 강화된 통신 채널 영역 보다 보안이 취약한 채널의 종단(사용자PC 등)영역을 공격한다. 최근 전자금융거래 공격 기술은 악성코드 및 바이러스 등을 통하여, 키로거 프로그램을 설치하여 사용자 PC자체를 노리거나, 사회공학적 공격으로 사용자를 위·변조된 사이트로 유도하는 피싱(Phishing) 공격, 그리고 사용자PC의 DNS 호스트 정보를 조작하는 파밍(Pharming) 공격 등 사용자의 실수를 유발시켜 공격을 하는 형태로 공격기술이 변화하고 있다[5].

이러한 공격을 보호하기 위해, 국내에서는 다양한 요소(Multi-Factor) 인증 기술 및 다양한 채널(Multi-Channel) 인증 기술을 도입하였다. 이를 위하여 OTP, 휴대폰SMS 인증 등을 도입하였고, 사용자PC에 저장되는 정보가 평문으로 존재하는 구간을 없애기 위해 키보드 보안 프로그램, 종단 간 암호화 모듈 등을 도입하였다[1].



[Fig. 1] Provided Secure Service on Electronic Finance

국내 전자금융거래에서 사용되는 보안기술은 Fig. 1과 같으며, 거래이용수단별로 Table 1과 같이 보안등급을 부여하고, 부여된 보안등급에 따라 거래 방법, 거래량 등에 한도가 적용되어 있다.

[Table 1] Secure Method Layer

Security Level	Transaction Authentication Method
Level 1	- OTP + Certificate - HSM Certificate + SecureCard - Two-Channel AUTH + SecureCard + Certificate
Level 2	- SecureSMS + Certificate
Level 3	- SecureCard + Certificate

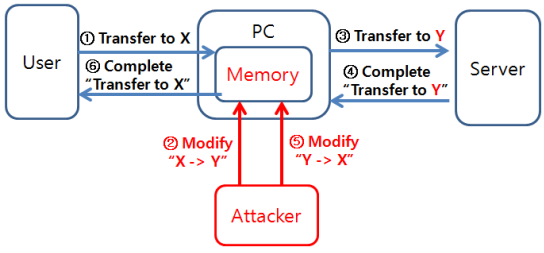
하지만, Table 1에서 알 수 있듯이, 국내 전자금융거래 보안기술은 다양한 요소(Multi-Factor) 인증 기술 위주로 보안기술이 구성되어 있다. 이러한 인증 기술은 MITB 공격에 취약하다. MITB 공격을 예방하기 위해서는 다양한 채널(Multi-Channel) 인증 기술이 도입되거나, HSM(Hardware Security Module)과 같은 하드웨어적으로 별도의 공간에서 인증이 이루어져야 한다. 하지만 디스플레이를 할 수 없는 HSM을 이용하는 경우, 서명되는 값의 진위여부를 확인할 수 없어, 여전히 MITB 공격에 취약한 단점이 있다.

현재 국내에서는 제공되는 유일한 다양한 채널 인증 기술로 투 채널(Two-Channel) 인증 기술인 ARS전화인증이 있다. 하지만 ARS전화인증의 경우 음성서비스를 통하여 인증이 이루어지므로, 인증 시간이 길고, 그 사용이 불편한 단점이 있다.

2.2 MITB 공격

MITB(Man-In-The-Browser) 공격은 통신 채널에 적용된 보안 인증 기술을 무력화 할 수 있는 대표적인 종단 공격 중 하나로 메모리 해킹 공격으로 잘 알려져 있다[6,7].

MITB 공격은 사용자PC에 설치된 악성코드가 웹 브라우저 또는 PC의 메모리를 직접 변경하는 공격 방식이다. Fig. 2는 전자금융거래가 이루어질 때 MITB 공격이 이루어지는 과정을 나타낸다.



[Fig. 2] Man-In-The-Browser(MITB) Attack

공격자는 사용자가 이체하고자 하는 계좌정보 및 이체금액을 공격자가 원하는 계좌정보와 이체금액으로 변조하고, 사용자에게는 정상적인 계좌정보 및 이체금액을 보여주어 최종적으로 공격자의 계좌에 금액을 이체하도록 공격한다. MITB 공격은 공격이 이루어 질 때 사용자가 공격 사실을 인지할 수 없다는 추가적인 위협을 가지고 있다.

2.3 종단 간 전자금융거래 보안기술

전자금융거래 시 사용자PC와 같은 종단에서 수행되는 공격을 예방하기 위하여 종단 대 종단 간(E2E : End to End) 보안기술이 개발 및 연구되었다[6,8].

대표적인 종단 대 종단 간 보안기술로 키보드 보안모듈이 있다. 키보드 보안모듈은 키보드를 통하여 입력된 데이터가 암호문으로 변환되어 전송되는 것으로, 공격자는 암호문의 키 값을 알 수 없어 데이터를 위·변조 하기 어렵다. 하지만, 종단 대 종단 간 보안기술은 현재 일부 금융기관에서만 적용하고 있다. 또한, 기술을 적용한 금융기관 중 일부는 사용자의 편의성 등을 위하여 보안설정을 낮게 설정하여, 여전히 보안에 취약한 단점을 가지고 있다[7]. 또한 금융보안연구원에 따르면 종단 대 종단 간 보안기술을 적용하더라도 일부 평문구간이 존재하는 문제점과 COM후킹에 취약한 문제점이 존재한다[6].

그 밖에도 사용자PC와는 별도로 독자적인 하드웨어를 사용하여 해당 하드웨어 영역에서 암호화를 수행하는 HSM(Hardware Security Module)과 같은 장비를 이용한 인증 기술이 등장하였다. 하지만, 장비 구입에 따른 비용적 이슈 및 항상 하드웨어를 소지하고 있어야 하는 불편 등 사용자의 편의성이 낮은 단점이 존재하여 널리 보급되지 못한 한계점을 지니고 있다.

이러한 문제점을 해결하기 위하여 다양한 디바이스 기반의 다양한 채널(Multi-Channel) 인증 기술을 통한 종단 대 종단 간 전자금융거래 보안 기술도 개발 및 연구되고 있으나, 특정 분야에 국한되어 기술이 제공되거나, 인증 절차 및 방식에 대한 체계화와 모델링이 되어있지 않아 그 활용성이 떨어지는 한계점이 있다[5,9-11].

3. 제안하는 모델

본 논문에서는 스마트 기기를 활용하여, 인터넷 서비스 이용 시 안전하게 이용할 수 있는 모델을 제안한다. 제안하는 모델의 특징은 스마트 기기를 통하여 중요한 정보를 입력함으로써, 사용자 PC가 악성코드에 감염되거나 키로거(KeyLogger)가 설치되어 중요정보가 외부로 유출되는 것을 원천적으로 차단한다.

제안하는 모델은 입력의 형태, 이용하는 스마트 기기의 정보, 접속 채널, 스마트 기기를 통해 전송하는 정보의 구분 등에 따라 다양한 형태로 서비스가 구성될 수 있다. 또한, 서비스 사업자는 서비스 제공을 위하여 구성된 구성주체에 따라 다양한 형태로 그 구조가 나누어 질 수 있다. 본 논문에서는 3가지 유형으로 사업자 구조를 분류하고 이를 기준으로 설명한다.

제안하는 모델을 이용하여 사용자는 스마트 기기를 통하여 서비스 제공자에 안전하게 데이터를 전송한다. 이때 이용되는 스마트 기기를 “스마트 보안패드”라 한다. 즉, 사용자는 스마트 보안패드를 이용하여 안전하게 인터넷 서비스를 이용할 수 있다.

이번 장은 다음과 같이 구성된다. 3.1절은 본 논문의 가정 사항을 정의하고, 3.2절과 3.3절은 제안하는 모델에서의 구성될 수 있는 서비스 제공의 형태와 서비스 제공자의 구조를 설명한다. 3.4절과 3.5절은 서비스를 이용하기 위한 가입단계 및 이용단계를 설명하고, 3.6절은 제안하는 모델을 적용한 서비스 예시를 보여준다.

3.1 가정 사항

본 논문은 다음과 같이 가정 사항을 정의한다.

1) 사용자는 컴퓨터(PC:Personal Computer)와 스마트 기기(SD:Smart Device)를 가지고 있다.
2) 스마트 기기는 탈옥(JailBreaking) 및 루팅(Rooting) 등과 같이 운영체제가 수정된 상태가 아니며, 악성코드 및 바이러스 등에 감염되지 않은 안전한 상태다.
3) 사용자와 서비스 제공자는 신뢰된 인증기관으로부터 발급받은 인증서를 신뢰하며, 전자서명을 생성하고 검증할 수 있다.

3.2 서비스 제공을 위한 형태 분류

제안하는 모델은 서비스 제공을 위하여 입력형태, 스마트 기기 식별방법, 이용채널, 이용정보에 따라 각기 다른 형태로 서비스를 제공할 수 있다.

3.2.1 입력형태

스마트 기기를 이용하여 사용자가 서비스 제공자에 정보를 입력하는 형태를 말하며 다음의 2가지 형태로 구성된다.

1) Key-Type1(숫자) : 0~9까지의 10가지 숫자를 입력할 수 있는 입력형태를 Key-Type1이라 한다.
2) Key-Type2(숫자+문자) : 일반적인 키보드와 같이 숫자를 포함한 모든 문자를 입력할 수 있는 입력형태를 Key-Type2라 한다.

3.2.2 스마트 기기 식별방법

서비스 제공자는 사용자의 스마트 기기를 구별하기 위하여 스마트 기기가 가지고 있는 정보를 활용하여 다음과 같이 3가지 타입으로 스마트 기기를 식별한다.

1) DI-Type1 : 스마트 기기 제조사에서 자체적으로 할당한 고유의 단말기정보인 시리얼번호(SN:Serial Number) 또는 스마트 기기의 무선랜 카드가 가지고 있는 MAC(Media Access Control) 주소를 이용하여 식별하는 것을 DI-Type1이라 한다.
2) DI-Type2 : 스마트 기기마다 유일하게 가지고 있는 국제모바일기기식별코드(IMEI:International Mobile Equipment Identity)값을 이용하여 식별하는 것을 DI-Type2라 한다.
3) DI-Type3 : IMEI 정보와 함께 이동통신사가 사용자에게 부여한 전화번호를 포함한 국제이동국식별번호(IMSI:International Mobile Subscriber Identity)를 이용하여 식별하는 것을 DI-Type3라 한다. 일반적으로 3G/4G에서 IMSI정보는 가입자식별모듈(USIM:Universal Subscriber Identity Module)카드에 저장되어 있다.

3.2.3 이용채널

스마트 기기와 서비스 제공자가 통신하는 통신 채널은 다음 3가지 채널로 구분한다.

1) Ch-Type1 : 스마트 기기와 무선AP 사이에 어떠한 암호 프로토콜도 적용하지 않고, WiFi를 이용하여 통신하는 형태를 Ch-Type1이라 한다.
2) Ch-Type2 : 스마트 기기와 무선AP 사이에 WPA, WPA2 등과 같은 암호화프로토콜을 적용하여 WiFi와 통신하는 형태를 Ch-Type2라 한다.
3) Ch-Type3 : 스마트 기기는 이동통신사에서 제공하는 이동통신망을 통하여 3G 또는 4G 형태로 통신하는 형태를 Ch-Type3라 한다.

3.2.4 이용정보

사용자가 스마트 보안패드를 통하여 입력하는 정보는 다음 3가지 종류로 분류한다.

1) UI-Type1 : 사용자의 로그인 비밀번호와 같이 사용자만 알고 있어야 하며, 외부로 노출되면 안되는 정보를 UI-Type1이라 한다. 일반적으로 사업자는 UI-Type1값을 일방향 암호화(Hash)하여 저장하므로, 비밀번호의 진위여부만 확인 가능하며, 그 실제 값은 알 수 없다.
2) UI-Type2 : 금융거래에 사용되는 계좌번호, 이체금액, 보안카드번호 등과 같은 금융정보를 UI-Type2라 한다. 국내의 경우 금융정보를 활용한 계좌이체 등의 정보는 반드시 그 정보를 전자서명해야 그 효력을 인정받는다.
3) UI-Type3 : 주민등록번호, 여권번호와 같은 사용자를 식별할 수 있는 개인정보를 포함하여, 입력 값이 위·변조 및 오·남용되었을 경우 문제가 될 수 있는 모든 중요정보를 UI-Type3라 한다. 예를 들어, 온라인 쇼핑몰에서 상품을 구입 시 중요정보는 상품의 수량 및 배송지 정보 등이 될 수 있다.

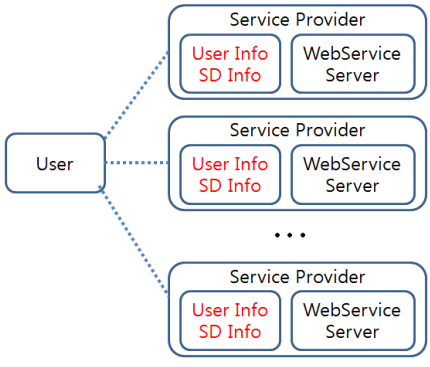
3.3 사업자 구조

서비스를 제공하는 사업자는 사용자의 정보 및 스마트 기기의 정보를 가지고 있는 주체에 따라 다양하게 사업자의 구조를 구성할 수 있다. 본 논문에서는 서비스 제공자 중심, 이동통신사 중심, 제3의 인증기관 중심의 3가지로 대표적인 사업자 구조를 분류하고 설명한다.

만약 서비스 제공자가 금융서비스 등과 같이 공인인증서를 이용해야 하는 경우, 인증기관(CA)을 통하여 인증서의 검증 및 전자서명의 검증이 이루어져야 한다.

3.3.1 서비스 제공자 중심 구조

서비스 제공자(SP:Service Provider) 중심 구조는 서비스 제공자가 사용자 및 스마트 기기의 모든 정보를 가지고 있는 구조로 Fig. 3과 같다. 스마트 보안패드의 프로그램은 해당 서비스 제공자에 특화될 수 있어, 서비스 제공자별로 상호호환을 지원하기 어려워 각기 다른 스마트 보안패드 프로그램을 설치해야 한다. 따라서, 서비스 제공자에 필요한 공통의 프로그램을 개발하고, 각 서비스 제공자별로 별도의 모듈을 이용하는 형태 등 호환성 제공을 위한 방안이 제공되어야 한다.

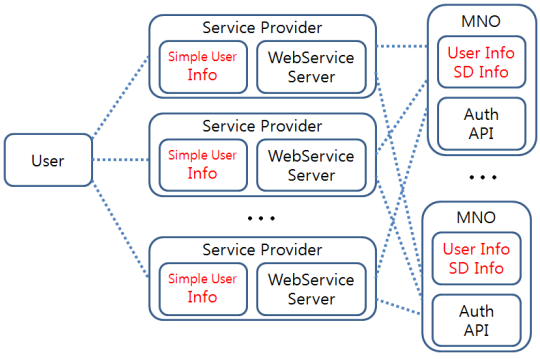


[Fig. 3] Service Provider Centric Structure

3.3.2 이동통신사 중심 구조

이동통신사(MNO:Mobile Network Operator) 중심 구조는 서비스 제공자는 사용자의 간단한 정보만 가지고 있고, 자세한 정보는 이동통신사가 가지고 있는 구조로 Fig. 4와 같다. 서비스 제공자는 이동통신사를 통하여 사

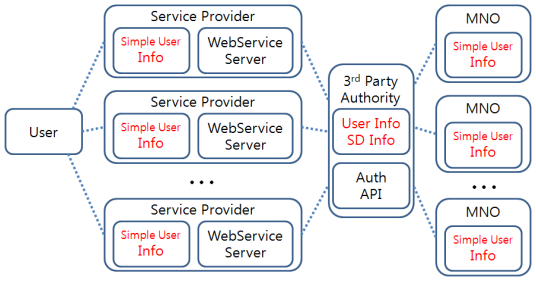
용자를 인증할 수 있다. 이동통신사는 다수의 서비스 제공자와 제휴를 통하여, 이동통신사가 제공하는 하나의 스마트 보안패드 프로그램을 이용하여 제휴된 모든 서비스 제공자와 서비스 이용이 가능하다.



[Fig. 4] MNO Centric Structure

3.3.3 제3의 인증기관 중심 구조

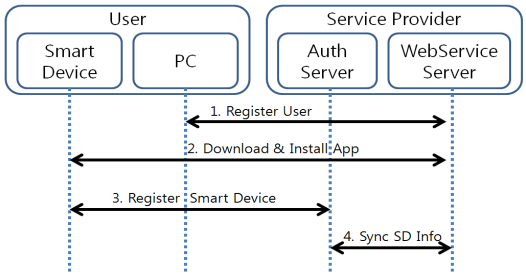
제3의 인증기관 중심 구조는 제3의 신뢰할 수 있는 인증기관이 이동통신사와 서비스 제공자 사이를 연결시켜주는 구조로 Fig. 5와 같다. 사용자 및 스마트 기기정보는 제3의 인증기관이 보유하고 있다. 제3의 신뢰된 인증기관은 다수의 이동통신사 및 다수의 서비스 제공자들과 제휴를 맺어, 하나의 스마트 보안패드 프로그램을 이용하여 제휴된 모든 서비스 제공자와의 서비스이용이 가능하다.



[Fig. 5] 3rd Party Authority Centric Structure

3.4 서비스 등록 단계

사용자는 서비스 이용을 위하여, 자신의 스마트 기기를 스마트 보안패드로 등록하고, 스마트 기기에 스마트 보안패드 프로그램을 다운로드 받아야 한다. 사업자의 구조에 따라 서비스 등록의 세부 과정은 달라 질 수 있으나, 전체적인 흐름은 크게 다르지 않으므로, 본 절에서는 서비스 제공자 중심 모델을 기준으로 서비스 등록 단계를 설명한다.



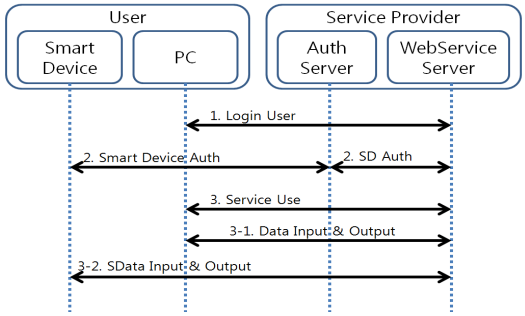
[Fig. 6] Service Register Phase

서비스 등록 과정은 Fig. 6과 같이 총 4가지 세부 단계로 나누어져 있으며 각 단계의 설명은 다음과 같다.

1) 사용자 등록 : 사용자는 PC를 이용하여 서비스 제공자의 인터넷서비스 서버에 접속하고, 서비스 가입을 한다.
2) 다운로드 & 설치 : 사용자는 서비스 제공자가 제공하는 스마트 기기용 어플리케이션을 다운로드 받고 설치한다.
3) 스마트 보안패드 등록 : 사용자는 스마트 보안패드 프로그램 이용하여 해당 서비스 제공자의 인증서버에 사용자의 스마트 기기를 등록한다. 스마트 기기의 구분을 위하여 3.2.2항에서 설명한 3가지 타입(DI-Type1~3)으로 정보를 등록한다. 또한 사용자는 스마트 기기의 분실 등에 대비하여 스마트 보안패드 프로그램에 PIN 번호를 설정할 수 있다.
4) 스마트 기기 정보 전달 : 서비스 제공자는 등록된 사용자의 기기정보를 인터넷 서비스 서버에 전달하고 등록한다.

3.5 서비스 이용 단계

서비스 가입을 마친 사용자는 Fig. 7과 같이 서비스를 이용한다. 서비스 이용과정은 3가지 세부 단계로 이루어져 있으며, 각 단계별 설명은 다음과 같다.



[Fig. 7] Service Use Phase

1) 사용자 로그인 : 사용자는 서비스 제공자의 인터넷 서비스 서버에 접속하고, 사용자 정보를 이용하여 로그인을 한다. 전송되는 데이터는 SSL/TLS 등과 같은 암호화 프로토콜을 이용하여 암호화 되거나 독자적인 암호화 프로토콜을 적용하여 암호화 된 형태로 통신한다. 만약 비밀번호 입력에 대한 강력한 보안성이 요구되는 경우, 서버는 사용자의 아이디만 입력받고, 비밀번호는 스마트 기기와 통신과정에서 3.2.4항의 UI-Type1 으로 입력받아, 사용자가 인증된 경우만 서비스를 제공한다. 이와 관련된 자세한 내용은 3.6.3항의 서비스 예시에서 다룬다.
2) 스마트 기기 인증 : 서비스 제공자는 서비스 등록 단계에 등록되어 있는 사용자의 스마트 기기를 등록된 DI-Type 정보에 따라 인증한다. 이때 3.2.3항의 3가지 이용채널(Ch-Type1~3)을 이용하여 스마트 기기와 서비스 제공자는 통신한다. 사용자 로그인 단계와 같이 전송되는 데이터는 SSL/TLS 등과 같은 암호화 프로토콜을 이용하여 암호화 되거나 독자적인 암호화프로토콜을 적용하여 암호화 된 형태로 통신한다.
3) 서비스 이용 : 로그인이 끝난 사용자는, 인터넷서비스 서버로부터 서비스를 제공 받는다. 서비스 이용 시 전송되는 데이터는 PC와 통신하는 과정과 스마트 보안패드와 통신하는 2가지 세부과정으로 이루어진다.

3-1) PC와 통신과정 : 사용자는 PC를 이용하여 데이터를 입력하고, 인터넷서비스 서버와 통신한다. 이러한 정보는 MITB 등의 공격에 취약할 수 있으므로, 중요성이 요구되는 정보는 이 채널을 통하여 전송하지 않는다.

3-2) SD와 통신과정 : 사용자는 스마트 보안패드를 이용하여 3.2.4항에 설명된 3가지 Type으로 데이터를 입력한다. 데이터 입력 시 입력방법은 3.2.1항에 설명된 2가지 형태인 Key-Type1(숫자) 또는 Key-Type2(숫자+문자)로 입력한다.

3.6 제안하는 모델을 적용한 서비스 예시

제안하는 스마트 보안패드는 인터넷 뱅킹의 로그인 및 계좌이체 과정, 인터넷서비스의 로그인 과정, 온라인 쇼핑몰의 제품 주문 과정 등 다양한 분야에 활용할 수 있으며, 각각의 활용 예를 자세히 살펴보면 다음과 같다.

3.6.1 인터넷 뱅킹의 로그인 및 계좌이체 과정

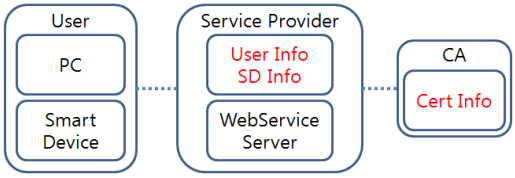
인터넷 뱅킹은 온라인으로 금전을 주고받는 서비스로, 계좌이체 등과 같은 서비스 제공시 계좌번호의 입력, 이체금액의 입력 등이 필요하다. 계좌이체 시 제안하는 스마트 보안패드를 이용하여 계좌번호 및 이체금액 등을 입력하고 안전하게 서비스 이용할 수 있다.

인터넷 뱅킹과 같은 금융서비스는 서비스의 특성상 보안이 강화된 형태로 서비스를 제공해야 한다. 또한, 금융정보는 공인인증서를 이용하여 전자서명 되어야 한다. 이를 위하여, 스마트 보안패드 프로그램은 사용자의 공인인증서를 저장하고 있어야 하고, 전자서명이 가능해야 한다. 그러므로 별도의 독립적인 스마트 보안패드 프로그램을 필요로 한다. 따라서 이러한 형태의 서비스는 서비스 제공자 중심의 구조가 적합하다. Table 2은 인터넷 뱅킹 서비스의 구성예시이다.

[Table 2] Setting Type - Internet Banking Service

Item		Type	Contents
Input Type	Login	Key-Type2	Number + Text
	Transfer	Key-Type1	Number
Smart-Device(SD) Identify Method		DI-Type3	IMEI + IMSI
Channel (SD <-> SP)		Ch-Type3	3G/4G
Input Data	Login / Certification Password	UI-Type1	Password
	Transfer	UI-Type2	Account Info, Transfer Amount
Structure		Service Provider(SP) Centric Structure	

사용자는 인터넷 뱅킹의 로그인 시 스마트 보안패드를 이용하여 Key-Type2 방식으로 비밀번호를 입력한다. 그리고 계좌이체 시 계좌번호, 이체금액 숫자로만 구성되어 있으므로 Key-Type1 방식으로 입력한다. 서비스 제공자는 사용자의 스마트 기기를 인증하기 위하여 사전에 등록된 DI-Type3 정보인 IMEI와 IMSI정보를 이용하여 기기 및 사용자를 인증한다. 또한, 스마트 기기와 서비스 제공자는 Ch-Type3인 3G/4G망을 이용하여 채널을 구성하고 연결한다. 로그인 시 입력되는 데이터는 UI-Type1이며, 계좌이체 등 금융거래 시 발생하는 전자서명에 이용되는 데이터는 UI-Type2 이다. 금융거래 시 이용되는 데이터는 스마트 기기를 통하여 최종 전자서명을 한다. 전사서명 시 이용되는 사용자의 인증서 검증은 외부의 인증기관(CA:Certificate Authority)을 통하여 이루어진다. Fig. 8은 인터넷 뱅킹의 구조다.



[Fig. 8] Internet Banking Structure

3.6.2 인터넷서비스의 로그인 과정

사용자는 일반적으로 인터넷서비스를 이용할 때, 사용자의 아이디와 비밀번호를 입력하여 로그인을 한다. 만약 사용자의 PC에 키로거(KeyLogger) 등이 설치된 경우, 사용자의 계정정보(아이디/비밀번호)는 쉽게 공격자에 노출될 수 있다. 따라서 본 논문에서 제안한 스마트 보안패드를 통하여 비밀번호를 입력하여, 원천적으로 비밀번호의 노출을 차단할 수 있다. Table 3은 이동통신사 중심의 구조에서 인터넷서비스의 로그인 서비스를 제공하는 예시이다.

[Table 3] Setting Type - Web Service's Login

Item		Type	Contents
Input Type	Login	Key-Type2	Number + Text
Input Data	Password	UI-Type1	Password
Smart-Device(SD) Identify Method		DI-Type1 or DI-Type2	Device SN or IMEI
Channel (SD <-> SP)		Ch-Type2 or Ch-Type3	WiFi (WPA, WPA2) or 3G/4G
Structure		Mobile Network Operator(MNO) Centric Structure	

서비스 제공자는 사용자에게 사용자의 아이디를 입력받는다. 그리고 이동통신사에게 해당 사용자의 인증을 요청한다. 이동통신사는 사전에 미리 등록된 사용자의 스마트 기기에 인증요청을 보낸다. 사용자는 해당 서비스 제공자에 등록된 아이디에 대한 비밀번호(UI-Type1)를 스마트 보안패드 프로그램을 이용하여 입력(Key-Type2)한다. 비밀번호는 서비스이용자만이 알 수 있으므로, 서비스 제공자는 사용자의 단말기에 대한 인증만 수행하면 된다. 따라서, DI-Type1 또는 DI-Type2 형태로 단말을 인증하고, 비밀번호는 암호화되어 전송되어야 하므로, WiFi에 보안이 적용된 Ch-Type2 또는 Ch-Type3의 형태로 스마트 기기와 서비스 제공자 사이에 채널을 구성한다.

3.6.3 온라인 쇼핑몰의 제품 주문 과정

온라인 쇼핑몰은 온라인으로 물품을 구매하는 서비스를 제공한다. 물품 구매 시 최종 단계에서, 사용자는 결제가 필요하며, 이때 본 논문에서 제안하는 스마트 보안패드 구조로 결제정보를 입력할 수 있다. 즉, 물품의 수량 및 배송지 정보 등을 스마트 보안패드를 통하여 입력 받음으로써, 정확한 물품의 구매 및 배송이 가능하다. Table 4는 제3의 인증기관 중심의 구조로 온라인 쇼핑몰의 물품 구매를 지원하는 구성의 예시이다.

[Table 4] Setting Type - Online Shopping Mall's Order

Item		Type	Contents
Input Type	Order	Key-Type1	Number
Input Data	Item Amount	UI-Type3	Item Amount
Input Type	Shipping	Key-Type2	Number + Text
Input Data	Address Info	UI-Type3	Address Info
Smart-Device(SD) Identify Method		DI-Type1 or DI-Type2	Device SN or IMEI
Channel (SD <-> SP)		Ch-Type1 or Ch-Type2 or Ch-Type3	WiFi (Non-Secure) or WiFi (WPA, WPA2) or 3G/4G
Structure		3rd Party Authority Centric Structure	

본 예시에서, 서비스 제공자들은 사용자의 인증을 위하여 제3의 인증기관과 협력을 맺고, 사용자 인증을 제3의 인증기관에 위탁한다. 제3의 인증기관은 사용자 인증을 지원하기 위하여 이동통신사들과 협력을 맺어, 서비스 제공자들과 이동통신사 사이의 사용자 인증을 중계한다. 이러한 구조는 Fig. 5과 같이 다수의 서비스 제공자와 다수의 이동통신 사업자들이 하나의 인증기관을 통하여 연결되는 구조로, 사용자의 정보를 한 곳(제3의 인증기관)에서 관리할 수 있는 장점이 있다. 이러한 모델은 NFC(Near Field Communication) 서비스에서 TSM(Trusted Service Manager)을 이용하는 모델과 비슷한 구조라 할 수 있다.

온라인 쇼핑몰의 제품 주문 과정은 다음과 같이 이루어질 수 있다. 사용자는 사전에 자신의 스마트 기기를 스마트 보안패드로 등록(DI-Type1 or DI-Type2)한다. 서비스 제공자는 사용자의 스마트 보안패드 프로그램(Key-Type1)을 이용하여 주문제품의 물품 수량(UI-Type3)을 입력받는다. 물품수량 값은 노출되어도 큰 의미가 없을 수 있어 Ch-Type1을 통하여 스마트 보안패드와 서비스 제공자 사이에 채널을 형성하여 서비스를 제공할 수 있으나, 권장하는 방식은 아니다. 또한, 새로운 배송지 주소(UI-Type3)로 제품을 배송받기 원하는 경우,

사용자는 스마트 보안패드를 이용하여 배송지 주소를 입력한다. 이때, 배송지 주소가 노출될 경우 문제가 될 수 있어, 스마트 보안패드와 서비스 제공자 사이의 채널은 안전한 채널(Ch-Type2 or Ch-Type3)을 이용할 것을 권장한다.

4. 제안방법의 보안성 평가

본 논문에서 제안하는 스마트 보안패드를 이용한 서비스 제공 모델의 안전성을 평가하기 위하여, 공격자의 공격 기법을 분류하고, 각 공격 기법에 대하여 안전성을 분석하면 다음과 같다.

4.1 공격자의 공격 분류

공격자의 대표적인 공격을 분류하면 다음과 같다.

1) MITM(Man-In-The-Middle) 공격 : 공격자는 사용자와 서비스 제공자 사이에 존재하여, 서로간의 통신 내용을 가로채서 비밀정보를 획득하거나, 정당한 사용자로 위장하는 공격
2) MITB(Man-In-The-Browser) 공격 : 공격자는 사용자 PC의 웹브라우저에 접근하여, 거래내용을 조작하고, 이 사실을 사용자가 인지하지 못하게 하는 공격
3) 키로거(KeyLogger) 공격 : 공격자는 사용자의 PC에 키로거 프로그램을 설치하여, 사용자가 입력하는 내용을 볼 수 있는 공격
4) 피싱(Phishing) 공격 : 공격자는 사용자에게 위·변조된 웹페이지로 접속을 유도하여, 해당 웹사이트 이용을 위해 필요한 정보를 빼내가는 공격
5) 파밍(Pharming) 공격 : 피싱 공격의 진화된 형태로 공격자는 사용자 PC의 DNS정보(예를 들어, 윈도우의 경우 hosts 파일)를 조작하여 정상적인 웹사이트로 접속을 해도 위·변조된 웹사이트로 접속되는 공격

4.2 공격 기법별 안전성 분석

스마트 보안패드를 이용한 구조에서 공격자의 공격 기법 별 안전성을 분석하면 다음과 같다.

1) MITM 공격 : MITM 공격은 통신 주체 상호간에 검증을 하지 않고 통신을 하기 때문에 발생하는 공격이다. 즉, 공격자는 사용자에게 자신이 서비스 제공자라고 속여야 한다. 제안하는 모델은 사용자의 PC와 서비스 제공자 사이에 SSL/TLS 등과 같은 암호화 프로토콜을 적용하므로 공격자는 서비스 제공자로 위장할 수 없다. 이는 SSL/TLS 프로토콜을 적용하여 서비스를 제공할 경우 서비스 제공자는 사전에 웹브라우저가 신뢰하는 인증기관으로부터 발급받은 인증서를 이용하여 상호 키교환을 하기 때문이다. 사용자의 스마트 기기와 서비스 제공자 사이의 채널에서 발생할 수 있는 MITM 공격도 스마트 보안패드 프로그램을 통하여 스마트 기기 식별정보(DI-Type1,2,3)를 이용하여 서비스 제공자와 상호 인증하므로 안전하다.
2) MITB 공격 : 제안하는 모델은 공격자가 사용자 PC의 웹브라우저 정보를 조작하여도, 인터넷 서비스를 위한 중요한 정보는 사용자의 PC가 아닌 스마트 보안패드를 통하여 입력받는다. 따라서, 공격자가 조작할 수 있는 정보의 범위는 한정적이므로, MITB 공격을 통하여 피해를 줄 수 있는 부분은 매우 제한적이다. 즉, 서비스를 방해하는 정도의 공격이 가능하며 이러한 경우 사용자는 백신프로그램 등을 통하여 사용자PC를 치료하고 서비스를 이용할 수 있다.
3) 키로거 공격 : 공격자의 키로거 프로그램을 통하여 입력될 수 있는 중요한 정보는 모두 스마트 보안패드를 통하여 입력받는다. 즉, 공격자는 키로거 프로그램을 통하여 공격자에게 무의미한 정보만을 획득할 수 있다. 따라서, 공격자는 키로거를 통해 획득한 정보로 사용자에게 어떠한 피해도 줄 수 없다. 이는 중요한 정보는 모두 스마트 보안패드를 이용하여 입력되기 때문이다.
4) 피싱/파밍 공격 : 피싱/파밍 공격은 사회공학적 공격의 한 형태로, 사용자는 공격자의 조작된 웹사이트를 방문하거나, 조작된 웹사이트로 방문이 유도되어 인터넷 서비스를 이용함으로써 피해가 발생된다. 제안하는 모델을 통하여 인터넷 서비스를 제공받을 경우, 공격자의 조작된 피싱/파밍 사이트로 제공될 수 있는 정보는 매우 제한적이다. 즉, 공격자는 사용자PC를 통하여 획득한 정보를 이용하여 사용자에게 어떠한 피해도 줄 수 없다. 이는 중요한 정보는 모두 스마트 보안패드를 이용하여 입력되기 때문이다.

5. 결론

본 논문에서 스마트 보안패드를 이용하여 인터넷 서비스 제공시 안전하게 서비스를 제공할 수 있는 모델을 제

안하였다. 이를 위하여, 중요한 정보를 스마트 기기를 통하여 입력하는 스마트 보안패드의 개념을 도입하였다. 즉, 사용자와 서비스 제공자는 스마트 보안패드를 이용하여 중요한 정보를 전송함으로써, 사용자PC 영역인 종단 영역에서 발생할 수 있는 다양한 공격을 예방할 수 있다.

또한 제안모델은 서비스 제공자가 스마트 보안패드를 활용하여 구성할 수 있는 다양한 형태를 정의한다. 서비스 제공을 위한 입력형태, 스마트 기기 식별방법, 이용채널, 이용정보의 형태를 정의하여 제공서비스에 따라 달리 구성할 수 있도록 하였다. 또한 서비스 제공을 위하여 구성될 수 있는 대표적인 사업자의 구조를 설명하고, 각각 적용될 수 있는 서비스 예시를 들었다. 각 예시 별로 적용될 수 있는 구성을 표 형태로 나열하여 실제 서비스 사업자가 서비스 제공시 참고할 수 있도록 하였다.

마지막으로 제안하는 모델의 보안성 평가를 통하여 기존에 발생할 수 있는 공격자의 공격 기법을 정의하고 각 공격 기법별로 안전성을 분석하였다.

사업자는 제안하는 모델을 이용하여, 서비스 모델 별로 최적화된 형태로 스마트 보안패드를 적용할 수 있어, 보안성 및 사용자 편의성을 고려하여 안전한 서비스를 제공할 수 있을 것으로 기대한다.

References

[1] Financial Security Agency, "A Research Paper for a New Authentication Technology on Electronic Finance", March, 2011.

[2] Korea Internet & Security Agency, "Research on security criteria for extension to electronic authentication method usage-based", December, 2011.

[3] Financial Security Agency, "A Report for Internet-Banking Security Current Status in Foreign Country", February, 2010.

[4] Financial Security Agency, "A Comprehension of interlocked transaction Authentication Technology", November, 2010.

[5] Hiltgen, A.; Kramp, T.; Weigold, T.; , "Secure Internet banking authentication," Security & Privacy, IEEE, vol.4, no.2, pp.21-29, March/April 2006
DOI: http://dx.doi.org/10.1109/MSP.2006.50

[6] Financial Security Agency, "A Guide for Application of End-to-End Cryptography", October, 2007.

[7] Young-Jae Maeng, Dong-Oh Shin, Sung-Ho Kim, Dae-Hun Nyang, Mun-Kyu Lee, "A Vulnerability Analysis of MITM in Online Banking Transactions in Korea", Internet and Information Security, Vol. 1, No. 2, pp. 101-118, 2010.

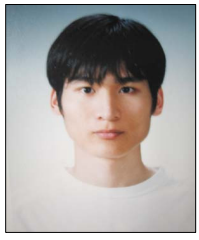
[8] Jae-Mo Seung, Su-Mi Lee, Seung-Ho Ahn, Bong-Nam Noh, "The End-to-End Encryption for Enhancing Safety of Electronic Financial Transactions", Journal of the Korea Academia-Industrial Cooperation Society, Vol. 10, No. 8, pp. 1920-1925, 2009.
DOI: http://dx.doi.org/10.5762/KAIS.2009.10.8.1920

[9] Han-Na You, Jae-Sik Lee, Jung-Jae Kim, Jae-Pio Park, Moon-Seog Jun, "A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment", J-KIVS vol.36, no.8, pp.939-946, August, 2011.
DOI: http://dx.doi.org/10.7840/KICS.2011.36B.8.939

[10] Jae-Sik Lee, Han-Na You, Chang-Hyun Cho, Moon-Seog Jun, "A Design Secure QR-Login User Authentication Protocol and Assurance Methods for the Safety of Critical Data Using Smart Device", KICS vol.37C, no.10, September, 2012.

[11] Hyung-Woo Lee, Yeong-Joon Park, "A Design and Implementation of User Authentication System using Biometric Information", Journal of the Korea Academia-Industrial Cooperation Society, Vol. 11, No. 9, pp. 3548-3557, 2010.
DOI: http://dx.doi.org/10.5762/KAIS.2010.11.9.3548

이 재 식(Jae-Sik Lee) **[정회원]**



- 2005년 8월 : 가천대학교 컴퓨터공학과(공학사)
- 2007년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2007년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

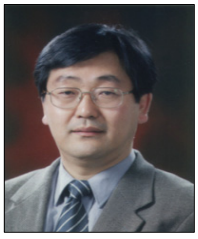
<관심분야>
인증 이론 및 시스템, 암호프로토콜, 개인정보보호

김 형 주(Hyung-Joo Kim) **[정회원]**

- 2008년 8월 : 단국대학교 컴퓨터과학과 졸업
- 2010년 8월 : 숭실대학교 컴퓨터학과 석사
- 2010년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
Authentication, M2M, NFC, RFID, Security Scheme

전 문 석(Moon-Seog Jun) **[정회원]**



- 1989년 2월 : University of Maryland Computer Science (공학박사)
- 1989년 3월 ~ 1991년 2월 : New Mexico State University physical Science Lab 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<관심분야>
인터넷 보안, 네트워크 보안, 인증 시스템, 정보보호