Journal of The Korea Society of Computer and Information
Vol. 17 No. 4 , April 2012

2012-17-4-3-6

모바일 장치에서 OTP 기반의 바이오 인식 보안을 위한 프레임워크

한 승 진*

A Framework for Biometric Security based on OTP in Mobile Devices

Seung-Jin Han*

요 약

바이오 인식 기술은 기존의 PIN이나 패스워드와 달리 분실하거나 도용될 가능성이 적기 때문에 PIN이나 패스워드를 대체할 새로운 수단으로 대두되고 있다. 그러나 바이오 인식은 PIN이나 패스워드와 달리 노출되어 도용이 된다면 수정할 방법이 없다. 따라서, 바이오 인식 정보를 이용한 OTP를 모바일 장치에 적용함으로써 기존의 PIN이나 패스워드 혹은 바이오 인식 정보만을 이용한 인증의 문제점을 해결하고자 한다. 본 논문에서는 모바일 장치에서 바이오 인식 정보를 OTP로 사용하여 바이오 인식 정보를 안전하게 서버(TTP)로 전달하는 프레임워크를 제안하고, 기존의 방법과 보안 및 성능을 비교한다.

▸ Keyword : 바이오 인식, OTP, PIN, 패스워드, 모바일 장치, 제3의 신뢰기관, USIM

Abstract

Biometric technology has been proposed as a new means to replace conventional PIN or password because it is hard to be lost and has the low possibility of illegal use. However, unlike a PIN or password, there is no way to modify the exposure if it is exposed and used illegally. To solve the problems, we propose to apply OTP using biometric information to mobile devices for more secure and adaptable authentication. In this paper, we propose a secure framework for delivering biometric information as mobile OTP to the server (TTP) and compared this paper with existed methods about security and performance.

▸ Keyword : Biometric, OTP, PIN, Password, Mobile Device, TTP, USIM

• 제1저자 : 한 승 진
• 투고일 : 2011. 12. 16, 심사일 : 2012. 02. 04, 게재확정일 : 2012. 03. 18.
* 경인여자대학교 e-비즈니스과 부교수(Dept. of e-Business, Kyungin Women's College)

I. 서론

정보 기술의 시대에 휴대전화는 점점 더 널리 세계적으로 사용되고 있고, 기본적인 통신뿐 아니라 개인 업무와 프로세스 정보를 다루는 도구는 언제 어디서나 사용이 가능하다[1]. 4십억 명 이상의 휴대전화 사용자가 전 세계에 있고 이 숫자는 여전히 지속적으로 증가추세이며 2015년까지 세계 인구의 86%가 하나 이상의 휴대전화를 소유한다고 예측하고 있다[2]. 그림 1처럼 이러한 휴대전화(모바일 장치)에 바이오 인식 정보를 적용하여 기존의 PIN이나 패스워드를 대체하고자 하는 연구들이 있다[3-5,8,9]. 기존의 바이오 인식 기반의 시스템은 단일 장치내에서 바이오 인식 정보의 획득, 처리, 인식 등을 모두 처리하는 장치에 적용되지만, 최근에는 단일 시스템에서 서버와 클라이언트 방식으로 변경되는 추세이다. 이러한 추세는 바이오 인식 데이터를 금융거래[3], 의료정보[3-5]에 적용하고자 하는 많은 노력들이 있다.

그림 1. 바이오 인식 정보를 이용한 모바일 장치구조
Fig. 1. Mobile Device using Biometrics

바이오 인식 기술은 기존의 PIN(Personal Identity Number)이나 패스워드와 달리 분실하거나 도용될 가능성이 적기 때문에 PIN이나 패스워드를 대체할 새로운 수단으로 대두되고 있다. 그러나 바이오 인식은 PIN이나 패스워드와 달리 노출되어 도용이 된다면 수정할 방법이 없다. 따라서, 바이오 인식 정보를 이용한 OTP(One Time Password)를 모바일 장치에 적용함으로써 기존의 PIN이나 패스워드 혹은 바이오 인식 정보만을 이용한 인증의 문제점을 해결하고자 한다.

본 논문에서는 모바일 장치에서 바이오 인식 정보를 OTP로 사용할 경우 안전하게 바이오 인식 정보를 안전하게 서버로 전달하는 프레임워크를 제안한다.

II. 관련 연구

모바일 장치에 적용된 바이오 인식 정보가 모바일 장치에 적용된 사례를 살펴보고, 모바일 장치에 적용된 OTP에 대해 살펴보고 문제점을 기술한다.

2.1 모바일 장치에서 바이오 인식을 이용한 보안

모바일 환경의 음성기반 일회용 암호시스템이 응용되어 상용화된 시스템은 스위스의 인증보안 업체인 BIOMETRY사의 MobiComBiom[6] 제품의 경우, 바이오 인식 정보인 얼굴인식과 음성인식, 입술움직임, 단어인식의 4가지 인증절차로 구성되어 있다. 먼저 휴대폰의 두 개의 숫자 버튼을 누르게 되면 화면에 4개 숫자로 구성된 일회용 암호가 표시되고, 사용자는 휴대폰에 내장된 카메라와 마이크를 통해 이들 숫자를 말하게 되면 암호화되어 인증 센터에 전송되어 미리 학습 저장된 사용자의 0, 1, 2, 3, ... , 9까지의 숫자 발음 정보와 비교하여 화자가 일치할 경우 인증을 받게 된다. 또 다른 예로 voicevault사[7]의 VoiceAuth는 모바일 장치에서 특정키(전화번호)를 입력하면 서버로부터 4자리의 번호를 전송받는다. 사용자는 4자리의 번호를 음성을 통해 전달하면 서버는 이를 인증한다. 구글의 안드로이드 운영 체제 중 최신 버전인 안드로이드 4.0(아이스크림 샌드위치)을 탑재한 삼성 전자의 갤럭시 넥서스 스마트폰은 휴대전화 잠금을 해제하기위한 새로운 방법을 제공한다. 얼굴 잠금 해제는 갤럭시 넥서스의 전면 카메라와 휴대전화의 사용자를 인식하기 위해 얼굴 인식 소프트웨어를 사용해서 화면의 잠금을 해제한다[8]. 홍채 바이오 인식은 홍채에 생겨있는 긴 띠 모양의 망(빗살무늬의 인대), 코라지를 한 듯한 붉은 색의 섬유질, 속눈썹 모양의 돌기, 꾸불꾸불한 혈관계, 링 모양의 원들, 동공을 둘러싸는 코로나 모양의 인대, 홍채 고유의 색, 얼룩점 등이 각 사람마다 다른 생물학적 특성을 가진다[9]. [10]은 바이오 인식의 지문과 음성의 특징을 이용한 모바일 통합 OTP의 일회용 암호키 토큰을 생성하는 방법을 제안하였다.

2.2 모바일 장치에서 OTP를 이용한 보안

OTP는 매번 로그 인 할 때마다 해당 세션에서 1번만 사용이 가능한 패스워드를 생성하는 보안매체로서, 현재 사용하는 패스워드로부터 다음에 사용할 패스워드를 유추하는 것이 불가능하다. 기존의 ID/Password 인증방식에서 문제가 된 재생 공격(Replay Attack), 키로거(Keylogger) 프로그램을 이용한 패스워드 탈취 공격 등의 여러 공격들로부터 안전성을 제공하기 때문에 관공서 공문서 발급 인증, 금융권 전자금융

거래, 기업체 사내시스템 접근 통제, 전자상거래의 고액(30만원 이상) 결제, 인터넷 포털 사이트의 사용자 인증 등 민감한 자원을 다루는 분야에서 사용되고 있다. 바이오 인식 데이터를 OTP와 PKI(Public Key Infrastructure)에 적용하고자 하는 연구들이 있다[10-12].

OTP는 난수를 사용하는 방식과 타임스탬프를 사용하는 방식으로 나뉘고 있다. 난수를 사용하는 OTP는 중간자 공격(Man-in-the-Middle-Attack)과 재생 공격에 취약하다[13]. 따라서 본 논문에서는 모바일 장치의 바이오 인식 데이터를 안전하게 서버에 전달하기 위해 타임스탬프가 적용된 OTP[14]를 모바일 장치와 서버 구간에 적용한다. 또한 바이오 인식 데이터만 적용된 방법인 SAA[15]에 기존의 패스워드 방법을 함께 사용하여 보안성을 높인다.

본 논문과 SAA의 방법과의 차이점은 SAA는 바이오 인식 정보를 USIM(Universal Subscriber Identity Module)에 저장하였다. USIM에 바이오 인식 정보를 저장하는 것은 부채널 공격(Side Channel Attack)에 매우 취약하다[16]. 따라서 본 논문에서는 패스워드 정보는 USIM과 ME(Mobile Equipment)에 각각 저장하지만, 바이오 인식 정보는 TTP(Trusted Third Party)에 저장하여 부채널 공격과 같은 해킹으로부터 보호한다.

III. 모바일 장치에서 바이오 인식을 이용한 OTP 프레임워크

본 논문에서는 장치간 혹은 장치와 TTP간의 인증, 기밀성, 무결성을 보장하기 위해 PKI를 이용한다. 모바일 장치에서 획득하는 바이오 인식 정보는 어떠한 바이오 인식 정보도 상관이 없지만 사용자 본인을 구분할 수 있는 정보라 가정한다. 모바일 장치와 USIM간의 디지털 서명은 자체의 디지털 서명 알고리즘(SX)을 사용하고, USIM과 TTP간의 디지털 서명은 사용자와 TTP 각각의 개인 키를 사용한다. 본 논문에서 제안하는 수식을 간단하고 명료하게 하기 위해 다음과 같은 기호를 정의한다.

표 1. 기호
Table 1. Notations

기호	설명
X→Y: { M }	X가 Y에게 메시지 M을 전송
h	보안성이 강한 단방향 함수
S_X	엔티티 X의 디지털 서명
P_X	엔티티 X의 개인 키
P_X	엔티티 X의 공개 키
E_X	엔티티 X가 자신이 소유한 키를 이용하여 메시지를 암호화
EK_{XY}	엔티티 X와 Y간에 공유하는 대칭 키
TS_X	엔티티 X에 의해 생성된 타임스탬프
$Cert_X$	엔티티 X의 인증서
ID_X	엔티티 X의 ID

본 논문에서 제안하는 방법을 설명하기 전에 다음을 가정한다. ME와 USIM은 이미 제조사가 보안 모듈을 장착했다고 가정한다. ME는 International Mobile Equipment Identity(IMEI ; ESN : Electronic Serial Number), TS_{ME}(타임스탬프), 사용자가 지정한 패스워드를 알고 있다. 또한 개인키와 공인 인증서를 알고 있다. USIM은 IMSI(International Mobile Subscriber Identity : 가입자 번호), PIN(Personal Identification Number)와 PUK(Pernal Unlock Key)를 알고 있다. USIM은 TTP의 공개키인 P_{TTP}를 알고 있고, TTP는 USIM의 공개키 P_{USIM}을 알고 있다.

3.1 단말기(ME)와 USIM간의 프로토콜 초기화

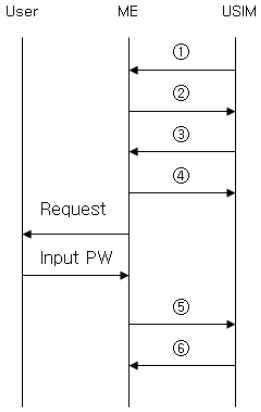

그림 2. ME와 USIM간의 인증
Fig. 2. Authentication between ME and USIM

단말기(ME)와 USIM간의 보안 프로토콜은 SAA의 방법을 따르지만, 본 논문에서는 인증을 위해 사용자로부터 패스워드 정보만 입력받는다. 바이오 인식 정보는 최초에 TTP에 등록을 하고, 본 논문에서는 TTP에 안전하게 저장되어 있다고 가정한다. 또한 OTP 생성시 각 엔티티에서 생성한 난수를 이용하지 않고, 타임스탬프를 사용한다.

(1) USIM에 대한 프로토콜 초기화

USIM은 키 쌍을 생성해서 TTP(Trusted Third Party, 혹은 Certification Authority, CA)로 공개 키를 전송한다. CA는 USIM의 인증서를 생성해서 보안 채널을 통해 USIM으로 전송한다. BCS(Biometrics Comparison Software)는 USIM에 저장되어 있다.

(2) ME에 대한 프로토콜 초기화

사용자는 자신의 식별 데이터를 서명하고 암호화된 메시지

$\{E_{CA}S_{ME}(IMEI\|TS_{ME}), TS_{USIM}, ID_{USIM}\}$을 CA에게 전송한다. CA는 다시 식별 데이터를 서명하고 메시지 $\{O=S_{CA}(S_{ME}(IMEI\|TS_{ME}), TS_{USIM}, ID_{USIM}), Cert_{CA}\}$를 반환한다. 이 메시지는 사용자의 적법한 식별을 위해 ME와 USIM에 안전하게 저장된다.

Step ① USIM → ME :

$\{request, TS_{USIM}, ID_{USIM}, Cert_{USIM}\}$

USIM은 무결성 검사 요구를 ME로 전송한다. TS_{USIM}은 메시지의 유일성을 보장한다.

Step ② ME → USIM :

$\{response, ID_{ME}, TS_{ME}, S_{ME}(TS_{USIM}, ID_{USIM}, TS_{ME}, response), Cert_{ME}\}$

메시지를 수신한 후 ME는 TS_{USIM}을 저장하고 USIM에 응답한다.

Step ③ USIM → ME :

$\{E_{ME}(EK_{MU}, ID_{ME}, TS_{ME}), S_{USIM}(TS_{USIM}, ID_{USIM}, O, E_{ME}(EK_{MU}, ID_{ME}, TS_{ME}))\}$

ME의 메시지를 수신하면, USIM은 디지털 서명과 무결성 검사 결과를 검증한다. USIM은 자신이 발행한 TS_{USIM}이 올바른지 검사한다. 마지막으로 USIM은 ME와 USIM에서 사용하는 암호화 키 EK_{MU}을 생성하고 배포한다.

Step ④ ME → USIM :

$\{S_{USIM}(EK_{MU}, TS_{USIM}, ID_{ME}, O)\}$

USIM의 메시지를 수신하면, ME는 디지털 서명을 검증하고 메시지를 복호화한다. 디지털 서명이 맞다는 것은 USIM이 O를 갖고 있다는 의미이다. O가 ME에 저장된 것과 동일하다면 ME는 USIM의 소유자와 동일하다고 판단하고, 그렇지 않다면 소유자는 다르다.

ME의 메시지를 수신하면 USIM은 디지털 서명을 검증하고 디지털 서명이 올바르다면 ME의 O라고 추정한다. O가 USIM에 저장된 것과 동일하다면 USIM은 ME의 소유자와 동일하다고 판단하고, 그렇지 않다면 소유자는 다르다.

Step 1부터 4까지는 ME에 대한 무결성 검사와 ME와 USIM간 상호 인증을 보인 것이다. 4개의 단계에 의해 소유자가 동일한지를 판단할 수 있다. 이러한 판단은 모바일 장치에 대한 접근 제어에 중요한 사항이다.

Step ⑤ ME → USIM :

$\{E_{EK_{ME\text{-}USIM}}(TS_{ME}, h(PW), S_{ME}(E_{EK_{ME\text{-}USIM}}(TS_{ME}, h(PW))))\}$

사용자의 패스워드(PW)는 ME에 의해 안전하게 획득된다. ME는 암호 메시지를 구성하고 USIM으로 $h(PW)$를 전송한다.

Step ⑥ USIM → ME :

$\{E_{EK_{MU}}(TS_{ME}, TS_{USIM}, result), S_{USIM}(E_{EK_{MU}}(TS_{ME}, TS_{USIM}), result)\}$

ME의 메시지를 수신하면, USIM은 디지털 서명을 검증하고 메시지를 복호화한다. 저장된 (PW)와 $h(PW)$를 비교한다. ME가 반환된 메시지를 수신하면 디지털 서명을 검증하고 비교 결과를 수신한다.

3.2 단말기(USIM)와 TTP간의 프로토콜 초기화

단말기(USIM)와 TTP간의 보안 프로토콜은 인증을 위해 사용자로부터 패스워드 정보와 바이오 인식 정보를 입력받는다. 바이오 인식 정보는 최초에 TTP에 등록을 하고, 본 논문에서는 TTP에 안전하게 저장되어 있다고 가정한다. OTP 생성시 각 엔티티에서 생성한 난수를 이용하지 않고, 타임스탬프를 사용한다. USIM과 TTP는 디지털 서명을 위해 각각의 개인 키를 사용한다. 또한 USIM과 TTP간에 공유하는 암호키, 타임스탬프, ID는 각각의 공개 키를 이용하여 암호화하여 전송한다.

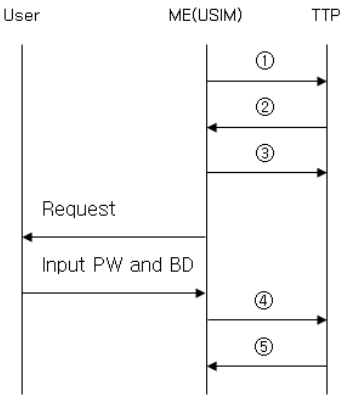

그림 3. USIM과 TTP간의 인증
Fig. 3. Authentication between USIM and TTP

Step ① USIM → TTP :

$\{request, TS_{USIM}, ID_{USIM}, Cert_{USIM}\}$

USIM은 무결성 검사 요구를 TTP로 전송한다. TS_{USIM}은 메시지의 유일성을 보장한다.

Step ② TTP → USIM :

$\{response, ID_{TTP}, TS_{TTP}, R_{TTP}(TS_{USIM}, ID_{USIM}, response), P_{USIM}(EK_{UT}), Cert_{TTP}\}$

메시지를 수신한 후 TTP는 TS_{USIM}를 저장하고 USIM에 응답한다. TTP는 USIM으로부터 ($TS_{USIM}, ID_{USIM}, response$) 를 자신의 개인키로 서명하여 USIM으로 전송하고, TTP는 USIM의 공개키로 EK_{UT}를 암호화하여 USIM으로 전송한다.

Step ③ USIM → TTP :

$\{R_{USIM}(ID_{TTP}, TS_{TTP}), P_{TTP}(EK_{UT}, TS_{USIM}, ID_{USIM})\}$

TTP의 메시지를 수신하면, USIM은 디지털 서명과 무결성 검사 결과를 검증한다. USIM은 자신이 발행한 TS_{USIM}이 올바른지 검사한다. 마지막으로 USIM은 TTP로부터 수신한 EK_{UT}를 자신의 개인키로 복호화하여 EK_{UT}를 공유한다. USIM은 TTP로부터 수신한 ID_{TTP}와 TS_{TTP}를 자신의 개인키로 암호화 하고, $EK_{UT}, TS_{USIM}, ID_{USIM}$을 TTP의 공개키로 암호화하여 TTP로 전송하여 TTP로부터 받은 $EK_{UT}, TS_{USIM}, ID_{USIM}$가 올바른지 확인한다.

Step ④ USIM → TTP :

$\{R_{USIM}(E_{EK_{UT}}(TS_{USIM}, h(PW\|BD)))\}$

사용자의 패스워드(PW)와 바이오 인식 데이터(BD)는 ME(USIM)에 의해 안전하게 획득된다. USIM의 타임스탬프와 획득한 PW, BD를 단방향 함수인 h를 이용하여 $h(PW\|BD)$를 TTP와 공유하는 키인 $E_{EK_{UT}}$로 암호화한다. 이를 R_{USIM}으로 디지털 서명하고 TTP로 전송한다.

Step ⑤ TTP → USIM :

$\{R_{TTP}(E_{EK_{UT}}(TS_{USIM}, TS_{TTP}, result))\}$

TTP는 USIM으로부터 수신한 $TS_{USIM}, h(PW\|BD)$를 $E_{EK_{UT}}$를 이용하여 복호화하고, P_{USIM}을 이용하여 수신한 메시지의 송신자가 USIM임을 확인한다. 수신한 패스워드(PW)와 BD를 자신이 보유하고 있는 패스워드(PW)와 BD와 비교하여 이에 대한 결과를 포함하여 TS_{USIM}과 $TS_{TTP}, result$를 TTP의 개인키로 디지털 서명하여 USIM으로 전송한다.

IV. 보안 및 성능 분석

4.1 보안 분석

표 2에서는 SAA에서 제안하는 방법과 본 논문의 보안 특성과 비교한다. 본 논문에서 제안하는 방법은 비교하는 모든 분야에서 보안 요건을 충족함을 알 수 있다.

표 2. 보안 특성 비교
Table 2. Security property comparison

보안 특성		Zeng [18]	3G scheme [19]	SAA [16]	This Paper
상호 인증	ME ↔ USIM	Yes	No	Yes	Yes
	사용자 ↔ USIM	Yes	Yes	Yes	Yes
	사용자 ↔ ME	Yes	Yes	Yes	Yes
모바일 장치에서 사용자보호		Yes	No	Yes	Yes
재생 공격 방지		Yes	No	Yes	Yes
메시지 암호화		partial	No	Yes	Yes
메시지 무결성		partial	partial	Yes	Yes
바이오 인식 식별		Yes	No	Yes	Yes
BCS의 전송 필요성		Yes	N/A	No	No
다중 요소 인식		Yes	No	Yes	Yes
다중 사용자와 다중 모바일 장치를 위한 유연한 인증 메카니즘 제공		No	No	Yes	Yes
부채널 공격 방지		No	No	No	Yes
중간자 공격 방지		No	No	No	Yes

4.2 성능 분석

성능평가에서는 SAA[15]에서 사용한 7가지 평가요소로 Zheng, SAA 그리고 본 논문에서 제안하는 방법을 비교한다. 표 3에서처럼 본 논문의 방법은 SAA 방법과 성능면에서 2배의 차이가 나는 것은 SAA는 단말기내에서 인증이 이루어지기 때문이고, 본 논문의 방법은 단말기내에서의 인증 뿐만 아니라 단말기와 서버간의 인증이 이루어지기 때문이다.

표 3. 성능 비교
Table 3. Performance comparison

성능평가 요소	Zheng [17]	SAA [15]	This Paper
대칭형 암호화	8	0	0
대칭형 복호화	8	0	0
공개키 암호화	2	1	2
공개키 복호화	1	1	2
디지털 서명	2	3	6
디지털 서명 검증	0	3	6
해쉬	5	0	0

SAA는 바이오 인식 정보가 USIM에 있기 때문에 모바일 장치가 전원이 켜져 있는 상태 혹은 인터넷에 연결되어 있는 상태라면 언제든지 부채널 공격과 같은 해킹이 가능하다. 그러나 본 논문의 방법은 바이오 인식 정보가 TTP에 저장되어 있다. 모바일 장치가 해킹이 되어서 패스워드가 노출이 되더라도 바이오 인식 정보가 TTP에 저장되어 있기 때문에 최초에 등록한 패스워드와 바이오 인식 정보가 3.2에서 전송하는 패스워드와 바이오 인식 정보와 일치하지 않기 때문에 부정한 접속을 막을 수 있다.

SAA에서는 OTP 생성을 위해 난수를 사용하였지만 이는 중간자 공격을 막을 수 없다. 그러나 본 논문에서는 난수 대신에 타임스탬프를 사용하여 OTP를 생성하여서 중간자 공격을 막을 수 있다.

V. 결 론

본 논문에서는 바이오 인식 정보와 패스워드를 이용한 OTP를 모바일 장치에 적용 가능한 보안 인증 프로토콜을 제안하였다. 단말기(ME)와 USIM간의 상호 인증 프로토콜은 기존의 방법을 사용하였지만 난수를 사용한 기존의 방법과 달리 타임스탬프를 사용하여 재생공격이나 중간자 공격으로부터 안전하고, 바이오 인식 정보를 단말기가 아닌 TTP에 보관함으로써 부채널 공격으로부터 안전하다. 본 논문에서 제안하는 방법은 기존처럼 OTP 장치 없이 모바일 장치에서 금융거래, 원격의료, 전자상거래에서 본인 인증이 부분에 적용이 가능하다.

참고문헌

[1] Shuo Wang and Jing Liu, Shuo Wang and Jing Liu, “Biometrics on Mobile Phone”, www.intechopen.com /articles/show/title/biometrics-on-mobile-phone, Source : Recent Application in Biometrics, ISBN : 978-953-307-488-7, July, 2011.

[2] Tseng, D. et. al., “Lensfree Microscopy on a Cellphone”, Lab on a Chip, Vol. 10, No. 14, pp. 1782-1792, July, 2010.

[3] M. Gordon and S. Sankaeanaeayanan, "Biometric Security Mechanism in Mobile Payments", Proc., of the 5th National Conference; INDIACom-2011, Computing For Nation Development, March 10 - 11, 2011.

[4] Bao, X, Wang, J. and Hu, J, “Method of Individual Identification based on Electroencephalogram Analysis”, Proc., of 2009 International Conference on New Trends in Information and Service Science, pp. 390-393, Beijing, P.R.China, June 9-July 2, 2009.

[5] Nakanishi, I, Baba, S and Miyamoto, C, "EEG Based Biometric Authentication Using New Spectral Features", Proc., of 2009 International Symposium on Intelligent Signal Processing and Communication Systems, pp. 651-654, Kanazawa, Ishikawa, Japan, December 7-9, 2009.

[6] http://www.biometry.com/mobicombiom.html

[7] http://www.voicevault.com/voicevault-enterprise/voice auth/

[8] http://www.huffingtonpost.com/2011/10/19/face-unlock-ice-cream-sandwich_n_1020207.html

[9] Daugman, J, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan., 2004.

[10] Byung Rae Cha, Nam Ho Kim, Jong Won Kim, “Availability Verification of Integration OTP Framework using Biometrics Information”, Journal of The Korea Navigation Institute, Vol. 5, No. 1, Feb., 2011.

[11] Yun Su Chung, Yongjin Lee, Hyung-Woo Lee, Ki Young Moon, “Biometric Authentication Framework based on One-Time Template”, Journal of KIISC, Vol. 18, No. 4, pp.61~65, Aug., 2008.

[12] Yong-Nyuo Shin, Young-Jin Kim, Myung-Geun Chun, “Operational Management for Biometrics Hardware Security Module and PKI”, Journal of KIISC, Vol. 9, No. 5, May, 2011.

[13] Wenbo Mao, Modern Cryptography : Theory and Practice, Prentice Hall, July, 2003.

[14] Seungjin Han, “A Robust Pair-wise Key Agreement Scheme based on Multi-hop Clustering Sensor Network Environments”, Journal of KSCI, Vol. 16,

No. 3, Mar., 2011.
[15] Jian Wang, Nan Jiang, "Secure Authentication and Authorization Scheme for Mobile Devices," Proceedings of ICCTA2009, 2009.
[16] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer and Stephane Tinguely, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards", Proceedings of the 2002 IEEE Symposium on Security and Privacy, 2002.
[17] Y. Zheng, D. K. He, X. H. Tang and, H. X. Wang, "AKA and Authtentication Scheme for 4G Mobile Networks Based on Trusted Mobile Platform", ICICS 2005, pp. 976~980, 2005.
[18] 3GPP TS 24.002, Release 4. GSM-UMTS public land mobile network access reference configuration, June, 2003.

저 자 소 개

한 승 진

1985~1990 인하대학교 이과대학 전자계산학과 학사
1990~1992 인하대학교 일반대학원 전자계산공학과 석사
1999~2002 인하대학교 전자계산공학과 박사
1992~1996 대우통신 종합연구소
1996~1996 한국전산원 초고속사업단
1996~1998 SKTelecom 디지틀사업본부
2002~2004 인하대학교 컴퓨터공학부 강의조교수
2004~현재 경인여자대학교 e-비즈니스과 부교수
2007~현재 TTA PG505 표준화위원
2012~현재 TTA PG505 간사
관심분야 : USN, MANET, Mobile Computing, 임베디드 시스템, Security, Biometric, Computer Network,
Email : softman@kic.ac.kr