한국산학기술학회논문지
Vol. 12, No. 4 pp. 1911-1918, 2011

# 얼굴 정보 기반 일회용 패스워드 생성 메커니즘을 이용한 사용자 인증 시스템 설계 및 구현

장원준[1], 이형우[1*]
[1]한신대학교 컴퓨터공학부

# Design and Implementation of Facial Biometric Data based User Authentication System using One-Time Password Generation Mechanism

**Won-Jun Jang[1] and Hyung-Woo Lee[1*]**
[1]**School of Computer Engineering, Hanshin University**

요 약 최근 스마트폰을 이용한 인터넷뱅킹, 전자금융 서비스 및 인터넷전화 서비스 등을 이용할 수 있다. 스마트폰을 이용할 경우 보다 강화된 사용자 인증 기능이 제공되어야 한다. 본 연구에서는 스마트폰을 이용하여 각 사용자 얼굴 정보와 같은 바이오메트릭 ID 정보를 이용하여 일회용 패스워드를 생성하는 메커니즘을 구현하였다. 스마트폰내 카메라 모듈을 이용하여 얼굴 이미지를 캡춰하여 서버로 전송하면 서버에서는 일회용 바이오메트릭 ID를 생성하도록 하였다. 그리고 이를 기반으로 클라이언트에서 일회용 패스워드를 생성하는 시스템을 개발하였다. 본 연구에서 제시한 기법을 이용할 경우 스마트폰 기반 SIP 서비스에서의 사용자 인증을 보다 강화할 수 있다.

**Abstract** Internet banking, electronic financial services and internet telephony service can be available on smart phone recently. In this case, more robust authentication mechanisms should be provided for enhancing security on it. In this study, a facial biometric ID based one-time password generation mechanism is designed and implemented for enhancing user authentication on smart phone. After capturing a facial biometric data using camera module on smart phone, it is sent to server to generate one-time biometric ID. Finally one-time password will be generated by client module after receiving the one time biometric ID based challenge token from the server. Using proposed biometric ID based one-time password mechanism, it is possible for us to provide more secure user authentication service on smart phone for SIP protocol.

**Key Words :** Biometric Data, B-OTP, Authentication.

## 1. 서론

최근 스마트폰 사용자가 급증하면서 인터넷 뱅킹 및 SIP 기반 VoIP 서비스와 같이 기존의 PC 기반 유무선 네트워크 서비스를 손쉽게 이용할 수 있게 되었다. 하지만 스마트폰을 통해 인터넷 뱅킹 및 인터넷전화(VoIP : Voice Over Internet Protocol) [1] 서비스를 이용할 경우 사용자에 대한 인증 과정에서의 보안 취약성이 증가하고 있기 때문에 이에 대한 대응 방안이 제시되어야 한다. 인터넷 뱅킹에서는 사용자 인증을 강화하기 위해 일회용 패스워드(OTP : One Time Password)를 이용하고 있으며 인터넷 전화 서비스에서는 SIP(Session Initiation Protocal)을 사용하고 있으나 클라이언트에 해당하는 스마트폰과 서버간 인증 취약점을 보완할 수 있도록 보다 강화된 사용자 인증 메커니즘(User Authentication Mechanism)이 제공되어야 한다[2,3].

이 논문은 2008년도 정부재원(교육과학기술부 학술연구조성사업비)으로 연구재단의 지원을 받아 연구되었습니다. (KRF-2008-521-D00444)
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 11년 03월 18일 수정일 11년 04월 04일 게재확정일 11년 04월 07일

인터넷 뱅킹 서비스에서 사용하는 기존 OTP 방식은 OTP 토큰에 대한 실제 소유자에 대한 확인 과정의 취약점을 이용한 우회공격이 가능하고, 악의적 공격자에 의해 OTP 정보에 대해 MITM(Man in the Middle Attack) 공격이 가능하기 때문에 이를 능동적으로 보완할 수 있는 방법이 기술적으로 제시되어야 한다[2]. SIP 프로토콜 역시 기존의 IP 프로토콜을 이용하기 때문에 공격자가 적법한 클라이언트를 대신하여 패킷을 변경하여 전송하더라도 SIP 호 연결이 가능하다는 문제점이 있다. 따라서 이러한 문제점을 해결하기 위해서는 SIP 프로토콜에서의 사용자 인증을 한층 더 강화할 수 있는 방법이 필요하다.

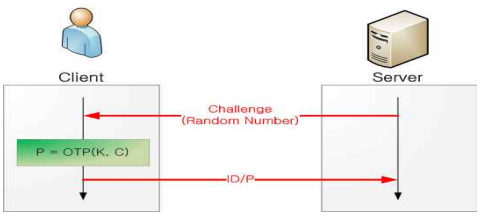
따라서 본 연구에서는 최근 이슈가 되고 있는 스마트폰 기반 SIP 사용자에 대한 인증을 강화하기 위해 사용자가 SIP 호 연결 과정에서 자신의 스마트폰내 카메라 모듈 등을 이용하여 얼굴 이미지 정보를 입력하게 하고 이와 같은 바이오메트릭 정보(Biometric data)를 이용하여 서버와의 통신 과정을 통해 OTP 값을 생성하여 스마트폰 사용자 인증에 활용하는 방식을 제시하고자 한다. 이 경우 기존의 스마트폰 기반 서비스에서 발생하는 인증 문제를 해결할 수 있으며, 스마트폰을 이용한 OTP 기반 다중 인증(Multifactor Authentication)에도 활용 가능하다는 장점이 있다.

2장에서는 기존 OTP 및 SIP 프로토콜의 보안 취약성에 대해 살펴보고, 3장에서는 본 연구에서 제안하는 스마트폰에서의 얼굴 정보 기반 OTP 생성 방법을 제시한다.

## 2. 기존 OTP 및 SIP 서비스 취약성

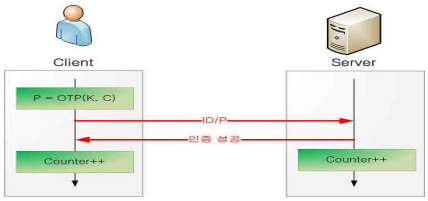
### 2.1 OTP 기술 분석[6]

기존의 OTP(One-Time Password)[4] 기술은 일회용 패스워드를 생성하는 기술이다. OTP 생성기술은 크게 비동기화 방식과 동기화 방식으로 나눌 수 있다. 비동기화 OTP 방식[5]은 그림 1과 같이 Challenge Response 방식으로 작동하는 것이며, 질의 값에 대한 응답 결과로 인증 과정을 수행한다. 이 방식은 서버와의 동기화가 필요 없는 방식이지만 사용자의 입력이 필요하며 네트워크 과부하를 유발하기도 한다.




[그림 1] 비 동기화 OTP 방식

동기화 OTP 방식[5]은 그림 2와 같이 시간 동기화 방식, 이벤트 동기화 방식, 이벤트-시간 동기화 방식으로 작동하며 OTP 토큰과 인증 서버 사이에 정확한 동기화 과정이 필요하며 서버와 OTP 단말간의 동기화된 시간 정보를 기준으로 특정 시간 간격마다 패스워드를 생성하는 방식으로 MITM(Man-In-The-Middle) 공격에 취약하며, 재사용 시간의 제약이 있다는 문제점이 있다.



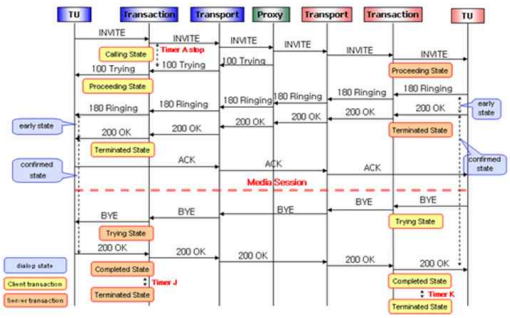

[그림 2] 동기화 OTP 방식

### 2.2 기존 OTP 생성 방법 분석

OTP 생성의 기본적인 원리는 사용자가 OTP 생성매체를 통하여 사용자 고유의 비밀 키(PIN)값을 입력하게 되면 MD5나 MD4 같은 Hash함수를 통하여 암호화를 한 뒤 그것을 이용하여 OTP값을 생성하는 것이다[2]. 시간 정보, 이벤트 및 질의응답 정보 등을 이용하여 매번 다른 OTP 값이 생성하도록 한다. 서버와 OTP 생성매체는 항상 동일한 일방향 해쉬함수를 이용하였기 때문에 만일 공격자에 의해 OTP 값이 노출된다 할지라도 원래의 비밀키 값에 대한 안전성을 보장할 수 있다.

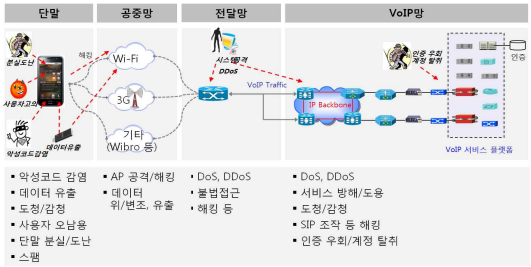
### 2.3 인터넷전화 서비스

SIP 프로토콜은 그림 3과 같이 Proxy 서버를 통해 호 연결 및 해제 요청을 수행하며 DNS와 Location 서버를 이용한다. 하지만 이와 같은 과정에서 공격자에 의해 비정상 메시지 공격(Malformed Message Attack), SIP 메시지 폭주 공격(SIP Message Flooding Attack), SIP 스푸핑 공격(Spoofing Attack), 도청, DoS(Denial of Service) 등이 가능하다.




[그림 3] SIP 프로토콜 구조

하지만 스마트폰을 이용할 경우 그림 4와 같이 인증 취약점을 이용한 공격 등이 가능하다.




[그림 4] 스마트폰 기반 SIP 공격 기법

## 2.4 해결 방안

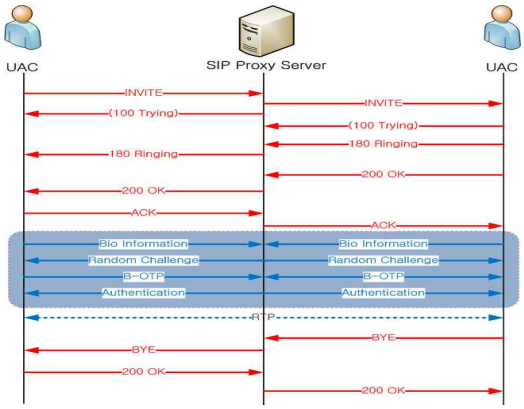
본 연구에서는 스마트폰을 이용한 인터넷 뱅킹 및 인터넷전화 서비스에서의 보안성을 강화하고 인증 취약점을 개선하기 위해 SIP 프로토콜에서 스마트폰과 Proxy 서버간 송수신되는 메시지를 중심으로 사용자 인증을 강화하기 위해 바이오메트릭 ID 정보와 인터넷 뱅킹에서 사용되는 OTP 기술을 접목한 B-OTP 방식을 제시하고자 한다. Proxy 서버에 등록하는 과정에서 스마트폰 사용자의 ID, PW 및 관련 정보 등을 저장하는 과정에서 스마트폰에서 이용 가능한 카메라 모듈을 통해 각 사용자의 고유한 바이오메트릭 정보를 활용하여 바이오메트릭 ID를 이용하여 OTP를 생성하고 이를 통해 사용자 인증을 제공하는 방식을 제시한다.

물론 바이오메트릭 정보를 전송하는 과정에서 개인 프라이버시 문제 및 보안 취약점이 발생할 수 있기 때문에 본 연구에서는 스마트폰을 통해 캡쳐된 바이오메트릭 정보를 원본 그대로 전송하지 않고, 캡쳐된 이미지에서 일정 부분만을 선택하여 전송하고 이를 이용하여 OTP를 생성하는 방법을 사용하여 보안 문제를 줄이도록 하였다.

# 3. 제안하는 얼굴 기반 OTP 생성 기법 및 SIP 인증 시스템 구조

## 3.1 SIP 등록 및 인증 전체 구조

일반적인 SIP 시그널링 절차에 바이오 정보를 이용한 OTP 생성 과정을 추가함으로써 UAC 간의 사용자 인증이 강화된 통신을 할 수 있다. 각 UAC는 자신이 속한 도메인 프록시 서버에 B-OTP 기반의 사용자 인증을 함으로써 안전한 통신을 한다. 본 논문에서 제안한 SIP 프로토콜 기반 사용자 인증 구조는 다음 그림 5와 같다.

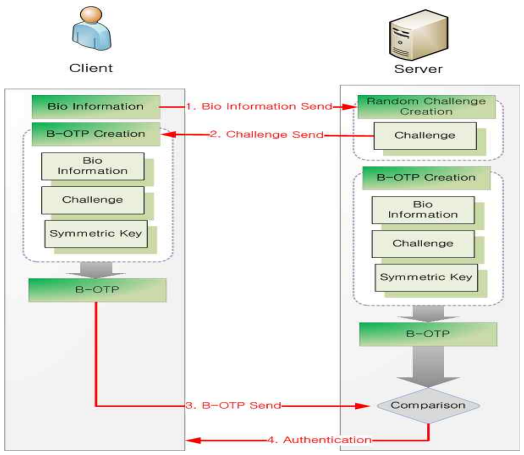



[그림 5] 바이오메트릭 정보 기반 SIP 인증 구조

사용자는 스마트폰 등에 있는 카메라 장치/모듈을 이용하여 사진/이미지를 캡쳐하게 되고 이를 이용하여 SIP 프록시 서버와의 OTP 기반 인증 과정을 수행하게 된다. 카메라 모듈을 통해 획득되는 정보는 각 개인마다 고유한 바이오메트릭 정보이다.

## 3.2 B-OTP 기반 사용자 인증 구조

구체적으로 B-OTP 인증을 위한 정보 생성 및 절차는 다음 그림 6과 같다. UAC는 자신의 스마트폰에 있는 카메라 모듈을 이용하여 캡쳐한 바이오메트릭 정보를 서버에게 보내며, 서버는 임의의 난수 도전값을 생성하여 UAC에게 전송한다. UAC는 자신의 바이오메트릭 정보와 서버로부터 전송받은 도전 값으로부터 B-OTP를 생성하고 이를 다시 서버로 전송한다. 서버도 UAC에서의 B-OTP과정과 동일하게 B-OTP를 생성하며, UAC로부터 받은 B-OTP와 비교하여 사용자 인증을 수행하게 된다.




[그림 6] B-OTP 기반 사용자 인증 전체 구조

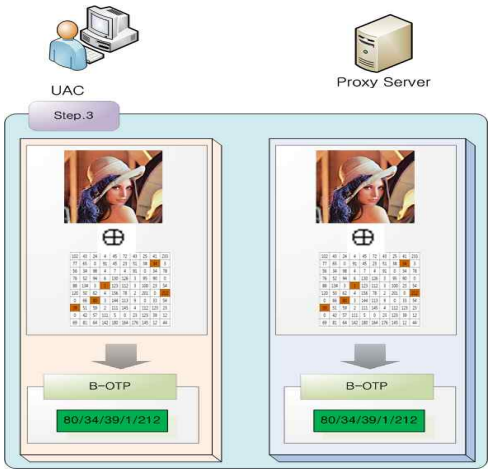
B-OTP 기반의 사용자 인증을 위한 세부 구조는 다음과 같다. 1단계, UAC가 개인의 바이오 정보를 서버로 보내게 되며, 바이오 정보가 서버로 수신되면 서버는 랜덤한 챌린지 값을 생성하게 된다. 바이오 정보는 사용자 인증을 강화하기 위하여 자신의 얼굴을 이용한다. 이 후, 이 바이오 정보에서 B-OTP 값을 추출하게 됨으로 UAC와 Proxy서버는 바이오 정보를 임시로 보관한다. 이때 사용되는 사용자의 바이오메트릭 정보는 각 사용자로부터 획득된 이미지에서 Proxy로부터 전달받은 도전값에 해당하는 좌표값에 해당하는 이미지 픽셀 정보를 이용하여 B-OTP 정보를 생성하는 방식이다.

2단계, 생성된 챌린지 값은 UAC로 전송하게 되며, UAC는 카메라 모듈로부터 획득된 바이오메트릭 정보와 서버로부터 받은 챌린지값, 그리고 비밀키를 이용하여 B-OTP를 생성한다. 3단계, 생성된 B-OTP는 서버로 보내지며, 서버는 UAC와 동일한 방식으로 B-OTP를 생성하게 된다. 4단계, 서버는 UAC에서 생성한 B-OTP 값과 서버에서 생성한 B-OTP 값을 비교하여 인증여부를 UAC에게 알려준다.

일반적으로 사용자는 서버에 로그인하기 위해 ID 및 PW를 생성하고 이를 통해 원격 접속자에 대한 인증 과정을 수행하게 된다. 만일 사용자 ID에 대해 고정적인 패스워드를 사용하는 경우 보안상의 문제로 인해 일정 주기가 되면 패스워드를 바꾸도록 권장하고 있다.

본 연구에서 구현한 일회용 패스워드 방식은 사용자 ID 및 PW로부터 매번 다른 패스워드를 생성하도록 하여 이를 통해 사용자 인증을 수행하는 방식으로, 네트워크를 통해 직접적인 원본 패스워드의 전송 없이 얼굴 등과 같은 바이오메트릭 정보를 이용하여 일정한 시간 동안만 사용 가능한 패스워드를 생성하고 이를 통해 원격 사용자에 대한 인증을 수행하는 방식이다. 이와 같은 방식을 이용할 경우 스마트폰 기반 SIP 프로토콜과 같은 응용 서비스에서의 인증 문제를 해결하는데 적용 가능한 방식으로 활용할 수 있다.

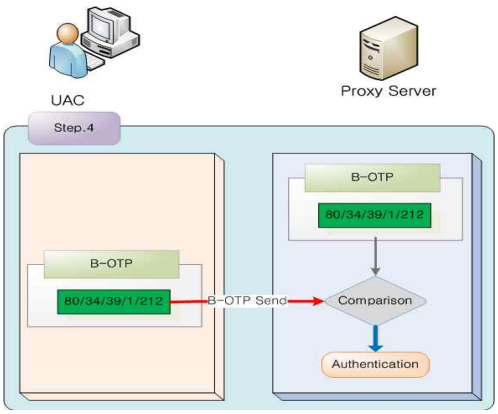
이때 사용되는 난수 함수는 암호학적으로 안전한 해쉬 함수와 큰 소수 p에 대한 mod 연산을 통해 계산된다. UAC는 Proxy Server로부터 받은 챌린지 값을 이용하여 UAC의 카메라 모듈로부터 획득된 이미지에 대해 B-OTP를 생성하게 된다. OTP Key 값의 정보를 이용하여 이미지내 특정 위치에 대한 픽셀 값을 추출하고 이 정보를 이용하여 그림 7과 같이 B-OTP 정보를 생성하게 된다.




[그림 7] B-OTP 생성 단계

B-OTP 값을 생성한 UAC는 Proxy 서버로 B-OTP 값을 전송한다. Proxy 서버는 그림 8과 같이 UAC로부터 전송 받은 B-OTP 값과 전 단계에서 생성한 B -OTP 값을 비교한다.

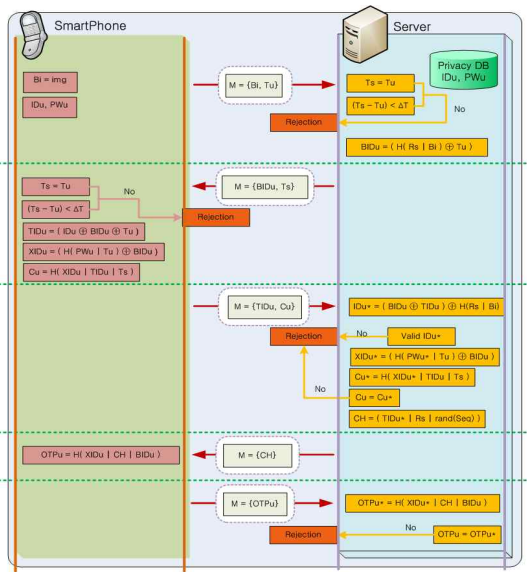
바이오메트릭 정보에 대해 전송하는 과정에서 원본 이미지에 대한 보안성을 향상시키기 위해서 기존의 영상 보안 기술에서 사용하는 퓨리에 변환 등을 사용하여 이미지에 대한 변환함수를 적용할 수 있으며, 역변환 과정을 통해 원본 이미지를 획득할 수 있다.




[그림 8] B-OTP 기반 인증 단계

### 3.3 얼굴 정보 기반 OTP 생성 방식

얼굴과 같은 바이오메트릭 정보를 이용하여 OTP 정보를 생성하고 이를 이용하여 인증 과정에 사용할 수 있다. 이와 같은 기본적인 방식을 토대로 보다 구체적인 B-OTP 생성 과정은 아래 단계와 같으며 전체적인 작동 과정은 그림 9에 제시하였다.




[그림 9] 얼굴 정보 기반 OTP 인증 단계

1단계 : 사용자는 자신의 스마트폰내 카메라 모듈을 이용하여 자신의 얼굴 이미지를 캡춰하여 Biometric Image 정보 Bi를 생성하고 이를 시간정보(Timestamp) Tu와 함께 서버로 전송한다.

2단계 : 서버는 자신의 시간정보 Ts와 클라이언트로부터 전달받은 Tu 값을 비교하여 일정한 오차범위 ΔT에 속할 경우 이를 받아들이고 서버가 임의로 생성한 난수값 Rs 값을 이용하여 바이오메트릭 정보 기반 사용자 u의 ID값 BIDu = H(Rs | Bi ) ⊕ Tu)를 생성한 후에 서버의 시간정보 Ts와 함께 {BIDu, Ts} 값을 클라이언트에 전송한다.

3단계 : 클라이언트는 서버로부터 전달받은 값에 대해서 Tu-Ts < ΔT에 속할 경우 이를 받아들이고 다음과 같이 TIDu, XIDu 및 Cu 값을 생성한다.

$$TIDu = ( IDu \oplus BIDu \oplus Tu )$$
$$XIDu = ( H( PWu \mid Tu ) \oplus BIDu ) \text{ ----------(1)}$$
$$Cu = H( XIDu \mid TIDu \mid Ts )$$

이때, TIDu 값은 사용자 ID 정보 IDu와 자신의 카메라 모듈을 통해 캡춰한 바이오메트릭 이미지 정보 Bi 를 포함하고 있는 BIDu 값과 시간정보 Tu 값을 이용하여 생성하게 되며, XIDu 값은 사용자 IDu에 대한 패스워드 정보 PWu와 서버로부터 전달받은 BIDu 값을 이용하여 생성하게 된다. 그리고 이 두 정보를 이용하여 클라이언트는 Cu = H( XIDu | TIDu | Ts )를 생성하게 된다. BIDu 값은 서버가 생성한 난수값 Rs를 이용하여 생성된 일회용 바이오메트릭 ID 정보(One-Time Biometric ID)가 되는 것을 알 수 있다. 클라이언트는 생성된 TIDu 값과 Cu 값을 서버로 전송한다.

4단계 : 이제 서버는 클라이언트로 전달받은 TIDu, Cu 값을 이용하여 우선 다음과 같이 IDu* = ( BIDu ⊕ TIDu ) ⊕ H(Rs | Bi* ) 값을 생성하여 자신의 DB에 저장된 IDu 정보에 대해서 IDu == IDu* 인지를 확인하게 된다. 만일 동일한 값을 얻게 되면 클라이언트 ID 정보에 대한 유효성을 확인하게 된다.

그런 다음에 서버는 클라이언트로 전달받은 TIDu, Cu 값을 이용하여 다음과 같이 XIDu* 와 Cu* 값을 생성하여 클라이언트에 대한 인증 과정을 수행하게 된다. XIDu* 값은 서버가 자신의 DB에 저장한 PWu* 값을 이용하여 아래와 같이 생성 및 검증이 가능하다.

$$XIDu^* = ( H( PWu \mid Tu ) \oplus BIDu ) \text{ ----------(2)}$$
$$Cu^* = H( XIDu^* \mid TIDu \mid Ts )$$

이제 클라이언트로부터 전달받은 Cu 값과 서버에서 생성된 Cu* 값을 비교하여 만일 동일한 값이 생성된다면 서버는 사용자 u의 일회용 바이오메트릭 ID 정보인 TIDu* 값을 이용하여 챌린지 값 CH = (TIDu* | Rs | rand(Seq)) 값을 생성하여 이를 클라이언트에 전송한다.

5단계 : 클라이언트는 서버로부터 전달받은 CH 값을 이용하여 다음과 같이 OTPu 값을 생성하고 이를 다시 서버에 전송하게 된다.

$$OTPu = H(XIDu \mid CH \mid BIDu) \text{ ----------(3)}$$

6단계 : 서버는 클라이언트로부터 전달받은 OTPu에 대해서 OTPu* 값을 생성하고 동일한 값이 생성되면 사용자에 대한 인증 과정을 완료하게 된다. 이와 같은 과정을 수행하는 과정에서 사용자 u의 IDu에 대한 패스워드 정보 PWu는 네트워크 전송 과정에서 외부로 유출되지 않으면서도 안전하게 사용자에 대한 인증 과정을 수행할 수 있다.

## 4. 안전성 분석 및 구현 결과

### 4.1 안전성 분석

앞에서 제시된 프로토콜 구조에서 사용자는 자신의 스마트폰내 카메라 모듈을 이용하여 자신의 얼굴 이미지를 캡춰하여 Bi와 Tu를 서버로 전송 한 후에 서버는 일정한

오차범위 ΔT에 속할 경우 서버가 임의로 생성한 난수값 Rs 값을 이용하여 바이오메트릭 정보 기반 사용자 u의 ID값 BIDu = H(Rs | Bi ) ⊕ Tu)를 생성하게 된다. 이때 생성되는 BIDu 값은 Tu라는 시간정보와 관련되어 일회용으로 생성되는 정보이며 클라이언트로부터 생성된 Bi 값에 대해 개인 프라이버시 관련 정보에 대한 유출 없이 사용되는 정보이다. 따라서 인터넷 전화 또는 인터넷뱅킹과 같은 서비스에서 MITM(Man-In-The-Middle) 공격 등을 사용한다고 할지라도 클라이언트에 전송되는 BIDu 정보 내에 서버가 임의로 선택한 난수값 Rs가 포함되어 있기 때문에 시간정보 Tu 및 Ts와 연관지어 재사용이 불가능한 형태라는 것을 알 수 있다.

일반적으로 인터넷뱅킹에서 사용되는 OTP 토큰은 MITM 공격이 가능하다. 하지만 본 연구에서 사용하는 기법인 경우에는 각 개인이 본인이 캡춰한 이미지 정보를 서버로 전송한 후에 일회용 바이오메트릭 ID 정보를 기반으로 서버가 생성한 시간정보 및 난수값 정보와 함께 최종적으로 일회용 OTP 값을 생성하게 되므로 기존의 OTP 방식에서 문제가 되는 MITM 공격에 대해 보다 강화된 보안성을 제공할 수 있다.

### 4.2 인증 기능 분석

인터넷전화에서 사용하는 SIP 프로토콜을 통해 송수신되는 패킷은 텍스트 형식이다. 따라서 공격자에 의해서 손쉽게 수정 및 삭제가 가능하다. 따라서 본 논문에서 제시한 기법을 이용할 경우 SIP 프로토콜 호 설정 과정에서 바이오메트릭 ID 정보 등을 이용하여 INVITE 패킷에 대한 사용자 인증을 강화할 수 있다. 또한 인증 과정에서 일방향 해쉬 함수를 사용하여 클라이언트-서버간 송수신되는 메시지에 대한 무결성을 확인할 수 있도록 하였다.

인터넷뱅킹에서 사용자 인증을 위해 사용하고 있는 OTP 방식과 인터넷전화 기반 SIP 프로토콜에서의 사용자 인증은 각각의 서비스에 대한 보안성을 강화하기 위해 반드시 필요한 모듈이다. 본 논문에서 제시한 바이오메트릭 일회용 ID를 이용한 OTP 방식인 경우 각 개인이 카메라 모듈을 통해 캡춰한 후에 전송하는 바이오메트릭 정보를 기반으로 생성되며 이 정보에 서버에서 생성한 난수값을 적용하였기 때문에 원본 바이오메트릭 정보를 사용하지 않고서도 인증 과정을 수행하도록 구성되었다. 따라서 SIP 프로토콜 기반 인터넷전화 서비스에서 B-OTP 과정을 통해 정상적인 사용자의 여부를 확인하여 보다 안전한 사용자 인증 과정을 수행하게 된다.

아래 표 1과 같이 본 연구에서 제시한 기법과 기존 기법에서의 인증 성능에 대해 비교 분석하였다. 단계별 일방향 해쉬함수에 대한 사용 회수 Th를 기준으로 계산량을 비교하였다.

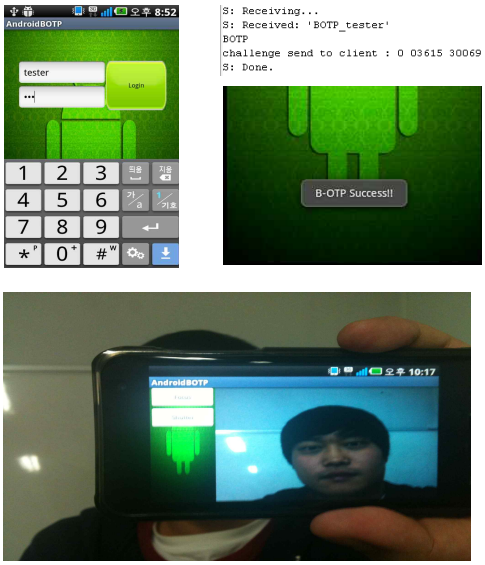
[표 1] 인증 계산량 및 기능 비교 분석

| 구분 | 제안기법 | Wang-Li[7] | Yoon-Yoo[8] | Khan et al[9] |
|---|---|---|---|---|
| 등록단계 | 3*Th* | 3*Th* | 3*Th* | 2*Th* |
| 로그인 | 2*Th* | 2*Th* | 3*Th* | 2*Th* |
| 인증단계 | 4*Th* | 5*Th* | 4*Th* | 2*Th* |
| 상호인증 | O | O | O | O |
| 서버 시간정보 | O | X | X | O |
| 시간 동기화 | X | X | O | O |
| B-OTP 생성 | O | X | X | X |
| 바이오 정보 | 얼굴 | 지문 | 지문 | 지문 |

본 연구에서 제시한 기법은 기존 기법과 유사한 계산량을 보이고 있다. 바이오메트릭 정보를 이용하여 인증 기능을 제공하면서도 추가적으로 OTP 생성 기능을 제공하는 것을 확인할 수 있다. 그리고 본 연구에서 제시한 기법은 MITM 공격을 방지하기 위해 서버에서 시간정보를 사용하도록 하였다. 그리고 인증 과정에서 사용하는 바이오메트릭 정보인 경우 기존의 기법[7-9]인 경우 주로 지문 정보를 이용하였으나 본 연구에서 제시한 기법인 경우 바이오메트릭 정보 중에서 얼굴 정보를 사용하도록 하였다. 물론 본 연구에서 제시한 기법은 기존의 기법과 마찬가지로 지문 정보에도 적용 가능하다.

### 4.3 구현 결과

본 연구에서 제안한 메커니즘에 대해 안드로이드 OS를 기반으로 구현하였다. 클라이언트 모듈 개발을 위해 Eclipse를 기반으로 Android SDK 2.2를 이용하여 구현하였다. 그리고 서버 부분은 MySQL을 기반으로 하였으며 클라이언트와 서버간 인증 과정을 수행하도록 하였다. 그림 10과 같이 클라이언트에서는 안드로이드 OS 기반 스마트폰에서 카메라 모듈을 이용하여 사용자 얼굴 이미지를 캡춰한 후에 전송하면 서버에서 일회용 바이오메트릭 ID 정보를 생성하도록 하였고 클라이언트로 전송하여 사용자 인증을 위한 OTP 값을 생성하도록 하였다.

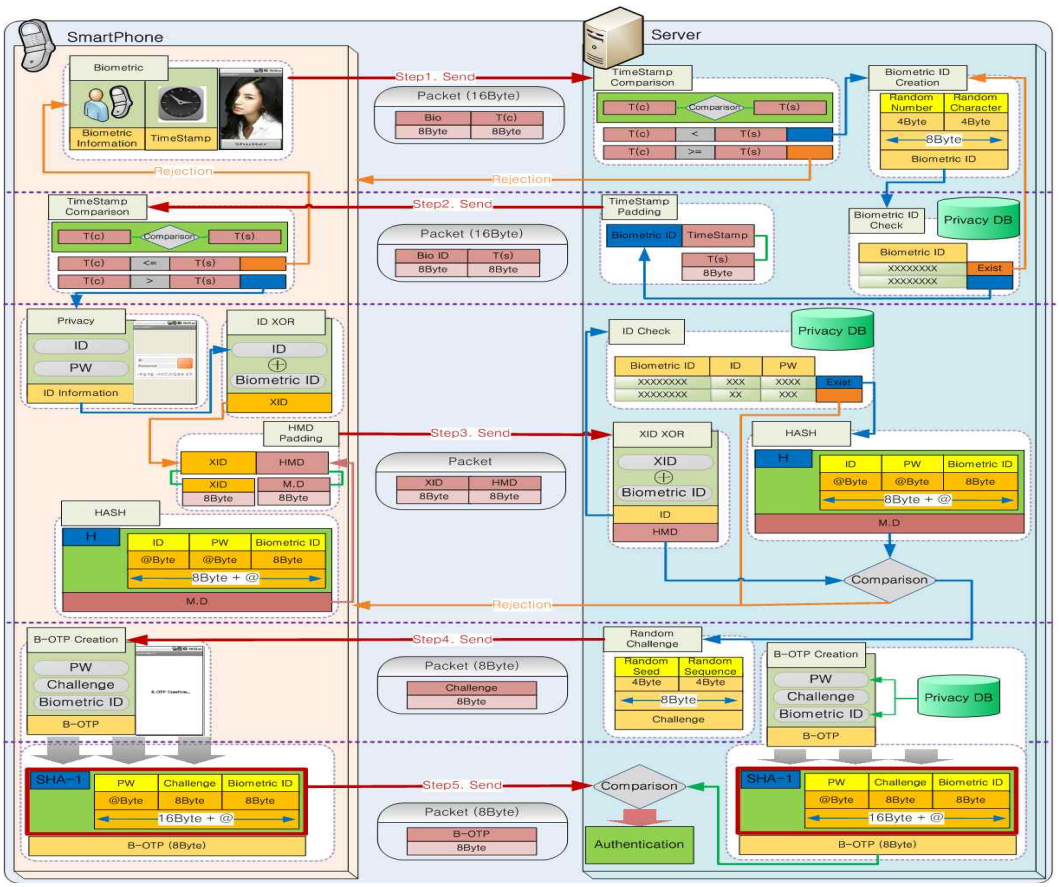



[그림 10] 구현 결과

시스템 구현 결과 및 내부 작동 방식은 그림 11과 같다. 사용자는 자신의 스마트폰내 카메라 모듈을 이용하여 얼굴 이미지를 획득하게 되고 서버와의 상호 인증 과정을 수행한 후에 얼굴 이미지 정보를 이용하여 일회용 패스워드를 생성하고 이를 이용하여 스마트폰 서비스에 대한 일회용 인증 과정을 수행하게 된다. 물론 사용자 인증에 사용된 이미지 정보는 원본 그대로 전송되는 것이 아니라, 내부에 랜덤 픽셀을 추출하는 모듈에서 8바이트 크기의 일부 바이오메트릭 정보만을 획득하여 OTP 생성 과정에 적용된 후에 삭제 및 재사용하지 않는 방식을 통해 보안성을 높일 수 있도록 하였다.

## 5. 결론

기존의 인터넷뱅킹 및 인터넷전화 서비스 역시 스마트폰을 통해 이용 가능하게 되었다. 하지만 스마트폰을 통




[그림 11] 시스템 구현 결과 및 작동방식

해 전자금융이나 인터넷 서비스 등에 이용할 경우에 보다 강화된 사용자 인증 기능을 제공해야 할 필요가 있다. 그 이유는 스마트폰 분실 및 신분정보를 도용하여 발급된 불법 휴대폰 등을 이용한 불법적인 인터넷 서비스 사용 등이 가능하기 때문이다. 따라서 스마트폰 환경에서는 보다 강화된 사용자 인증 기능을 제공할 필요가 있다.

이에 본 연구에서는 스마트폰내 카메라 모듈을 이용하여 사용자가 자신의 얼굴 바이오메트릭 정보를 전송하도록 하였으며 서버에서는 난수값 및 시간정보 등을 이용하여 일회용 바이오메트릭 ID를 생성하도록 하였다. 그리고 도전-응답 방식으로 일회용 바이오메트릭 ID 기반 OTP 값을 생성토록 하여 SIP 프로토콜에서의 사용자 인증에 적용하거나 스마트폰 기반 인터넷뱅킹에 적용할 수 있도록 하였다. 본 연구에서 제시된 기법을 이용할 경우 최근 널리 확산되고 있는 스마트폰 기반 전자금융 및 인터넷 서비스에서의 보안성을 한층더 강화할 수 있는 방안이 될 것으로 기대한다.

## 참고문헌


[1] 한국전자통신연구원(ETRI), “VoIP 기술 및 시장 동향”, 기술평가팀 P.4-13, P.19-45, 2006.

[2] 장원준, 이형우, “바이오메트릭 정보를 이용한 일회용 패스워드(B-OTP) 생성 기법 개발 및 응용”, 한국융합학회논문지, Vol.1, No.1, pp.93-100, 2010.

[3] http://www.voip-forum.or.kr, VoIP 국내표준, “SIP 기반 인터넷 텔레포니 단말”, 2005.

[4] 최동현, 김승주, 원동호, “일회용 패스워드(OTP: One-Time password)기술 분석 및 표준화 동향”, 한국정보보호학회지), Vol.17, No.3, pp12-17, 2007.

[5] 김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 한국정보보호학회지, Vo1.17, No.3, pp26-13, 2007.

[6] 이형우, 박영준, “바이오 정보를 이용한 사용자 인증 시스템 설계 및 구현", 한국산학기술학회논문지, Vol.11, No.9, pp.3548-3557, 2010.

[7] De-Song Wang, Jian-Ping Li, "A new fingerprint-based remote user authentication scheme using mobile devices", International Conference on Apperceiving Computing and Intelligence Analysis, ICACIA 2009, pp.65-68, 2009.

[8] Yoon E.J., and Yoo K.Y., “A secure chaotic hash-based biometric remote user authentication scheme using mobile devices”, APWeb/WAIM 2007, Huang Shan, pp. 612-623, June 2007.

[9] Khan M.K., Zhang J.S., and Wang X.M., “Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices”, Chaos, Solitons & Fractals, Vol. 35, pp. 519-524, 2008.

[10] Yoon E.J., Ryu E.K., and Yoo K.Y., “An improvement of Hwang-Lee-Tang’s simple remote user authentication scheme”, Computers & security, Vol. 24, pp. 50-56, 2005.



장 원 준(Won-Jun Jang) [정회원]

- 2010년 2월 : 한신대학교 정보시스템공학과 (학사)
- 2010년 2월 ~ 현재 : 한신대학교 컴퓨터공학부 석사과정

<관심분야>
스마트폰 보안, 네트워크 보안, 정보보호

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 전산과학과 (이학사)
- 1996년 2월 : 고려대학교 일반대학원 전산과학과 (이학석사)
- 1999년 2월 : 고려대학교 일반대학원 전산과학과 (이학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 조교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 부교수

<관심분야>
네트워크 보안, 정보보호, 무선네트워크, SIP 보안