DOI: 10.3745/KIPSTC.2011.18C.2.079

스마트폰에서 음성 정보를 이용한 일회용 패스워드(V-OTP) 기반 사용자 인증 메커니즘 설계 및 구현

조 식 완† · 이 형 우††

요 약

음성 정보를 이용한 인증과정을 통해 스마트폰 서비스에서의 보안성을 향상시킬 필요가 있다. 본 연구에서는 스마트폰 사용자의 음성 정보를 이용하여 일회용 패스워드를 생성하는 메커니즘을 설계 및 구현하였다. 서버에서 전송된 PIN 값에 대해 스마트폰내 마이크 장치를 이용하여 음성 데이터를 캡춰하여 서버로 전송하면 서버에서는 검증 과정을 수행하고 일회용 토큰을 생성하도록 하였다. 그리고 클라이언트-서버간 상호 인증 과정 수행 후에 최종적으로 스마트폰 환경에서 음성 정보를 이용하여 일회용 패스워드(V-OTP)를 생성하는 메커니즘을 개발하였다. 본 연구에서 제시한 기법을 이용할 경우 스마트폰 기반 서비스에서의 사용자 인증을 보다 강화할 수 있다.

키워드 : 음성, 일회용 패스워드, 인증, 정보보안

Design and Implementation of Voice One-Time Password(V-OTP) based User Authentication Mechanism on Smart Phone

Sik-Wan Cho† · Hyung-Woo Lee††

ABSTRACT

It is necessary for us to enhance the security service on smart phone by using voice data on authentication procedure. In this study, a voice data based one-time password generation mechanism is designed and implemented for enhancing user authentication on smart phone. After receiving a PIN value from the server, a user inputs his/her own voice biometric data using mike device on smart phone. And then this captured a voice biometric data will be used to generate one-time token on server side after verification procedures. Based on those mutual authentication steps, a voice data based one-time password(V-OTP) will be generated by client module after receiving the one-time token from the server finally. Using proposed voice one-time password mechanism, it is possible for us to provide more secure user authentication service on smart phone.

Keywords : Voice, OTP, Authentication, Data Security

1. 서 론

스마트폰 등과 같은 모바일 환경에서 음성 정보 등을 접목한 연구가 수행되고 있다[1,2,3]. 하지만 스마트폰을 통해 전자금융 서비스를 이용할 경우 개인정보에 대한 유출 및 사용자에 대한 인증 과정에 대한 공격을 통해 전자금융 서비스의 취약성이 발견되고 있다. 따라서 기존의 인터넷 뱅킹 관련 전자금융 서비스에서는 사용자 인증을 강화하기 위해 일회용 패스워드(OTP : One Time Password)를 이용하도록 권장하고 있으며 표준화 과정도 진행중에 있다[4]. 하지만 스마트폰 등을 통해 전자금융 서비스를 이용할 경우 불법적으로 인가된 단말 등을 통해 사용할 수 있기 때문에 보다 강화된 사용자 인증 과정이 제공되어야 한다[5,6].

스마트폰 기반 전자금융 서비스에서 사용하는 기존 OTP 방식은 OTP 토큰에 대한 실제 단말 소유자에 대한 정확한 확인 과정을 제공되지 못하고 있고, OTP 정보에 대해 MITM(Man in the Middle Attack) 공격이 가능하기 때문에 이를 능동적으로 보완할 수 있는 방법이 기술적으로 제시되어야 한다[6].

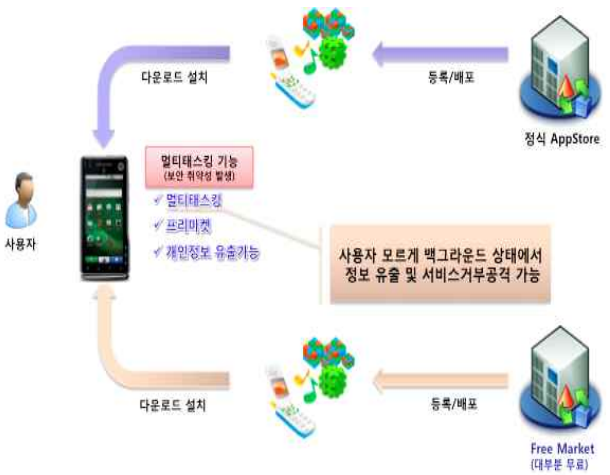
※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2009-0071654).
† 준 회 원 : 한신대학교 컴퓨터학과 석사과정
†† 종신회원 : 한신대학교 컴퓨터학부 교수
논문접수 : 2011년 2월 25일
수 정 일 : 1차 2011년 3월 30일
심사완료 : 2011년 3월 31일

따라서 본 연구에서는 스마트폰 사용자에 대한 강화된 인증 과정을 제공하기 위해 일회용 패스워드 기반 인증 과정에서 사용자 음성 정보(voice data)로부터 최종적으로 OTP 값을 생성하여 스마트폰 사용자 인증에 활용하는 방식을 제시하고자 한다. 이 경우 기존의 스마트폰 기반 서비스에서 발생하는 불법 사용자에 의한 인증 우회 공격 문제를 해결할 수 있으며, 스마트폰을 이용한 다중 인증(Multifactor Authentication) 기능을 제공할 수 있다는 장점이 있다.

2. 기존 OTP 및 음성 기반 인증

2.1 스마트폰 사용자 인증 취약성

최근 스마트폰 관련 보안사고가 다수 발생하고 있어 사회적 문제로 대두되고 있으며 특히 단말내 저장된 개인정보 등이 외부로 유출되는 등의 문제가 발생하고 있다. 스마트폰을 이용할 경우 악성코드 등에 의해 원격제어, 정상 동작 방해 및 전자금융 서비스 관련 과금유도 등의 문제가 발생할 수 있다. 또한 (그림 1)과 같이 스마트폰에 설치되는 소프트웨어가 멀티태스킹 방식으로 구동되는 과정에서 개인정보가 유출되는 문제가 발생하여 이에 대한 대응 기술이 제시되어야 한다.



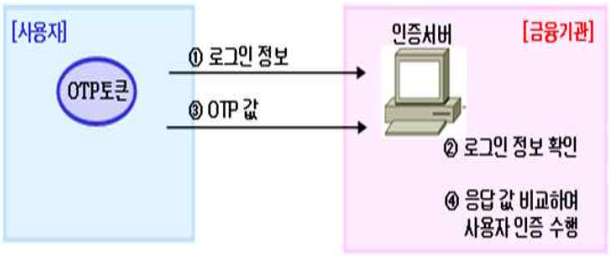
(그림 1) 스마트폰 개인정보 유출 및 인증 문제

스마트폰 단말에서의 보안 취약성으로는 악성코드 감염, 데이터 유출, 사용자 오남용 및 단말 분실/도난등의 보안 취약성이 발생할 수 있으며, 공중망 및 전달망에서의 보안 취약성으로는 Wi-Fi 기반 통신시 AP에 대한 공격/해킹으로 인한 데이터 위/변조 및 유출 취약점이 발생할 수 있다. 그리고 스마트폰을 통한 인터넷망 사용시 보안 취약성으로는 스마트폰내 악성코드 등을 통한 DoS/DDoS 공격 및 인증 우회/계정 탈취 등의 보안 취약점이 발생하고 있다.

따라서 이와 같은 문제를 해결하기 위해서는 스마트폰 사용자에 대한 인증을 강화하는 방법이 제시되어야 한다. 스마트폰 내부 정보에 대한 접근권한을 중심으로 보다 강화된 인증 메커니즘이 필요하다.

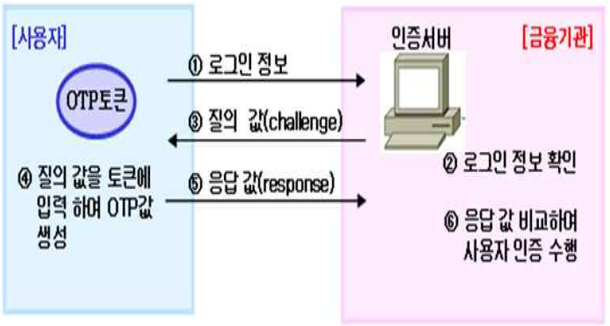
2.2 OTP 기술 분석

기존의 OTP(One-Time Password)[4] 기술은 일회용 패스워드를 생성하는 기술이다. OTP 생성기술은 크게 비동기화 방식과 동기화 방식으로 나눌 수 있다.



(그림 2) 비 동기화 OTP 방식

비동기화 OTP 방식[4,5]은 (그림 2)와 같이 Challenge Response 방식으로 작동하는 것으로 인증 서버 또는 애플리케이션이 임의의 난수값을 생성해서 사용자에게 보내면(Challenge), 사용자는 이 난수값을 일회용 패스워드 생성 토큰 또는 소프트웨어에 입력하고, 여기서 나오는 출력값을 일회용 패스워드로 입력해(Response) 사용자 인증이 수행된다. 이 방식은 서버와의 동기화가 필요 없는 방식이지만 사용자의 입력이 필요하며 네트워크 과부하를 유발하기도 한다.



(그림 3) 동기화 OTP 방식

동기화 OTP 방식[5]은 (그림 3)과 같이 시간 동기화 방식, 이벤트 동기화 방식, 이벤트-시간 동기화 방식으로 나눌 수 있다.

먼저 시간 동기화란 이름에서 알 수 있듯이 시간 동기화 방식은 시간을 일회용 비밀번호의 입력값으로 사용되어 동기화 방식에서 인증 서버가 보내주던 챌린지 전달 절차 없이 사용자가 일회용 비밀번호를 생성해 PIN(사용자 비밀번호, 비밀키)과 함께 인증 서버에 전달하면, 서버는 PIN을 인덱스로 하여 해당 비밀키를 찾고, 생성된 일회용 패스워드가 수신한 것과 일치하는 지를 확인한다.

시간 동기화 방식은 인증 서버와 사용자 모두 같은 시간을 일회용 비밀번호의 입력값으로 넣어야 하기 때문에 인증 서버와 사용자 토큰 사이에 시간이 일치하지 않으면 사용자 인증에 실패할 수 밖에 없다. 일회용 비밀번호의 입

력값을 서버로부터 받지 않는 장점이 있는 반면 서버와 사용자 토큰의 정보를 일치시켜야 하는 단점을 안고 있어 사용자 수가 많은 경우 여러 개의 시간을 동시에 일치시키기 힘들기 때문에 문제 발생 가능성이 있다. 따라서, 많은 경우 시간의 오차 범위를 설정해서 그 범위 안에서는 인증이 성공하도록 허용하고 있다. 또한, 대체로 1분, 2분 단위로 일회용 패스워드가 생성되기 때문에 인증 실패 시에는 인증 재시도를 위해 기다려야 하는 불편함과 일정 시간 동안 입력하지 못하면 중간에 패스워드가 바뀌어 다시 입력해야 하는 점 등도 단점으로 꼽히고 있다.

이벤트 동기화 방식은 시간 동기화 방식이 갖고 있는 단점을 극복한 방식으로 인증서버와 사용자 토큰 간에 시간 정보를 일치시킬 필요가 없으면서도 잘 알려진 암호 알고리즘을 사용하기 때문에 안전성이 높은 방식이며 시간 정보 대신에 인증서버와 인증 횟수(Counter) 기록을 공유하고 인증 횟수를 일회용 패스워드 생성시 입력값으로 활용한다.

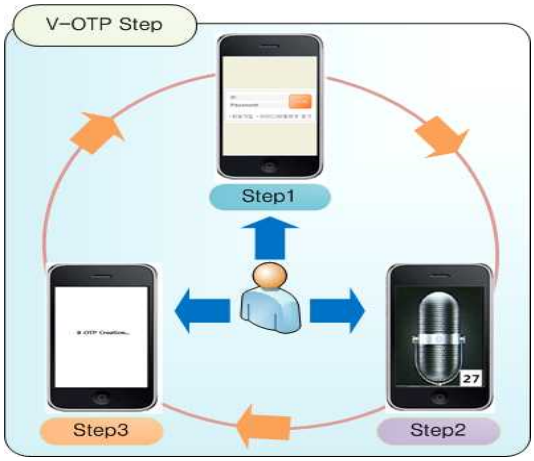
시간 동기화 방식이 인증 서버와 OTP 토큰 사이에 시간을 일치시켜야 하는 것처럼, 이벤트 동기화 방식에서는 카운터를 인증 서버와 OTP 토큰 사이에 일치시켜야 정상적으로 인증이 수행된다. 이벤트 동기화 방식에서 생길 수 있는 문제점은 사용자가 실수 또는 호기심에 의해 일회용 패스워드를 생성해 인증 서버의 카운터와 OTP 토큰의 카운터가 맞지 않는 경우에 발생할 수 있다. 이 경우 세이프워드 OTP는 인증 서버에서 카운터의 오차 범위(카운터~카운터 +16 범위를 일반적인 오차 범위로 허용함)를 정해 범위 내에 들어올 경우에 사용자 인증을 허용하는 방법과 오차 범위를 벗어날 경우 연속된 2번의 일회용 비밀번호가 올바른 값으로 판단될 경우 사용자 인증을 허용하는 방식으로 문제점을 극복하고 있다.

마지막으로 이벤트-시간 동기화 방식은 이러한 시간 동기화 방식과 이벤트 동기화 방식의 단점을 보완하기 위해 두 동기화 방식을 결합하여 사용하는 방식으로 다양한 조합이 나올 수 있다.

2.3 음성 데이터 기반 인증

최근 음성 정보 일회용 패스워드 생성 과정과 접목하고자 하는 연구가 진행되고 있다[7]. 하지만 구체적인 내용 등이 아직 발표되지는 않은 상태이다. 이에 본 연구에서는 최근 국내외적으로 이슈가 되고 있는 스마트폰을 이용한 전자금융 서비스에서의 보안성을 강화하고 사용자 인증 취약점을 개선하기 위해 각 개인이 고유하게 소유하고 있는 음성 정보와 기존의 전자금융 서비스에서 사용되는 OTP 기술을 접목한 V-OTP 메커니즘을 제시하고자 한다.

본 연구에서 제안하는 구조는 (그림 4)와 같이 스마트폰 사용자의 인증 취약점을 보완하고 보안성을 강화하기 위해 ID와 패스워드 만을 사용하던 기존의 인증 방식에 추가적으로 사용자의 음성 정보를 이용하여 일회용 패스워드를 생성하고 이를 통해 스마트폰 사용자의 인증을 강화하는 메커니즘에 대해 설계 및 구현하고자 한다.



(그림 4) 음성 정보를 이용한 OTP 생성

3. 제안하는 V-OTP 기반 인증

3.1 V-OTP 기반 사용자 인증 구조

전자금융 서비스 이용시 사용자는 자신에 대한 인증 과정을 통과하기 위해 스마트폰 등에 있는 마이크를 이용하여 서버로부터 전송된 도전값에 대해 음성으로 해당 숫자 정보를 읽은 후에 캡춰된 음성 정보를 이용하여 OTP를 생성하는 과정을 수행하게 된다. 구체적으로 V-OTP 인증을 위한 사용자 음성 정보 입력 및 OTP 생성 절차는 다음과 같다.

서버는 임의의 난수 도전값을 생성하여 클라이언트에게 전송한다. 클라이언트는 자신의 스마트폰에 탑재되어 있는 마이크 모듈을 이용하여 도전값 정보에 대해 직접 마이크를 통해 음성 정보를 입력하고 이를 서버에게 전송한다. 서버는 클라이언트로부터 수신된 정보를 이용하여 클라이언트 단말에 대한 인증 과정을 수행하고 서버에서 생성한 난수값을 이용하여 클라이언트에게 전송한다. 마지막으로 클라이언트는 서버로부터 전송 받은 정보에 대한 확인 과정을 수행한 후에 자신이 입력한 음성정보와 서버로부터 전송받은 도전 값 등을 이용하여 V-OTP를 생성하고 이를 다시 서버로 전송하며 서버는 이를 검증하여 최종적으로 클라이언트에 대한 인증 과정을 수행하게 된다.

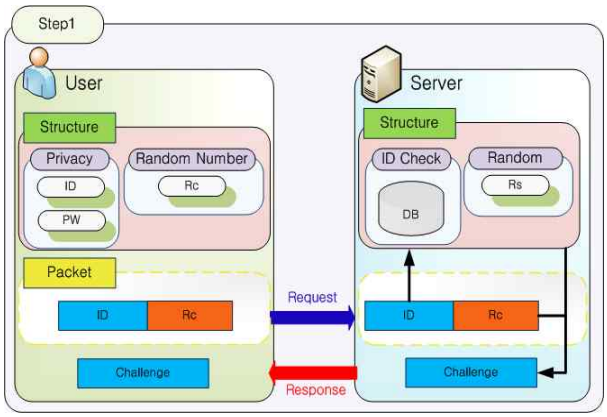
3.2 V-OTP 생성 단계

V-OTP 기반의 사용자 인증을 위한 세부 단계는 다음과 같다. 1단계, (그림 5)와 같이 클라이언트는 자신의 ID 정보 IDu와 클라이언트가 임의로 선택한 난수값 Rc를 서버에 전송하게 되며, 서버는 자신의 DB에 있는 정보를 확인하여 등록된 사용자인지 확인하는 과정을 수행한다. 만일 등록된 사용자가 아닐 경우에는 OTP 생성 과정을 종료하게 된다. 그리고 만일 클라이언트로부터 수신한 IDu가 등록된 ID라면 서버는 난수값 Rs를 생성하고 클라이언트로부터 수신한 Rc와 함께 아래 수식 (1)과 같이 도전값(Challenge)에 해당하는 $Chal = H(Rc \oplus Rs)$을 생성하여 이를 클라이언트로 전송하게 된다.

$IDu == IDu^*$

$Chal = H(Rc \oplus Rs)$ (1)

이때 전송되는 *Chal* 값은 숫자 또는 문자로 구성된 것으로 클라이언트의 스마트폰 단말에 표시된다. 클라이언트와 서버가 임의로 선택하게 되는 난수값 *Rc*와 *Rs* 값은 V-OTP 기반 사용자 인증을 수행할 때마다 매번 다르게 선택하는 값이다.



(그림 5) V-OTP 초기 단계

2단계, 클라이언트는 서버로부터 전송받은 *Chal* 값에 해당하는 내용에 대해 스마트폰 단말에 있는 마이크를 통해서 해당 내용을 음성으로 읽는 과정을 수행하게 된다. 이 때 발생한 Chal 값은 9자리 숫자로 구성되어 있으며 일반적으로 10자리 숫자에 기준하여 사용자가 입력/발성 시 5초 동안 사용자가 마이크로 음성 데이터를 입력하도록 하여 Ai 값을 생성하게 하였다. 그 후 수식 (2)와 같이 사용자가 직접 입력한 음성 정보 Ai 값과 사용자의 *IDu*, 패스워드 정보 *PWu* 값 및 클라이언트가 임의로 선택한 난수값 *Rc*를 이용해서 해쉬 결과값 $Au= H((Ai \mid IDu \oplus PWu \oplus Rc))$를 생성하도록 하였고, 서버로부터 수신한 *Chal* 값을 이용하여 수식 (3)과 같이 응답값(Response)에 해당하는 $Cu= H(Ai \mid Chal \mid Au)$ 값을 생성하여 사용자가 입력한 음성 데이터 값 Ai와 함께 서버로 전송하도록 하였다.

$Ai = voice\ data$

$Au = H((Ai \mid IDu \oplus PWu \oplus Rc))$ (2)

$Cu = H(Ai \mid Chal \mid Au)$ (3)

3단계, 이제 서버는 클라이언트로부터 수신한 *Cu* 및 *Ai* 값에 대해 검증하는 과정을 수행한다. 수식 (4)와 같이 자신의 DB에 저장된 사용자u의 ID, 패스워드 값과 클라이언트로부터 수신한 난수값 Rc, 음성 데이터 Ai를 이용하여 $Au^* = H((Ai^* \mid IDu^* \oplus PWu^* \oplus Rc))$ 값을 생성하고, 수식 (5)와 같이 서버가 생성한 *Chal* 값에 대해 $Cu^* = H(Ai^* \mid Chal \mid Au^*)$ 값을 생성하여 클라이언트로부터 수신한 *Cu* 값과 비교하여 클라이언트-서버간 상호인증 (Mutual Authentication) 과정을 수행하게 된다. 만일 상호인증 결과가 일치한다면 이제 V-OTP를 생성하기 위한 과정을 수행한다. 수식 (6)과 같이 서버는 자신이 생성한 난수값 *Rs*를 이용하여 V-OTP 생성을 위한 일회용 토큰 (One-time Token) $Ts= Cu^* \oplus Rs \oplus H(Rc \mid Au^*)$를 생성하여 클라이언트에게 전송한다. 위 단계를 수식으로 표현하면 다음과 같다.

$Ai^* = Ai$

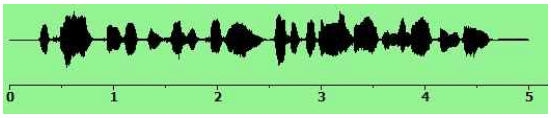
$Au^* = H((Ai^* \mid IDu^* \oplus PWu^* \oplus Rc))$ (4)

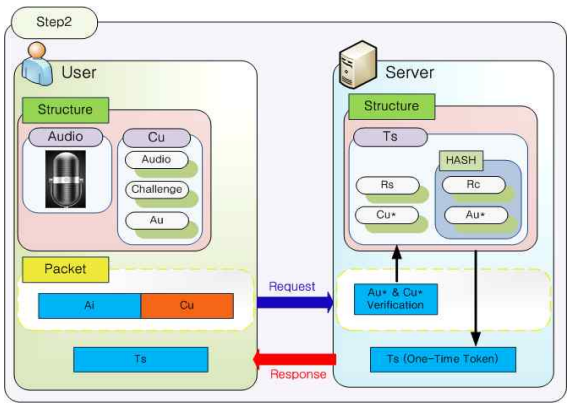
$Cu^* = H(Ai^* \mid Chal \mid Au^*)$ (5)

$Cu^* == Cu$

$Ts = Cu^* \oplus Rs \oplus H(Rc \mid Au^*)$ (6)

음성 정보를 이용한 상호 인증 및 일회용 토큰 생성 구조는 (그림 6)과 같다.





(그림 6) 음성 정보 기반 상호 인증 및 토큰 생성 단계

4단계, 클라이언트는 서버로부터 수신한 *Ts* 값에서 수식 (7)과 같이 서버가 임의로 선택한 난수값 $Rs^* = Ts \oplus Cu \oplus H(Rc \mid Au)$ 값을 획득하는 과정을 수행한다. 그리고 수식 (8)과 같이 2단계에서 서버로부터 수신한 *Chal* 값과 $H(Rc \oplus Rs^*)$ 값이 동일한 값인지를 확인하는 서버 재인증 과정을 수행한다. 그리고 수식 (9)와 같이 음성 데이터가 포함되어 있는 *Au* 값을 이용하여 일회용 패스워드 $VOTPu= H(Au \oplus H(Ts \mid Rs^* \mid Chal))$ 값을 생성하여 이를 다시 서버에 전송하게 된다.

$Rs^* = Ts \oplus Cu \oplus H(Rc \mid Au)$ (7)

$Chal == H(Rc \oplus Rs^*)$ (8)

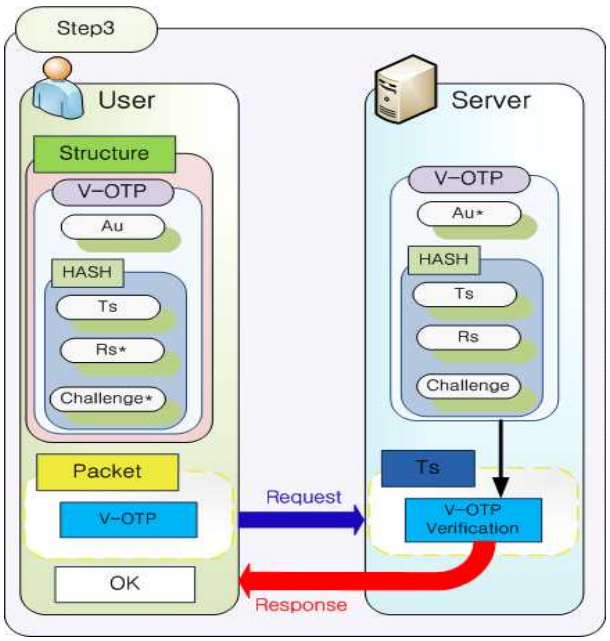
$VOTPu = H(Au \oplus H(Ts \mid Rs^* \mid Chal))$ (9)

마지막 5단계에서 서버는 수식 (10)과 같이 클라이언트

로부터 전달된 음성 일회용 패스워드 *VOTPu*에 대한 확인/검증 과정을 수행하여 스마트폰 사용자에 대한 인증 과정을 마무리하게 된다. 클라이언트로부터 전달되는 *VOTPu* 값에는 사용자가 직접 마이크를 통해 입력한 음성 데이터 *Ai*와 사용자 u의 ID, 패스워드 및 난수값 *Rc*로부터 생성된 *Au* 값과 서버로부터 수신된 *Chal* 값 및 상호인증 과정에서 서버로부터 수신한 *Ts* 및 *Rs** 값을 이용하여 생성된 일회용 패스워드 정보이다.

$$VOTPu^* = H(Au^* \oplus H(Ts \mid Rs \mid Chal))$$
$$VOTPu^* == VOTPu \qquad (10)$$

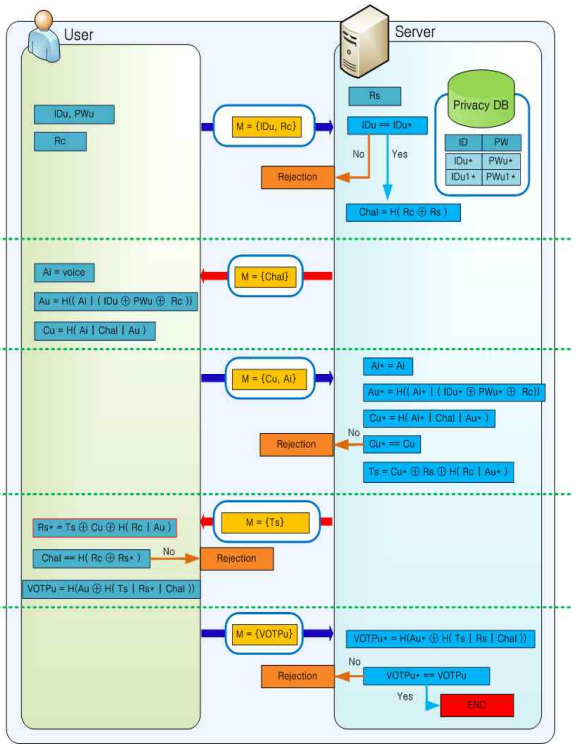
결국 본 연구에서 제시한 기법을 이용할 경우 기존의 스마트폰 환경에서 발생하는 사용자 인증 문제를 해결할 수 있는 방법이 되며 사용자의 음성 데이터 값을 이용하였기 때문에 MITM 공격 등에 안전한 특성을 보이고 재전송 공격을 막는 방법이기도 하다. 암호학적으로 안전한 해쉬함수와 난수발생기 및 XOR 함수만을 이용하여 인증 과정을 수행하도록 하였다.



(그림 7) V-OTP 생성 및 검증 단계

3.3 음성 기반 OTP 생성 메커니즘

아래 그림에서와 같이 사용자는 기존의 전자금융 서비스 이용시와 동일하게 사전에 서버에 자신의 ID와 패스워드에 대한 등록 과정을 수행하게 된다. 이제 사용자의 ID/PW 정보는 서버에 저장되어 있다는 가정하에 본 연구에서 설계 및 구현한 방식인 경우 실제적인 사용자 인증 과정에서 네트워크를 통해 사전에 등록된 자신의 패스워드 정보를 전송하지 않고 클라이언트 단말과 서버 내부에서만 사용되면서도 V-OTP 방식을 통해 사용자에 대한 인증 과정을 안전하게 수행하는 방식이다.



(그림 8) 음성 정보 기반 V-OTP 인증 알고리즘 구성도

4. 구현 결과

4.1 구현 결과

본 연구에서 제안한 메커니즘에 대해 iPhone iOS4.2를 이용하여 구현 결과를 테스트 하였다. Apple에서 제공하는 Xcode 3.2.5 개발 환경을 이용하였으며 V-OTP 서버 부분은 MySQL을 기반으로 구현하였다. 그림과 같이 클라이언트에서는 iOS 기반 스마트폰에서 마이크 컨트롤러 모듈을 이용하여 서버에서 생성하여 전송된 Chal 값에 대해 5초 동안 사용자 본인이 직접 자신의 음성을 통해 해당 숫자 정보를 마이크를 통해 읽도록 하였고 이를 스마트폰 단말에서 캡쳐하도록 하였다. 클라이언트와 서버는 상호 인증 과정을 수행하도록 하였고, 서버는 음성 정보로부터 생성된 일회용 토큰 값을 다시 스마트폰으로 전송하면 최종적으로 음성 정보로부터 일회용 패스워드를 생성하도록 하였다. 본 연구에서 V-OTP 방식에 대해 구현 결과 실행화면은 다음 (그림 9)와 같다.

(그림 9) V-OTP 초기 실행화면

(그림 9)와 같이 본 연구에서 구현한 V-OTP 소프트웨어에 대해 실행하는 과정에서 기존 방식과 동일하게 서버에 등록된 ID 및 패스워드 정보를 입력하게 된다. 이때 사용자가 입력한 패스워드 정보는 스마트폰 단말 내부에서만 사용되는 정보이며 네트워크를 통해 서버로 전송되지 않는 정보이다. 사용자가 입력한 ID 값에 대해 클라이언트 단말에서 생성한 난수값 *Rc*와 함께 서버로 전송하면 일차적으로 서버 DB에 저장된 ID 목록과 확인하여 만일 등록되지 않은 ID일 경우에는 이후 과정을 종료하고 이에 대해 [그림 9]과 같이 스마트폰 단말에 표시하도록 하였다. 사용자 ID에 대한 확인 과정 후에 서버는 *Chal* 값을 생성하여 이를 스마트폰 단말에 전송하게 된다. 아래 (그림 10) 실행화면인 경우 서버로부터 도전값 '205871198'이 수신된 것을 볼 수 있으며, 사용자는 이제 스마트폰에 내장된 마이크 장치를 이용하여 해당 숫자 정보를 음성으로 직접 읽는 과정을 수행하게 된다.

본 연구에서는 9자리 숫자에 대해 사용자에게 5초 동안의 시간을 주어 음성 정보를 입력하도록 하였다. 입력된 정보에 대해서는 다시 앞에서 제시한 수식 등을 이용하여 *Cu* 값을 생성하고 이를 서버로 전송하도록 하였다.

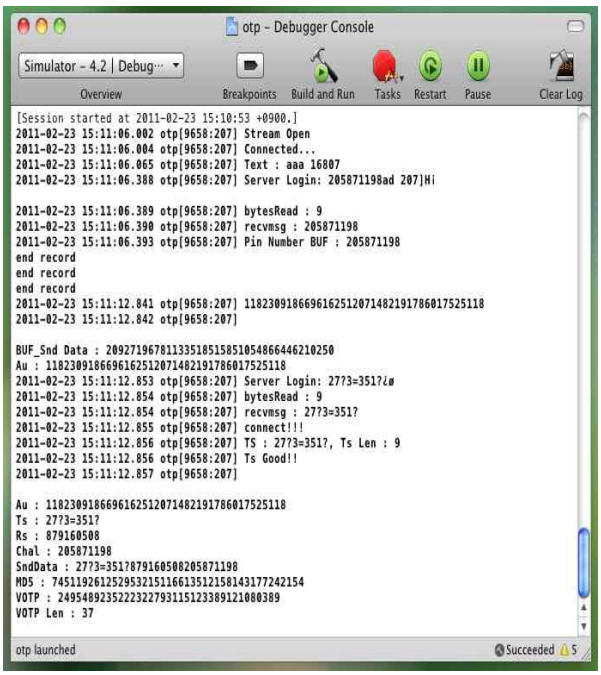
(그림 10) V-OTP 음성 정보 기반 인증 실행화면

4.2 V-OTP 실행 결과값 확인 및 검증

본 연구에서 구현한 V-OTP 방식에서 음성 정보를 이용하여 스마트폰 단말과 서버에서 각각 생성되는 결과값은 아래의 그림과 같다. 먼저 (그림 11)을 보면 스마트폰에서 사용자 ID 'aaa'에 대해 난수값(*Rc*) 16807이 생성되어 서버로 전송되었으며, 서버가 생성하여 전송한 *Chal* 값 '205871198'을 수신하게 된다. 이제 클라이언트는 사용자가 입력한 음성 정보를 버퍼에서 읽어 *Au, Cu* 값을 생성하게 되고 이를 서버에 전송하게 된다.

다시 클라이언트 모듈에서는 서버가 생성하여 보내온 일회용 토큰 *Ts* 값을 이용하여 *Rs* 값을 추출하게 되고 앞에서 검증 과정으로 동일한 *Chal* 값이 나오는 것을 확인하게 된다. 이제 최종적으로 음성 정보를 이용하여 클라이언트에서의 V-OTP 값을 생성하고 이를 서버에 전송하게 된다.

서버에서의 실행 후 결과값은 (그림 12)와 같다. 클라이언트로부터 사용자 ID 및 난수값을 수신하고 서버 역시 난수값 '879160508'을 생성한 것을 확인할 수 있다. 그리고 이



(그림 11) V-OTP 클라이언트 실행 후 결과

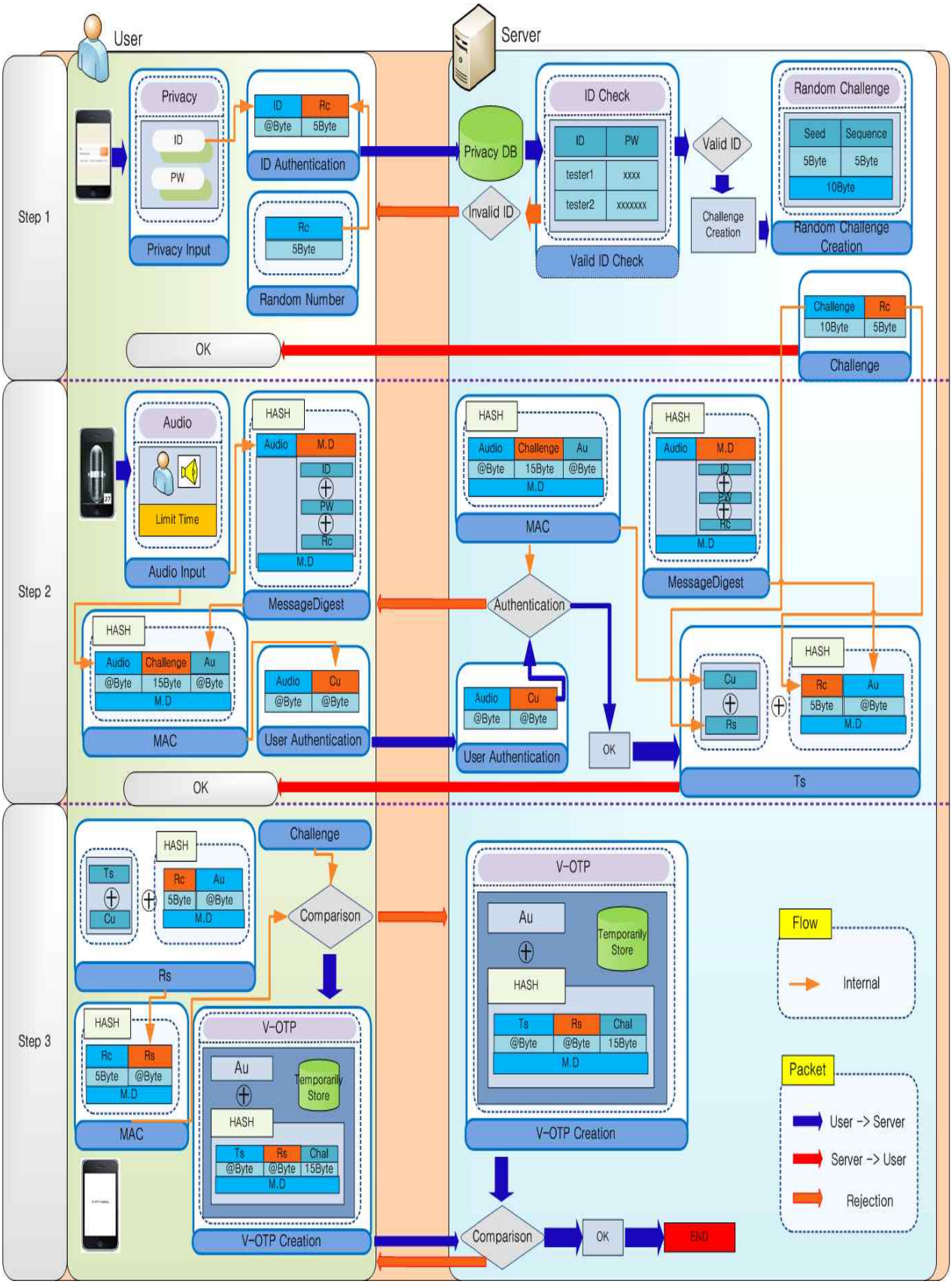
값을 이용하여 *Chal* 값에 해당하는 PIN 값 '205871198'을 생성하여 이를 클라이언트 단말로 전송하게 된다.

다시 서버는 클라이언트로부터 송신된 값 Cu에 대한 확인/검증 과정을 수행하고 *Ts*를 생성하여 이를 다시 스마트폰에 전송한다. 마지막으로 클라이언트로부터 수신된 V-OTP 값에 대한 확인/검증 과정을 수행하여 최종적으로 스마트폰 환경에서 사용자의 음성 정보를 이용한 일회용 패스워드 기반 인증 과정을 완료하게 된다.

```
10.0.18.50로 접속하셨습니다.
ID, Client Rand : aaa 16807
select id,pwd from user_info where id = 'aaa'
ID : aaa
Rand:16807
Pin Create.
Server Rand : 879160508
Pin :205871198
1. Info : 6QMpBCEENARaBI8E2gQIBQoF6gTCBLAEngR0BEAE+
ANYA48C8AFIAcEAlgBjAOv/bP85/2H/hv9b/yr/Df/R/r3+5v4k/37/0f8L
2. Info : 209271967811335185158510548664462102 50
Au : 118230918669616251207148219178601752511 8
Server Cu : 209271967811335185158510548664462102 50
Password :bbb
Server와 Client. Cu 값 비교중..
Cu 값이 일치합니다.
TS : 27?3=351?
TS Len : 9

Au : 118230918669616251207148219178601752511 8
Ts : 27?3=351?, Rs : 879160508 Challenge : 205871198
MD : 745119261252953215116613512158143177242154
Server VOTP : 249548923522232279311512338912108038 9
Client VOTP : 249548923522232279311512338912108038 9
Server VOTP Len : 37
Client VOTP Len : 37
VOTP Success!!
```

(그림 12) V-OTP 서버 실행 후 결과



(그림 13) V-OTP 전체 구조도

5. 안전성 및 성능 분석

5.1 안전성 분석

본 연구에서 제시한 스마트폰에서의 음성 정보를 이용한 일회용 패스워드(V-OTP) 메커니즘은 스마트폰내 마이크 장치를 이용하여 자신의 음성 정보를 캡춰하도록 하였다. 이후 자신의 *IDu*와 패스워드 *PWu* 및 인증 요청시 매번 다르게 선택되는 난수값 *Rc*를 이용하여 $Au=H((Ai \mid IDu \oplus PWu \oplus Rc))$를 생성하도록 하였다. *Au* 값에는 단순히 ID/PW 정보만 들어가는 것이 아니라 난수값 *Rc*를 포함하게 하였기 때문에 네트워크를 통해 전송되는 정보 *Au*는 해쉬함수의 일방향성에 따라서 원래의 패스워드 값을 알아내기는 어렵다. 또한 *Au*에서 사용하는 음성 정보 *Ai*는 사용자가 5초 동안 입력한 정보 중에서 일부 정보만을 사용하도록 하였기 때문에 사전공격(Dictionary attack)에 의한 패스워드 유출 가능성을 낮출 수 있도록 하였다. 따라서 전자금융 서비스에서 MITM (Man-In-The-Middle) 공격 등을 사용한다고 할지라도 클라이언트에 전송되는 *Au* 정보 내에 *Rc*가 포함되어 있기 때문에 재사용이 불가능한 형태라는 것을 알 수 있다.

또한 *Au* 값에는 클라이언트가 서버로 전송한 *Rc* 값에 대해 서버가 생성한 *Rs* 값을 이용하여 생성된 해쉬값을 Chal 값으로 다시 PIN 값을 수신하여 음성 정보를 생성한 것이므로 클라이언트에 대한 인증 확인 및 부인봉쇄 기능으로도 사용할 수 있는 방식이 된다.

일회용 패스워드 생성 과정의 보안성을 강화하기 위해 *Au* 값을 바로 서버로 전송하는 것 대신에 클라이언트는 서버로부터 수신한 *Chal* 값을 *Au* 및 음성 정보 *Ai*와 함께 해쉬값을 계산하여 축약된 형태로 전송하였기 때문에 서버에서는 메시지에 대한 무결성을 확인함과 동시에 전달된 메시지에 대한 검증 기능까지도 제공하게 하였다.

서버가 마치 클라이언트인 것처럼 위장하여 앞에서 제시한 2단계 및 3단계 과정에서 생성되는 정보를 서버가 자체적으로 생성한 후에 클라이언트 대신 인증 과정을 수행하는 경우도 생각할 수 있다. 하지만 이와 같은 경우 첫째로 서버는 클라이언트 대신에 *Chal* 값에 대한 음성 정보를 생성하는 과정을 수행해야 한다. 서버가 클라이언트인 것처럼 위장해서 5초 기간에 해당하는 음성 정보를 생성해야 한다. 이에 서버는 자신이 직접 음성 정보를 생성하는 공격을 수행할 수도 있도 또 다른 방법으로는 이전에 수행된 트랜젝션에서 클라이언트가 보내온 음성 정보 *Ai_old*를 사용할 수도 있다. 하지만 이 경우 서버가 자체 생성해야 하는 *Au*_*fake* 정보에 클라이언트 난수값 *Rc* 값 또한 변조/생성해야 한다. 또한 서버가 자체 인증과 V-OTP 생성을 위해 클라이언트로 전송하는 일회용 토큰 내에도 포함되는 자체 생성 위조값 *Cu*_*fake* 역시 *Chal* 값이 포함되어 있고 이 값 역시 $H(Rc \oplus Rs*)$ 형태로 클라이언트가 보내온 난수값을 포함하도록 되어 있다. 따라서 서버가 클라이언트를 위장해서 2단계 및 3단계 과정을 위장공격 할 가능성은 없다는 것을 확인할 수 있다.

음성 정보 기반 일회용 패스워드를 생성하는 4단계 및 5단계 과정에서 서버로부터 전송된 일회용 토큰 *Ts*를 사용하여 클라이언트는 *Rs** 값을 추출/계산하게 되고 다시 자신이 선택하였던 난수값 *Rc*와 해쉬과정을 수행하여 이를 2단계에서 서버로부터 수신한 *Chal* 값과 비교하는 과정을 수행하도록 하였다. 따라서 전체 트렌젝션이 서로 유기적인 관계를 갖도록 하였으며 클라이언트는 서버에 대한 인증 과정을 수행하고 다시 서버는 클라이언트에 대한 인증 과정을 수행하는 상호 인증(Mutual Authentication) 과정을 수행하도록 하였다

제안한 기법의 안전성을 분석하면 ID, Password, Voice 등 각 단계별 정보에 대하여 훼손이나 분실 등으로 인한 정보 손상 및 데이터 위변조, 재전송 공격, MITM 공격 등의 침해 사고 공격에 대해 상호인증 과정을 거치기 때문에 기존 기법에 비해 연산과정이 많이 쓰이는 것을 볼 수 있다. 또한 중간 과정의 일부가 노출되어도 그것을 통해 재사용하거나 다음 과정에 대한 예측이 불가능하기 때문에 서버나 클라이언트 등의 사칭 공격에 안전성을 보이는 것을 확인할 수 있다.

인증 과정에서 클라이언트-서버간 송수신되는 정보는 일방향 해쉬 함수와 XOR 함수 및 암호학적으로 안전한 길이의 난수값 만을 이용하도록 하였다. 이는 스마트폰에서의 계산 성능을 고려하고 최소한의 리소스를 사용하면서도 사용자에 대한 인증 기능을 강화하기 위한 방법으로 제안한 것이다. 스마트폰 기반 전자금융 서비스에서 사용자 인증을 위해 현재 사용되고 있는 OTP 방식에서 보안성을 강화하기 위해 각 개인이 마이크 장치를 통해 서버로부터 전송된 PIN 값에 대해 음성 정보로 입력한 후에 상호 인증 및 검증 과정을 통해 최종적으로 V-OTP 정보를 이용하여 스마트폰 사용자에 대한 인증 과정을 수행하게 되어 네트워크를 통해 사용자의 패스워드 정보에 대한 노출 없이 인증 과정을 수행할 수 있다.

5.2 성능 분석

아래 <표 1>과 같이 본 연구에서 제시한 기법과 기존 기법에서의 보안 및 인증 성능에 대해 비교 분석하였다. 단계별 일방향 해쉬함수에 대한 사용 회수 *Th*를 기준으로 본 연구에서 제안한 메커니즘에 대한 성능을 평가하기 위해 기존 연구와 계산량을 비교 분석하였다.

본 연구에서 제시한 기법은 인증 단계에서 타 기법에 비해 많은 계산량을 가지고 있는 것을 확인할 수 있다. 이는 많은 인증 기법을 통해 더욱 깊이가 있는 절차과정을 거치고 있으며 이로 인해 OTP의 주요 취약점에 대응할 수 있도록 설계되었기 때문이다. 또한 스마트폰이라는 휴대성 있는 단말기의 특징을 활용하여 음성정보를 통해 OTP 값을 생성하기 때문에 다른 바이오 정보에 비해 그 특징이

〈표 1〉 인증 계산량 및 기능 비교 분석

구분	제안 기법	Jang-Lee [6]	Wang-Li [8]	Yoon-Yoo [9]	Khan et al [10]
등록단계	*2Th*	3*Th*	3*Th*	3*Th*	2*Th*
로그인	*3Th*	2*Th*	2*Th*	3*Th*	2*Th*
인증단계	*6Th*	4*Th*	5*Th*	4*Th*	2*Th*
상호인증	O	O	O	O	O
서버 시간정보	X	O	X	X	O
시간 동기화	X	X	X	O	O
B-OTP 생성	X	O	X	X	X
V-OTP 생성	O	X	X	X	X
바이오 정보	음성	얼굴	지문	지문	지문

부곽되는 것을 확인할 수 있다. 특히 지문의 경우 현재 아이폰 패드의 기술력으로 지문 인식이 불가능 한 것으로 알고 있다. 그렇기 때문에 스마트폰에서의 지문 인식 경우 지문의 너비, 면적 정보 등을 이용하여 수치해석을 통해 인식 여부를 결정하는 형태로 되어 있으며 정식으로 지문 인식 기능을 행할 시 관련 장비가 필요하기 때문에 사용에 있어서 매우 제한적일 수밖에 없다. 또한 얼굴 인식의 경우 주위의 시간과 공간의 제약에 따라 어둡거나 화려한 곳에선 잘 인식이 안될 수 있다. 따라서 본 기능을 통해 OTP 기능을 적용하였을 경우 시간과 공간의 제약을 받거나 기기에 있어 제한적이지 않다는 장점이 있다.

따라서 본 연구에서 사용한 기법인 경우 OTP 사용자의 편의성 및 스마트폰 이용 환경을 고려한 메커니즘이라고 할 수 있다. 물론 본 연구에서 제시한 기법은 기존의 기법과 마찬가지로 지문 정보에도 적용 가능하다.

6. 결 론

스마트폰을 통해 전자금융이나 인터넷 서비스 등에 이용할 경우에 보다 강화된 사용자 인증 기능이 필요하다. 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 마이크 장치를 이용하여 서버로부터 전송된 PIN 값에 대해 사용자가 자신의 음성 정보를 전송하도록 하였으며 서버에서는 검증 과정을 수행한 후에 난수값 및 음성정보 등을 이용하여 일회용 토큰을 생성하도록 하였고 보안성 및 성능을 향상시킬 수 있었다. 그리고 클라이언트에서 생성된 음성 정보 기반 OTP 값을 이용하여 전자금융 서비스에서의 사용자 인증을 강화할 수 있는 방안을 제시하였다. 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.

참 고 문 헌

[1] Voice Authentication: Making Access a Figure of Speech, http://www.computerworld.com/s/article/86897/Making_access_a_figure_of_speech.

[2] "Voice verification - for mobile banking security?", http://www.finextra.com/community/fullblog.aspx?id=3949

[3] Voice PIN 2.0, http://www.voiceverified.com/products.htm

[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, Vol.17, No.3, pp26~13, 2007.

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

[7] Agnitio, "One-Time Password (OTP) Management Secured with Voice Biometrics", Voice Biometrics White Paper, 2009.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

조 식 완

e-mail : whtlrdhks3355@hanmail.net
2010년 한신대학교 소프트웨어공학과 (공학사)
2010년~현 재 한신대학교 컴퓨터공학부 석사과정
관심분야 : 정보보호, 포렌식, 네트워크 보안, 모바일 보안

이 형 우

e-mail : hwlee@hs.ac.kr
1994년 고려대학교 전산과학과(이학사)
1996년 고려대학교 전산과학과(이학석사)
1999년 고려대학교 전산과학과(이학박사)
2003년~현 재 한신대학교 컴퓨터공학부 부교수
관심분야 : 정보보호, 포렌식, 네트워크 보안, 모바일 보안