情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

음향 주파수 분석을 이용한 스마트폰 사용자 인증*

김 진 복† , 송 정 은, 이 문 규‡
인하대학교 컴퓨터정보공학부

Authentication of a smart phone user using audio frequency analysis*

Jin-Bok Kim† , Jeong Eun Song, Mun-Kyu Lee‡
School of Computer and Information Engineering, Inha University

요 약

본 논문에서는 스마트폰에 내장되어있는 다양한 장치들 중 가장 기본적인 장치인 마이크와 스피커를 이용한 사용자 인증 방법을 제안한다. 제안 방법은 음향 채널을 통해 챌린지를 전달함으로 인해 인증 대상이 사용 대상 장치로부터 근거리에 위치함을 보장할 수 있다. 본 논문에서 제안하는 인증 방법은 두 가지로, 스마트폰을 일종의 하드웨어 토큰으로 활용하여 고정시스템 또는 웹사이트 등에 로그인하는 방법과 스마트폰을 사용하고자 하는 사용자가 스마트폰에 로그인하기 위해 가까운 고정 PC를 토큰으로 활용하는 방법이다. 특히 제안 방식은 일반적으로 사용하는 마이크와 스피커를 이용함으로써 추가적인 장치가 필요 없으며 간단한 조작만으로 인증을 수행 할 수 있어 노약자나 장애인 등이 쉽게 사용할 수 있다.

ABSTRACT

In this paper, we propose user authentication methods using a microphone and a speaker in smart phones. The proposed methods guarantee that the user is located close to the target device by transmitting the challenge via an audio channel. We propose two authentication methods; user authentication for a PC or a website using a smart phone as a hardware token, and user authentication to log on to a smart phone using a PC as a token. Because our methods use typical peripheral devices such as a microphone and a speaker, they do not require any special-purpose hardware equipment. In addition, the elderly and the handicapped can easily use our methods because the methods are activated by simple operations.

Keywords: user authentication, audio frequency analysis, smart phone

I. 서 론

최근 스마트폰의 보급이 빠르게 확대됨에 따라 스마트폰 가입자는 천만 명을 넘어 섰으며[1], 이러한 스마트폰 보급의 빠른 확산은 여러 가지 새로운 서비스들을 가능하게 하고 있다. 스마트폰은 인터넷 상에서 인간관계를 형성하는 SNS(Social Networking Service)를 활성화 시키고 있으며[2], 개인이 인터넷 상에 각종 콘텐츠를 저장하고 언제 어디서나 컴퓨터, 노트북, 스마트폰 등을 이용하여 접속하여 사용할 수 있는 개인형 클라우드 서비스(Cloud service) 기술 발전을 가속화 시키고 있다[3]. SNS나 클라우드 서비스 등과 같이 개인의 데이터를 언제 어디서든 자유롭게 접근할 수 있는 서비스가 증가함에 따라 개인정보보호 문제도 해결해야할 큰 과제로 남게 되었다. 사

접수일(2011년 7월 27일), 수정일(2011년 10월 10일), 게재확정일(2011년 12월 15일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [K1001824, 장애인 및 고령자를 위한 Digital Guardian 기술개발]
† 주저자, maljb85@hotmail.com
‡ 교신저자, mklee@inha.ac.kr

용자의 개인 데이터를 안전하게 유지하기 위해서는 데이터에 접근할 수 있는 권한을 제한하는 절차가 필요하며 이를 위해 올바른 접근 권한을 갖는 사용자인지를 확인하는 것이 중요하다. 따라서 본 논문에서는 스마트폰 이용자의 데이터 보호를 위해 두 가지의 사용자 인증 프로토콜들을 제안한다.

본 논문에서 제안하는 인증 방법 중 첫 번째는 스마트폰을 일종의 하드웨어 토큰으로 활용하여 고정시스템 또는 웹사이트 등에 로그인하는 방법이다. 일반적으로 사용자 인증 방식은 PIN(Personal Identification Number)이나 패스워드를 입력하는 지식 기반 방식, 사용자가 소유하고 있는 장치를 이용하는 토큰 기반 방식과 사용자의 지문이나 행동패턴 등을 이용하는 생체정보 기반 방식으로 분류할 수 있다. 지식기반으로 인증하는 방법의 경우 PIN이나 패스워드 등을 기억해야하는 번거로움이 있고, 생체정보 기반으로 인증하는 방법의 경우 생체정보 이용에 대한 사용자 거부감과 생체정보가 유출될 경우 복원할 수 없다는 단점이 있다. 토큰 기반 인증은 이러한 문제점들을 해결할 수 있는 반면 인터넷 뱅킹을 위한 OTP(One-Time Password)의 예와 같이 인증을 위해 별도의 토큰을 항상 지니고 있어야 한다는 단점이 있다. 별도의 토큰을 지니고 있어야 한다는 단점을 보완하기 위해 휴대 전화나 스마트 폰을 토큰으로 활용하는 연구가 활발하게 진행되고 있다. 인터넷 뱅킹을 위한 OTP를 휴대 전화나 PDA등 모바일 기기에 탑재하거나[3], 스마트폰을 이용하여 2-D 바코드를 촬영함으로 시스템에 로그인 할 수 있는 인증 방법이 개발되었다[4]. 따라서 본 논문에서는 사용자가 항상 지니고 있는 스마트폰을 하드웨어 토큰으로 활용함으로써 불편함을 최소화한 사용자 인증 방식을 제안한다.

특히 본 논문에서 챌린지 전달을 위해 이용하는 채널은 음향 채널로, 스마트폰의 마이크와 사용 대상 시스템의 스피커를 이용하므로 특별한 추가 하드웨어를 필요로 하지 않는다. 반면에 기존의 방식들은 신호의 전달을 위해 인증 대상 시스템이 무선랜, 블루투스(Bluetooth), RF(Radio Frequency) 등의 전파 송수신 장치를 탑재함을 가정하는 경우가 많은데[6, 7, 8], 일반적으로 노트북 이외의 고정 시스템은 무선 송수신 장치가 기본적으로 장착되어 있지 않으므로 본 제안 방식에 비해 활용도가 떨어진다. 기존 연구 중 초음파 송수신 장치를 이용하는 방식[9]도 토큰 및 사용 대상 시스템에 모두 초음파 송수신 장치를 필요로 하므로 같은 문제점을 가지고 있다. 또한, 스마트폰을 이용하여 2-D 바코드를 촬영하여 인증을 수행하는 방법[4]의 경우 사용자가 2-D 바코드를 촬영하는 동작을 수행해야 되는 번거로움이 있을 수 있으나, 본 논문에서 제안하는 인증 방법을 이용하면 사용자의 조작을 최소화하면서 인증을 수행할 수 있기 때문에 스마트폰의 정밀한 조작을 하기 어려운 고령자나 장애인들 또한 편리하게 사용할 수 있다.

본 논문에서 제안하는 두 번째 인증 프로토콜은 스마트폰을 사용하고자 하는 사용자가 스마트폰에 로그인하기 위해 가까운 고정 PC를 토큰으로 활용하는 방법이다. 이는 특정 PC가 근거리에 있을 때만 스마트폰의 사용을 허용하는 방법으로, 스마트폰의 사용 중 반복적인 비밀번호 입력 실패 등으로 스마트폰이 잠겼을(Screen lock) 때 이를 푸는 방안으로 이용할 수 있다. 앞의 첫 번째 인증 방법과 마찬가지로 음향 채널을 이용하되 챌린지 및 응답의 방향이 반대가 되므로, 두 번째 프로토콜은 고정 PC가 마이크를 탑재하고 있는 경우에 이용 가능하다.

인증을 위해 음향 채널을 이용하는 방법은 이미 [10]에서 제안된 바 있으나, 이는 기기 간의 인증을 위해 음향 신호를 전달하고 사용자가 이 음향을 직접 확인함으로써 인증하는 방식으로, 사용자의 개입이 필요 없는 본 제안 방식과는 차이가 있다. 특히 제안 방식은 가청 주파수 중 상대적으로 사람이 듣기 어렵고 소음에 의한 간섭이 적은 15,800~20,000Hz 대역을 이용함으로써 사용자의 불편함을 최소화하는 동시에 신호 전달 효율을 최대화하였다. 한편 최근에 발표된 음향 발생 토큰 기반의 스마트폰 인증 방법[11]은 음향 발생 장치를 포함하는 별도의 하드웨어 토큰이 필요하고 챌린지-응답 기반이 아닌 같은 음향의 반복 전송 방식으로 재사용 공격(Replay attack)이 가능한 점 등 안전성 측면에서 한계를 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 인증 프로토콜에서 이용하는 음향 신호와 해당 신호의 전달 방법에 대해 설명한다. 3장에서는 시스템 사용을 위해 스마트폰을 토큰으로 활용하는 사용자 인증 방법에 대해서 설명하고 4장에서는 스마트폰 단말기 사용을 위한 사용자 인증 방법을 설명한다. 5장에서는 제안한 프로토콜을 구현하고 실험한 내용을 기술하고 마지막으로 6장에서는 결론을 맺으며 향후 연구 방향을 제시한다.

II. 음향 신호의 전달

본 논문에서 제안하는 인증 방식들은 음향 신호를 통해 챌린지를 전달하고 별도의 유·무선 채널을 통해 응답을 수신하는 형태로 구성된다. 음향을 통해 전달하는 챌린지의 경우 특정한 주파수 조합의 비프(Beep)를 이용하며 마이크를 통해 해당 비프를 수신하는 기기에서 이를 스펙트럼 방식을 통해 분석하여 인식하도록 하였다. 스펙트럼 방식은 마이크를 통해 입력된 음향 신호를 FFT(Fast Fourier Transform) 알고리즘을 통해 해당 음향 신호에 사용된 주파수의 신호강도 형태로 변환하여 분석하는 방식이다. 이때 사용한 신호 강도의 단위는 dBFS(Decibels relative to full scale)이며 디지털 출력의 모든 비트가 1이 되도록 하는 아날로그 입력 레벨을 0dBFS로 나타낸다.

본 논문에서 제안하는 인증방법은 두 종류로, 첫 번째는 PC나 키오스크(KIOSK)와 같은 고정 시스템을 사용하거나 웹서비스를 이용하기 위해 웹브라우저 상에서 사용자 인증을 수행할 때 사용자가 지닌 스마트폰을 일종의 하드웨어 토큰으로 사용하는 방법이며, 두 번째는 스마트폰의 인증을 위해 사전에 지정한 시스템(예를 들면 회사나 집의 특정 PC)을 활용하는 방법이다. 전자의 경우는 고정 시스템에서 일반적으로 많이 사용하는 스피커를 이용하여 사용자가 지닌 스마트폰으로 음향 챌린지를 전달하므로 추가 하드웨어가 필요하지 않다. 후자의 경우에는 스마트폰에서 지정된 PC로 챌린지를 전달하게 되므로 지정된 PC에 마이크가 제공되는 상황에 적합하다.

본 논문에서 챌린지를 전달하기 위하여 사용하는 비프는 표 1과 같이 구성하였다. 일반적으로 음성 통화에 사용되는 스마트폰의 마이크와 스피커는 사람이 들을 수 있는 가청 주파수(20~20,000Hz)에 최적화되어 있으므로 음향의 전달을 위해서는 이 영역을 활용하는 것이 바람직하다. 다만 사람이 쉽게 들을 수 있는 소리를 이용할 경우 사용자의 불편을 초래할 수 있으므로 가청 주파수 영역 중에서도 듣기 어려운 소리에 속하는 15,800~20,000Hz 영역을 사용하였다. 이러한 주파수 대역을 챌린지로 사용했을 때 인체에 주는 영향은 크지 않을 것으로 판단되며[12], 상대적으로 잡음에 의한 간섭도 적다고 볼 수 있다. 다만 기기마다 인식하는 주파수 영역에 약간의 차이가 있을 수 있으므로, 음향 챌린지 대상 주파수의 선정은 가능한 많은 기기에서 공통적으로 사용하는 영역을 이용하는 것이 바람직하다. 본 논문에서는 5장에서 설명하는 바와 같이 현재 많이 이용되고 있는 5개 스마트폰을 대상으로 주파수 영역을 확인하였으며, 이들 단말기에서는 위에서 제시한 15,800~20,000Hz 영역이 문제없이 동작함을 확인하였다.

동일 시간의 음향 발생으로 많은 데이터를 전달하기 위해서는 해당 주파수 영역을 세분화하여 여러 음향 신호들을 동시에 송신하여야 하나, 음향 신호의 특성상 주파수간 상호 간섭에 의한 잡음인 상호변조잡음(Intermodulation noise)과 원하는 주파수 근방에서 나타나는 불필요한 에너지원에 의한 잡음인 위상잡음(Phase noise) 등으로 인해 동시에 송신될 수 있는 신호의 수에는 한계가 있다. 본 논문의 실험에 의하면 간섭을 최소화하여 데이터 전달이 가능한 주파수 간격은 약 600Hz이며, 2채널 방식(스테레오 방식)을 이용해 1채널당 하나의 주파수를 발생시킬 경우 위 대역에서 동시에 4 비트의 신호를 전달할 수 있다. 가령 두 채널 중 하나의 채널에 15,800Hz, 나머지 한 채널에서 17,000Hz에 해당하는 음향이 감지될 경우 이를 0x0로 인식하게 된다.

본 논문에서 제안하는 프로토콜에서 하나의 음향 챌린지는 2바이트의 길이를 가지며, 4비트로 구성된 비프를 4번 발생시켜 전달한다. 또한, 신호간의 구분을 위하여 1초의 간격을 두고 발생시키며 신호는 1초

〔표 1〕 비트별 할당 주파수

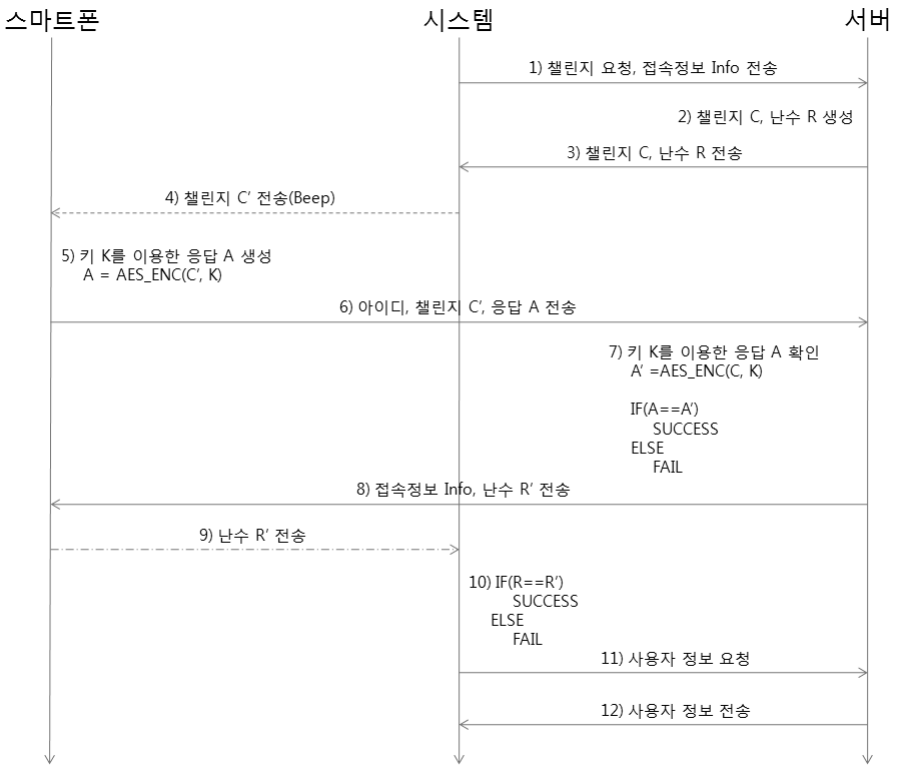
Bit	주파수(Hz)
0x0	15800, 17000
0x1	16400, 17600
0x2	17000, 18200
0x3	17600, 18800
0x4	18200, 19400
0x5	18800, 20000
0x6	15800, 17600
0x7	16400, 18200
0x8	17000, 18800
0x9	17600, 19400
0xa	18200, 20000
0xb	15800, 18200
0xc	16400, 18800
0xd	17000, 19400
0xe	17600, 20000
0xf	15800, 18800

간 지속되도록 하여 하나의 챌린지 전달에 약 8초가 소요된다.

III. 시스템 사용을 위한 사용자 인증

이 장에서는 특정 시스템에 로그인하기 위해 스마트폰을 토큰으로 활용하는 인증 방법을 설명한다. 이 인증 방법은 인증 대상 시스템이 사용자의 고정 PC인 경우 이외에도 키오스크나 웹브라우저와 같이 고정 시스템을 경유 장치로 활용하는 경우에도 적용할 수 있다. 예를 들어 온라인상에서 예매한 승차권을 현장에서 키오스크를 통해 발매 받는 경우 스마트폰은 원격 서버에서 키오스크를 경유하여 제공되는 챌린지 정보에 응답하여 키오스크에 로그인하게 되며, 또한 PC에서 웹브라우저를 통해 웹서비스에 로그인을 할 경우 스마트폰은 웹서버에서 제공하는 챌린지에 응답하여 웹사이트에 로그인할 수 있다. 따라서 본 프로토콜의 참여주체는 스마트폰, 사용 대상 시스템, 인증 서버(웹서버)로 구성되며, 스마트폰과 인증 서버는 사전에 신뢰 관계가 성립되어 16바이트 길이의 키 K를 공유한다고 가정한다. 이러한 설정은 사용자가 고정 PC에 로그인하는 경우에도 유동 IP 주소 등의 문제로 응답 전송을 위한 목적지 정보를 정할 수 없을 때 유용하게 사용될 수 있으며, 고정 PC가 고정 IP를 보유할 경우에는 인증 서버가 고정 PC와 같은 기기가 되도록 구성하는 것도 가능하다.

제안 프로토콜에서 챌린지 정보는 인증 서버로부터 생성되어 사용 대상 시스템을 경유한 후 다시 음향 채널을 통해 스마트폰에 전달되며, 응답은 스마트폰의 3G IP 망을 통해 직접 인증 서버로 전달된다. 응답의 전송 전까지 사용 대상 시스템이나 서버는 사용자의 신원 정보를 알 수 없으며, 신원 정보는 응답과 함께 서버로 전달되도록 하였다. 그림 1은 이러한 사용자 인증 프로토콜을 구체적으로 나타낸 그림이다. 실선은 HTTP(Hypertext Transfer Protocol)를 기반으로 한 유·무선통신을, 점선은 음향 채널을 나타낸다. 또한, 긴 파선-점선은 소켓통신을 나타낸다. 인증절차는 먼저 시스템이 해당 시스템의 접속정보로 소켓통신에 사용할 랜덤한 포트를 설정하여 챌린지 요청과 함께 서버로 전송한다. 서버는 2바이트의 챌린지 C와



〔그림 1〕 시스템 사용을 위한 사용자 인증 프로토콜

16바이트 길이의 난수 R 쌍을 생성하여 서버 내에 저장한 후 시스템에 전송하며 챌린지를 전달받은 시스템은 스피커를 통해 챌린지에 해당되는 비프를 발생시킨다. 스마트폰은 내장된 마이크로 챌린지를 전달 받은 후 서버와 사전에 교환한 키 K를 이용하여 응답 A를 생성한다. 이때 응답 A는 사전에 교환한 키 K를 이용하여 음향을 통해 전달받은 챌린지 C'을 암호화하여 생성한다. 다음으로 스마트폰에서 미리 지정된 사용자의 아이디와 음향을 통해 전달받은 챌린지 C' 그리고 앞서 생성한 응답 A를 전송한다. 서버에서는 함께 전송된 아이디에 해당하는 사용자의 키 K를 이용하여 응답 A를 검증한 후에 동일하면 챌린지 C'에 연관된 난수 R'과 시스템 접속정보(IP, 포트 등)를 스마트폰으로 전송한다. 서버에 정상적인 응답이 도달하였다는 것은 음성으로 전달되는 챌린지를 스마트폰이 정상적으로 수신하였음을 의미하므로 스마트폰을 지닌 사용자의 위치가 시스템과 근접한 거리에 있음을 보장할 수 있으며, 또한 서버와 사용자만 지닌 키 K를 이용하기 때문에 등록된 사용자인 사실도 확인할 수 있다. 다음으로 스마트폰은 서버로부터 받은 접속정보를 이용하여 시스템에 접근 후 소켓통신을 통해 난수 R'을 전송한다. 난수 R'을 전송받은 시스템은 서버로부터 받은 난수 R과 사용자의 스마트폰으로부터 받은 난수 R'을 비교하여 세션 정보를 확인하고 해당 사용자의 신원 정보를 서버로부터 제공받아 인증을 완료한다.

본 논문에서 제안하는 방식은 일정시간 내에 음향을 이용한 챌린지가 모두 전달되지 않거나, 주어진 챌린지에 대한 응답이 잘못된 경우 인증에 실패하게 된다. 악의적인 공격자 이외에 정상적인 사용자의 경우에도 주변 환경에 따른 챌린지 전달 및 무선 통신 문제 등으로 인증에 실패할 수 있으므로, 사용자는 일정 회수 챌린지를 재요청하여 인증을 다시 수행할 수 있도록 구성하였다.

제안 프로토콜은 스마트폰에서 시스템에 접속하기 위한 인증 과정 중 서버로부터 시스템의 접속정보를 전달받는 과정에서 공격자가 통신로 상에서 데이터를 몰래 획득하는 엿듣기(Sniffing) 공격을 시도할 경우 HTTP 통신만으로는 접속정보가 유출될 수 있다. 그러나 이 부분은 SSL/TLS 기반의 HTTPS(Secure Hypertext Transfer Protocol)로 간단하게 전환할 수 있으므로 위 프로토콜의 HTTP 구간은 안전하다고 보아도 무방하다. 또한 공격자가 과거 인증 세션에서 교환했던 챌린지나 응답을 기록하였다가 이후 세션에 재사용하는 재사용 공격을 고려해 볼 수 있는데, 기본적으로 16비트 챌린지를 이용하고 있으므로 $\frac{1}{2^{16}}$ 확률로 공격에 성공할 수 있다. 이러한 위험 요소는 응답 생성에 있어 타임스탬프(Timestamp)를 포함하거나 스마트폰과 서버 사이에 카운터(Counter) 등 상태 정보를 추가적으로 공유하여 응답 생성 시 포함하도록 함으로써 위협을 감소시킬 수 있다. 보다 근본적으로는 챌린지의 비트 수를 늘리는 방안을 고려해 볼 수 있으나, 이는 음향 신호 전달을 위해 더 긴 시간이 필요함을 의미하므로 사용자의 불편을 초래할 수 있다.

IV. 스마트폰 단말기 사용을 위한 사용자 인증

이 장에서는 스마트폰 단말기 사용을 위한 사용자 인증방법에 대해 설명한다. 현재 일반적으로 사용하는 안드로이드 OS나 iOS의 경우 패스워드 기반의 인증이 일정횟수 이상 실패하였을 경우에도 같은 인증강도를 지닌 인증방식을 사용하는데, 이는 단말기를 분실하였을 경우 추측공격(Guessing attack)이나 무작위 대입공격(Brute-force attack)에 대해 대응하지 못한다. 제안한 방식은 단말기의 사용을 지정된 특정 PC와 근거리에 있을 때만 허용하는 변형된 토큰 기반 사용자 인증 방식으로, 일반적으로 사용하는 PIN입력방식이나 패턴입력방식보다 높은 인증강도를 지닌다고 볼 수 있다. 따라서 평소에는 비교적 간단한 기존 인증방식을 사용하되 일정횟수 이상 실패하거나 이상행위가 감지될 시 스마트폰을 잠그고(Screen lock) 제안한 방식을 사용하여 특정 위치에서만 잠금을 풀 수 있도록 하면 기존 방식들에 비해 안전성을 높일 수 있다.

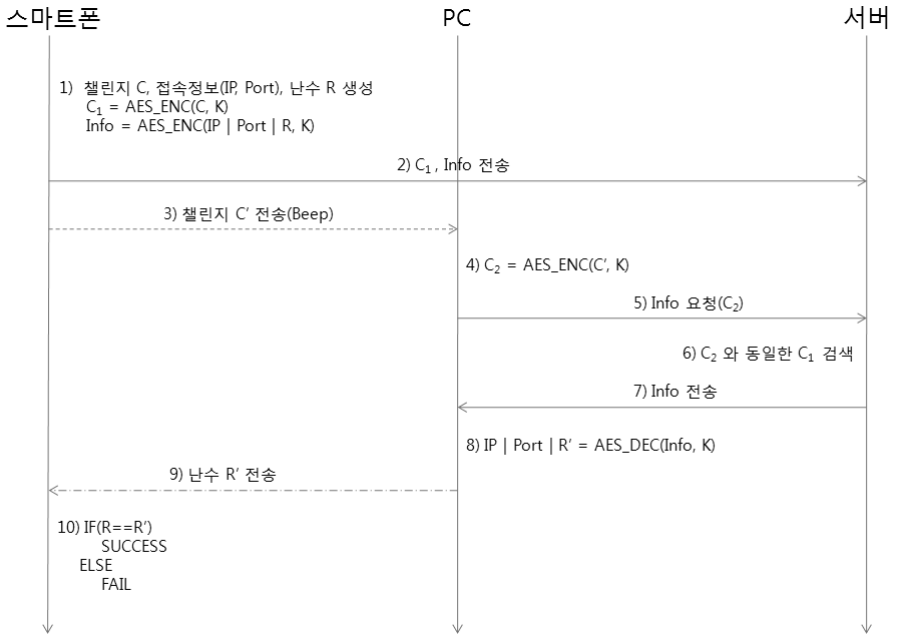
그러나 본 제안 방식이 부주의하게 구현될 경우 오히려 보안성을 약화시킬 수도 있음을 고려하여야 하는데, 예를 들어 사용자가 지정 PC 근처에서 다른 용무를 수행하는 동안에 타인이 해당 사용자의 스마트폰을 이용하여 스마트폰에 대한 무단 인증을 수행하는 경우를 생각해볼 수 있다. 이러한 문제점은 PC를 이용하여 스마트폰의 잠금을 풀기 전 지정된 PC에 패스워드를 입력하는 등의 방법을 추가적으로 사용함으로써 해결할 수 있다.

위에서 언급한 방식은 3장에서 제안한 프로토콜에서 음향을 이용한 챌린지 전송의 방향을 시스템에서 스마트폰이 아니라 스마트폰에서 시스템(PC)으로 변경하여 쉽게 구현할 수 있으며, 음향을 이용하여 챌린

지를 전달하기 때문에 스마트폰이 지정된 PC와 근거리에 있음을 보장할 수 있다. 또한 3장에서와 같이 유동 IP 등의 문제를 고려하여 제 3의 서버가 필요하나, 인증에 사용할 키 K는 3장과 달리 지정된 PC와 스마트폰만 사전에 교환하여 저장한다. 이는 3장에서 제안한 방식의 경우 어떠한 사용자가 시스템을 사용할 지 알 수 없지만 본 방식은 사용자가 직접 지정한 PC를 통해 인증을 수행함으로 PC가 정상 사용자로 판단해야 할 사용자를 한명으로 제한 할 수 있기 때문이다.

그림 2는 단말기 사용을 위한 사용자 인증 프로토콜이다. 그림 1과 동일하게 실선의 경우 HTTP를 기반으로 한 유·무선통신이며 점선의 경우 음향을 이용한 챌린지 전달을 나타낸다. 또한, 긴 파선-점선의 경우 소켓통신을 나타낸 것이다. 인증절차는 먼저 스마트폰에서 2바이트 크기의 챌린지 C를 생성하고 지정된 PC와 사전에 교환한 키 K를 이용해 암호화하여 C_1을 생성한다. 또한, 난수 R과 소켓통신에 사용할 스마트폰의 접속정보를 키 K를 이용하여 암호화한다. 앞서 암호화하여 생성한 C_1과 접속정보의 쌍을 서버에 전송하고 챌린지 C를 음향을 통해 지정된 PC로 전송한다. 이때 스마트폰에서 생성한 접속정보 및 난수 R을 스마트폰과 PC만 가지는 키 K를 통해 암호화하여 서버로 전송하였기 때문에 만약 서버의 정보가 공격자로부터 탈취 당했을 경우에도 정보의 유출을 최소화 할 수 있다. PC는 음향을 통해 전달받은 챌린지 C'을 키 K를 이용해 암호화하여 C_2를 생성한다. PC는 접속정보를 요청하기 위해 앞서 생성한 C_2를 서버로 전달하며, 만약 스마트폰으로부터 전달받은 챌린지 C'과 사전에 공유된 키 K가 동일하다면 C_1과 C_2는 정확히 같은 값이기 때문에 PC는 서버로부터 C_1과 쌍으로 저장되어있는 접속정보를 받을 수 있다. 전달받은 암호화된 접속정보는 키 K를 통해 복호화 할 수 있으며 복호화 된 내용 중 난수를 스마트폰으로 전송한다. 스마트폰은 앞서 생성한 난수 R과 PC로부터 전송받은 난수 R'을 세션 정보로 비교하여 같다면 인증을 완료한다.

제안한 단말기 사용을 위한 사용자 인증 프로토콜은 접속정보가 사전에 스마트폰과 서버 사이에 교환된 키로 암호화 되어 전송되기 때문에 사용자가 단말기를 사용하기 위해 서버와 통신하는 과정이나 PC와 서버가 통신하는 과정에서 공격자가 엿듣기 공격을 시도할 경우에도 접속정보를 취득할 수 없게 된다. 또한 3장에서 설명했던 시스템 사용을 위한 인증 프로토콜과 마찬가지로 재사용 공격을 시도할 경우 공격에 성공할 수 있으나 타임스탬프나 카운터를 이용하여 공격을 무력화 시킬 수 있다. 또한 이 프로토콜이 사용되는 상



〔그림 2〕 단말기 사용을 위한 사용자 인증 프로토콜

황을 고려할 때, 재사용 공격이 시도되기 위해서는 공격자가 사용자의 고정 PC 근처에서 세션 정보를 획득하여야 하는데 이러한 세션 정보 획득이 성공할 가능성은 희박하다고 볼 수 있다. 또한 만약 공격자가 서버 DB의 직접 공격을 통해서 사용자 정보를 얻으려고 시도할 경우라 해도 본 프로토콜에서는 서버가 스마트폰과 PC 사이에서의 통신의 중계역할만 하기 때문에 직접적으로 어떠한 정보도 얻을 수 없게 된다.

제안한 방식의 경우 PC가 신뢰할 수 있는 장치이거나 신뢰할 수 있는 장소에 있다는 것을 전제로 한다. 따라서 스마트폰에서 전달하는 음향 챌린지가 제대로 전달되지 않는 경우 재전송을 통해, 즉 프로토콜 상의 3번 항목을 재수행하여 사용자의 편의성을 높일 수 있다. 다만, 재전송이 가능한 시간이나 횟수를 제한하여 무작위 대입공격에 대한 내성을 가질 수 있다.

V. 실험

이 장에서는 본 논문에서 제안한 두 가지 인증방법에 대한 실제 구현내용에 대해 기술한다. 실험에 사용한 스마트폰 단말기는 안드로이드 2.2가 탑재된 LG 전자의 Optimus Q(LU-2300)와 HTC의 Desire (A8181), 안드로이드 2.3이 탑재된 LG 전자의 Optimus 3D(LU-SU760), 삼성전자의 Galaxy S (SHW-M110S), 삼성전자의 Galaxy S2(SHW-M250S)이며, 모두 제안 프로토콜들이 정상적으로 동작함을 확인하였으나, 본 절에서는 Galaxy S2 상에서의 구현 내용을 중심으로 설명한다.

실험에 사용한 시스템(PC)에는 주파수 응답이 60Hz~20,000Hz인 2채널을 지원하는 스피커와 스탠드 형태의 마이크를 장착하였다. 또한, 서버에는 Ubuntu 10.04에 APM(Apache + PHP + Mysql)을 구축하여 HTTP를 이용하여 단말기 및 시스템과 통신 할 수 있도록 구현하였다. 스마트폰의 마이크나 시스템에 장착된 마이크를 통해 입력되는 음향신호를 스펙트럼 방식으로 분석하기 위하여 사용하는 FFT 알고리즘은 다양한 버전이 존재하며 본 연구에서는 Cooley-Tukey FFT 알고리즘[13]을 사용하였다.

〔그림 3〕 시스템 사용을 위한 사용자 인증 중 스마트폰 실행화면

또한, 스피커를 통해 발생하는 비프의 경우 표 1의 구성으로 비트 전송률이 1411kbps인 기본적인 PCM 코덱의 Wave 파일로 사전에 저장하였다. 이를 통해 상대적으로 제한적인 성능을 지닌 스마트폰에서도 큰 부하 없이 챌린지를 생성할 수 있다.

시스템을 사용하기 위한 사용자 인증방법에서는 스마트폰에 내장된 마이크에 입력 가능한 음량이 최대일 때를 0dB라고 할 때 챌린지에 사용하는 주파수와 주변 주파수의 음량의 차이가 12dB이 되면, 즉 챌린지의 음량이 주변 주파수의 음량에 비해 4배가 되면 챌린지를 감지 할 수 있도록 설계하였다. 이는 상대적인 수치로 소음이 강한 장소에서는 스피커의 출력을 높여 인증을 수행 할 수 있다. 스마트폰 기기를 사용하기 위한 사용자 인증방법에서는 챌린지에 사용하는 주파수와 주변 주파수의 음량의 차이가 6dB일 때, 즉 챌린지의 음량이 주변 주파수의 음량에 비해 2배일 때 챌린지를 감지 할 수 있게 하였다. 제안한 두가지 방식의 챌린지를 감지하는 수치는 변경 가능한 파라미터로 수행 환경에 따라 최적의 값으로 설정하여 사용할 수 있다.

그림 3은 3장에서 제안한 시스템 사용을 위한 사용자 인증 중 스마트폰의 실행화면이다. 해당 어플리케이션을 실행하면 시스템의 스피커를 통해 발생시킨 비

〔표 2〕 음향 챌린지 사용자 편의성 실험 결과 (4회 챌린지 중 인지한 챌린지의 횟수)

시스템 사용을 위한 사용자 인증		스마트폰 단말기 사용을 위한 사용자 인증	
마스킹 음향이 없는 경우	마스킹 음향이 있는 경우	마스킹 음향이 없는 경우	마스킹 음향이 있는 경우
1.62	1.18	3.74	1.84

〔그림 4〕 시스템 사용을 위한 사용자 인증

〔그림 5〕 단말기 사용을 위한 사용자 인증

프를 통해 챌린지가 모두 수신 될 때까지 대기한다. 그림 4는 시스템으로부터 챌린지를 수신하는 모습이다.

그림 5는 4장에서 제안한 단말기 사용을 위한 사용자 인증을 수행하는 모습으로 스마트폰에서 발생시킨 챌린지를 대기 중인 PC에 장착된 마이크를 통해 수신하는 모습이다. 단말기는 사용자가 사용할 수 없는 상태로 스크린락(Screen lock)이 설정되어있는 상태이며 스마트폰 화면에 표시된 버튼을 통해 챌린지를 발생시킬 수 있다. 만약 챌린지 전달에 실패 시 재 전송이 가능하도록 구현되어있다.

본 논문에서는 사용자의 불편을 최소화하기 위해 가청주파수 대역 중 고주파 영역을 음향 챌린지로 사용하나, 일부 민감한 사용자의 경우 여전히 불편함을 느낄 수 있다. 이를 보완하기 위하여 음향 챌린지 전송 시 사용자에게 좀 더 친숙한 음향을 함께 출력하여 고주파 음향을 마스킹 함으로써 상대적으로 고주파 음향 챌린지를 느끼지 못하도록 할 수 있다. 본 논문에서는 이러한 마스킹의 실질적인 효과를 확인하기 위한 실험을 수행하였다. 피실험자는 24세부터 28세의 남, 여 10명이며 제안한 방식을 수행하면서 총 4번의 음향 챌린지 중 피실험자가 느끼는 음향 챌린지의 횟수를 측정하고 마스킹 음향을 함께 출력하였을 때 느끼는 음향 챌린지의 횟수를 측정하였다. 마스킹 음향은 제안한 방식에 대한 설명을 녹음한 것으로 피실험자가 인증 절차를 시작할 때부터 끝낼 때까지 재생하였다. 피실험자가 음향 챌린지를 감지한 평균 횟수는 표 2와 같으며 실험 결과를 통해 마스킹 음향을 음향 챌린지와 함께 출력하였을 때 피실험자가 느끼는 음향 챌린지의 횟수가 줄어듦을 확인 할 수 있었다. 특히, 피실험자 중 4명은 시스템 사용을 위한 사용자 인증 방식에서 음향 챌린지를 전혀 느끼지 못하였는데, 만약 음향 챌린지 주파수의 최소치를 15,800Hz보다 높일 수 있다면 더 많은 사용자들이 챌린지를 인지하지 못하도록 할 수 있을 것으로 예상된다. 모바일 기기 사용을 위한 사용자 인증의 결과가 시스템 사용을 위한 사용자 인증에 비해 실험 결과가 수치가 높은 것은 스마트폰에 내장된 스피커의 성능 상의 문제로 판단된다.

VI. 결론

본 논문에서는 스마트폰에 내장되어있는 여러 가지 센서 중에서 기본적인 장치인 마이크 및 스피커를 이용하여 근거리 상의 사용자를 인증하는 방법을 제안하였다. 본 논문에서 제안된 인증 방법은 두 가지로, 스마트폰을 일종의 하드웨어 토큰으로 활용하여 고정시스템 또는 웹사이트 등에 로그인하는 방법과 스마트폰을 사용하고자 하는 사용자가 스마트폰에 로그인하기 위해 가까운 고정 PC를 토큰으로 활용하는 방법이다.

본 논문에서 제안한 방식은 간단한 조작으로 시스템을 사용할 수 있기 때문에 특히 노인이나 시각 장애인등을 위한 인증 방법으로 활용할 수 있으며 엿보기 공격(Shoulder-surfing attack)에 강하다. 또한 두 번째 인증 방법의 경우 단말기에서 쓰이는 지식기반 인증방식을 보완하는 방법으로 활용할 수 있다. 향후 연구로써, 다양한 소음이 발생하는 상황에서 간섭에 대한 내성을 더욱 강화하는 연구를 진행할 계획이다. 또한, 현재 600Hz인 인접 챌린지 주파수간 간격과 현재 1초인 전송 시간을 줄여 음향 챌린지의 효율을 높일 수 있는 연구를 진행할 계획이다. 특히 향후 연구에서 챌린지의 주파수간 간격을 줄일 수 있다면 인증에 이용하는 주파수 최소치를 현재의 15,800Hz보다 더 높일 수 있을 것이므로, 음향 챌린지가 일부 사용자에게 인지되는 문제를 현저히 줄일 수 있을 것으로 판단된다.

참고문헌

〔1〕 방송통신위원회 보도자료, http://www.kcc.go.kr/user.do?mode=view&page=P05030000&dc=K05030000&boardId=1042&boardSeq=30991, 2011년 3월.

〔2〕 2011년 상반기 스마트폰 이용실태조사, http://isis.kisa.or.kr/board/index.jsp?pageId=040100&bbsId=7&itemId=776&pageIndex=1, 2011년 7월.

〔3〕 디지털타임즈 보도자료, http://www.dt.co.kr/contents.htm?article_no=2011060902011831699001, 2011년 6월.

〔4〕 Fred Cheng, "A secure mobile OTP Token", Mobilware 2010, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 48, pp.3-16, July, 2010.

〔5〕 Mun-Kyu Lee, Bo Kyoung Ku, and Jin Bok Kim, "Easy Authentication Using Smart Phones and 2-D Barcodes", ICCE 2011, pp. 139-140, January, 2011.

〔6〕 A. J. Nicholson, M. D. Corner and B. D. Noble, "Mobile device security using transient authentication," IEEE Transactions on Mobile Computing, vol. 5, no. 11, pp.1489-1502, Nov, 2006.

〔7〕 R. Want, A. Hopper, V. Falcao and J. Gibbons, "The Active Badge Location System," ACM Transactions on Information Systems, vol. 10, no.1, pp.91-102, Jan, 1992.

〔8〕 P. Bahl and V. N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," INFOCOM 2000, 2, pp.775-784, March, 2000.

〔9〕 윤민, 한태윤, 이문규, "간섭에 내성을 지닌 초음파 기반 사용자 인증 프로토콜", 차세대컴퓨팅학회논문지, 5(3), pp.20-28, 2009년 9월.

〔10〕 M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik and E. Uzun, "Loud and Clear: Human-Verifiable Authentication Based on Audio," ICDCS 2006, pp. 10-10, July, 2006.

〔11〕 H. Bojinov and D. Boneh, "Mobile Token-Based Authentication on a Budget," ACM HotMobile 2011, March, 2011.

〔12〕 김정태, "소음이 인체에 미치는 영향 (I) 청감의 신비", 한국소음진동학회(소음진동), 2(4), pp. 243-252, 1992년 10월.

〔13〕 Cooley–Tukey FFT algorithm, Wikipedia the free encyclopedia, http://en.wikipedia.org/wiki/Cooley-Tukey_FFT_algorithm

〈著者紹介〉

김 진 복 (Jin-Bok Kim) 학생회원
2010년 8월: 인하대학교 정보공학계열 학사
2010년 9월~현재: 인하대학교 컴퓨터정보공학 석사과정
관심분야: 정보보호, 유비쿼터스보안 등.

송 정 은 (Jeong Eun Song) 학생회원
2007년 2월: 인하대학교 컴퓨터공학과 졸업(학사)
2009년 2월: 인하대학교 정보공학과 졸업(공학석사)
2009년 3월~현재: 인하대학교 컴퓨터정보공학부 박사과정
관심분야: 암호알고리즘, 부채널분석 등.

이 문 규 (Mun-Kyu Lee) 종신회원
1996년 2월: 서울대학교 컴퓨터공학과 학사
1998년 2월: 서울대학교 컴퓨터공학과 석사
2003년 8월: 서울대학교 전기컴퓨터공학부 박사
2003년 8월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 인하대학교 컴퓨터정보공학부 부교수
2011년 2월~2012년 1월: University of California, Davis 방문교수
관심분야 : 정보보호, 암호학, 컴퓨터이론 등.