정 보 보 호 학 회 지
제 25 권 제 3 호, 2015. 6

오디오 채널을 이용하는 인증 시스템의 동향

정 창 훈*, 양 대 헌**

요 약

최근 스마트폰의 보급률이 급속도로 증가하면서 사용자가 언제 어디서나 인터넷에 쉽게 접근하여 정보를 얻을 수 있게 되었지만, 그만큼 해커들이 특정한 사용자의 중요한 정보를 훔칠 수 있는 환경이 되었다. 그로 인해 보안 전문가들은 이러한 중요한 정보를 보호하기 위하여 다양한 인증 시스템을 연구하고 있다. 이 논문에서는 키의 입력과 생체정보를 이용한 인증방법에 대한 보안위협과 취약점을 설명하고, 해당 위협을 회피하기 위하여 오디오 채널을 이용한 인증 시스템의 동향을 소개한다.

Ⅰ. 서 론

네트워크 통신의 발달은 사용자가 언제 어디에서나 인터넷에 쉽게 접근할 수 있는 환경을 만들었고, 그로인해 사용자는 원하는 정보를 더욱더 빠르고 정확하게 얻을 수 있게 되었다. 이로 인해 사용자들의 삶의 질이 향상되는 결과를 가져왔지만, 반대로 해커들이 특정한 사용자의 정보를 무단으로 훔치는 일도 빈번하게 일어나게 되었다. 특히 스마트폰의 보급률이 급속도로 증가하면서 더욱더 빈번하게 되었는데, 표 1에 나와있는 것처럼 시장 조사 기관인 온디바이스 리서치(ondevice research)가 조사한 2014년 세계 스마트폰 보급률에 따르면 우리나라는 80%로서 싱가포르 다음으로 세계 2위를 차지하고 있으며, 이러한 결과는 그만큼 보안위협에 쉽게 노출이 될 수 있다는 것을 의미한다.

해커들은 특정한 사용자의 정보를 무단으로 훔치거나 접근하고 싶을 때 인증 시스템만 통과를 하면 되는데, 이 시스템은 정당하게 허가받은 사용자임을 확인하는 절차를 의미한다. 또한 이러한 의미 외에도 전송된 메시지가 변조되거나 위조되지 않은, 송신자가 보낸 그대로의 것인지를 확인하는 것을 의미한다.

그림 1에 나와 있는 것처럼 인증 시스템의 종류는 아이디와 비밀번호를 입력하는 일반적인 비밀번호 인증, 매번 새로운 비밀번호를 생성하는 OTP(One Time Password) 인증 그리고 다수의 비밀번호 중 특정 몇 개만 입력하는 보안카드 인증 등이 있다. 또한 이것 외에 손가락의 지문을 이용하는 지문인증, 눈의 홍채를 이용하는 홍채인증 그리고 얼굴의 생김새를 이용하는 얼굴인증 등이 있다.

여기서 비밀번호 인증, OTP 인증, 보안카드 인증은 키보드의 키를 입력하는 인증에 해당하고, 지문인증, 홍채인증, 얼굴인증은 사람의 생체정보를 입력하는 생체

〔표 1〕 2014년 세계 스마트폰 보급률

순위	국가	스마트폰 보급률
1위	싱가포르	85%
2위	대한민국	80%
3위	스웨덴	75%
4위	홍콩	74%
5위	스페인	72%

〔그림 1〕 인증 시스템의 종류

* 인하대학교 대학원 컴퓨터정보공학과 (mizno@isrl.kr)
** 인하대학교 컴퓨터정보공학과 교수 (nyang@inha.ac.kr)

인증에 해당한다.

그러나 이렇게 다양한 인증 시스템은 해커로부터 다양한 방법으로 공격 받을 수 있는데 키의 입력을 이용하는 인증 시스템은 키로깅, 숄더서핑, 브루트포스, 스니핑, 스푸핑 등의 공격으로 위협받을 수 있다. 그리고 키를 입력하는 것이 아닌 일종의 이미지를 입력하는 생체인증 또한 여러 가지 방법으로 공격당할 가능성이 있기 때문에 더욱더 다양한 인증방법의 연구 및 개발이 필요한 실정이다.

이 논문에서는 키의 입력 또는 생체인증을 이용하는 인증시스템의 대한 보안위협을 알아보고, 이에 대응하기 위하여 오디오 채널을 이용하면서 사람과 상호작용을 하는 인증방법을 소개 한다.

Ⅱ. 보안 위협

2.1. 키 입력 인증의 보안위협

2.1.1. 키로깅 공격

사용자가 키보드로 입력을 하면 입력된 데이터는 운영체제에서 처리되어 해당 결과가 모니터에 출력되는 것이 일반적인 키보드의 처리 과정이다. 그런데 운영체제에서 입력한 키를 처리 할 때 정보를 가로채어 파일 등으로 저장하였다가 지정된 서버로 전송하여 정보를 빼내는 것을 키로깅 공격이라 한다. 공격자는 키로깅을 통해 사용자의 인터넷 사이트 로그인 정보, 사적으로 주고받은 메신저의 대화 내용 등 키보드로 작성한 모든 정보를 알 수 있기 때문에 개인 정보 및 기밀의 유출로도 이어질 수 있다.

키로깅은 보통 불법으로 유통되는 프로그램이나 악성 사이트를 통해 컴퓨터에 설치가 되므로 이를 탐지할 수 있는 백신 프로그램 사용하거나 불법 프로그램 대신 정품 프로그램을 사용함으로서 예방할 수 있다. 또는 로그인시 키보드로 비밀번호를 입력하는 방법 대신에 생체인증 또는 마우스를 이용하여 입력하는 인증을 사용하면 키로깅 공격을 피할 수 있다.

2.1.2. 숄더서핑 공격

숄더서핑 공격이란 한국어로는 어깨너머 훔쳐보기 공격이라 하며, 말 그대로 비밀번호를 입력하는 사람을 어깨너머 훔쳐봄으로서 비밀번호를 탈취하는 공격이다. 이 공격은 스마트폰의 사용이 급격히 증가하면서 더욱 주목 받게 되었는데, 보통 사람들은 사람이 많은 지하철이나 버스 등에서도 아무렇지도 않게 공개적으로 스마트폰의 잠금을 해제하기 위하여 패턴을 그리거나 비밀번호를 입력하기 때문이다.

공격자가 숄더서핑 공격을 하려면 타겟이 되는 사용자와 가까이 있어야 한다. 그러나 최근 메사추세스 로웰 대학 연구진들은 구글 글라스를 착용한 상태에서 아이패드 등의 스마트 기기에 입력하는 손동작을 보고 비밀번호를 알아 낼 수 있는 기술을 개발하였다. 또한 구글 글라스 대신에 고화질 카메라를 사용하면 약 40미터 떨어진 곳에서도 충분히 비밀번호를 알아낼 수 있음을 보여주었다[1].

이러한 숄더서핑 공격을 방어하기 위해서는 비밀번호를 입력하는 시스템이 아닌 일종의 이미지를 입력하는 생체 인증을 이용하거나 일회용 비밀번호를 이용하는 OTP 인증을 사용하면 된다.

2.1.3. 브루트포스 공격

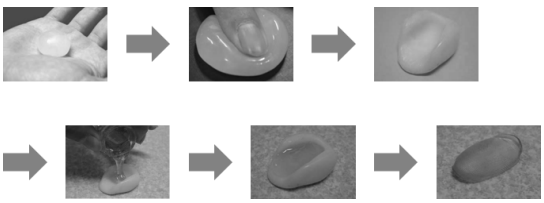
보안을 위협하는 공격 방법 중 가장 단순하면서도 위험한 공격이 브루트포스 공격이다. 이 공격은 어떠한 계정의 비밀번호를 알아내기 위하여 입력 가능한 모든 값을 대입해보는 것이다. 예를 들어 4자리의 숫자로 비밀번호를 사용하는 경우 0000에서부터 9999까지 1만개의 숫자를 하나하나 입력해보는 것이다. 이 브루트포스 공격은 가장 단순하기 때문에 널리 알려져 있으며, 그로 인해 대응하는 방법도 많이 개발된 상태이다. 공격자는 일반적으로 자동으로 비밀번호를 입력하는 프로그램을 이용하며, 서버 측에서는 어떠한 계정에 로그인이 10번 이상 실패하는 것을 인지하면 잠시 동안 그 계정의 로그인 시도를 할 수 없게 하여 이 공격을 방어할 수 있다. 또는 왜곡된 텍스트나 이미지를 보여주고 그에 따른 입력을 요구하여 로그인하는 대상이 사람인지 컴퓨터인지를 구별하는 캡차를 이용하여 방어 할 수 있다[2].

2.2. 생체인증의 보안위협

2.2.1. 지문인증의 취약점

지문인증이란 사람의 생체 정보 중 개개인마다 다른

손가락의 지문을 판독하여 특정인을 확인하는 인증방법이며, 생체인증 기술 중 가장 대중적으로 사용되고 있다. 지문은 잃어버릴 위험도 없고 기억할 필요도 없는 장점을 가지고 있으나, 물리적인 상처나 노동으로 닳아 없어질 수 있다는 단점을 가지고 있다. 뿐만 아니라 일본 요코하마 대학의 마쓰모토 교수는 그림 2처럼 잔류 지문을 젤라틴으로 얻은 후 인공 손가락을 만들어 지문 인식기를 통과시킴으로서 지문인증이 안전하지 않다는 것을 증명하였다[3].



〔그림 2〕 젤라틴을 이용하여 인공손가락을 만드는 과정

2.2.2. 홍채인증의 취약점

생체인증 분야에서 다소 높은 정확성을 보장하는 홍채인증은 주로 고도의 보안이 필요한 곳에 사용된다[4]. 홍채인증은 사람마다 다른 고유한 홍채의 무늬를 판독하여 특정인을 인증하는 방법이며 오랜 기간 변하지 않는다는 특징을 가지고 있기 때문에 생체인증 기술에 적용될 수 있다. 또한 동일한 무늬를 지닌 홍채를 발견할 확률은 매우 낮기 때문에 보안성이 상당히 높은 편이다. 그렇지만 다른 생체인증 장비에 비해서 운용비용이 비싼 편이며, 그림 3처럼 사람의 홍채를 고화질 카메라로 촬영한 후 프린트한 홍채 이미지로 홍채인증 시스템을 통과할 가능성이 지적되어 안전성의 문제가 제기되고 있다[5].

이를 통해 홍채인증의 보안성도 위협을 받고 있는 실정이며 홍채가 아닌 동맥, 청각, 얼굴 등의 다른 생체정보를 이용한 인증이 연구·개발되고 있다.

〔그림 3〕 가짜 홍채 이미지를 이용한 홍채 인증

Ⅲ. 오디오 채널을 이용하는 인증 시스템

3.1. 화자인증

사람마다 목소리관의 모양과 후두의 크기 등 목소리를 만드는 목의 여러 기관이 다르기 때문에 그에 따라 발성속도, 발음습관, 악센트 등이 같을 확률은 매우 낮다[6]. 이렇게 개개인마다 다른 음성을 컴퓨터로 분석 후 데이터화하면 인증 시스템에 적용하여 사용할 수 있다. 화자인증은 컴퓨터에서 입력으로 들어오는 음성 데이터를 데이터베이스에 저장된 음성 데이터들과 비교하여 화자가 누구인지 식별하는 것을 말한다.

화자인증은 그림 4처럼 우선 사람의 목소리가 컴퓨터에 입력이 되면 음성신호에서 잡음을 제거하여 언어적 데이터만 추출하기 위한 전처리 과정이 진행된다. 전처리 과정을 거친 음성 데이터는 특징 벡터 시퀀스를 추출하기 위하여 STFT, Mel filter bank, log, DCT의 과정을 지난다. 특징 추출이 완료되면 화자인증에 쓰일 수 있는 음성 데이터가 되며, 컴퓨터는 이러한 데이터를 데이터베이스에 저장되어 있던 음성 데이터와 비교하여 화자를 식별할 수 있게 된다[7].

사람의 목소리를 인증에 적용하면 물리적으로 분리되거나 변경되기 어렵기 때문에 타인에게 도용 또는 복제될 위험과 분실의 가능성이 낮으며 기억할 필요가 없다는 장점을 가지고 있다. 그리고 키의 입력을 이용하는 인증이 아니기 때문에 키로깅, 숄더서핑, 브루트포스 등의 공격을 막을 수 있으며, 목소리를 이용하므로 지문인증이나 홍채인증에서 발견된 취약점과 같은 취약점이 발견될 수 없는 생체인증이다. 또한 마이크만 있으면 하드웨어적인 구현이 모두 가능하며, 화자를 식별하는 것은 소프트웨어가 담당하는 것이기 때문에 비용이 저렴한 오디오 채널 인증 시스템 중 하나이다.

화자인증을 할 때에는 잡음이 최대한 없는 장소에서 하는 것이 좋기 때문에 길거리, 지하철, 버스에서는 식별률이 떨어진다는 단점을 가지고 있긴 하지만 이러한 단점을 보완하기 위한 기술 개발도 지속적으로 이루어

〔그림 4〕 화자인증의 과정

지고 있다. 예를 들면, 음성신호의 위상으로부터 순시 주파수를 계산하여 대역별로 순시 주파수를 모두 모아 구한 히스토그램으로부터 특징을 추출함으로서 잡음을 제거하는 화자인증 시스템도 개발되어 사용되고 있다[8].

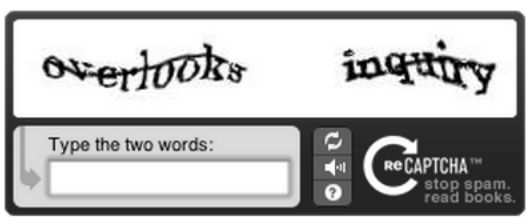
3.2. 오디오 캡차

캡차란 왜곡된 텍스트나 이미지를 보여주고 입력하게 하여 사용자가 실제 사람인지 컴퓨터인지를 구별하는 기술이다[2].

그림 5는 텍스트 기반 캡차로서, 왜곡된 텍스트를 보여주면 컴퓨터 프로그램은 제대로 인식할 수 없지만 사람은 정확하게 텍스트를 인식하여 입력할 수 있다. 이러한 방법으로 컴퓨터와 사람을 구별할 수 있으며, 흔히 웹사이트 회원가입시 프로그램을 통한 자동가입을 방지하기 위해서 사용된다.

이러한 텍스트 및 이미지 캡차의 단점은 시각장애인이 이용할 수 없다는 점인데, 이것을 보완한 것이 오디오 캡차이다. 그림 5의 텍스트 기반 캡차에서 소리모양의 아이콘을 클릭하면 왜곡된 텍스트는 없어지면서 오디오 캡차 상태로 변경이 된다. 오디오 캡차 상태가 되면 잡음이 섞인 단어가 재생이 되고, 사용자는 그 단어를 듣고 정확히 입력하면 오디오 캡차를 통과할 수 있다[9].

오디오 캡차에서 잡음을 섞는 이유는 컴퓨터가 소리를 정확하게 인식할 수 없게 하기 위해서인데, 이를 강화하기 위하여 잡음을 많이 섞으면서도 사람의 인식률을 높이는 방법이 있다. 오디오 캡차는 단어를 들려주는 것이 아니라 사람들에게 친숙한 구절을 들려주며, 여기에 잡음이 많이 섞여 있어도 사람들은 문맥적으로 단서를 알 수 있기 때문에 정확한 구절을 입력할 수 있게 된다[10]. 이 외에도 캡차의 종류는 드래그 앤 드롭을 이용한 슬라이드 캡차, 사람의 얼굴과 이름을 매치시키는 소셜 캡차, 커서가 이동한 경로를 확인하는 모션 캡차 등이 있다.



〔그림 5〕 텍스트 기반 캡차

3.3. Loud and Clear

Loud and Clear는 서로 통신이 가능한 디바이스 사이에 안전한 페어링을 위하여 사람이 보조하면서 오디오 채널을 이용하는 인증 시스템이다[11]. 이 방법은 페어링을 위해 하나의 기기에서 메시지를 해시한 후 그것의 결과를 다른 디바이스로 전송하는 것을 기반으로 하는데, 이것을 사용하기에 앞서 요구되는 조건은 다음 표 2과 같다.

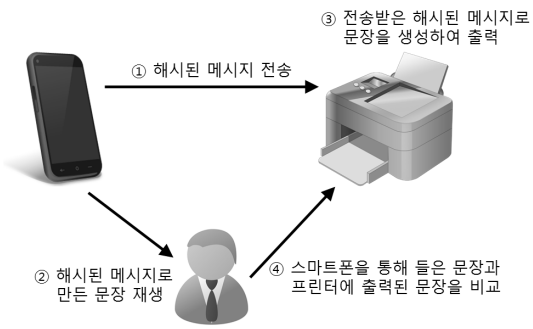
예를 들어 하나의 디바이스에 스피커가 있으면 다른 디바이스에는 최소한 스피커 또는 디스플레이가 있어야 한다. 이유는 두 디바이스간 페어링을 위해 메시지를 해시한 후 전송할 때 어떠한 문장을 생성하는데, 사람이 이 문장을 스피커를 통해 듣거나 디스플레이를 통해 보아야 하기 때문이다.

Loud and Clear의 방법은 3가지가 있는데 첫 번째는 하나의 기기에서 해시된 메시지로부터 생성된 문장을 소리로 내보낸 후 다른 기기에 전송하고, 다른 기기는 해시된 메시지를 받은 후 생성된 문장을 소리로 내보낸다. 그 후 사람은 이것을 듣고 그 두 소리가 일치하는지 비교하는 방법이다. 두 번째는 그림 6처럼 하나의 기기에서 문장을 소리로 내보내면 다른 기기에서는 디스플레이로 출력하여 사람이 중간에서 비교하는 방법이고, 세 번째는 이와 반대로 하나의 기기에서 디스플레이로 문장 출력하면 다른 기기에서는 소리로 내보내어 두 번째와 같이 중간에서 사람이 비교하는 방법이다. 이를 통

〔표 2〕 Loud and Clear의 사용 조건

디바이스 1		디바이스 2	
스피커	디스플레이	스피커	디스플레이
있음	없음	있음	없음
		없음	있음
		있음	있음
없음	있음	있음	없음
		없음	있음
		있음	있음
있음	있음	있음	없음
		없음	있음
		있음	있음

해 두 개의 디바이스는 페어링을 위한 메시지가 변조되거나 위조되는 것을 막을 수 있으며, 키교환 같은 페어링을 안전하게 성공시킬 수 있다.

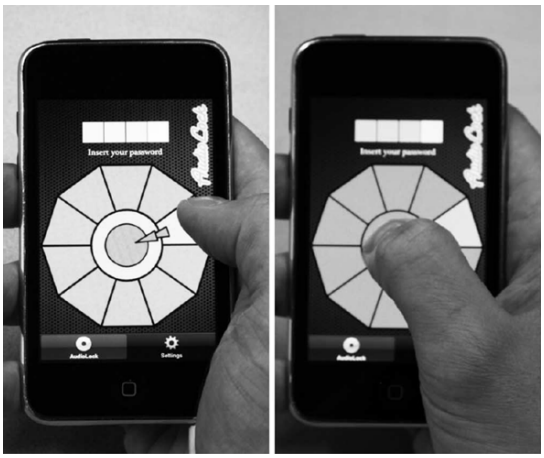


〔그림 6〕 Loud and Clear의 두 번째 방법

3.4. The Phone Lock

스마트폰에서 오디오 채널과 시각적인 채널을 이용하여 숄더서핑 공격을 효과적으로 방어할 수 있는 인증 시스템이 바로 The Phone Lock이다[12].

The Phone Lock의 인터페이스는 그림 7에 보이는 것과 같이 한 개의 원이 있고 그 주위에 10개의 도형이 배치된다. 사용자는 이어폰을 착용한 상태에서 10개의 도형 중 하나의 도형을 터치하면 0부터 9까지의 숫자 중 하나가 영어로 재생되는 것을 들을 수 있으며, 도형 하나에 연결이 되어있는 숫자들은 시계방향의 오름차순으로 정렬이 되어 있다. 그러므로 사용자는 10개의 도형 중 하나를 터치하면 보이지 않는 숫자들의 위치들을 알 수 있기 때문에 자신이 입력해야 하는 번호가 어디에 있는지 알 수 있다. 또한 도형과 연결되어 있는 숫자들은 매번 입력할 때마다 변경이 된다. 사용자가 숫자의 위치를 알아낸 후에는 그림 7처럼 원하는 숫자와 연결되는 도형을 터치한 상태에서 손가락을 가운데로 가져가서 떼면 원하는 숫자가 입력이 된다. 이를 통하여 사용자는 공격자의 숄더서핑 공격을 효과적으로 막을 수 있으며, 한 가지 단점은 The Phone Lock을 통하여 인증을 할 때마다 이어폰을 착용해야 한다는 것이다.



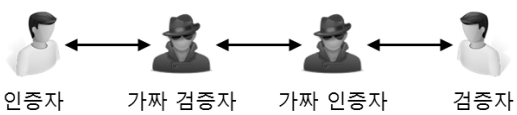
〔그림 7〕 The Phone Lock에서의 숫자 입력 방법

3.5. 소리를 이용한 릴레이 공격 공격의 탐지

릴레이 공격이란 두 명의 공격자가 협력하여 NFC 또는 RFID 같은 무선 근거리 통신 시스템을 속일 수 있는 공격 기법이다.

이 공격 기법의 시나리오는 다음과 같다. 정상적인 인증자와 검증자가 물리적으로 무선 근거리 통신을 할 수 없는 거리에 위치해 있을 때 가짜 검증자와 가짜 인증자는 그림 8처럼 위치한다. 그 다음 가짜 인증자는 진짜 검증자가 전달하는 어떠한 값을 가짜 검증자에게 전송하고, 가짜 검증자는 그것을 인증자에게 전송하여 인증자가 인증을 요구하게 만든다. 그 후 인증자가 가짜 검증자에게 인증 요청 메시지를 전달하면 가짜 검증자는 가짜 인증자에게, 가짜 인증자는 그것을 그대로 검증자에게 전송한다. 이와 같이 릴레이 공격은 암호화된 메시지에 대해 복호화를 하지 않고 단순히 메시지를 전달하는 것만으로도 정상적인 인증자와 검증자가 정상적으로 통신을 하고 있다고 속이는 것에 목적을 둔다.

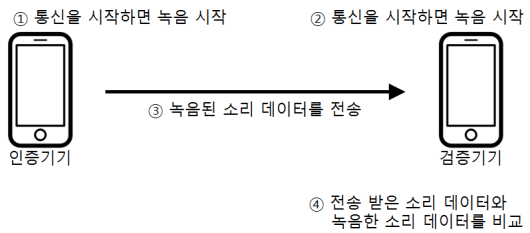
이러한 릴레이 공격을 방어하기 위해서 김종욱 등은 소리를 이용하여 릴레이 공격을 탐지하는 방법을 제안하였다[13]. 이 방법에서는 인증자와 검증자 역할을 하는 두 기기가 다음과 같은 기능을 가지고 있어야 한다고 가정한다. 첫 번째는 소리를 녹음할 수 있어야 하고, 두 번째는 데이터를 전송할 수 있어야 하고, 세 번째는 음향 데이터를 분석할 수 있어야 한다.



〔그림 8〕 릴레이 공격의 예

위 가정을 바탕으로 릴레이 공격을 탐지하는 방법은 우선 두 기기간 무선 통신이 시작되면 인증기기와 검증기기가 동시에 주위 소리를 녹음한다. 그 후 인증기기는 녹음한 소리 데이터를 검증기기에 전송하고, 그것을 받은 검증기기는 자기가 녹음한 소리 데이터와 비교를 하여 유사한 소리면 인증을 하고 아니면 인증 거부를 한다. 만약 인증기기와 검증기기가 무선 통신을 위해 가까이 근접해 있다면 두 기기에서 녹음한 음원이 당연히 비슷할 것이고, 그렇지 않고 그림 9처럼 녹음한 음원이 비슷하지 않아서 인증이 되지 않을 것이다. 이러한 방법을 통해 무선 통신 기기가 근접해있지 않을 때 릴레이 공격에 대한 취약점을 해결 할 수 있다.

이 방법은 오디오 채널을 이용한 인증이지만 사용자의 개입은 요구하지 않는 방법으로서, 보안적인 측면에서는 단점이 되지만 편의성에서는 장점이 되는 인증 시스템이다.



〔그림 9〕 오디오 채널을 이용한 릴레이 공격 탐지 방법

Ⅳ. 결 론

키를 이용하거나 생체정보를 이용하는 인증 시스템들은 이 논문에 소개된 여러 보안 위협과 취약점 때문에 완벽하게 안전하지 않다는 것을 알 수 있었고, 이를 해결하기 위하여 사람과 상호작용을 하면서 오디오 채널을 이용하는 인증 시스템들을 살펴보았다.

현재 존재하는 보안 위협과 취약점은 이 논문에서 살펴본 것보다 더 다양하면서 지능적인 것들도 많으며, 그로 인해 보안 전문가들은 이에 대응하기 위한 다양한 인증 시스템을 연구·개발하고 있다. 특히 보안성을 높이기 위해서 사람이 직접 개입하여 상호작용을 하면서, 사용자가 보안에 대한 지식이 많지 않아도 쉽게 사용할 수 있는 인증 시스템이 필요하다.

즉, 사용자의 편의성 및 접근성과 보안성 사이에서 트레이드 오프를 해결하는 것이 인증 시스템을 연구하는데 가장 중요한 점이라고 생각한다.

참 고 문 헌

[1] Qinggang Yue, Zhen Ling, Xinwen Fu, Benyuan Liu, Kui Ren and Wei Zhao, “Blind Recognition of Touched Keys on Mobile Devices,” *ACM CCS 2014*, pp. 1403-1414, Nov 2014.

[2] Luis von Ahn, Manuel Blum and John Langford, “Telling Humans and Computers Apart Automatically,” *Communications of the ACM*, Vol. 47, pp. 56-60, Feb 2004.

[3] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, “Impact of Artificial "Gummy" Fingers on Fingerprint Systems,” *Proceedings of SPIE*, Vol. 4677, pp. 275-289, Apr 2002.

[4] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, “Biometric Template Security,” *EURASIP Journal on Advances in Signal Processing*, Vol. 2008, No. 113, Jan 2008.

[5] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez and Javier Ortega-Garcia, “Direct Attacks Using Fake Images in Iris Verification,” *Lecture Notes in Computer Science*, Vol. 5372, pp. 181-190, 2008.

[6] Tomi Kinnunen, Haizhou Li, “An Overview of Text-Independent Speaker Recognition: from Features to Supervectors,” *Speech Communication*, Vol. 52, pp. 12-40, Jan 2010.

[7] 박현신, 김성웅, 진민호, 유창동, “최신 기계학습 기반 음성인식 기술 동향,” *전자공학회지*, Vol. 41, pp. 18-27, Mar 2014.

[8] 권철홍, “열악한 환경에 강인한 화자인증을 위한 위상 기반 특징 추출 기법,” *한국정보통신학회논문지*, Vol. 14, pp. 613-620, Mar 2010.

[9] K. A. Kluever, “Evaluating the Usability and Security of a Video CAPTCHA,” *Master’s thesis, Rochester Institute of Technology*, 2008.

[10] Jennifer Tam, Jiri Simsa, David Huggins-Daines, Luis von Ahn and Manuel Blum, “Improving

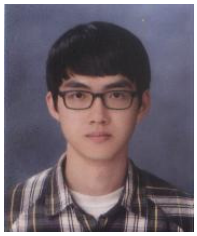
Audio CAPTCHAs," *In Proc. of the 4th Symp. on Usability, Privacy and Security (SOUPS '08)*, Pittsburgh, PA, USA, July 2008.

[11] Michael T. Goodrich, Michael Sirivianos, John Solis, Gene Tsudik and Ersin Uzun, "Loud and Clear: Human-Verifiable Authentication Based on Audio," *In Proceedings of the IEEE International Conference on Distributed Computing Systems*, 2006.

[12] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices.", *Proc. Conf. on Tangible, embedded, and embodied interaction*, TEI '11, pp. 197-200, January 2011.

[13] 김종욱, 강석인, 홍만표, "소리를 이용한 릴레이 공격 공격의 탐지," *정보보호학회논문지*, Vol, 23, No. 4, Aug 2013.

〈저자소개〉



정 창 훈 (Changhun Jung)
학생회원

2014년 9월~현재 : 인하대학교 대학원 컴퓨터정보공학과 석사과정
관심분야 : 인증프로토콜, 생체인증

양 대 헌 (DaeHun Nyang)
정회원

1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자공학과 학사
1996년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 8월 : 연세대학교 컴퓨터과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 3월~현재 : 인하대학교 컴퓨터정보공학과 교수
관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, 네트워크 보안, 모바일 보안