정 보 보 호 학 회 지
제26권 제6호, 2016. 12

다중 요소 인증에 사용 가능한 행위기반 바이오 인증

사 경 진*, 우 재 연**, 염 흥 열***

요 약

IT 기술의 발달로 다양한 인터넷 서비스를 사용하게 되면서 개인정보의 유출 등 위협이 증가하고 있다. 이에 개인정보의 중요도가 높아지면서 정보보안에 대한 관심도 높아지고 있다. 현재까지 많이 사용되고 있는 인증기술들은 단일 요소 인증으로 다중 인증(multi-factor authentication) 기술에 비하면 취약하다. 본 논문에서는 행위기반 바이오 인증 기술들 중 다중 인증을 하는데 이용 가능한 기술들에 대해 분석하고, 특성을 제시한다.

Ⅰ. 서 론

최근 기술발달로 모바일과 인터넷 등의 사용이 당연해지면서 관련된 많은 서비스가 나타남과 동시에 개인정보의 위협 또한 증가되었다.

일반적으로 사용자는 인증 방법으로 패스워드, SMS인증, 일회용비밀번호, 디지털인증서 등의 기술을 사용하고 있으며, 최근에는 바이오 정보를 이용하는 지문, 홍채, 정맥 등의 인증도 이용되기 시작하고 있다. 점점 더 교묘해지는 범죄 기술로 인해 단일요소 인증기술로는 다양하고 지능적인 해킹 등의 범죄의 위협에 효과적으로 대응하기 어려워지고 있는 현실이다.[5]

개인정보의 중요도가 증가하면서 간편하면서도 타인이 도용하기 힘든 바이오 인증의 관심이 높아지고 신체를 이용하는 생체기반 인증뿐만 아니라 행동의 특징들을 이용하는 행위기반의 인증도 개발되고 있다.

본 논문에서는 현재 사용 중인 인증수단과 다중 인증에 사용될 수 있는 바이오 정보 인증 중 행동을 기반으로 하는 행위기반 바이오 인증에 대해 알아보려고 한다. 논문의 구성은 2장에서는 인증요소에 따른 사용자인증의 기술을 분류하였고 3장에서는 다중인증에 사용될만한 행위기반 바이오 인증의 특징과 과정을 설명하였고, 현재 사용되고 있는 인증기술과 함께 쓰일 수 있는 방안을 알아보았다. 그 후 4장에서는 결론을 맺는다.

본 논문은 2016년도 한국정보보호 하계학술대회에 제출한 논문을 수정하고 개선하였습니다.[13]

Ⅱ. 사용자인증 기술 분류

비대면 특징으로 인해 사용자가 허가된 사용자임을 입증하는 사용자인증이 매우 중요하다. 현재 사용되고 있는 인증 기술을 인증요소에 따라 분류하면 소지기반, 지식기반, 특성기반으로 분류할 수 있다. 각 특징은 아래와 같다.[5]

2.1. 소지기반 인증(What you have)

사용자가 소지하고 있는 별도의 매체에 고유정보를 이용해 사용자를 인증하는 방식이다. 소지기반 인증방식의 예로는 OTP인증과 보안카드, 공인인증서 등이 있다.

2.2. 지식기반 인증(What you know)

사용자가 가지고 있는 지식을 통해 인증하는 방식이다. 지식기반 인증방식의 예로는 i-Pin, ID/Password 등이 있다.

본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구 결과로 수행되었음.
* 순천향대학교 융합서비스보안학과 (kyeong477@naver.com)
** 순천향대학교 융합서비스보안학과 (wjo553300@hanmail.net)
*** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

2.3. 특성기반 인증(What you are)

사용자가 가지고 있는 고유한 특징을 이용해 사용자를 인증하는 방식이다. 특성기반 인증은 크게 두 가지로 나뉘어져 있는데 신체적 특징과 행위적 특징을 이용한 인증이 있다.

2.3.1. 신체적 특징

신체적 특징을 이용한 인증방식으로 지문, 홍채, 안면 등이 있다. 신체를 기반으로 하여 사용자의 정보가 변할 가능성이 거의 없기 때문에 행위적 특징에 비해 정확성과 영구성이 높은 편이고 간편하다는 특징이 있지만 사용자의 신체 정보를 등록, 인증과정에서 거부감을 느낄 수 있다.

2.3.2. 행위적 특징

행위적 특징을 이용한 인증방식으로는 키스트로크, 음성인식, 서명 등이 있다. 행위를 기반으로 하는 인증은 비접촉식으로 사용자의 행동의 정보를 수집하여 사용자의 거부감이 적다는 장점이 있다. 하지만 사용자의 행위를 기반으로 하여 사용자의 행위가 변하게 될 가능성이 존재한다. 음성인식에서 감기 등 음성의 변화에는 대처할 수 없는 것처럼 사용자의 행동에 변화가 생기면 인증되기 어렵다는 단점이 있다.

위에 나온 인증 기술 중 하나만으로 인증을 하는 경우를 단일 요소 인증이라고 하고 두개 이상의 기술로 인증을 하는 경우를 다중 요소 인증이라고 한다. 다중 요소 인증은 단일 인증의 경우보다 보안의 안전성이 높아지게 된다.

Ⅲ. 다중 인증 기술

3.1. 키스트로크(Keystroke)

패스워드를 사용하는 인증방법은 가장 흔한 인증 방식으로 개발이 쉽고 다른 인증들에 비해 비용이 적게 들고 편리하다는 장점이 있다. 하지만 간편하기 때문에 보안이 취약한 문제를 가지고 있다. 이러한 문제점을 해결하기 위해서 키스트로크가 이용될 수 있다.

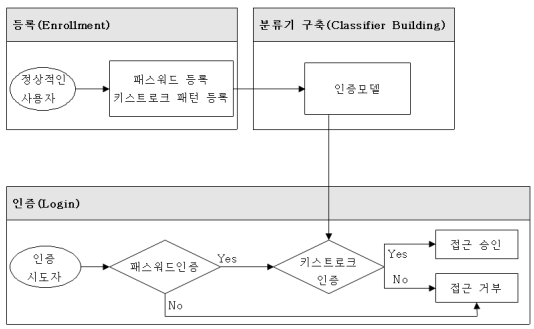
3.1.1. 키스트로크 특징

키스트로크(keystroke)는 키보드를 이용하여 사용자가 패스워드의 각 문자를 입력할 때 시간차를 패턴으로 인식하여 사용자를 인증하는 방법이다. 만약 패스워드가 노출되어도 키스트로크의 패턴이 다르면 사용자로 인식되지 않도록 하여 로그인을 할 수 없게 한다.

키스트로크는 짧은 문장이나 고정된 텍스트를 입력하거나 길거나 자유롭게 입력하는 경우로 나뉘게 된다. 짧거나 고정된 텍스트인 경우에는 주로 패스워드 등록 시 입력하여 사용되므로 로그인할 때 사용자 인증에 사용된다. 반대로 길거나 자유로운 텍스트를 입력하는 경우에는 키보드를 사용하는 동안 지속적으로 키스트로크 정보를 인증에 사용할 수 있으므로 실시간으로 인증이 가능하다. 타인이 무단으로 사용자의 PC를 사용 하는 경우에 대한 보안을 강화할 수 있다.[3]

3.1.2. 키스트로크의 인증 과정

키스트로크 인증 과정은 아래의 [그림 1]과 같다. 등록(Enrollment)과정과 인증 분류기 구축(Classifier Building)과정, 마지막으로 인증(Login)과정으로 구성되어 있다. 등록과정에서는 사용자를 정상적인 사용자로 등록하고, 스스로 정한 패스워드에 대한 키스트로크 패턴을 등록한다. 패턴이 복잡할수록 등록과정에서 패턴을 수집하기 위해서 요구하는 데이터 수집 횟수는 증가하게 된다. 분류기 구축 과정에서는 등록과정에서 제공된 사용자의 키스트로크 패턴을 바탕으로 패턴 인식 알고리즘을 사용하여 인증을 할 수 있는 분류기를 구축한다. 인증과정에서는 사용자가 인증을 시도 할 때 첫 번째로는 패스워드를 비교하여 일치하는지를 비교

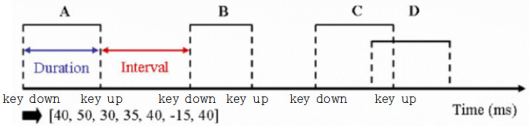


〔그림 1〕 키스트로크 구조〔1〕

후 일치하지 않으면 사용자의 접근을 거부하고 일치하는 경우에는 두 번째로 패스워드에 대해 구축되어 있는 키스트로크를 패턴을 비교 후 일치 여부로 접근을 승인하거나 거부한다.[1]

3.1.3. 키스트로크 특징 추출

사용자가 키보드를 이용할 때 키보드를 누르는 과정과 손을 때는 과정이 있다. 누를 때는 key-down 이벤트가 때는 경우에는 key-up이벤트가 발생한다〔4〕. 아래의 [그림 2]는 A, B, C, D의 키를 누를 때 발생하는 패턴을 나타낸 것이다. Duration은 키를 누른 후부터 손을 뗄 때까지의 시간이고, Interval은 다음 키를 누르기까지의 시간을 나타낸 것이다. [표 2]는 [그림2]의 Duration과 Interval의 시간을 나타낸 것이다. 개인마다 같은 텍스트를 입력해도 키보드 패턴의 시간이 다르다는 특징을 이용한다.



〔그림 2〕 키스트로크의 특징 추출〔2〕

〔표 1〕 키스트로크의 패턴 시간

	Duration(ms)		Interval(ms)
A	40	A-B	50
B	30	B-C	35
C	40	C-D	-15
D	40		

3.2. 음성인증

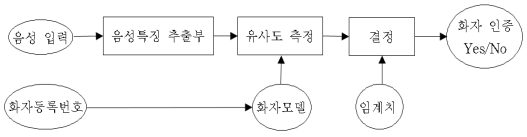
요즘은 대부분 사람들이 휴대폰을 소지하고 있고 휴대폰에는 기본적으로 마이크가 달려있기 때문에 손쉽게 음성인증을 사용할 수 있다. 이 때문에 모바일 관련 서비스 이용 중 추가로 하드웨어 설치할 필요 없고 음성 인증을 할 수 있다.

3.2.1. 음성인식 특징

음성인식 형태는 구분 발성한 단어를 인식하는 고립단어인식과 연속 발음을 인식하는 연속 음성인식, 핵심어 인식 등으로 구분된다. 고립단어는 문장이 아니라 단어 단위로 인식하는 방식이고, 연속 발음은 말 그래도 단어가 아니라 연속적인 문장을 인식하는 방식이다. 핵심어 인식은 대화에서 핵심적인 단어만을 골라서 인식하는 방식이다. 현재 높은 인식률을 보이는 시스템의 대부분은 고립단어 음성인식 시스템이다. 시스템의 인식범위를 늘리려면 검색하려는 단어수를 늘려야 하는데 단어수가 늘어남에 따라 시스템의 속도 및 인식 성능이 저하되는 문제점이 있다.[6]

3.2.2. 음성인증 시스템 구조

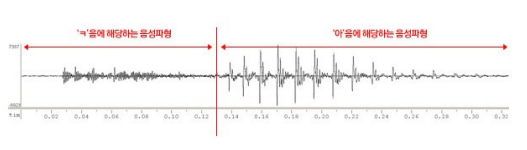
음성인증 시스템은 화자의 음성 신호에서 특징을 추출하여 사용자 인증을 위한 보안 시스템이다. 인증된 사용자는 시스템에 접근권한을 얻게 된다〔8〕. 처음에는 입력된 음성이 정상적 사용자인지 구분하기 위해 사용자에 대한 등록이 요구된다. 음성인증 시스템은 입력된 음성을 분석하여 특징을 추출한다. 그 후 저장되어있는 정보와 비교하고 유사도를 계산한다. 최종적으로 계산된 유사도 값과 정해진 문턱 값을 비교해 유사도 값이 문턱 값보다 큰 경우엔 인증을 수락하고 작은 경우엔 인증을 거부한다.



〔그림 3〕 음성인증시스템의 구성〔14〕

3.2.3. 음성인증 특징 추출

아래의 [그림 4]는 '카'라고 발성했을 때의 음성 파형이다. 0.13초까지 'ㅋ'음에 해당하는 음성파형이고 이후에는 '아'음에 해당한다. '아'파형을 관찰해보면 시간 축 상에서 나타나는 피크(peak)들이 보이고 성대



〔그림 4〕 '카'라고 발성했을 때의 음성 파형〔7〕

가 떨리는 주기와 일치하게 된다. 반면, 'ㅋ'은 무성음이기 때문에 피크가 보이지 않는다. 개개인의 음성의 파형은 다르기 때문에 이를 이용해 인증에 사용된다.[7]

3.3. 온라인서명

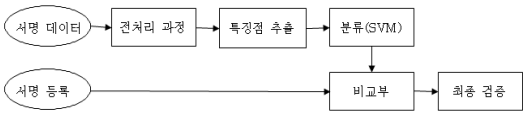
온라인서명이란 인터넷상이나 모바일에서 본인 확인을 위해 사용된다. 종이에 펜으로 서명하는 오프라인 방식 대신 전자펜이나 마우스 등을 이용하여 하는 온라인 방식이다. 요즘은 기술의 발달로 스마트 폰 사용이 당연시 되면서 추가적인 장비 없이 사용자가 사용하는 스마트 폰을 이용하여 온라인서명을 할 수 있다.

3.3.1. 온라인서명 특징

온라인서명은 인증은 접근 방법에 따라 크게 두 분류로 나눠지는데 첫 번째는 매개변수 특징을 이용하는 방법이고, 두 번째는 함수적인 특징을 이용하는 방법이다. 첫 번째 방법은 서명을 특정 매개변수로 바꾸고, 그 매개변수를 이용해서 서명 인증을 하는 것이다. 서명 인증을 하는데 모든 정보를 이용할 필요가 없어서 인증에 필요한 산술적인 시간이 줄어들고 서명을 매개변수로 바꾸기 때문에 표본의 데이터 크기가 일정하여 서명을 비교하는 알고리즘이 간단하다. 하지만 매개 변수로 바꾸는 과정에서 미세한 정보 손실이 있어 높은 신뢰성을 기대하기는 힘들고, 표본 데이터 집합의 크기가 클수록 인증 가능성이 높기 때문에, 많은 데이터를 요구한다. 함수적인 특징을 이용하는 두 번째 방법은 서명을 시간에 대한 함수의 형태로 나타낸다. 서명의 동적인 특성이 이용하기 때문에 매개변수를 이용한 접근 방법보다 정교하게 상이도를 측정할 수 있지만, 서명을 표본 데이터로 사용하여 데이터의 길이가 비선형적인 왜곡으로 인해 일정하지 못한다는 점이 있다. 그 부분은 보완하기 위해서 가변적인 길이의 데이터를 비교하기 위한 알고리즘이 필요하다.[9]

3.3.2. 온라인서명 인증과정

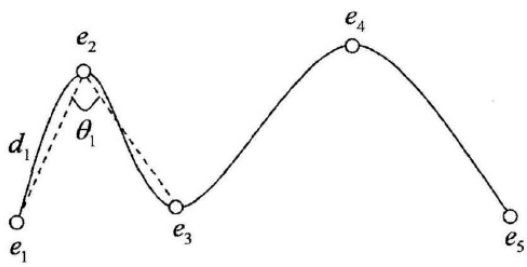
사용자가 서명을 하게 되면 서명 데이터가 입력된다. 하지만 서명은 심리적이나 신체적 상태에 따라 변화가 보이기 때문에 전처리부는 이러한 서명의 변화를 줄여주는 과정이다. 잡음제거과정과 샘플링과정으로 나누어지게 된다. 잡음제거는 손 떨림 등으로 인한 잡음을 제거 하는 과정이고 샘플링 과정은 입력된 좌표점이 많은 경우, 일부분을 제거하는 과정이다. 특징점 추출 과정은 사용자가 입력한 서명에서 전체 획수, 좌표점 수, 교차점의 개수, 획 상의 pen up이나 down시간, 획 사이의 시작점과 끝점간의 길이 등 다양하고 사용 가능하고 특징 점을 추출한다. 이렇게 추출된 특징은 비교부에서 이미 등록된 서명과 비교하여 본인의 서명이 맞는지 혹은 모조서명이 아닌지 유사도를 계산하게 된다. 최종 검증에서는 유사도가 문턱 값을 넘을 경우 인증이 승인되고 그렇지 않을 경우는 인증이 거절된다.[12]



〔그림 5〕 온라인서명 인증과정〔12〕

3.3.3. 온라인서명 특징 추출

임의의 온라인서명 S의 길이를 N이라고 하면 pt는 온라인서명 S에서 t번째 (x,y)의 좌표를 나타낸다. $p_t(x)$는 x좌표를 나타내고, $p_t(y)$는 y좌표를 나타낸다. S에서 추출된 k개의 변곡점은 아래의 식(2)와 같이 나타낼 수 있다. e_t는 S에서 t번째 변곡점을 나타내고 $e_t(x)$는 변곡점의 x좌표를 나타내고, $e_t(y)$는 y좌표를 나타낸다. 아래의 그림속의 θ는 인접하고 있는 세 개의 변곡점 사이의 각도이고 d는 인접하고 있는 두 변곡점 사이의 거리를 나태난다. △는 변곡점과 서명의 관계를 잘 표현하는 특징정보이다. k개의 변곡점을 가지는 서명은 아래의 식(6)과 같이 특징정보 집합으로



〔그림 6〕 변곡점(e)과 특징정보〔9〕

나타낼 수 있다.[9]

$$S = p_1, p_2, \cdots, p_N \quad (1)$$

$$E_s = e_1, e_2, \cdots, e_k,\ 0 \le k \le N \quad (2)$$

$$\theta_t = \begin{cases} \angle(e_t, e_{t+1}, e_{t+2}) & \text{if } t < k-1 \\ 0 & otherwise \end{cases} \quad (3)$$

$$d_t = \sqrt{(e_t(x) - e_{t+1}(x))^2 + (e_t(y) - e_{t+1}(y))^2} \quad (4)$$

$$\triangle_t = |e_t(i) - e_{t+1}(i)| \quad (5)$$

$$f = (\theta_1, d_1, \triangle_1), (\theta_2, d_2, \triangle_2), ..., (\theta_{k-1}, d_{k-1}, \triangle_{k-1}) \quad (6)$$

3.4. 다중 인증 방식

키스트로크는 지식기반의 인증 중 하나인 패스워드와 특성기반의 인증 중 행위기반 인증인 사용자의 키보드 패턴을 합친 다중 인증에 사용될 수 있을 것이다. 혹은 캡차(CAPTCHA) 시스템에 적용하면 개인정보가 유출될 경우 아이핀 인증이나 휴대폰 인증 이외에 보안 문자를 타이핑하면서 한 번 더 인증을 할 수 있게 되어 개인정보가 도용되지 않을 것이다. 또, 운영체제가 시작될 때 패스워드와 키스트로크를 합친다면 사용자 본인 외에 타인이 컴퓨터나 노트북을 사용 할 수 없어 해킹이나 악성코드 등에 의한 유출을 제외한 정보유출에 대한 보안을 좀 더 높일 수 있을 것이다. 또한 이 기술은 휴대폰에도 적용할 수 있어 향후에 기술이 좀 더 발전되면 사용자가 휴대폰을 이용하면서 주기적으로 저장된 키스트로크 값과 비교하여 본인이 아닌 경우 휴대폰 화면이 잠기게 할 수 있을 것이다.

현재 사람에게 쉽고 편리한 인터페이스는 음성으로 이를 이용한 인증 방법은 카드나 열쇠보다 매우 편리하고, 분실위험이 전혀 없어 매우 안전하며, 손이나 다른 도구를 필요로 하지 않으므로 중요한 기술로 자리매김하고 있다.[11] 음성인증은 현재는 당연시 사용되는 스마트 폰을 이용한 모바일 서비스에 사용될 수 있을 것이다. Pin번호나 공인인증서 등의 인증수단과 스마트 폰에 있는 마이크를 이용한 음성인증을 합치면 강력한 다중인증이 될 것이다. 앞으로 스마트폰 잠금해제 시 익숙하게 사용되는 지문과 더불어 음성인식을 같이 수행해 사용자의 지문와 음성이 일치할 경우 잠금이 해제되고, 일치하지 않을 경우 잠금이 해제되지 않는 기술이 나올 수 있다.

요즘은 대부분 스마트 폰을 사용하다보니 화면이 전체 터치가 가능하여 온라인서명을 자유롭게 쓸 수 있게 되었다. 신용카드 등에 온라인서명을 등록하게 된다면 모바일을 이용한 결제 시 공인인증서나 문자를 이용한 본인확인 이후 카드에 등록된 온라인서명을 이용하여 다중 인증을 하게 된다면 지금 사용되는 결제 수단보다 보안이 좀 더 강화될 것이다. 그리고 카드 번호와 공인인증서가 유출되어도 온라인서명은 사용자가 직접 서명을 해야 하기 때문에 타인이 따라 하기 힘들다는 점에서 유출되어도 피해 가능성을 낮춰줄 것이다.

또한, 다른 인증들과는 달리 세 가지 방법은 추가로 하드웨어가 필요하지 않고 소프트웨어만으로 처리할 수 있다는 장점이 있다[1].

Ⅳ. 결 론

본 논문에서는 다중 인증에 사용될 수 있는 행위기반의 바이오 인증에 대해 연구해보았다. 먼저, 사용되고 있는 인증 기술들을 소지기반, 지식기반, 특성기반으로 나누어 간단하게 특징과 사례를 알아보았다. 그 후 행위기반 바이오 인증 기술의 특징과 과정에 대해 알아보았다.

현재의 경우 사용자 인증 방식에서 패스워드 등 개인정보가 노출될 경우에 대한 확실한 대응방안이 아직은 없지만, 이러한 문제점의 개선하는 방안으로 로그인 도중에 추가로 본인 인증을 할 수 있는 키스트로크를 제안한다. 또, 흔히 사용하는 모바일을 이용한 인증 방법으로는 음성인식과 온라인서명 있다. 다른 인증에 비해 영구성이나 정확성이 낮은 편이지만 기만성 또한 낮다. 영구성이나 정확성을 높일 수 있는 방안을 찾는다면 편리하면서 강력한 본인 인증 수단이 될 것이다.

앞으로 기술이 발달을 하면서 현재보다 다양한 위협과 공격이 나타날 것이다. 이에 개인정보의 유출가능성도 점차 증가하게 될 것이므로 이를 대비해 정보를 보호할 수 있는 다중 인증기술과 같은 다양한 보안 방법이 필요하다.

향후에는 사용자가 사용 중에도 지속적으로 인증이 가능한 키스트로크나 기술적 단점이 보완된 음성 인증 시스템과 온라인서명을 구축하여 편리성과 보안성을 높이는 방법이 개발되기를 기대한다.

참 고 문 헌

[1] 강필성, 조성준, “자유로운 문자열의 키스트로크 다이나믹스를 활용한 사용자 인증 연구”, 산업공학 제25권 제3호, pp1-3, September, 2012.

[2] 황성섭, 조성준, 박성훈, “키스트로크 다이나믹스 분석을 이용한 모바일 사용자 인증”, *한국경영과학회 추계학술대회 논문집*, pp1-2, November, 2006.

[3] 박주성, 강필성, 박성훈, 윤준하, 조성준, “임의의 문자열에 대한 Kolmogorv- smirnov 테스트 기반 키스트로크 다이나믹스 인증- 터치폰 소프트키보드 이용”, *대한산업공학회 춘계공동학술대회 논문집*, pp2-9, June 2010.

[4] 김천식, 윤의중, 홍유식, 문남미, “이러닝 시스템에서 사용자 인증을 위한 키스트로크의 응용 기술”, *전자공학회논문지*, 45(5), pp1-4, September, 2008.

[5] 김근옥, 정영곤, 심희원 ,강우진, “모바일 기기 기반의 다중요소 인증기술 국제 표준화 동향”, *정보보호학회지*, 24(4), pp1-3, August, 2014.

[6] 김종훈, 심재호, 송창우, 이정현, “스마트 홈 환경에서 사용자 상황정보 기반의 음성 인식 시스템 개발”, *한국콘텐츠학회논문지*, 8(1), pp1-6, January, 2008.

[7] Navercast, 2016, 음성인식의 원리 , May 28, 17: 19 from http://navercast.naver.com/contents.nhn?rid=102&contents_id=4939.

[8] 이문구, “음성인식 보안 시스템의 구현”, 대한전자공학회 하계종합학술대회, pp1-2, June, 2006.

[9] 손기형, 박재현, 차의영, “변곡점과 필자고유특징을 이용한 온라인 서명 인증”, *멀티미디어학회논문지*, 10(9), pp1220-1228, September, 2007

[10] 심재성, 양승수, 박석천, “안전한 공인전자서명 신기술 확보를 위한 운용 방안”, 한국인터넷정보학회 춘계학술대회, pp201-202, May, 2015.

[11] 최홍섭, “휴대폰음성을 이용한 화자인증시스템에서 배경화자에 따른 성능변화에 관한 연구”, *한국음성학회*, 12(3), pp105-114, September, 2005.

[12] 김진환, “사용자 인증 보안을 위한 온라인 서명검증시스템”, *한국정보보호학회 학회지*, 12(2), pp34-40, April, 2002.

[13] 사경진, 우재연, 오에지, 염홍열, “다중 요소 인증에 사용 가능한 행위기반 바이오 인증”, 한국정보보호학회 하계학술대회, June, 2016.

[14] 최홍섭, “화자인증 시스템에서 배경화자 선정 방법에 관한 연구”, 음성과학 제9권 2호, pp135-146, June, 2002.

〈저 자 소 개〉

사 경 진 (Kyeong-Jin Sa)
학생회원

2016년 2월 : 순천향대학교 전기공학과 졸업
2016년 3월~현재 : 순천향대학교 융합서비스보안학과 석사 과정
관심분야 : 개인정보보호, 바이오인증, IoT 보안, 악성코드

우 재 연(Jae-Yeon Woo)
학생회원

2016년 2월 : 강원대학교 컴퓨터정보통신공학과 졸업
2016년 3월~현재 : 순천향대학교 융합서비스보안학과 석사 과정
관심분야 : 통신공학, 정보보호, 사이버보안, IoT, 자동차보안

염 흥 열(Heung-Youl Youm)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신 연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 11월 : ITU-T SG17 부의장
2016년 11월~현재 : ITU-T SG17 의장
2009년~현재 : ITU-T SG17 WP2/WP3 의장
2012년 6월~2015년 5월 : 정보보호포럼 의장
2016년 5월~현재 : 개인정보보호표준포럼 의장
관심분야 : 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜