Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1033

내재적 리스크 감지 모델을 사용한 사용자 인증 편의성 향상 프레임워크*

김 평,[1†] 서 경 진,[1] 조 진 만,[2] 김 수 형,[2] 이 윤 호[1‡]
[1]서울과학기술대, [2]한국전자통신연구원

The Framework for Cost Reduction of User Authentication Using Implicit Risk Model*

Pyung Kim,[1†] Kyongjin Seo,[1] Jin-Man Cho,[2] Soo-Hyung Kim,[2] Younho Lee[1‡]
[1]SeoulTech, [2]ETRI

요 약

사용자의 인증 프로세스에 대한 인식을 필요로 하는 기존의 명시적 인증은 그 과정에서 사용자에게 많은 부담이 되며 이는 사용자가 인증을 기피하는 원인이 되고 있다. 본 연구를 통해, 우리는 바이오 인식 및 위치 기반 인증 방법과 같은 내재적 인증 방법을 사용하여 사용자 인증의 편의성을 달성하는 방안을 제안한다. 이를 위해 명시적 인증으로 달성할 수 있는 4단계 보증 레벨을 정의하고, 내재적 인증 방법과 명시적 인증 방법과 같이 사용하여 보다 적은 인증 비용으로 동일 단계의 신뢰 보증 레벨에 도달할 수 있음을 보인다. 제안 방법의 유효성을 보이기 위해, 스크린 키보드 기반 인증, 얼굴인식 기반 인증, 위치 기반 인증을 내재적 인증 기법으로 도입하며 이를 안드로이드 응용으로 구현하였다. 실험 분석 결과, 제안 방법은 패스워드 인증 대비 21.7%, 6자리 PIN 인증 대비 14.9%의 비용 절감 효과를 달성하였다.

ABSTRACT

Traditional explicit authentication, which requires awareness of the user's authentication process, is a burden on the user, which is one of main reasons why users tend not to employ authentication. In this paper, we try to reduce such cost by employing implicit authentication methods, such as biometrics and location based authentication methods. We define the 4-level security assurance model, where each level is mapped to an explicit authentication method. We implement our model as an Android application, where the implicit authentication methods are touch-stroke dynamics-based, face recognition based, and the location based authentication. From user experiment, we could show that the authentication cost is reduced by 14.9% compared to password authentication-only case and by 21.7% compared to the case where 6-digit PIN authentication is solely used.

Keywords: Smartphone authentication, Biometric system, Implicit authentication, Touchstroke-based dynamics, Authentication cost

I. 서 론

최근 IT 기술의 성장을 통해 스마트폰을 사용하는 다양한 서비스가 보급되고 있고, 인터넷 뱅킹, 주식 투자, 스마트 지갑 등과 같이 사용자 보안이 중요시 되는 서비스도 급격히 확산되고 있다. 스마트폰의 보안은 패스워드, PIN(Personal Identification Number), 시각적 패턴(visual pattern) 등과 같

Received(04. 10. 2017), Modified(1st: 08. 01. 2017, 2nd: 09. 01. 2017), Accepted(09. 04. 2017)
* 본 연구는 2016년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2015-0-00168, "상황인지 기반 멀티팩터 인증 및 전자서명을 제공하는 범용 인증 플랫폼 기술 개발")
† 주저자, firimir@gmail.com
‡ 교신저자, younholee@seoultech.ac.kr (Corresponding author)

이 사용자 지식 기반의 인증 도구가 지원되고 있으며, 바이오 정보 인식 센서를 통해 얼굴인식, 지문, 목소리 등과 같은 인증 방법론 또한 제안되고 있다〔1〕. 그런데, 기존의 많은 스마트폰의 인증 기술은 일반적으로 사용자에게 현재 상황이 인증이 필요한 상황임을 인지시키고, 인증 관련 작업의 독립적 수행을 요구하는 명시적 인증 형태를 취한다. 이와 같은 명시적인 인증 기술(explicit authentication)은 보안이 필요할 때마다 사용자에게 인증을 반복해서 요구하기 때문에 스마트폰을 통한 서비스가 가지는 가장 큰 장점인 사용자 편의성을 저해하는 요소가 된다. 이와 대비되는 스마트폰 인증 기술로 〔2〕 연구는 사용자의 행동이나 바이오 정보(biometric information)를 수집하고 이를 분석하여 인증의 기준으로 사용하는 내재적 인증 기술(implicit authentication)들을 다루고 있다. 내재적 인증이 진행되고 있는 과정에서는 스마트폰의 입력 장치, 카메라, 센서 등을 통해 내재적 인증에 필요한 정보를 상시 수집하고 인증 통과 여부를 판별하기 때문에 독립적인 인증 절차가 요구되지 않는다. 그러나 내재적 인증 기술은 수집되는 데이터의 노이즈, 인증의 정확도의 문제가 존재하며, 인증이 실패했을 경우, 별도의 접근을 허가하기 위한 과정(명시적 인증)이 필요하다.

본 연구는 스마트폰에서의 내재적 리스크(implicit risk) 판정 방법을 제안하고 이를 바탕으로 사용자의 명시적 인증의 부담을 경감시키는 것을 목적으로 한다. 구체적으로 기존에 가장 많이 사용되는 패스워드 기반 인증 및 그래픽 기반 인증 등의 사용자에게 명시적인 인증의 빈도를 줄여 사용자의 편의성을 증대시키는 것을 목적으로 한다. 또한 이러한 명시적인 인증 빈도의 감소로써 발생하는 잠재적인 보안 위험성을 내재적인 인증 기법을 통하여 경감 시킨다.

스마트폰에서 현재 리스크를 판별하고 그 리스크에 적합한 인증 방법론을 채택하기 위해서는 현재 보안 상태를 정량화하는 방법과 각 인증 방법의 보안 수준에 대한 분석이 필요하다. 기존의 스마트폰 인증의 보안에 대해서 국내외의 조사보고서 및 연구들이 보고되고 있다〔3-9〕. 그러나 스마트폰에서 사용되는 인증 방법의 취약점을 분석하는 〔3,4〕연구의 경우 이를 정량화하는 것에는 문제점이 있으며, 인증 방안의 위험성 평가에 대한 〔5-9〕 문건의 경우도 사용자 편의성을 증대시키기 위한 방안으로 직접적인 적용은 어렵다. 이와 관련해서 본 연구의 공헌은 다음과 같다.

첫째, 스마트폰 인증을 통해 달성할 수 있는 4단계의 신뢰 보증 수준(4-level trust assurance level)을 추측가능성(guessabiliy)〔10〕을 기준으로 정의하였다. 본 연구에서는 패스워드(password), PIN (Personal Identification Number), 스크린 키보드 입력 패턴(touch stroke dynamics), 얼굴 인식(face recognition), 그리고 WiFi AP 정보를 이용한 지역 기반 인증 방법의 5개의 인증 방법을 고려한다. 이들을 이용하여 추측가능성이 가장 높은 인증을 성공했을 경우를 4단계의 신뢰 보증을 할 수 있는 상태로 정의하며, 아무런 인증을 수행하지 않은 상태를 1단계로 둔다. 본 연구에서는 1~4단계의 각 단계별 요구되는 적정 보안 수준과 이를 달성하는 과정에서 필요한 사용자 비용을 같이 고려하기 위한 인증 프레임워크(framework)를 제안한다.

둘째, 내재적 인증에서 가장 중점적으로 사용될 스크린 키보드 기반 인증의 구현 및 성능향상이다. 본 연구에서는 기존 데스크탑(desktop)에서 효율적인 키보드 인증(keystroke based authentication)을 제안한 〔11〕 연구의 R 척도(R-measure)와 A 척도(A-measure)를 스마트폰의 스크린 키보드 입력 패턴(touch stroke dynamics)에 적용하고, R-A 척도 선형 조합의 최적화를 수행한 〔12〕 연구를 구현하였으며, 인증 과정에서 R-A 지표와 얼굴 인식 정보를 융합하여 성능을 높였다.

셋째, 스마트폰의 현재 내재적 리스크를 실시간으로 모니터링 할 수 있는 안드로이드(android)기반 어플리케이션을 설계하였다. 그리고 실제 제안방법을 통해 얼마나 사용자 인증의 비용(authentication cost)이 경감되는지를 사용자 실험을 통해 조사, 분석하였다.

이후 본 논문의 구성은 다음과 같다. 2장에서는 스마트폰 인증의 보안 수준, WiFi AP의 신뢰도, 스크린 키보드 기반 인증으로 확장할 수 있는 키보드 기반 인증(keystroke-based authentication)에 관련된 기술 및 연구를 다룬다. 3장에서는 본 연구를 통해 제안하는 인증 방안을 설명하고 시스템을 설계한다. 4장에서는 사용자 실험을 통해 제안 방법의 효율성 분석한다. 5장에서는 최종적으로 본 논문을 결론짓는다.

II. 관련 연구 및 선행 기술 분석

본 절에서는 본 연구의 목적인 내재적인 스마트폰 정보 및 상황정보를 이용한 위험도 분석 및 인증과 관련 된 관련 연구를 소개한다. 2.1에서는 바이오 정보를 이용한 인증 강도의 기준들과 그 적용을 조사한다. 2.2에서는 WiFi AP에 대한 사용자 신뢰도에 관한 조사를 정리한다. 2.3에서는 본 연구에서 사용할 내재적 인증의 기본 도구라 할 수 있는 키보드 기반 인증기술에 대해 알아보고 이에 대한 확장 및 바이오정보(biometrics information)와의 융합에 관련된 기술을 소개한다.

2.1 바이오 기반 인증 시스템 보안 강도

스마트폰 인증 시스템의 보안에 관련된 〔3,4〕연구의 경우 스마트폰에서 사용되는 바이오 인식 시스템의 취약점을 분석하고 공격 방안을 다루었으나 위험도에 대한 별도의 정량화는 이루어지지 않았다.

미국국가표준연구소 NIST(National Institute of Standards and Technology)는 바이오 인식 시스템의 보안 강도를 측정하기 위한 프레임워크를 제안하였다〔5,6〕. 〔5〕에서는 인증 강도와 시스템 내부의 데이터 관리 측면도 고려하여 바이오 인식 시스템에서 5가지 보안위협 시나리오를 프레젠테이션 공격(presentation attack), 바이오 정보 획득 장치(biometric capture device), 바이오 정보 샘플(biometric samples), 바이오정보 비교 판별로 정의하고 보안 지침을 제안한다. 〔6〕에서는 인증 시스템을 공격하기 위해 필요한 시간, 전문성, 장비를 합친 공격노력(attack effort)을 3단계로 구분한다. 그리고 이를 공격 성공률, 오인식률(false acceptance rate)을 합쳐서 SOFA-B(Strength of Function for Authenticators - Biometrics) 측정법을 제안하고 있다. 그리고 정보보안기술 국제표준화위원회 또한 EAL(Evaluation Assurance Level)에 따라 바이오 인식 시스템의 강도를 구분하고 있다〔7〕. 그러나 이 결과들은 보안 안전성 및 정확성에 대한 기준이며, 사용자 편의성을 고려한 내재적 인증에 관련된 지표로는 활용할 수 없다.

국내에서도 금융보안원이 발표한 인증의 안전성 평가방안 〔8〕과 다중 인증 보증 프레임워크〔9〕가 존재하지만 다수의 인증 방안에 대한 평가 지표이며 바이오 정보에 특화된 관리지침이나 사용자의 인증 비용에 관련된 고려가 이루어지고 있지 않다.

2.2 WiFi AP를 기점으로 한 지역적 신뢰도

2012년, 2013년에 수행된 〔13,14〕의 조사에 따르면, 모바일 디바이스의 사용자들은 거의 하루 종일 WiFi를 연결한다는 점과 집, 사무실 등과 같이 자주 사용하는 공간에서의 WiFi AP를 신뢰한다는 점이 밝혀졌다. 이는 WiFi AP를 기점으로 한 위치정보가 사용자의 디바이스의 현재 신뢰 수준을 결정짓는 단서가 될 수 있음을 의미한다.

구체적으로 특정 지역에 대한 안전성을 가정하고, GPS 정보나 WiFi AP의 접속 정보를 신뢰도 기준으로 활용하는 방식은 위치기반서비스(LBS, Location Based Service) 분야에서 사용되어 왔다. 가령, 의료관련 서비스를 열람하기 위해서는 병원의 특정 위치에서만 접근을 허용하기 위해 WiFi 정보를 사용할 수 있으며〔15〕, 보험회사에서 할인혜택을 제공하기 위해 운전자의 과거 운전 경로를 확보하기 위해 차의 주행시간 동안의 GPS나 WiFi AP 접속 기록을 사용할 수 있다〔16〕. 그리고 〔17〕 연구는 구체적으로 모바일 장치의 상황 정보(context)에 대한 프로파일링(profiling)을 통해 일상적인 환경, CoI(Context of Interest)를 정의하고 있다. 본 연구도 이와 같은 CoI 정보를 내재적 위험 판별을 위해 사용한다. 본 연구에서 활용할 CoI 정보는 집, 사무실과 같은 제한된 공간에서 CoI 정보가 지속적으로 유지되는 경우로 한정하며, 공격자가 수행할 수 있는 공격 유형과 공격 시간을 제한하는 도구로 사용된다. 이와 같은 공격자에 대한 제한은 CoI 정보를 통해 일정 수준의 신뢰도를 달성할 수 있음을 의미하며, 구체적인 내용은 세부절 3.1에서 다룬다.

2.3 자유 텍스트 기반 스크린 키보드 인증 기법 및 성능 향상

2.3.1 키보드 입력 기반 사용자 인증 기법

키보드 기반 인증 기법에 대한 간단한 통계적 접근은 〔18〕에서 다루어졌다. 〔18〕연구에서는 각 사용자가 2개 키 눌림(key down-key down) 시간 간격의 누적 분포 함수를 근사한 히스토그램을 기준으로 인증을 수행한다. 실용적인 기법이지만 실험에서 사용된 데이터가 통계적으로 의미 있는 결과를 산출

하기에 부적절하다는 단점이 있다.

〔11〕연구는 두 사람의 키 입력 시간과 입력 키의 전후 관계를 고려하여 두 사용자간의 상대적(‘R’elative)/절대적(‘A’bsolute) 순서 불일치(degree of disorder)를 사용자 인증에 사용하는 R-A 척도(measure)를 제안 하였다. R 척도는 입력 시간 자체 보다는 상대적 순서의 불일치 정도를 측정하는 데 초점을 두고 있으며, A 척도의 경우 동일한 음절의 입력 시간 비율 차이를 측정하는 데 초점을 두고 있다. R 척도의 경우 두 명의 사용자가 비슷한 수의 문자 타이핑 속도 순서를 사용할 경우, 동일한 사용자로 식별된다. 따라서 이 방법에서는 유사한 두 번째 문자를 사용하는 두 명의 사용자를 구별하는 것이 어려울 수 있다. 이 때문에 두 사용자의 절대적인 타이핑 속도를 측정하는 A 척도를 동시에 측정하며, R 척도, A 척도의 선형결합을 통해 효과적인 사용자 인증 알고리즘을 구축한다. R-A 척도는 자유 텍스트에 대한 가장 효율적인 인증 방법 중 하나이기 때문에 인증 성능을 향상시키기 위한 〔12, 19,20〕과 같은 후속 연구가 제안 되었다. 그 중 〔12〕의 연구는 〔9〕 연구를 스마트폰의 스크린 키보드 입력을 기반으로 구현하였으며, 가장 최적화된 R-A 척도의 선행조합을 구하였다. 본 연구에서도 〔12〕 연구를 기반으로 하는 인증 매커니즘을 구현하였다.

〔21〕연구는 클러스터링(clustering) 기법을 적용을 사용하여 분석에 필요한 키보드 입력 패턴(keystroke dynamics)의 총량을 개선하였다. 그러나 실제 구현에 있어 중요한 사용자 특징하는 매개변수(ex: 클러스터 수, 다중 클래스 분류 임계 값)를 결정하는 부분에 어려움이 존재한다.

키보드 입력 데이터를 다양한 거리 기준(distance-metric)을 사용한 인증 기법들에 대한 연구로 〔22-25〕가 있다. 그러나 이러한 연구들은 잠재적인 비인가 된 사용자(imposter)라고 볼 수 있는 전체 데이터의 량이 인가된 사용자 데이터 량을 크게 초과하였기 때문에 매우 낮은 오인식률(false acceptance rate)을 달성할 수 있다는 단점이 존재한다. 〔26〕연구는 이를 극복하기 위해 다중 거리 기준(distance-metric)을 사용하였으며, 동일오류율(equal-error rate)을 감소시켰다.

2.3.2 스마트폰에서의 다중 바이오 정보 인식 시스템

단일 바이오 정보 인식 방법론들에 대해서 최근 이를 활용하여 모바일 환경으로 확장하기 위한 연구〔22, 27-30〕가 수행되어 왔다. 그러나 단일 바이오 정보는 데이터 노이즈(data noise), 비범용성(non-university), 바이오정보의 특성(distinctiveness) 부족, 정확도 문제(unacceptable error rate)와 같은 내재적 한계로 인해, 실제 구현을 통한 적용에 충분한 결과를 얻기가 어렵다는 것이 밝혀졌다. 따라서 1개 이상의 바이오 정보를 융합(fusion)할 수 있는 다중 바이오 정보 인식 시스템의 제안을 통해 이를 극복하기 위한 연구〔4, 31-36〕가 제안되고 있다. 그 중에서 다중 바이오 정보 인식 시스템 중에서 키보드 입력 패턴과 다른 바이오 정보를 융합하는 기술은 〔4, 34-36〕연구가 있다. 〔4〕의 경우 얼굴인식과 결합을 시도하였으나 실험 대상의 수가 너무 적어서 타당성의 검증이 어렵다는 제한이 있다. 〔34〕의 경우 100명을 대상으로 키보드 입력 패턴 데이터와 2D 얼굴 이미지를 수집하고 분류 점수(classification scoring) 단계에서 융합하여 동일오류율(equal error rate, EER) 2.22%를 달성하였다. 〔35〕의 경우 30명을 대상으로 키보드 기반 입력 패턴 데이터, 행동 프로파일링(behavioral profiling), 언어 프로파일링(language profiling) 데이터를 수집하고 이를 융합하여 동일오류율(equal error rate, EER) 8%를 달성하였다. 또, 키보드 입력 패턴 데이터와 걸음걸이 데이터를 수집한 연구인 〔36〕과 같은 연구도 존재한다.

III. 제안 방법

본 연구에서는 스마트폰에서의 내재적 리스크 판정 방법을 제안하고 이를 바탕으로 사용자의 명시적 인증의 부담을 경감시키는 것을 목적으로 한다. 이를 위한 전체 시스템 구성도는 Fig. 1과 같다.

3.1 에서는 2.2에서 조사한 WiFi AP의 신뢰도와 사용자 편의성을 반영할 수 있는 4단계의 신뢰보증 모델(4-level trust assurance model)의 수립한다. 3.2에서는 행위 인증 기반으로 사용할 수 있는 주요 방법 중의 하나인 〔12〕의 스크린 키보드 입력 패턴(touch stroke dynamics) 기반 인증을 설명한다. 3.3에서는 3.2의 인증 도구를 3.1의 4단

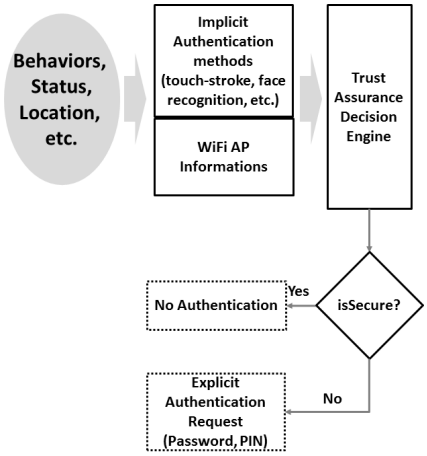

Fig. 1. The system framework

계 신뢰 보증 모델 구성의 한가지로 취합하고 안드로이드(Android) 기반의 신뢰 보증 수준 판별 엔진을 설계한다.

3.1 신뢰 보증 단계 및 인증 메커니즘

3.1.1 4 단계 신뢰 보증 단계 정의

본 연구에서 가장 중점을 둔 내용은 다양한 인증 방법들 간의 보안성 측면에서의 관계를 규명하고, 개별 인증 방법 또는 그것들의 조합을 이용하여 달성할 수 있는 신뢰 보증 단계를 정의하는 것이다. 신뢰 보증 단계를 정의해야 하는 이유는 사용자의 인지와 비용이 필요한 명시적 인증 방법을 사용자 편의성을 고려한 다양한 내재적 인증 방법으로 전환할 때, 달성해야하는 인증의 신뢰도의 최소한의 기준을 제시하기 위함이다. 우리는 신뢰 보증 단계 수립을 위해 패스워드 및 PIN 번호 기반 인증 방법을 고려한다. 두 인증 방법은 많은 사람들이 사용하는 전형적인 인증 방법으로써 사용자들의 인지를 필요로 하며, 이에 따라 본 연구에서는 사용자들의 해당 인증 방법의 횟수를 줄이는 것을 목적으로 한다.

본 연구는 안전성 측면에서 인증 도구의 추측가능성(guessability)을 인증 수준의 강도로 정의하고 이를 통해 1~4 단계 보증 레벨을 정의한다. 가령, 패스워드의 경우, 추측가능성은 “공격자가 몇 번의 시도를 통해서야만 해당 패스워드를 알아낼 수 있는가”로 정의할 수 있다.

〔9〕에 의하면 현존하는 가장 좋은 방법으로 알려진 패스워드 분석 전문가의 공격을 수행할 때, 사용자가 많이 사용하는 경우인 컴플렉스(Complex), 롱베이직(LongBasic), 그리고 롱컴플렉스(LongComplex) 패스워드에 대해서 10% 이상의 의미 있는 추측 성공률을 보이기 위해 최소 10^9 의 시도를 함을 알 수 있다. Table 1은 컴플렉스(Complex), 롱베이직(LongBasic), 그리고 롱컴플렉스(LongComplex) 패스워드들에 대한 정보를 나타낸다. 이와 같이 비교적 인증보다 높은 강도를 가지는 패스워드 입력으로 달성할 수 있는 보증 레벨을 최고의 보증 수준 (level 4)으로 정의한다.

Table 1. Password Structure Analysis

Type	Complex	Long-Basic	Long-Complex
Total	3000	2054	990
Length (std)	10.7 (3.2)	18.1 (3.1)	13.8 (2.6)
small	68%	73%	57%
capital	4%	4%	12%
number	26%	20%	22%
mark	1%	2%	8%

보증 수준 3 (Level 3)의 인증 방법으로는 6-digit PIN 인증을 정의하였다. 본 방법을 보증 수준 3로 선정한 이유는 다음과 같다.

첫 번째 이유는 많은 스마트폰 접근 제어 시스템에서 6-digit PIN을 사용하기 때문이다. iPhone을 접근 제어〔37〕, 안드로이드 기반 간편 결제 서비스〔38, 39〕, 본인 확인 인증을 간편하게 할 수 있는 SK Telecom 의 T 인증〔40〕과 같이 다방면에서 6-숫자 PIN 이 사용된다.

두 번째로는 패스워드 방식에 비교하여 보안성 및 편리성의 차이가 명백하기 때문이다. 보안성과 관련하여 〔41,42〕의 연구에 의하면 6자리 PIN 의 추측가능성은 평균적으로 약 $2^{13.098} \approx 15372$ 이며 패스워드 방법보다 현저하게 낮은 추측가능성을 갖는다. 반면 편리성 측면에서는 6-digit PIN 이 패스워드 방식을 능가함은 매우 명백하다. 〔43〕의 논문에 의하면, 패스워드 방식을 이용한 인증 시간은 평균적으로 4.1초가 걸리는 데 반하여, 우리는 실험을 통해 6-digit PIN 방식을 이용한 인증 시간은 평균적으로 3.1초 걸리는 것을 확인 할 수 있었다. 이와 같은 결과는 6-digit PIN 인증 방식을 3단계 보증 수준을 제공하기 위한 인증 방법으로 정의하기에 적절

Table 2. The feature of authentication methods corresponding to the trust assurance level

	Time cost	Strength (Guessability)
4 level(password)	4.1	10^9
3 level(6-digit PIN)	3.1	15372
2 level(4-digit PIN)	2.5	2566
1 level (no authentication)	0	1

함을 보여준다.

2단계 보증 수준을 제공하기 위한 인증 방법으로 4-digit PIN으로 정의하였다. 4-digit PIN도 6-digit PIN 과 비교하여 편리성과 보안성의 차이가 명백하고, 유사하게 많은 곳에서 사용이 되므로 2단계 보증 수준을 이루기 위한 인증 방법으로 4-digit PIN을 정의하였다. [41]에 의하면 4-digit PIN 입력을 위해 사용자가 소비하는 시간은 회당 약 2.5초 이며, 제공하는 추측가능성은 약 $2^{11.325}\approx 2566$ 이다. 1 단계 보증 수준은 기본 보증 수준으로써 아무런 보증을 하지 않는 것으로 정의하기로 한다. 이는 [44]에서 정의한 'Public' 보증 수준과 정확히 동일한 보증 수준으로 생각할 수 있다. Table 2는 4단계 보증 레벨에 대응되는 인증 방법의 특성에 대해 기술하고 있으며 강도에 해당되는 추측가능성의 최소 기준으로 정의한다. Fig. 2는 4단계 신뢰 보증 단계를 나타내고 있다.

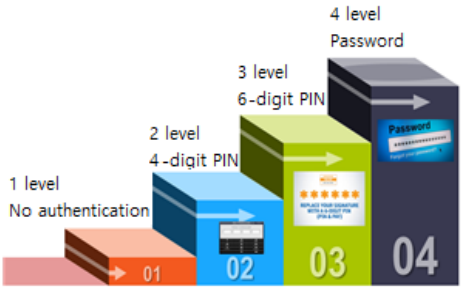

Fig. 2. 4-Level trust assurance

3.1.2 4 단계 신뢰 보증 단계와 행위/상황 기반 인증 방법 간의 관계

본 세부절에서는 3.1.1의 신뢰 보증 단계의 달성을 위한 내재적인 인증 방법인 행위 및 상황 기반 인증의 역할을 다룬다. 먼저, 사용자가 장시간 있는 곳의 Wi-Fi AP들의 집합을 등록하여 사용자가 자주 있는 곳에 존재하는지 아닌지 판단하는 것을 편의상 CoI(Context of Interest) 기반 인증이라 정의하며, CoI 정보가 지속되는 상황에서 제한받는 공격자의 공격 능력을 설명한다. 이후, 얼굴 인식 기반 인증, 스크린 키보드 기반 인증과 3.1.1의 신뢰 보증 단계와의 관계를 설명한다.

본 연구에서 사용하는 CoI 기반인증의 이론적 배경은 [17]을 기반으로 하며, 사용자가 자주 위치를 의미하는 CoI가 추측가능성에 미치는 영향을 파악하기 위해 다음과 같은 공격 시나리오를 가정한다.

만약 사용자가 자신의 스마트폰이 없어진 것을 파악한다면, 사용자는 최소한 물리적으로 스마트폰을 찾으려할 것이고, 공격자가 특정 지역에 갇혀 있다면 공격자가 발각될 확률이 높을 것이다. 즉, CoI는 공격자를 공간적으로 제약하며, 공격자가 스마트폰을 가지고 CoI에서 지정한 지역을 이탈할 경우 CoI로 인한 신뢰 보증 수준은 사라진다. CoI로 인한 신뢰 보증 수준 내의 공격자가 시도하는 공격은 사용자가 잠시 자리를 비운 사이 또는 사용자가 인지하지 못하는 상황에서 스마트폰에 접근을 시도하는 런치타임(lunch time) 공격이 되며, 스마트폰이 PIN 번호 등으로 잠겨 있다면, 공격자는 허용하는 시간 내에 잠금 해제를 시도할 것이다.

이와 같은 상황에서 안전을 위해 요구되는 신뢰 보증 수준을 파악하기 위해, 공격자의 가용한 최대 공격횟수를 산출한다. 런치타임 공격은 비주기적이고 1회성에 가까운 공격이라고 가정할 수 있고, 하루 이상 CoI 정보가 유지된다면 스마트폰의 분실, 도난이 발생하지 않았다고 가정한다. [45]에 의하면, 사용자의 스마트폰은 16.9%의 확률로 원하지 않는 위협에 노출되기 때문에 하루에 243.36분의 공격 가용 시간이 존재한다고 볼 수 있으며, 본 연구의 실험환경인 안드로이드 시스템의 경우 5회의 PIN 입력 오류 이후에는 30초의 대기 시간이 필요하다. 이를 감안하여 하루에 시도할 수 있는 Table 2의 3단계 신뢰 보증 수순을 제공하는 6-digit PIN의 공격 횟수는 9494회가 된다. 이는 6-digit PIN 강도가 충분히 감내할 수 있는 공격횟수이며, CoI 정보가 유지되는 상황에서의 요구되는 최소 신뢰 보증 수준을 3단계로 정의할 수 있다.

얼굴 인식 기반 인증, 스크린 키보드 기반 인증과 같은 바이오정보(biometric information) 기반

인증 방법과 신뢰 보증 단계의 관계를 정의하기 위해 바이오정보기반 인증 방법의 FMR(False Matching Rate)을 살펴본다. [44]에서는 바이오정보 입력 공간의 엔트로피(entropy)를 측정하기 위해 FMR을 기준으로 사용한다. 이론적으로 동일한 바이오정보를 가지는 사람은 없기 때문에 입력 공간의 엔트로피는 무한하며, 이를 사용한 인증은 항상 성공해야 한다. 그러나 실제 바이오정보를 샘플링(sampling)하고 처리하는 인증 과정에 사용되는 데이터는 유한하며 이는 인증 효율성 문제로 귀결된다. 즉, 타인이 인증을 성공할 오류를 나타내는 지표인 FMR은 인증과정에서 사용되는 데이터 공간의 유한성으로 인해 발생하며, 이를 공격자의 공격 성공확률로 재정의 할 경우, 인증과정에서 사용되는 데이터 공간의 크기를 의미하는 엔트로피로 환산할 수 있다. 본 연구에서는 이와 같은 아이디어를 바탕으로 패스워드 및 PIN 인증의 입력 공간의 크기를 의미하는 추측가능성과 FMR을 기반으로 구할 수 있는 바이오정보 입력 공간의 엔트로피를 동일 차원의 값으로 간주한다. 또한 패스워드 인증 방식에서 사용자의 오입력 확률이 대략 16% 임을 감안했을 때[46], 내재적인 인증 방법들도 동일한 FNMR(False Non-Match Rate)를 설정한 상태의 FMR값을 실험적으로 구한 결과는 얼굴 인식의 경우 1~5%, 스크린 키보드 기반 인증의 경우 5~10%가 됨을 실험적으로 확인하였다. 가령, 2단계 신뢰 보증 수준이 요구되는 경우의 최소 강도, 추측가능성은 Table 2에서 2566이다. 그런데, 사용되는 개별 인증 방법이 독립적으로 사용되기 때문에, FMR 5%의 스크린 키보드 기반 인증과 4-digit PIN 인증을 동시에 사용하여 지원할 수 있는 추측가능성은 3단계 신뢰 보장 수준의 15372보다 크다. 따라서 내재적인 사용자 인증이 이루어지고 있는 상황에서는 Fig 3과 같이 요구되는 신뢰 보증 단계가 바뀐다.

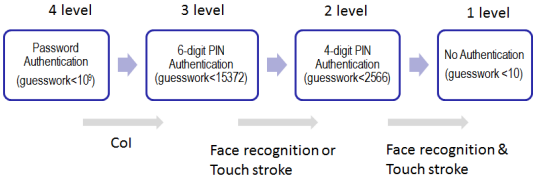

Fig. 3. The relation between trust assurance levels and authentication methods

3.2 스크린 키보드 입력 기반 인증 기법 및 성능향상을 위한 얼굴인식 융합 시스템 구성

본 연구를 통해 제안하는 내재적 인증 방안은 상시 인증은 스크린 키보드를 기반으로 하며 Fig. 4와 같이 얼굴 인식을 융합하여 인증 동일오류율(ERR)을 낮추는 것에 초점을 둔다.

세부절 3.2.1에서는 스크린 키보드 기반 인증을 위한 기반 연구인 [12]을 설명한다. 3.2.2에서는 스크린 키보드 기반 인증과 얼굴인식을 융합하기 위한 방법론을 제안한다.

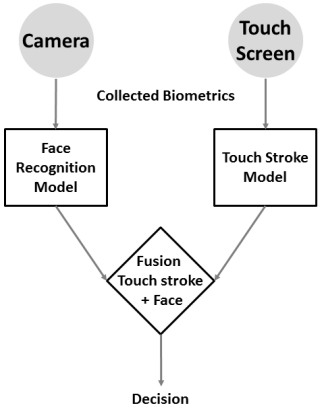

Fig. 4. Fusion of touch stroke dynamic and face recognition

3.2.1 스크린 키보드 기반 인증

본 연구에서는 행위 기반 내재적 인증 도구로써 스크린 키보드 입력 패턴(touch-stroke dynamics)을 사용한다. 동일한 음절에 대한 두 사용자 간의 입력 속도 비율을 계산하고 전체 입력 중 '비슷한 속도'로 입력 된 음절의 비율을 A 척도라고 하며, 수집된 두 개의 스크린 키보드 입력의 데이터에서 동일한 연속된 음절들의 순서가 얼마나 불일치하는 지를 판별하는 지표를 R 척도라고 한다. [11]에서는 단순한 덧셈으로 R-A 지표를 계산하였지만, [12] 연구에서는 R 척도와 A 척도를 취합하기 위한 방안으로 연구에서는 Table 3과 같이 [11]의 12가지 모델을 실험하였다. 본 연구에서는 [12]에서 사용한 가중치 $a_{t,1} \sim a_{t,12}$와 각 모델에서 인증 판별을 위한 임계값 $\beta_{t,1} \sim \beta_{t,12}$을 실험을 통해 구하였으며 R 척도와 A척도를 취합한다.

Table 3. Classification model for different R and A measures combined with weights and threshold of [12]

A measure / R measure	R_2	$R_{2,3}$	$R_{2,3,4}$
A_2	$R_2+\alpha_{f,1}A_2<\beta_{f,1}$	$R_{2,3}+\alpha_{f,5}A_2<\beta_{f,5}$	$R_{2,3,4}+\alpha_{f,9}A_2<\beta_{f,9}$
$A_{2,3}$	$R_2+\alpha_{f,2}A_{2,3}<\beta_{f,2}$	$R_{2,3}+\alpha_{f,6}A_{2,3}<\beta_{f,6}$	$R_{2,3,4}+\alpha_{f,10}A_{2,3}<\beta_{f,10}$
$A_{2,4}$	$R_2+\alpha_{f,3}A_{2,4}<\beta_{f,3}$	$R_{2,3}+\alpha_{f,7}A_{2,4}<\beta_{f,7}$	$R_{2,3,4}+\alpha_{f,11}A_{2,4}<\beta_{f,11}$
$A_{2,3,4}$	$R_2+\alpha_{f,4}A_{2,3,4}<\beta_{f,4}$	$R_{2,3}+\alpha_{f,8}A_{2,3,4}<\beta_{f,8}$	$R_{2,3,4}+\alpha_{f,12}A_{2,3,4}<\beta_{f,12}$

3.2.2 얼굴인식 정보 융합을 통한 스크린 키보드 기반 인증 성능향상 방안

본 스크린 키보드 기반 인증의 성능향상을 위해 얼굴인식 정보는 ETRI에서 개발된 얼굴인식 알고리즘을 통해 제공받은 라이브러리[47]를 사용하였다. 이를 활용한 스크린 키보드 기반 인증의 성능향상을 위해 얼굴인식 정보 융합하는 방법은 [48]에서 제안한 선형 결합방식의 기법을 사용한다. [48] 연구는 각기 다른 형태의 바이오 정보 인식 점수의 가중치 합계를 계산하기 위해 각 바이오 정보에 가중치 할당을 제안하였다. 본 연구에서 두 가지 바이오정보를 결합하기 위해서 선정해야 하는 매개변수는 각 바이오 인식 특성에 의해 출력되는 일치하는 점수의 중요성을 나타내기 위해 사용되는 가중치와 이를 통해 구한 점수가 인가된 사용자 또는 비인가된 사용자의 여부를 판별하는 데 사용되는 임계값이 있다. 3.2.1의 스크린 키보드 기반 인증의 12가지 모델과 얼굴인식 정보를 결합하는 과정에서 사용되는 가중치와 임계값을 구분을 위해 각각 $a_{f,1} \sim a_{f,12}$, $\beta_{f,1} \sim \beta_{f,12}$ 라고 표기한다. 이 방식은 R-A 척도를 취합하는 과정과 유사하며, 패턴 인식 과정에서 2개의 분류자(classifier)를 결합할 때, 선형 결합 또한 높은 성능을 보임이 [49]를 통해 검증되었다.

3.3 인증 시스템 설계 및 구현

본 세부 절에서는 3.1, 3.2에서 설명한 제안방법을 구현한 안드로이드(android) 스마트폰에서 사용 가능한 4단계 신뢰 보증 판별 엔진을 설명한다. 사용자는 신뢰 보증 판별 엔진을 통해 현재 신뢰 수준을 알 수 있으며, 현재 신뢰 수준에 따라 적합한 인증 방식을 선택가능하다. 전체 시스템은 Fig. 5와 같이 설계 되었다. 3.1의 CoI 관련된 기능을 담당하는 CoiService 모듈, 3.2의 스크린 키보드 입력 패턴 측정을 담당하는 MeasureThread 모듈, 얼굴인식을 담당하는 FaceRecogService 모듈로 구성되며 ResultControlThread에서 각 모듈의 행위/상태 기반 인증 정보를 취합하고 현재 신뢰 보증 수준을 결정한다.

3.3.1 ResultControlThread

ResultControlThread는 전체 인증 정보를 취합하고 현재 상태에서 요구되는 신뢰 보증 수준(trust assurance level)을 결정하는 역할을 한다.

- 전역 변수(static variable)인 coiResult에는

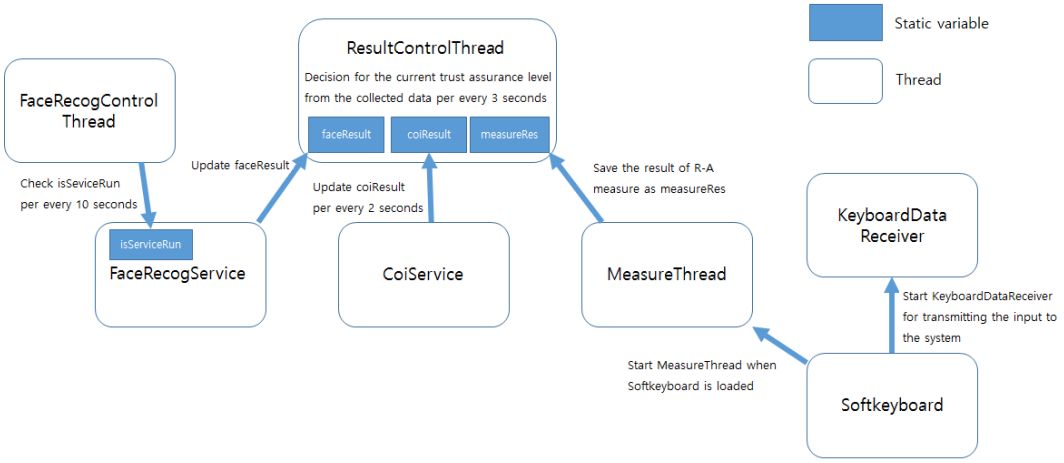

Fig. 5. An illustration of 4-level trust assurance engine for android smartphone environments

2초 간격으로 CoiService에서 판별한, 현재 CoI 정보를 갱신한다.

- 전역 변수인 faceRecogResult에는 FaceRecogService 모듈에서 수집한 얼굴인증 정보가 지속적으로 업데이트 된다.
- 전역 변수 measureRes에는 MeasureThread에서 판별한 스크린 키보드 기반 인증 정보가 10초마다 갱신된다.
- ResultControlThread는 3초 마다 3.1, 제안된 방법으로 coiResult를 반영하고, 3.2.2에서 제안된 방법을 통해 faceRecogResult과 measureRes를 융합한 값을 취합하여 현재 신뢰 보증 요구 수준을 갱신한다.

3.3.2 CoiService

CoiService 모듈은 사용자의 WiFi 접속 정보와 위치정보, 시간 정보를 바탕으로 사용자가 장시간 머무르는 체제 지점(stay point)에 CoI를 등록한다. CoiService 모듈은 등록된 CoI와의 거리를 측정해서, 현재 사용자가 어느 CoI에 속해 있는지를 판별한다. 판별의 결과는 ResultTControlThread에서 취합된다.

3.3.3 FaceRecogService

FaceRecogService는 현재 신뢰 보증 수준에서 얼굴인식을 수행해야 하는 지의 여부를 판별하는 플래그(flag) 역할을 하는 전역 변수 isServiceRun을 가지고 있다. 만약 이 값이 'true'일 경우 FaceRecogControlThread를 통해 얼굴인식 데이터를 수집한다. 수집된 얼굴인식 데이터는 ResultTControlThread에서 취합된다.

3.3.4 MeasureThread

스크린 키보드 기반 인증을 위해서는 사용자가 스마트폰에서 터치스크린을 통해 입력하는 데이터를 수집할 필요가 있다. 이를 위해서는 Fig. 5와 같이 안드로이드 스마트폰의 Softkeyboard와 KeyboardDataReceiver를 3.2.1의 스크린 키보드 입력 패턴을 수집할 수 있도록 하는 커스터마이징(customizing)이 필요하다.

스마트폰의 키보드가 커스터마이징이 된 후에는 터치 스크린을 통해 입력이 발생할 경우 항상 MeasureThread가 호출이 되며 MeasureThread는 3.1.1의 R-A 척도를 측정한다. 측정된 값은 ResultTControlThread에서 취합된다.

IV. 실험 결과 및 분석

본 절에서는 제안 방법의 기본이 되는 스크린 키보드 입력 패턴과 얼굴 인식 데이터를 유합했을 때의 성능을 살펴보고, CoI를 포함한 내재적 인증 도구와 명시적 인증 방법을 병용 했을 때, 인증 비용의 절감 비율을 추론한다. 다음 Table 4는 본 연구에서 사용한 내재적 인증을 위해 수집하는 바이오 정보와 위치정보, 그리고 융합 방법에 대한 요약이다.

스크린 키보드 기반 인증과 얼굴 인식 인증에 대한 실험을 위해 9명의 참여자로부터 20000개의 학습을 위한 스크린 키보드 입력을 수집하였으며, 인증 판별을 위한 스크린 키보드 입력 패턴 50개 200 세트, 100개 100세트, 200개 50세트, 500개 20세트 1000개 10세트를 수집하였다. 또 9명 상호간의 얼굴인식 데이터를 수집하였다. Table 3의 스크린 키보드 입력 패턴을 사용한 12가지 방법과 얼굴인식 정보를 취합한 인증과 동일오류율(EER, Equal Error Rate)의 비교를 통해 성능을 검증한다.

Fig 6은 스크린 키보드 기반 인증의 동일오류율이며, 이를 살펴볼 때, R-A 척도를 기반한 스크린 키보드 인증 시스템은 평균적으로 35.8% 의 동일오류율(EER)을 보인다는 것을 알 수 있었으며, 가장 좋은 성능을 보이는 경우는 인증을 위한 스크린 키보드가 1000개 수집되었을 때, 4번째 R-A 척도 모델을 사용하였을 경우 27.6%의 동일오류율(EER)을

Table 4. Authentication information and fusion method

	Input sensor	Authentication method	Fusion method
Touch Stroke Dynamics	touch screen	RA-measure [12]	weighted linear combination [48]
Face image	camera	Android face recognition library[47]	
CoI information	WiFi/ GPS	CoI list	on-off check

보였다. Fig 7은 얼굴 인식 정보를 융합한 인증의 동일오류율이며, 융합시스템의 동일오류율(EER)은 평균적으로 18.0%을 보여주었다. 가장 좋은 성능을 보여준 경우는 500개의 스크린 키보드를 사용한 9번째 R-A 모델이 5.3%의 동일오류율(EER)을 보여주었다. 실험 결과를 통해 스크린 키보드 인증 시스템과 얼굴인식 데이터의 융합을 통해 전반적으로 대략 10% 가량의 스크린 키보드 기반 상시 인증의 성능개선이 이루어짐을 확인할 수 있었다.

다음으로 사용자 편의성 향상의 정량화를 위해 CoI 정보가 유지되는 시간, 터치 패드를 통해 사용자 입력이 이루어지는 시간, 스마트폰 카메라를 통해 얼굴 인식이 가능한 시간에 대한 정보를 수집하였다. 이를 위해 5명의 사용자(2명 30대, 3명 20대, 각 평균 3일 동안 수행)에 대한 실험을 수행하였으며 가용 시간대비 내재적 인증으로 인해 요구되는 신뢰 수준 변경의 자세한 사항은 Table 5와 같다.

Table 5와 같이 내재적 인증 도구가 수행되고 있을 때 향상되는 사용자 편의성을 측정하기 위해 4단계 신뢰 보증 수준인 패스워드 기반 인증의 강도를 요구하는 사용자와 3단계 신뢰 보증 수준인 6-digit PIN 만큼의 강도를 요구하는 사용자를 정의한다.

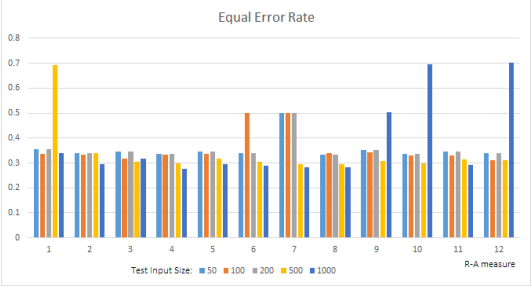

Fig. 6. EER of the touch stroke based authentication

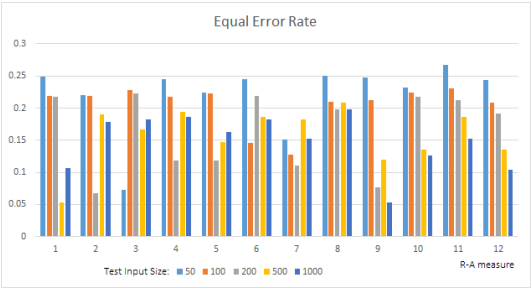

Fig. 7. EER of the touch stroke based authentication with face recognition data

Table 5. Time ratio of implicit authentication method processed

	Ratio	Changed Trust Assurance level
CoI Only	54.7%	4->3
CoI+1 method	21.4%	4->2, 3->2
CoI+2 method	10.5%	4->1, 3->1

각 유형의 사용자 편의성은 Table 2의 실제 인증에 필요한 사용자 비용, 즉 인증 시간이 얼마만큼 줄었는지를 지표로 사용한다. 가령, 첫 번째 유형의 사용자가 CoI 인증이 내재적으로 진행되는 54.7%의 사용 기간 동안 3단계 신뢰 수준의 인증만을 사용하였다면 (4.1-3.1)/4.1*0.547=16% 만큼의 성능향상이 이루어졌다고 측정한다. 이와 같은 방법으로 Table 2의 인증 수행 요구 시간 및 Fig 3의 보증 레벨 및 내재적 인증 관계를 바탕으로 패스워드 및 6자리 PIN 인증 방법에서 Table 6과 같은 인증 소요 시간 절감 효과를 파악 할 수 있다.

V. 결론 및 향후 연구 방향

본 연구를 통해 우리는 CoI 기반 신뢰 보증 수준, 상황인식 기능 및 행위 기반 인증을 통합한 인증 프레임워크를 제안하였다. 스마트폰에서의 내재적 리스크를 판정하고 현재 요구되는 신뢰 보증 수준에 적절한 인증 방법을 사용함으로써, 사용자의 명시적 인증의 부담을 경감시킬 수 있다는 것을 실험을 통해 검증하였다. 그러나 본 연구는 사용자 편의성의 정량화를 위해 적은 사용자의 장시간의 바이오 정보 및 CoI 정보를 수집하여 이루어졌기 때문에, [48]과 같은 단순한 융합 방식으로도 가시적인 성능 향상을 IV절에서 확인할 수 있었다. 그러나 다중 바이오 인식의 일반적인 정확성 분석을 위해 다양한 융합방법과 알고리즘에 대한 고려가 필요하기 때문에, 제안 방법의 다중 융합 인증을 위한 바이오정보 데이터베이스 구축과 정확도 향상을 향후 과제로 한다.

Table 6. Reduction of the authentication cost with the proposed 4-level trust assurance engine

	CoI only	CoI + 1 method	CoI + 2 method	Effects
Password	13.3% (=54.7% * 24.4%)	8.4% (=21.4%*39.1%)	10.5% (= 10.5%*100%)	21.7%
6-digit PIN	-	4.4% (=21.4%*20.4%)	10.5% (=10.5%*100%)	14.9%

References

〔1〕 W. Shi, J. Yang, Y. Jiang, and F. Yang, "Senguard: passive user identification on smartphones using multiple sensors," IEEE 7th International Conference on Wireless and Mobile Computing, pp. 141-148, Oct. 2011.

〔2〕 H. Khan, A. Atwater, and U. Hengartner, "A comparative evaluation of implicit authentication schemes," International Workshop on Recent Advances in Intrusion Detection. Springer, pp. 255-275, Sep. 2014.

〔3〕 V.M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: recent progress and remaining challenges," IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, Jul. 2016.

〔4〕 Y. Xu, T. Price, J.M. Frahm, and F. Monrose, "Virtual u: defeating face liveness detection by building virtual models from your public photos," 25th USENIX Security Symposium, pp. 497-512, Aug. 2016.

〔5〕 Information Technology Laboratory, "Measuring strength of authentication," version 1, NIST, Dec. 2015.

〔6〕 "Strength of function for authenticators - biometrics," https://pages.nist.gov/SOFA/SOFA.html, NIST, Apr. 2017.

〔7〕 ISO/IEC_JTC1/SC27, "Information technology – Security techniques – Evaluation criteria for IT security," ISO/IEC 15408-3:2009, Aug. 2009.

〔8〕 Shin-young Kim, "User authentication method evaluation and selection guide for electronic financial transactions," E-finance and finance security: AR - Ⅵ - 2015 - ① - 15, Financial Security Institute, Oct. 2015.

〔9〕 Seung-woo Han, "Comparative analysis on the security of major simple payment services," E-finance and finance security: AR - Ⅵ - 2015 - ① - 15, Financial Security Institute, Oct. 2015.

〔10〕 B. Ur, S.M. Segreti, L. Bauer, N. Christin, L.F. Cranor, S. Komanduri, and R. Shay, "Measuring real-world accuracies and biases in modeling password guessability," In USENIX Security, pp. 463-481, Aug. 2015.

〔11〕 D. Gunetti and C. Picardi, "Keystroke analysis of free text," ACM Transactions on Information and System Security (TISSEC) vol. 8, no. 3, pp. 312-347, Aug. 2005.

〔12〕 Pyung Kim, Youn-ho Lee, "Performance improvement of the touch stroke dynamics authentication based on free texts," Journal of Korean Institute of Information Technology, 15(4), pp. 45-54, Apr. 2017.

〔13〕 "What is the future of wi-fi and mobile?," http://www.ciscokrblog.com /186, Cisco Korea, Aug. 2012.

〔14〕 Jae-myung Im, Ji-youl Yoo, Se-jeong Jang, Jeong-hwan Lee, and Jae-min Yoo, "Report on the survey of the user behavior in mobile internet," 32902, KISA, Dec. 2013.

〔15〕 W. Luo and U. Hengartner, "Proving Your location without giving up your privacy,"

Proc. ACM 11th Workshop Mobile Computing Systems and Applications, pp. 7-12, Feb. 2010.

[16] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," Proc. ACM 10th Workshop Mobile Computing Systems and Applications, pp. 3, Feb. 2009.

[17] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, "Intuitive security policy configuration in mobile devices using context profiling," International Conference on Privacy, Security, Risk and Trust, International Conference on Social Computing, pp. 471-480, Sep. 2012.

[18] J.R.M Filho, and E.O. Freire, "On the equalization of keystroke timing histograms," Pattern Recognition Letters, vol. 27, no. 13, pp. 1440-1446, Oct. 2006.

[19] J. Hu, D. Gingrich, and A. Sentosa, "A k-nearest neighbor approach for user authentication through biometric keystroke dyanmics," Proceedings of the IEEE International Conference on Communications, pp. 1556-1560, May. 2008.

[20] A. Messerman, T. Mustafić, S. Ahmet, Camtepe, and S. Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics," Proceedings of the International Joint Conference on Biometrics, pp. 1-8, Oct. 2011.

[21] T. Shimshon, R. Moskovitch, L. Rokach, and Y. Elovici, "Continuous verification using keystroke dynamics," Proceedings of the International Conference on Computational Intelligence and Security, pp. 411 - 415, Dec. 2010.

[22] Y. Kaneko, Y. Kinpara, and Y. Shiomi, "A hamming distance-like filtering in keystroke dynamics," Proceedings of the Ninth Annual International Conference on Privacy, Security, and Trust, Montreal, pp. 93-95, Jul. 2011.

[23] S. Bleha, C. Slivinsky, and B. Hussein, "Computer-access security systems using keystroke dynamics," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, no. 12, pp. 1217-1222, Aug. 1990.

[24] H. Davoudi and E. Kabir, "A new distance measure for free text keystroke authentication," Proceedings of the 14th International Computer Conference, pp. 570-575, Oct. 2009.

[25] P.S. Teh, A.B.J. Teoh, C. Tee, and T.S. Ong, "A multiple layer fusion approach on keystroke dynamics," Pattern Analysis and Applications, vol. 14, no. 1, pp. 23-36, Feb. 2011.

[26] Y. Zhong, Y. Deng, and A. Jain, "Keystroke dynamics for user authentication," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 117-123, Jun. 2012.

[27] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A lightweight gait authentication on mobile phone regardless of installation error," IFIP International Information Security Conference, pp. 83-101, Jul. 2013.

[28] M. Trojahn and F. Ortmerier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," Advanced Information Networking and Applications Workshops, 27th International Conference on, pp. 697-702, Mar. 2013.

[29] T.Y. Chang, C.J. Tsai, and J.H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," The Journal of Systems and Software, vol. 85, no. 5, pp. 1157-1165, May 2012.

〔30〕 N. Jeanjaitrong and P. Bhattarakosol, "Feasibility study on authentication based keystroke dynamic over touch-screen devices," Proceeding of 13th International Symposium on Communications and Information Technologies, pp. 238-242, Sep. 2013.
〔31〕 N.K. Rantha, Advances in biometrics: sensors, algorithms and systems, Springer, pp. 447-472, Oct. 2007.
〔32〕 P. Tresadern, T.F. Cootes, N. Poh, P. Matejka, A. Hadid, C. Lévy, C. McCool, and S. Marcel, "Mobile biometrics: combined face and voice verification for a mobile platform," IEEE Pervasive Computing, vol. 12, no. 1, pp. 79-87, Jun. 2013.
〔33〕 J. Montalvao Filho and E. Freire, "Multimodal biometric fusionjoint typist (keystroke) and speaker verification," International Telecommunications Symposium, pp. 609-614, Sep. 2006.
〔34〕 J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," Audio-and Video-based Biometric Person Authentication, LNCS 2688, pp. 1056-1056, Jun. 2003.
〔35〕 H. Saevanee, N.L. Clarke, and S.M. Furnell, "Multi-modal behavioural biometric authentication for mobile devices," In IFIP International Information Security Conference, pp. 465-474, Jun. 2012.
〔36〕 Son Do, Thang Hoang, Chuyen Luong, Seung-chan Choi, Do-kyeong Lee, Ki-hyun Bang, and Deok-jai Choi, "Using keystroke dynamics for implicit authentication on smartphone," Transactions on Korea Multimedia Society, 17(8) pp. 968-976, Aug. 2014.
〔37〕 "Using access control in iPhone, iPad, or iPad Touch," https://support.apple.com/ko-kr/HT204060, Apple Inc., Apr. 2017.
〔38〕 "Kakao pay," http://www.kakao.com/kakaopay/index.php/sendmoney/, Kakaopay corp. Oct. 2017(accessed).
〔39〕 "KPay," https://www.inicis.com/blog/archives/40941, KGInicis corp, Dec. 2014.
〔40〕 Bong-sam Beak, "SKT launched T-authentication service for user verification," http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160802083636, ZDNET, Aug. 2016.
〔41〕 D. Wang, Q. Gu, X. Huang, and P. Wang, "Understanding human-chosen pins: characteristics, distribution and security," Proceedings of the 12th ACM ASIA Conference on Computer and Communications Security, Apr. 2017.
〔42〕 J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins," In International Conference on Financial Cryptography and Data Security, LNCS 7394, pp. 25-40, Mar. 2012.
〔43〕 A. Mahfouz, I. Muslukhov, and K. Beznosov, "Android users in the wild: their authentication and usage behavior," Pervasive and Mobile Computing, vol. 32, pp. 50-61, Oct. 2016.
〔44〕 L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of IEEE, vol. 91, no. 12, pp. 2021-2039, Dec. 2003.
〔45〕 M. Harbach, E.V. Zezschwitz, A. Fichtner, A.D. Luca, and M. Smith, " It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception," Symposium on usable privacy and security, pp. 213-230, Jul. 2014.
〔46〕 R. Chatterjee, A. Athayle, D. Akhawe, A. Juels, and T. Ristenpart, "Password typos and how to correct them securely," IEEE Symposium on Security and Privacy pp. 799-818, May 2016.

〔47〕 Hyper-connected Communication Research Laboratory, "Research on risk analysis on the service use activity and the method for evaluating authentication level," 2011-2016-00046, ETRI, May 2016.
〔48〕 A.K. Jain, A. Ross, "Learning user-specific parameters in a multibiometric system," Proceedings of International Conference on Image Processing, pp. 57-60, Sep. 2002.
〔49〕 C. Lobrano, R. Tronci, G. Giacinto, and F. Roli, "Dynamic linear combination of two-class classifiers," Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition and Structural and Syntactic Pattern Recognition, LNCS 6218, pp. 473-482, Aug. 2010.

〈저자소개〉

김 평(Pyong Kim) 정회원
2007년 2월: KAIST 전산학과 학사
2009년 8월: KAIST 전산학과 석사
2016년 8월: KAIST 전산학과 박사
2016년 9월~현재: 서울과학기술대학교 글로벌융합산업공학과 박사후 연구원
〈관심분야〉 응용암호, 정보보호

서 경 진(Kyungjin Seo) 학생회원
2013년 8월: 한성대학교 컴퓨터공학과 졸업
2017년 2월: 서울과학기술대학교 SW분석설계학과 석사
2017년 3월~현재: 서울과학기술대학교 글로벌융합산업공학과 연구원
〈관심분야〉 응용암호, 데이터보안, Firmware

조 진 만 (Jin-Man Cho) 종신회원
1989년: 충남대학교 계산통계학과 학사
1991년: 충남대학교 전자계산학과 석사
1991년~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 개인정보보호, 스마트카드

김 수 형 (Soo-Hyung, Kim) 종신회원
1996년: 연세대학교 공학사
1998년: 연세대학교 공학석사
2016년: 한국과학기술원 공학박사
1998년~2000년: 한국정보통신 연구소 연구원
2000년~현재: 한국전자통신연구원 인증기술연구실 실장 / 책임연구원
관심분야: 핀테크보안, 사용자인증, 개인정보보호, 모바일보안, IoT보안 등

이 윤 호 (Younho Lee) 종신회원
2006년 8월: KAIST 전산학과 박사
2007년 10월~2009년 2월: GeorgiaTech Information Security Center 방문 박사후과정
2009년 3월~2013년 8월: 영남대학교 정보통신공학과 조교수
2013년 9월~현재: 서울과학기술대학교 글로벌융합산업공학과 ITM전공 부교수
〈관심분야〉 응용암호, 데이터보안, 시스템보안